Monitoring Microsoft Office 365

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

1.1 Licensing 1

CHAPTER 2: HOW DOES EG ENTERPRISE MONITOR MICROSOFT OFFICE 365? 2

2.1 Pre-requisites for Monitoring Microsoft Office 365 Environments 2

2.1.1 Using Powershell Scripts to Fulfill Requirements for Monitoring Office 365 and/or its Service Offerings 4

2.1.2 How to Manually Fulfill Pre-requisites for Monitoring Office 365 Environments? 11

CHAPTER 3: HOW TO MONITOR MICROSOFT OFFICE 365 USING EG ENTERPRISE? 48

3.1 Adding a Microsoft Office 365 Component 48

3.2 Configuring Tests for the Microsoft Office 365 Component 51

CHAPTER 4: MONITORING MICROSOFT OFFICE 365 53

4.1 The Network Layer 54

4.1.1 SaaS Network Connectivity Test 54

4.2 The O365 Tenant Layer 57

4.2.1 Service Health Test 58

4.2.2 Service Provisioning Status Test 61

4.2.3 License Usage Test 65

4.2.4 Message Center Communications Test 69

4.2.5 Domains Test 73

4.2.6 API Logon Status Test 80

4.3 The O365 Users and Groups Layer 85

4.3.1 Distribution Groups 86

4.3.2 Dynamic Distribution Groups Test 90

4.3.3 Office 365 Groups Test 95

4.3.4 Security Groups Test 100

4.3.5 Groups Activity Test 103

4.3.6 Users by Service Test 110

4.3.7 Users Test 113

4.4 The Office 365 Usage Layer 117

4.4.1 Audit Activities by Service Test 118

4.4.2 User-Logins-Test 122

4.5 The User Experience Layer 125

4.5.1 O365 Portal Connectivity Test 125

CHAPTER 5: TROUBLESHOOTING OFFICE 365 MONITORING 128

ABOUT EG INNOVATIONS 130

Table of Figures

Figure 2.1: Selecting the components for which modules/packages should be automatically downloaded and installed 6
Figure 2.2: Automatically creating a new user with the required permissions 8
Figure 2.3: Using an existing user for monitoring purposes 9
Figure 2.4: Choosing to only install the Microsoft Graph App 10
Figure 2.5: Installing the Microsoft Online Module for Windows PowerShell 11
Figure 2.6: Installing the Azure Actuve Directory PowerShell for Graph module 11
Figure 2.7: Installing the Exchange Online Management module 12
Figure 2.8: Installing the SharePoint Online Management Shell 12
Figure 2.9: Installing the Microsoft Teams module 12
Figure 2.10: Welcome page of the Office 365 portal 15
Figure 2.11: The Microsoft Office 365 Admin Center 15
Figure 2.12: Adding a new user 16
Figure 2.13: Choosing the geographic location of the new user 17
Figure 2.14: Selecting the Admin center access 18
Figure 2.15: Reviewing your selection 18
Figure 2.16: Message confirming the successful addition of a user 19
Figure 2.17: Connecting to the Exchange Admin Center 20
Figure 2.18: The Exchange Admin Center 20
Figure 2.19: Clicking on the permissions option to view the admin role groups 21
Figure 2.20: Adding a new role group 22
Figure 2.21: Adding the View-Only Audit Logs permission to the new role 23
Figure 2.22: Clicking on the '+' icon in the Members section 24
Figure 2.23: Assigning the role group to a user 25
Figure 2.24: Saving the new role group 26
Figure 2.25: Clicking on Admin option in Office 365 portal 27
Figure 2.26: Clicking on Azure Active Directory under Admin Centers 28
Figure 2.27: Selecting the App registrations option to register a new app on Azure AD 29
Figure 2.28: Registering the Microsoft Graph app on Azure AD 30
Figure 2.29: Viewing and making a note of the Application ID of the Microsoft Graph app 31
Figure 2.30: Clicking on the New client secret button 32
Figure 2.31: Creating a new secret for the Microsoft Graph App 32
Figure 2.32: The key that is generated and assigned to the client secret of the Microsoft Graph app 33
Figure 2.33: Clicking on the Add a permission button 34
Figure 2.34: Selecting the Office 365 Management APIs option 35
Figure 2.35: Granting permission to the Microsoft Graph app to read service health 36
Figure 2.36: Clicking on the Add a permission button again to add permission to read from and write to user files 37
Figure 2.37: Selecting the SharePoint option 37

Figure 2.38: Granting permission to Microsoft Graph app to read from and write to user files 38
Figure 2.39: Granting permission to Microsoft Graph app to read items in all site collections 39
Figure 2.40: Selecting the Azure Active Directory Graph option 40
Figure 2.41: Granting the Microsoft Graph app permission to sign in and read user profile 41
Figure 2.42: Choosing the Microsoft Graph API 42
Figure 2.43: Granting the Microsoft Graph app permission to read all groups 43
Figure 2.44: Granting the Microsoft Graph app permission to read full profile of all users 44
Figure 2.45: Granting permission to the Microsoft Graph app to read all usage reports 45
Figure 2.46: Granting admin consent to the user 46
Figure 2.47: Generating MS Graph Dat 47
Figure 3.1: Adding a Microsoft Office 365 component 49
Figure 3.2: A message prompting you to add other Office 365 components 50
Figure 3.3: List of tests to be manually configured for Microsoft Office 365 51
Figure 3.4: Configuring the Distribution Groups test 52
Figure 4.1: Layer model for the Microsoft Office 365 component 53
Figure 4.2: The test mapped to the Network layer 54
Figure 4.3: The tests mapped to the O365 Tenant layer 58
Figure 4.4: The detailed diagnosis of the Service incidents measure 61
Figure 4.5: The detailed diagnosis of the Pending provisioning measure 65
Figure 4.6: The detailed diagnosis of the Days to expire measure 69
Figure 4.7: The detailed diagnosis of the Active message center communications measure 73
Figure 4.8: The detailed diagnosis of the Total capabilities measure 80
Figure 4.9: The tests mapped to the O365 Users and Groups layer 85
Figure 4.10: The detailed diagnosis of the Modified groups measure reported by the Distribution Groups test 90
Figure 4.11: The detailed diagnosis of the Empty groups measure reported by the Distribution Groups test 90
Figure 4.12: The detailed diagnosis of the Modified groups measure reported by the Dynamic Distribution Groups test 94
Figure 4.13: The detailed diagnosis of the Empty groups measure reported by the Dynamic Distribution Groups test 94
Figure 4.14: The detailed diagnosis of the Modified groups measure reported by the Office 365 Groups test 99
Figure 4.15: The detailed diagnosis of the Empty groups measure reported by the Office 365 Groups test 99
Figure 4.16: The detailed diagnosis of the Orphaned groups measure reported by the Security Groups test 103
Figure 4.17: The detailed diagnosis of the Empty groups measure reported by the Security Groups test 103
Figure 4.18: The detailed diagnosis of the Mailbox storage used by groups measure 108
Figure 4.19: The detailed diagnosis of the Mailbox items in groups measure 108
Figure 4.20: The detailed diagnosis of the Mails received measure 109
Figure 4.21: The detailed diagnosis of the SharePoint files measure 109
Figure 4.22: The detailed diagnosis of the SharePoint site storage used 110
Figure 4.23: The detailed diagnosis of the SharePoint active files measure 110

Figure 4.24: The detailed diagnosis of the Unlicensed users measure 117
Figure 4.25: The detailed diagnosis of the Deleted users measure 117
Figure 4.26: The detailed diagnosis of the Users with Non-Expiring Passwords measure 117
Figure 4.27: The test mapped to the O365 Usage layer 118
Figure 4.28: The detailed diagnosis of the Unique operations measure 121
Figure 4.29: The detailed diagnosis of the Unique users measure 121
Figure 4.30: The detailed diagnosis of the Unique client IPs measure 122
Figure 4.31: The detailed diagnosis of the Failed logins measure 124
Figure 4.32: The test mapped to the User Experience layer 125
Figure 5.1: Checking if the PackageManagement module has been installed properly 128

Chapter 1: Introduction

Office 365 is a line of subscription services offered by Microsoft, as part of the Microsoft Office product line. The brand encompasses plans that allow use of the Microsoft Office software suite over the life of the subscription, as well as cloud-based software as a service products for business environments, such as hosted Exchange Server, Skype for Business Server, and SharePoint among others.

In recent years, Office 365 has eclipsed all other cloud providers to emerge as the most widely used enterprise cloud service. Being able to deliver high service levels is a key to ensuring the success of Office 365 implementations. As with any cloud-hosted service, service disruptions, downtime and slow connectivity issues are bound to affect business continuity and Office 365 administrators require actionable insight to proactively alert them when performance starts to degrade and to help them resolve problems quickly. This is where eG Enterprise helps!

eG Enterprise is a 100% web-based monitoring, diagnosis and reporting solution for Office 365 environments. Embedding deep domain expertise, pre-built dashboards and KPIs, eG Enterprise empowers Office 365 administrators to continuously monitor health and performance metrics, diagnose issues, and isolate the root cause of Office 365 performance problems.

To provide in-depth performance insights into Office 365 environments, eG Enterprise provides specialized monitoring models - one each for Microsoft Office 365, and its most popular cloud-based offerings such as Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft OneDrive for Business etc.

This document focuses on the Microsoft Office 365 monitoring model alone. With the help of this document discussion, you will be able to understand how eG Enterprise monitors Microsoft Office 365, and how to manage and monitor the performance of Office 365 using eG Enterprise.

1.1 Licensing

Every *Microsoft Office 365* component you manage in eG Enterprise maps to a 'tenant' in an Office 365 deployment. Each 'tenant' so managed consumes a Premium Monitor license in eG Enterprise.

Chapter 2: How Does eG Enterprise Monitor Microsoft Office 365?

eG Enterprise monitors Microsoft Office 365 in an agentless manner. A single eG agent deployed on a remote Windows host in the environment can be configured to run Powershell cmdlets at periodic intervals to pull a wide range of useful diagnostics on Office 365. To ensure that the eG agent is able to run these cmdlets, the pre-requisites detailed in the Section **2.1** are to be fulfilled.

2.1 Pre- requisites for Monitoring Microsoft Office 365 Environments

Before attempting to monitor Microsoft Office 365 or any of its cloud-based service offerings (eg., Exchange Online, SharePoint Online etc.), make sure that the following pre-requisites are fulfilled:

1. The eG agent should be deployed on a remote host running one of the following Windows versions:
    - Windows Server 2016
    - Windows Server 2019
    - Windows 10
    - Windows 8.1
    - Windows Server 2012 or Windows Server 2012 R2
    - Windows Server 2008 R2 SP1
2. The Windows system hosting the remote agent should have internet connection.
3. .NET 4.8 (or above) should pre-exist on the eG agent host.
4. Windows Management Framework (WMF) 5.1.14 (or above) should be installed on the eG agent host
5. eG Enterprise provides proprietary PowerShell scripts, which you can run and have many of the pre- requisites for monitoring automatically fulfilled. These scripts and their purposes are discussed below:

- **O365_Step2_ModulesDwnldnInstall.ps1**: This script automatically installs the following modules/packages that are required for monitoring Office 365 environments:
  - A 64-bit version of the **Microsoft Online Services Sign-in Assistant for IT Professionals RTW**;
  - A 64-bit version of the **Microsoft Azure Active Directory Module for Windows PowerShell**;
  - Exchange Online Management Module, which is essential for monitoring Exchange Online;
  - SharePoint Online Management Shell, which is key for monitoring SharePoint Online;
  - Network Assessment Tool, which helps with Microsoft Teams / Skype for Business Online monitoring;
  - Microsoft Teams Module, which is important for Microsoft Teams monitoring;
  - Skype Online PowerShell module, which is imperative for Skype for Business Online monitoring
- **O365SetRolesAndpermissions.ps1**: The eG agent runs Powershell cmdlets to pull many of the metrics related to Office 365 and its services. To run these cmdlets, the eG agent requires certain permissions. These permissions vary according to the Office 365 service being monitored (i.e., the monitoring model in use).

  The table below describes these privileges:

Monitoring model	Permissions
Microsoft Office 365	A user who is vested with the **View-Only Audit Logs** permission
Microsoft Exchange Online	A user who is vested with the **View-Only Audit Logs, View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions.
Microsoft SharePoint Online and Microsoft OneDrive for Business	A user who has been assigned the **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission

  Using the **O365SetRolesAndpermissions.ps1** script, you can:

- Automatically create a user with the aforesaid permissions, or;
- Automatically assign these permissions to any existing user you choose

Also, to enable the eG agent to monitor service health, Message Center communications, and user activity, the **Microsoft Graph App** needs to be registered on Azure Active Directory (AD), with the following permissions:

- ServiceHealth.Read permission to the Office 365 Management APIs, which will allow the app to read the service health information for your organization;
- MyFiles.Read permission to the SharePoint API, which will allow the app to read from and write to user files;
- Sites.Read.All permission to the SharePoint API, which will allow the app to read items in all site collections;
- User.Read permission to the Azure Active Directory Graph API, which will allow the app to sign in and read the user profile;
- Group.Read.All permission to the Microsoft Graph API, which will allow the app to read all groups;
- User.Read.All permission to the Azure Active Directory Graph API, which will enable the app to read the full profile of all users;
- Reports.Read.All permission to the Microsoft Graph API, which will permit the app to read all usage reports;

This script automatically registers a Microsoft Graph app on Microsoft Azure Active Directory, auto-configured with all the permissions required for monitoring.

To know how to use these scripts, refer to Section **2.1.1**

6. On the other hand, if you choose not to use the scripts above, then you have to manually fulfill each of the requirements described in the table above. To know how, refer to Section **2.1.2**.

   Note:

   The Office 365 monitoring account should not be 2FA/ MFA enabled.

2.1.1 Using Powershell Scripts to Fulfill Requirements for Monitoring Office 365 and/or its Service Offerings

To ensure that pre-requisite 5 discussed in Section **2.1** is fulfilled without a glitch, eG Enterprise provides customized PowerShell scripts. By running these scripts, you can have these requirements

automatically fulfilled. This way, you can eliminate the effort, time, and the likelihood of errors in getting Office 365 monitoring up and running. These scripts and their purposes are discussed in the table below:

Script name	Purpose
O365_Step2_ModulesDwnldnInstall.ps1	Automatically installs the modules/packages required for monitoring Office 365
O365SetRolesAndpermissions.ps1	• Automatically creates a user and grants that user the permission to run Powershell cmdlets • If you want to use an existing user for this purpose, then you can run the same script to assign cmdlet execution permissions to that user; • Registers a Microsoft Graph app on Microsoft Azure Active Directory and assigns the required permissions to that user

These scripts are bundled with the eG agent and are available in the <EG_AGENT_INSTALL_DIR>\lib directory on the eG agent host.

If you run the **O365_Step2_ModulesDwnldnInstall.ps1** from the above location, Figure 2.1 will appear.

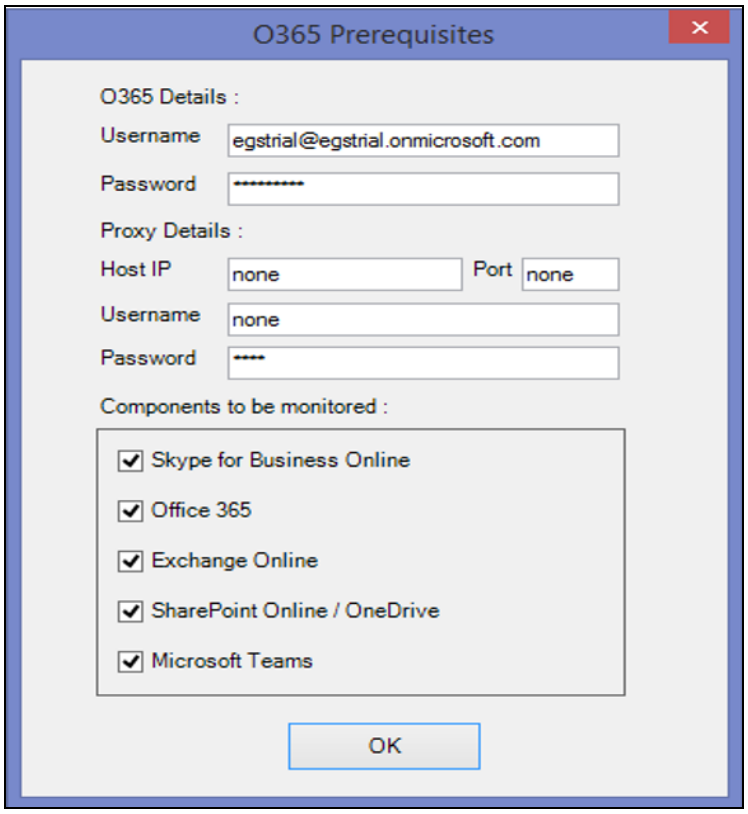


Figure 2.1: Selecting the components for which modules/packages should be automatically downloaded and installed

Specify the following in Figure 2.1:

1. First, enter the **Username** and **Password** of the global administrator. This is because, the eG agent requires global administrator privileges to connect to Office 365 and verify whether the required modules/packages have been successfully installed or not.
2. If the eG agent will be communicating with Office 365 via a Proxy server, then configure the **Host IP** and **Port** number of the Proxy server. If a proxy server is not used for eG agent - Office 365 communications, then let the default **Host IP** and **Port** remain.
3. If the Proxy server requires authentication, then provide a valid **Username** and **Password** for the Proxy user. If no authentication is required, then let the defaults remain.
4. Then, select the Office 365 components you want to monitor by selecting the relevant check boxes in the **Components to be monitored** section (see Figure 2.1). The script will automatically download and install the modules/packages that are required for monitoring the chosen components alone. To install the packages required for monitoring Office 365, select the **Office 365** check box.
5. Then, click the **OK** button. If the **Office 365** check box is selected in the **Components to be**

monitored section, then the following modules/packages will be automatically downloaded and installed on the agent host:

- A 64-bit version of the **Microsoft Online Services Sign-in Assistant for IT Professionals RTW**;
- A 64- bit version of the **Microsoft Azure Active Directory Module for Windows PowerShell**;
- Exchange Online Management Module, which is essential for monitoring Exchange Online;
- SharePoint Online Management Shell, which is key for monitoring SharePoint Online;
- Network Assessment Tool, which helps with Microsoft Teams / Skype for Business Online monitoring;
- Microsoft Teams Module, which is important for Microsoft Teams monitoring;
- Skype Online PowerShell module, which is imperative for Skype for Business Online monitoring

If you run the **O365SetRolesAndpermissions.ps1** script from the <EG_AGENT_INSTALL_ DIR>\lib directory, then the dialog box shown by Figure 2.2 will appear:

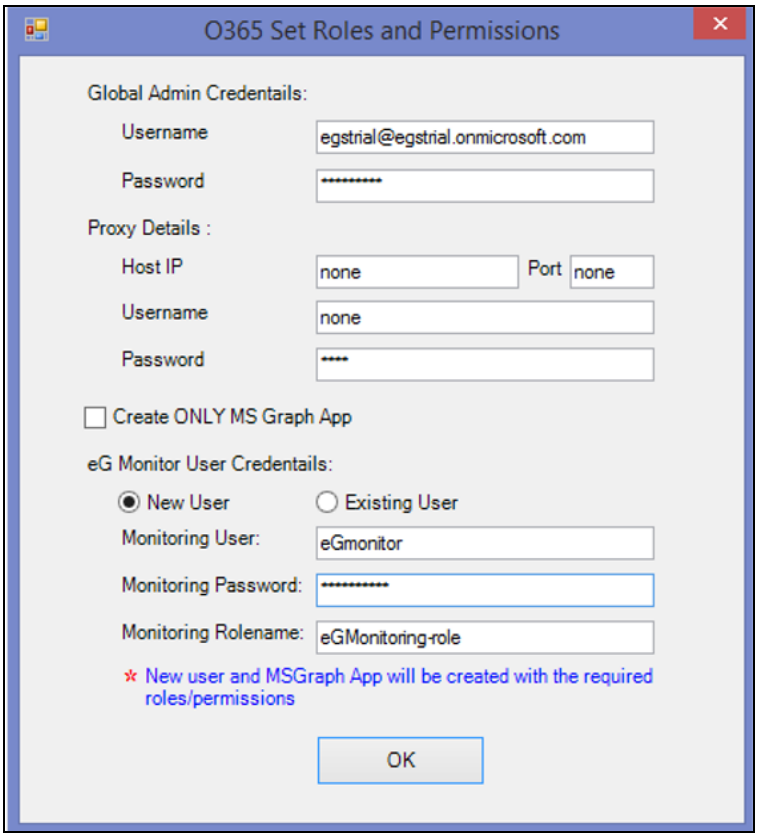


Figure 2.2: Automatically creating a new user with the required permissions

Specify the following in Figure 2.2:

1. First, enter the **Username** and **Password** of the global administrator. This is because, only a global administrator is authorized to create new users/apps and set their permissions.
2. If the eG agent will be communicating with Office 365 via a Proxy server, then configure the **Host IP** and **Port** number of the Proxy server. If a proxy server is not used for eG agent - Office 365 communications, then let the default **Host IP** and **Port** remain.
3. If the Proxy server requires authentication, then provide a valid **Username** and **Password** for the Proxy user. If no authentication is required, then let the defaults remain.
4. If you want the script to automatically create a new user and assign the required permissions to that user, select the **New User** option in Figure 2.2. Then, give a unique name to the new **Monitoring User** and assign a **Monitoring Password** to that user. By default, the script automatically creates a role named *eGMonitoring-role* in Office 365, and assigns that role to the new user. This is why, the *eGMonitoring- role* is displayed by default in the **Monitoring Rolename** text box. You can change the role name if required.

5. On the other hand, if you want to use an existing Office 365 user for monitoring purposes, select the **Existing User** option (see Figure 2.3). Then, specify the name of the existing **Monitoring User** and the **Monitoring Password** of that user. By default, the script automatically creates a role named *eGMonitoring-role* in Office 365, and assigns that role to the specified existing user. This is why, the *eGMonitoring-role* is displayed by default in the **Monitoring Rolename** text box. You can change the role name if required.

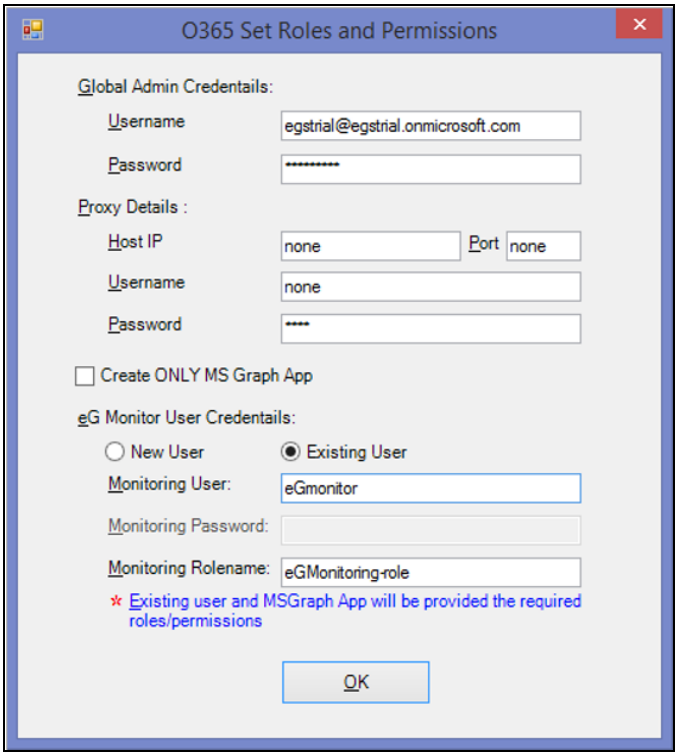


Figure 2.3: Using an existing user for monitoring purposes

6. Finally, click the **OK** button in Figure 2.3. Doing so, will result in the following:

   - If you have chosen to create a new user, then a new user with the given **Monitoring User** name and **Monitoring Password** will be automatically created in Office 365. Likewise, a role with the given **Monitoring Rolename** will be automatically created and assigned to the new user. The script ensures that this role is configured with the permissions required for monitoring Office 365. In this case, make sure you configure the **OFFICE 365 USER** and **OFFICE 365 PASSWORD** parameters of eG tests with the **Monitoring User** name and **Monitoring Password** of the new user.
   - If you have chosen to use an existing user, then a role with the given **Monitoring Rolename** will be automatically created in Office 365. When creating the role, the script

automatically configures the role with the permissions required for monitoring Office 365. The script also automatically assigns this role to the specified existing user. In this case, make sure you configure the **OFFICE 365 USER** and **OFFICE 365 PASSWORD** parameters of eG tests with the **Monitoring User** name and **Monitoring Password** of the existing user.

- A Microsoft Graph app will be automatically registered on Microsoft Azure Active Directory with all the required permissions.

7. If you already have an Office 365 user with the required permissions, then you may not want to use the script to create such a user or grant the required permissions to an existing user. In such a case, you can configure the script to only install the Microsoft Graph app and set its permissions. To achieve this, simply select the **Create ONLY MS Graph App** option, as depicted by Figure 2.4. Then, click the **OK** button.

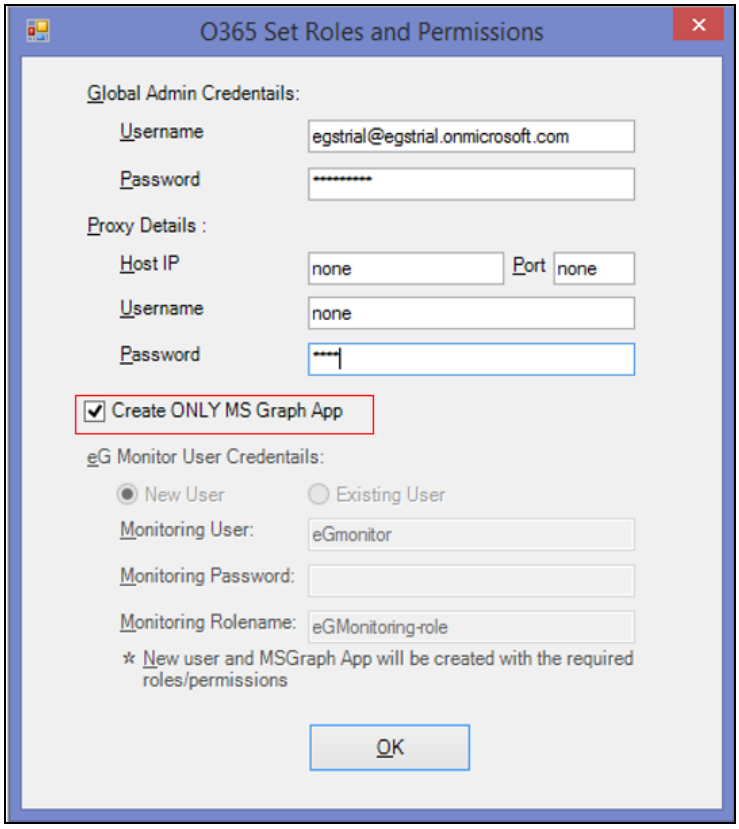


Figure 2.4: Choosing to only install the Microsoft Graph App

2.1.2 How to Manually Fulfill Pre- requisites for Monitoring Office 365 Environments?

The eG agent runs Powershell cmdlets to pull a few metrics from Office 365. To enable the eG agent to run these cmdlets, the following need to be installed and run on the eG agent host:

- A 64-bit version of the **Microsoft Online Services Sign-in Assistant for IT Professionals RTW** : You can download its installable from the URL : https://download.microsoft.com/download/7/1/E/71EF1D05- A42C- 4A1F- 8162- 96494B5E615C/msoidcli_64bit.msi. After downloading, use the installable to install the sign-in assistant, and then start it.
- A 64-bit version of the **Microsoft Azure Active Directory Module for Windows PowerShell**: To install this module, do the following:
  - First, install the **PackageManagement** and **PowerShellGet** modules on the eG agent host. You can download the installable from the URL: https://download.microsoft.com/download/C/4/1/C41378D4- 7F41- 4BBE- 9D0D- 0E4F98585C61/PackageManagement_x64.msi
  - Once the PackageManagement and PowerShellGet modules are successfully installed, open Windows PowerShell ISE in elevated mode on the eG agent host.
  - Then, run the cmdlet depicted by 2.1.2.

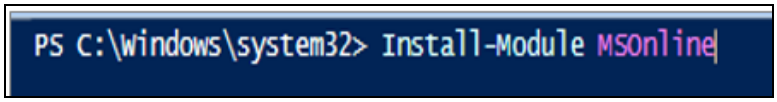


Figure 2.5: Installing the Microsoft Online Module for Windows PowerShell

  - Next, run the following cmdlet to install the Azure Active Directory PowerShell for Graph module:

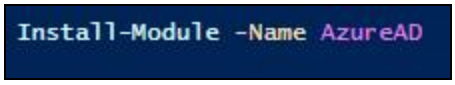


Figure 2.6: Installing the Azure Actuve Directory PowerShell for Graph module

- Then, proceed to install the Exchange Online Management Module. For this, run the following cmdlet from the PowerShell prompt:

Figure 2.7: Installing the Exchange Online Management module

- Now, install the SharePoint Online Management Shell, which is key for monitoring SharePoint Online. For that, run the following cmdlet:

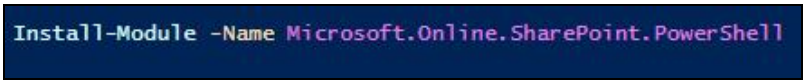


Figure 2.8: Installing the SharePoint Online Management Shell

- Next, install the Microsoft Teams module, which is important for Microsoft Teams monitoring. For this, run the following cmdlet:

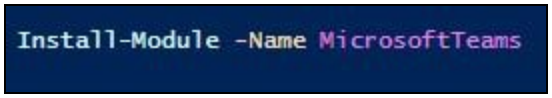


Figure 2.9: Installing the Microsoft Teams module

- Then, install the Network Assessment Tool, which helps with Microsoft Teams / Skype for Business Online monitoring. For this, you need to download and run the executable from the following URL: https://download.microsoft.com/download/D/D/6/DD65CA90-94CF-4B10-88A2-67432D8EB78F/MicrosoftSkypeForBusinessNetworkAssessmentTool.exe
- Finally, install the Skype Online PowerShell module, which is imperative for Skype for Business Online monitoring. For this, you need to download and run the executable in the URL, https://download.microsoft.com/download/2/0/5/2050B39B- 4DA5- 48E0- B768-583533B42C3B/SkypeOnlinePowerShell.Exe.

To run PowerShell cmdlets for metrics collection, the eG agent requires the credentials of a user who has been assigned specific privileges.

These privileges vary with the service being monitored - i.e., eG monitoring model in use.

The table below describes these privileges:

Monitoring model	**Permissions**
Microsoft Office 365	A user who is vested with the **View-Only Audit Logs** permission

Microsoft Exchange Online	A user who is vested with the **View-Only Audit Logs, View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions.
Microsoft SharePoint Online and Microsoft OneDrive for Business	A user who has been assigned the **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission

While you can use the credentials of any existing O365 user with the aforesaid privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and pass the credentials of that user to the eG agent.

To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to the Section **2.1.2.1**.

To enable the eG agent to monitor service health, Message Center communications, and user activity, you need to ensure that the **Microsoft Graph** App is registered on Azure Active Directory (AD), with the following permissions:

- ServiceHealth.Read permission to the Office 365 Management APIs, which will allow the app to read the service health information for your organization;
- MyFiles.Read permission to the SharePoint API, which will allow the app to read from and write to user files;
- Sites.Read.All permission to the SharePoint API, which will allow the app to read items in all site collections;
- User.Read permission to the Azure Active Directory Graph API, which will allow the app to sign in and read the user profile;
- Group.Read.All permission to the Microsoft Graph API, which will allow the app to read all groups;
- User.Read.All permission to the Azure Active Directory Graph API, which will enable the app to read the full profile of all users;
- Reports.Read.All permission to the Microsoft Graph API, which will permit the app to read all usage reports;

The steps for manually registering this app and granting the aforesaid permissions are detailed in Section **2.1.2.2**.

2.1.2.1 Creating a New User in the Office 365 Portal

To monitor Microsoft Office 365 and its cloud- based service offerings such as SharePoint Online, Exchange Online, OneDrive for Business etc., the eG agent has to be configured with the credentials of a user who has been assigned specific privileges. These privileges vary with the service being monitored - i.e., eG monitoring model in use.

The table below describes these privileges:

Monitoring model	**Permissions**
Microsoft Office 365	A user who is vested with the **View-Only Audit Logs** permission
Microsoft Exchange Online	A user who is vested with the **View-Only Audit Logs, View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions.
Microsoft SharePoint Online and Microsoft OneDrive for Business	A user who has been assigned the **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission

While you can use the credentials of any existing O365 user with the aforesaid privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and pass the credentials of that user to the eG agent. To create a new user using the Office 365 portal and assign the required privileges to that user, follow the steps detailed below:

1. Using a browser, connect to the Office 365 portal. The default URL of the portal is: https://portal.office.com
2. Login to the portal as a user with administrator privileges.
3. Figure 2.10 will then appear.

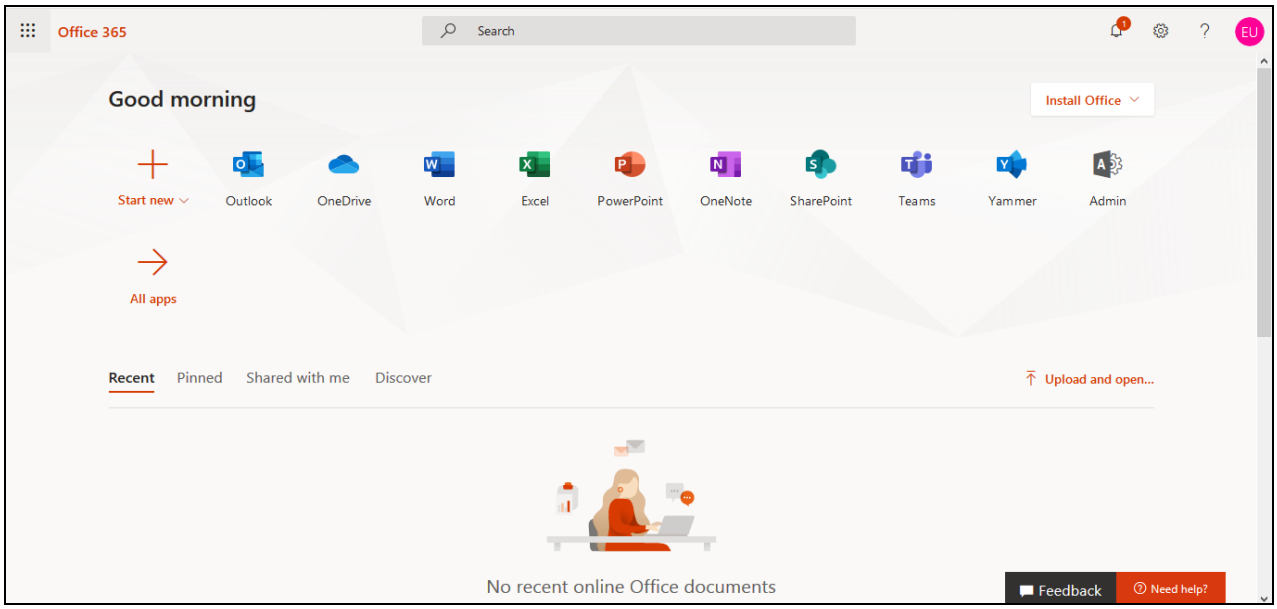


Figure 2.10: Welcome page of the Office 365 portal

4. Click on **Admin** under **Apps** (in Figure 2.10). The Microsoft Office 365 Admin Center will then appear (see Figure 2.11).

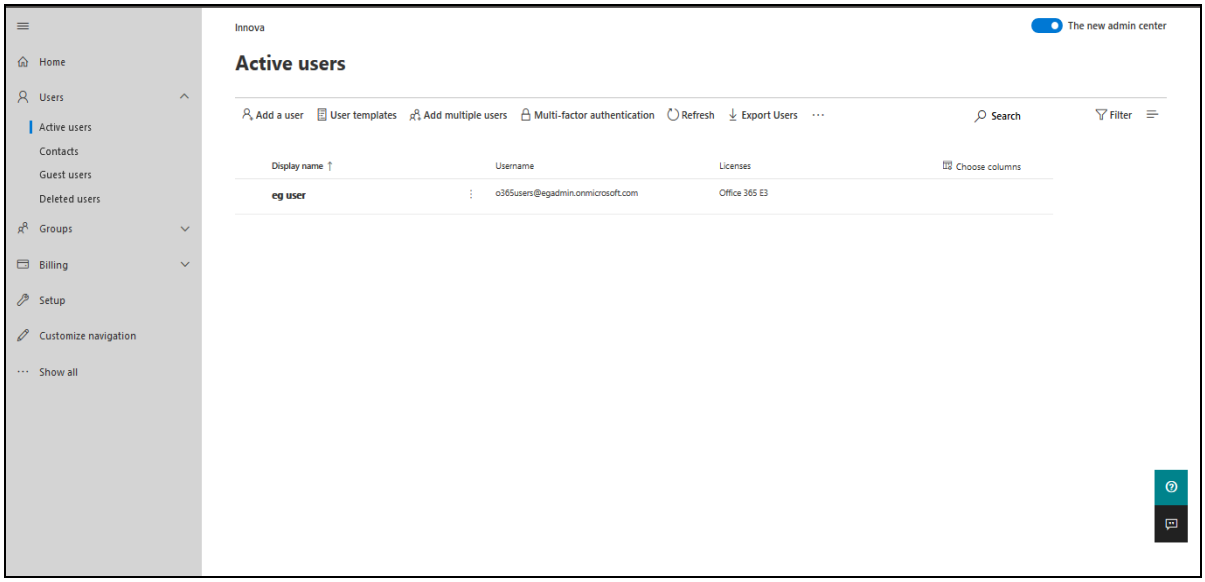


Figure 2.11: The Microsoft Office 365 Admin Center

5. To create a new user, click on the **Add a user** link under the **Active users** section in Figure 2.11.

6. Figure 2.12 will then appear.

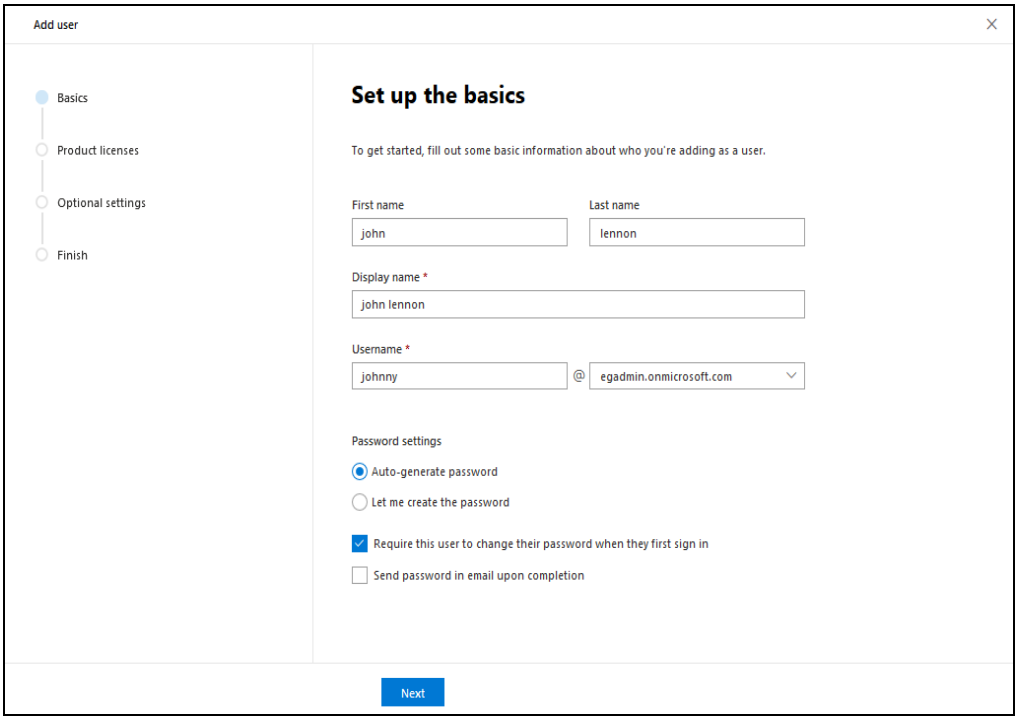


Figure 2.12: Adding a new user

7. Provide the **First name**, **Last name**, and **Display name** of the new user. Then, provide a **Username**, which will be automatically suffixed with the domain name of the **Domain** you have logged into. Click the **Next** button to select the geographic location of the new user.

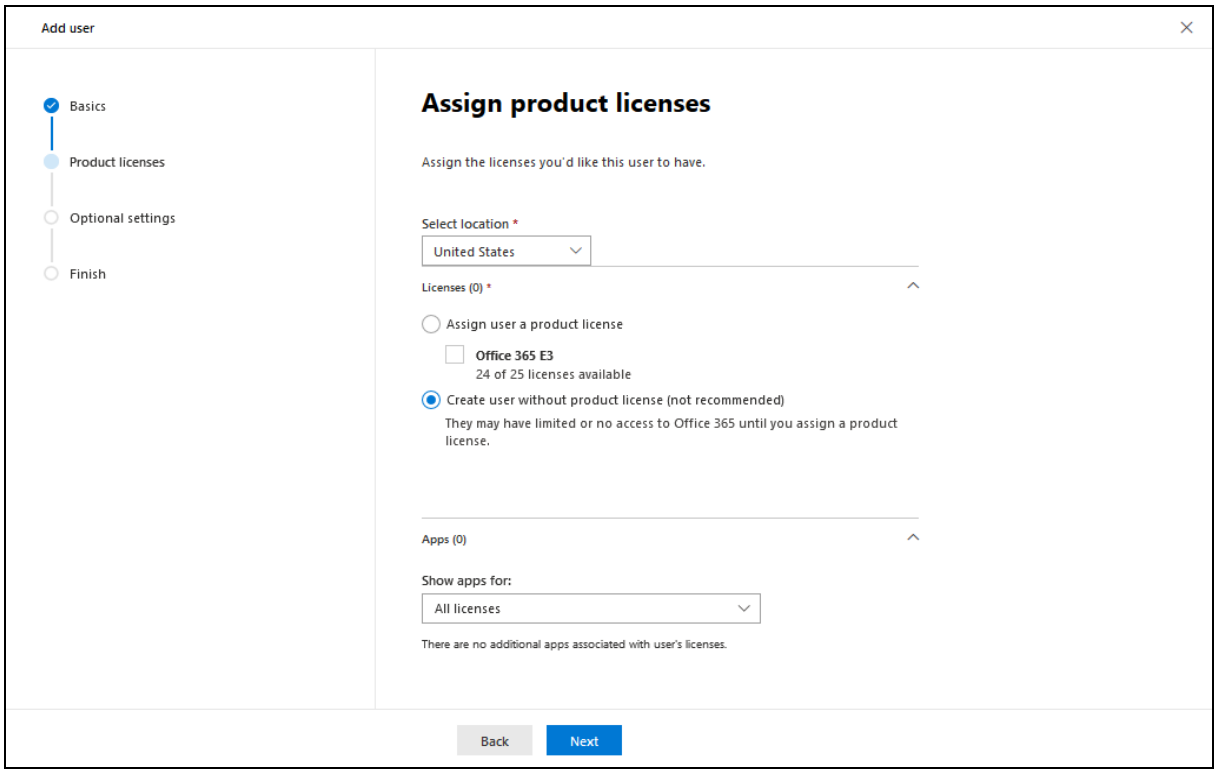


Figure 2.13: Choosing the geographic location of the new user

8. Then, select the geographic **Location** of the new user. Turn *On* the **Create user without product license** flag in Figure 2.13.
9. Clicking the **Next** button in Figure 2.13 will reveal Figure 2.14. Here, select the **Admin center access** option, and choose the **Service support admin** and **SharePoint admin** permissions as indicated by Figure 2.14.

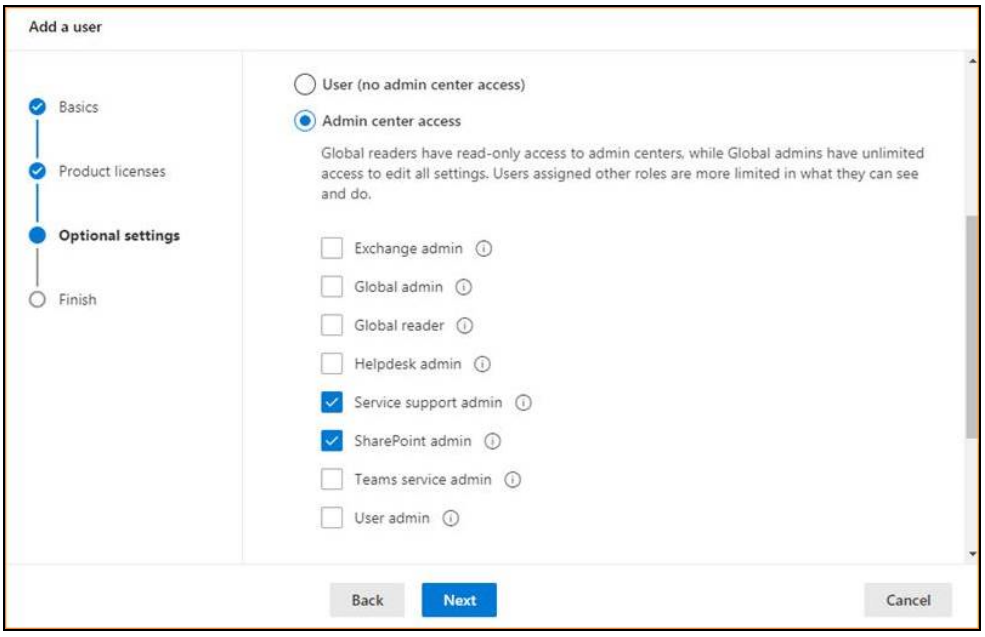


Figure 2.14: Selecting the Admin center access

10. Click the **Next** button in Figure 2.14 to review your selection which appears in Figure 2.15.

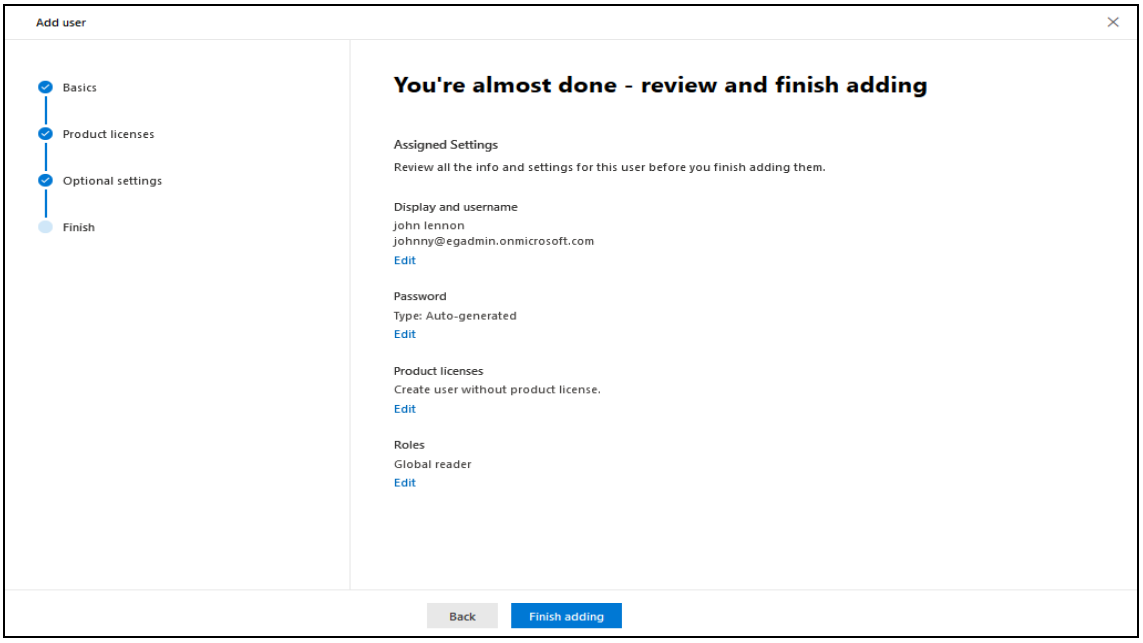


Figure 2.15: Reviewing your selection

11. Finally, click the **Finish adding** button in Figure 2.15 to add the new user. Figure 2.16 will then appear providing a quick summary of details of the user you just created. Office 365 also

automatically generates and assigns a password to the new user. Make a note of the **Username** and **Password** displayed in Figure 2.16, as this is what you need to configure against the **OFFICE 365 USER** and **OFFICE 365 PASSWORD** parameters of the eG tests.

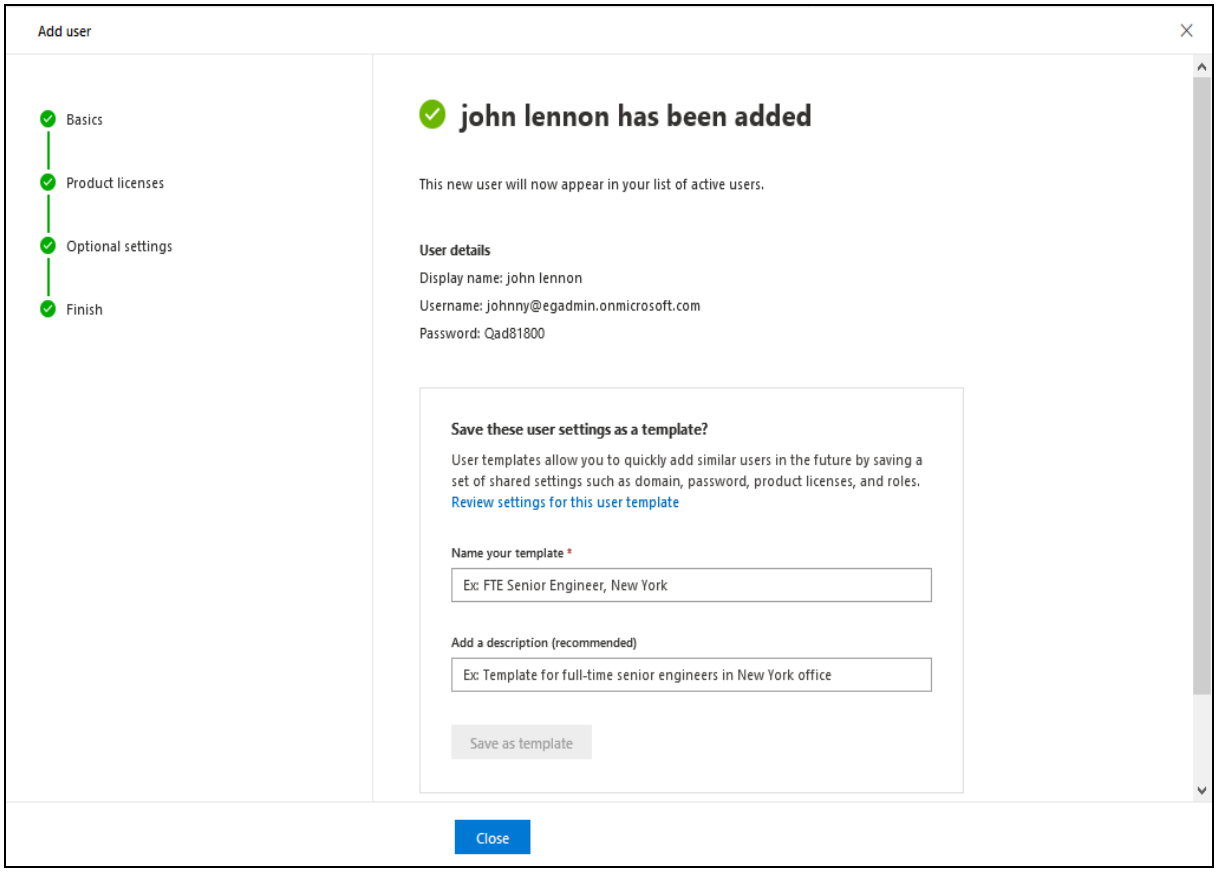


Figure 2.16: Message confirming the successful addition of a user

12. Next, proceed to assign the **View-Only Audit Logs** permission to the new user. For that, first click on the Admin Center tool in the tool bar depicted by Figure 2.17. From the menu that pops up, click on **Exchange**.

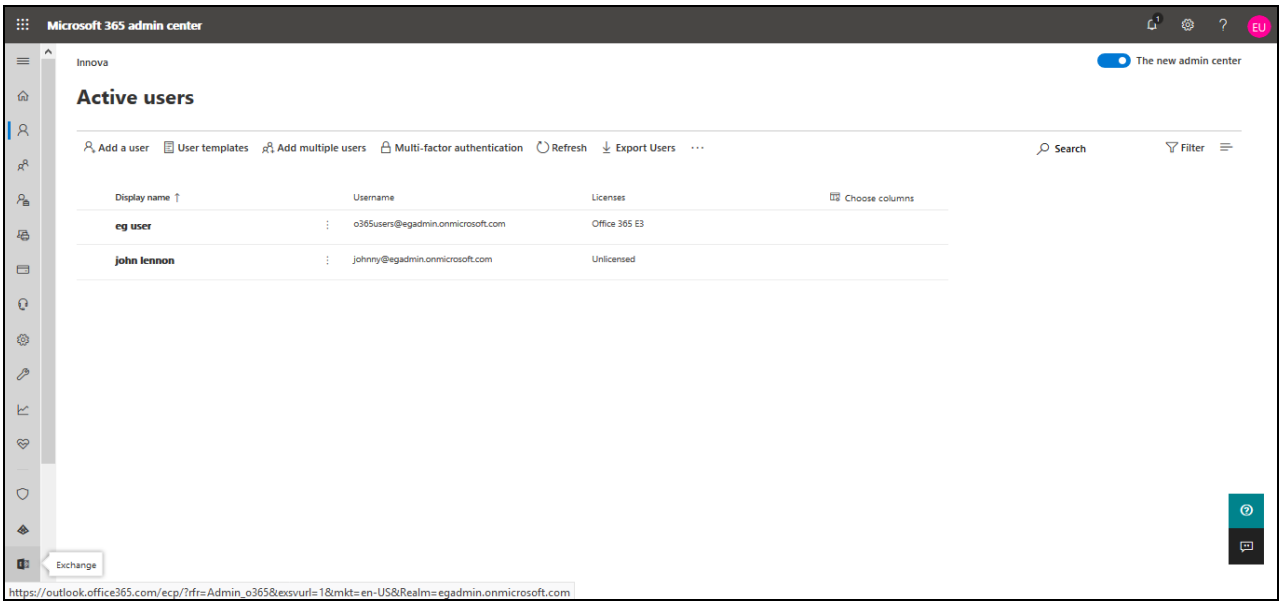


Figure 2.17: Connecting to the Exchange Admin Center

13. Figure 2.18 will then appear.

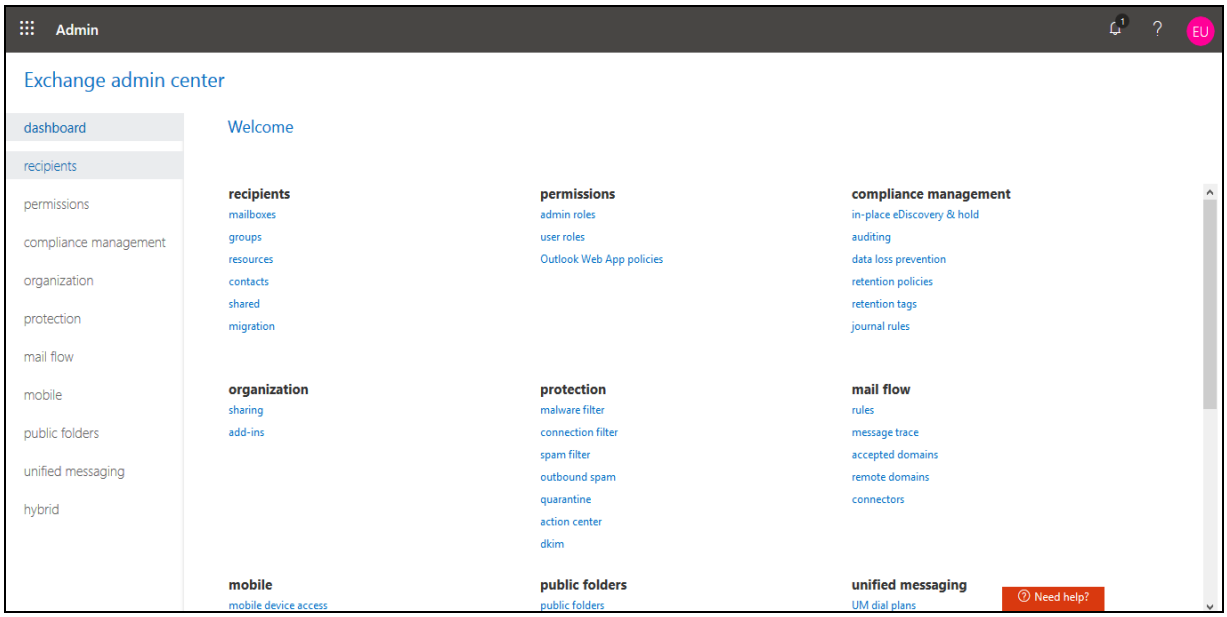


Figure 2.18: The Exchange Admin Center

14. From the list of options in the left panel of Figure 2.18, select **permissions**. Figure 2.19 will then appear listing the **admin** role groups that pre-exist.

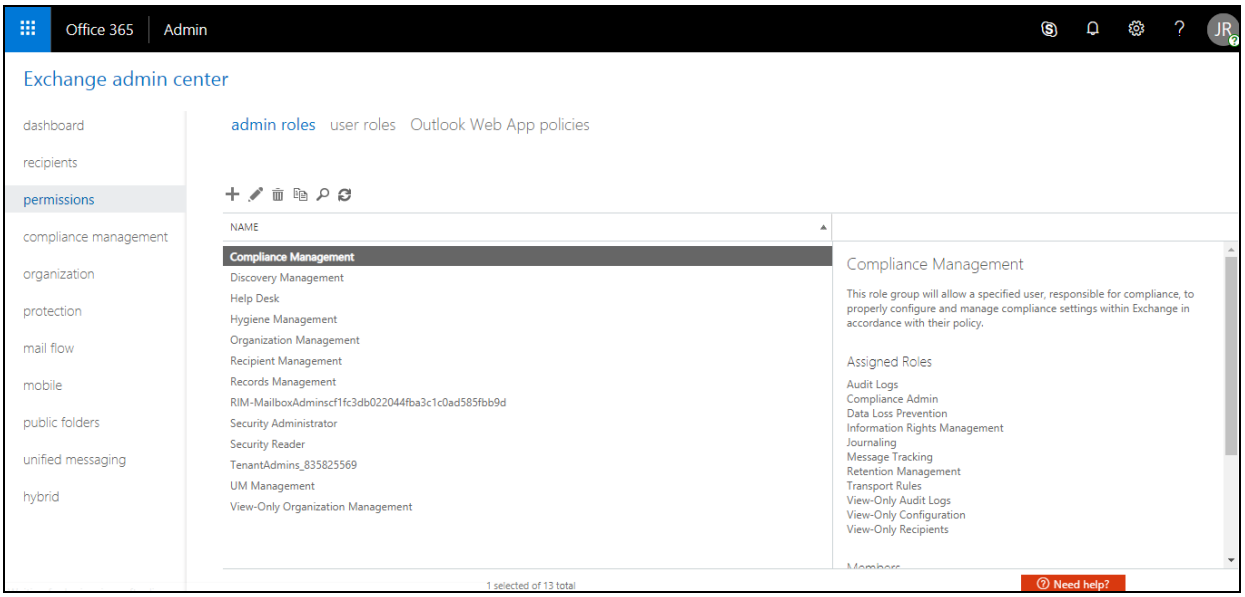


Figure 2.19: Clicking on the permissions option to view the admin role groups

15. Let us now proceed to create a role group that includes the **View-Only Audit Logs permission**. For that, click on the + button on top of the list of admin role groups (see Figure 2.19). Figure 2.20 will then appear.

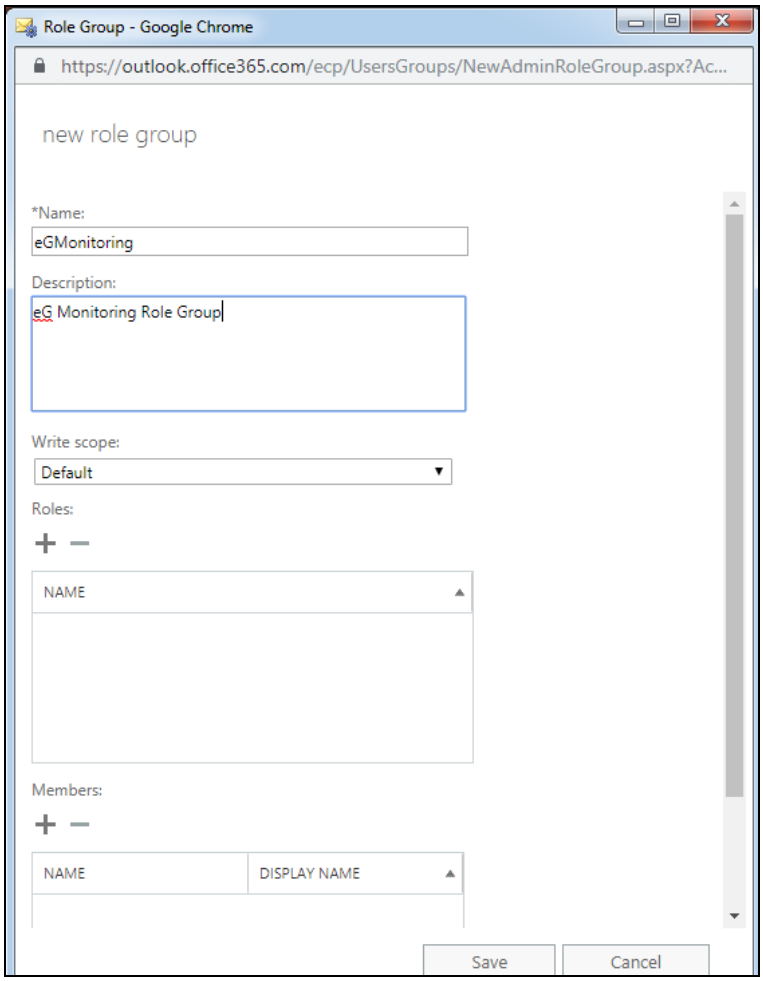


Figure 2.20: Adding a new role group

16. Provide a unique **Name** and **Description** for the new role group (see Figure 2.20). Then, click on the + button in the **Roles** section of Figure 2.20. Figure 2.21 will then appear listing the **DISPLAY NAME**s of permissions that you want to add to the new role. From this list, select the **View-Only Audit Logs** permission and click the **add ->** button to add the permission. Then, click **OK** to save the changes.

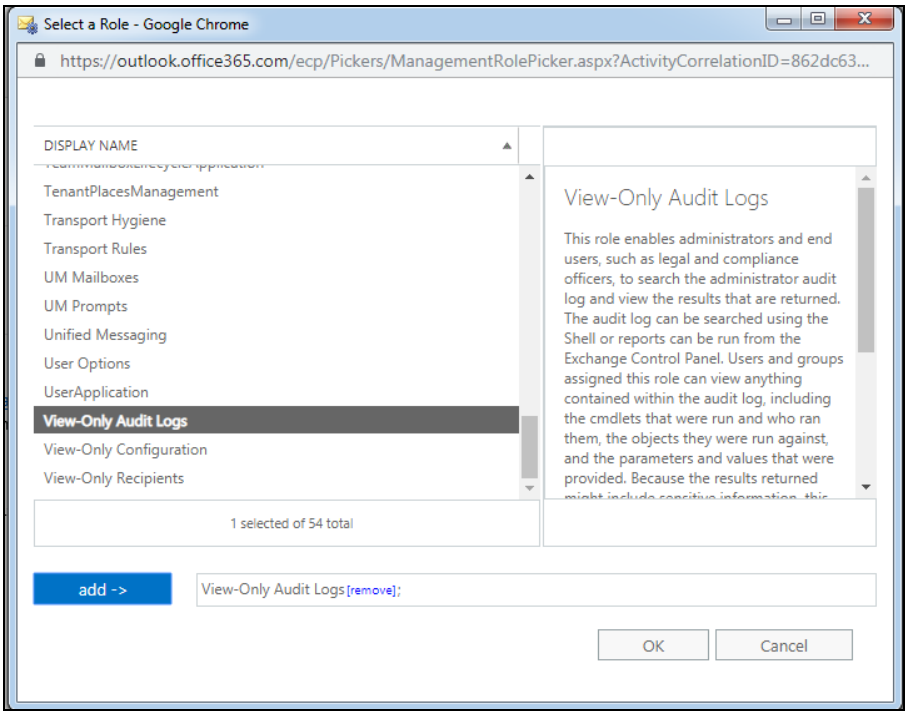


Figure 2.21: Adding the View-Only Audit Logs permission to the new role

17. Figure 2.22 will then appear. Next, proceed to assign the new role group (that includes the **View-Only Audit Logs** permission) to the user you created previously. For that, click on the + button in the **Members** section of Figure 2.22.

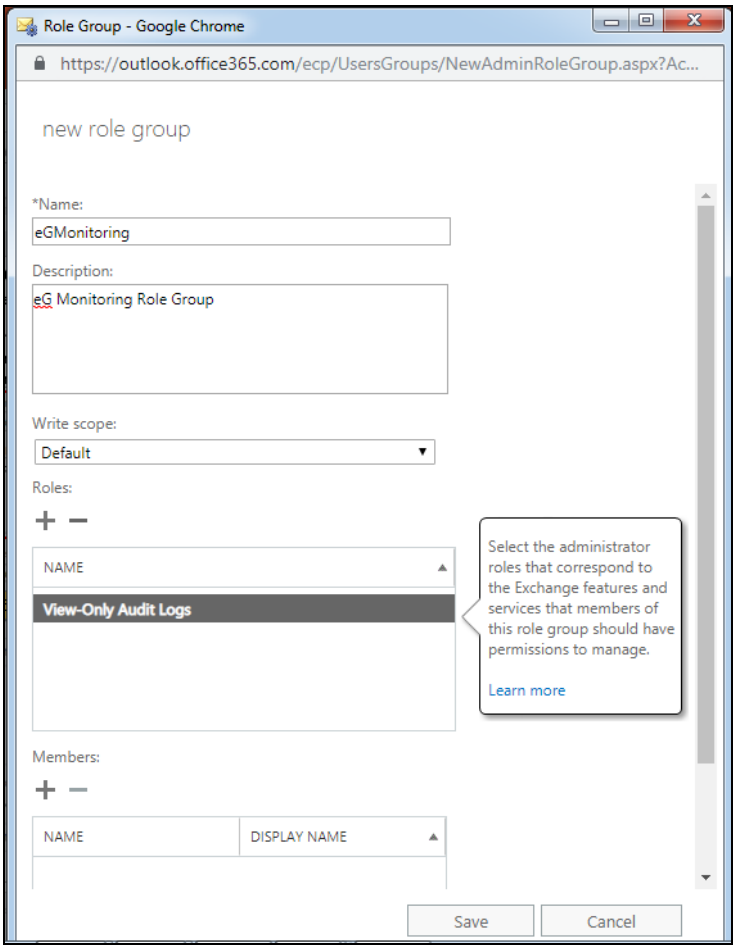


Figure 2.22: Clicking on the '+' icon in the Members section

18. Figure 2.23 will then appear. From the list of user names displayed in Figure 2.23, select the name of the user you created for monitoring purposes and click the **add ->** button. Then, click **OK**.

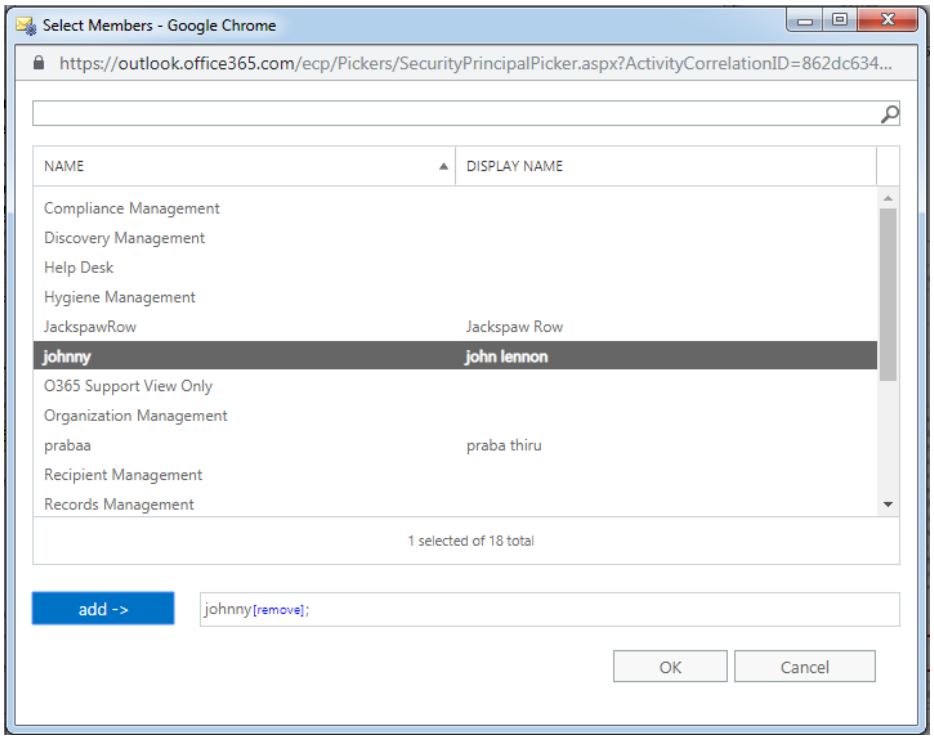


Figure 2.23: Assigning the role group to a user

19. When Figure 2.24 appears, click the **Save** button to save the new role group definition.

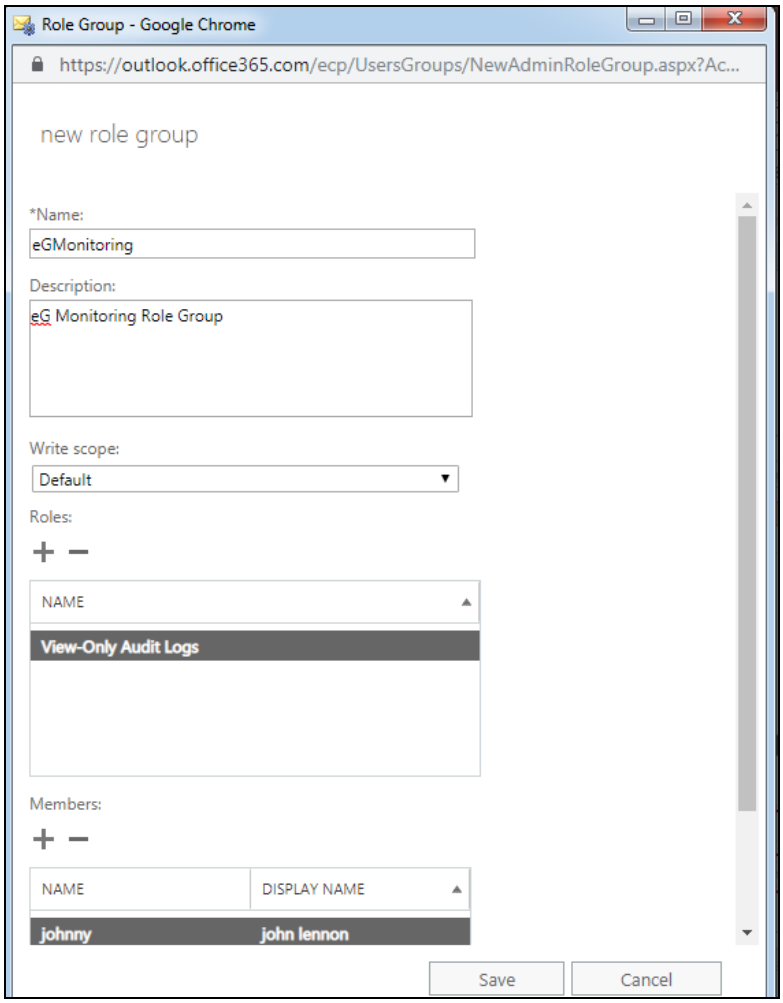


Figure 2.24: Saving the new role group

Assign other permissions(**View-Only Recipients**, **Mail Recipients**, **Mail Import Export**) to the newly added user by repeating steps 15 - 19 above.

2.1.2.2 Registering the Microsoft Graph App On Microsoft Azure Active Directory

To achieve this, follow the steps detailed below:

1. Login to the Office 365 portal as a Global Administrator and click on the **Admin** option within (see Figure 2.25).

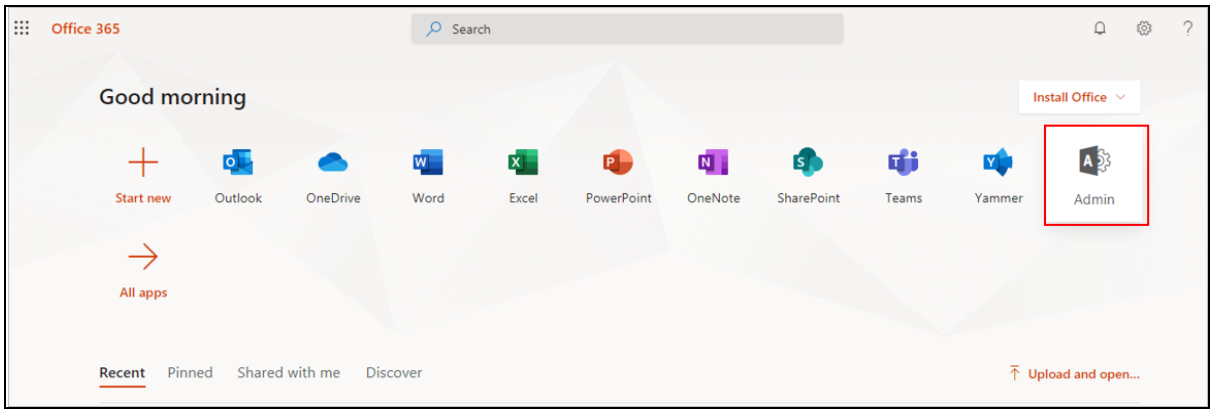


Figure 2.25: Clicking on Admin option in Office 365 portal

2. When Figure 2.26 appears, browse the left panel of Figure 2.26 for the **Admin Centers** node. Expand the node and select the **Azure Active Directory** sub-node within.

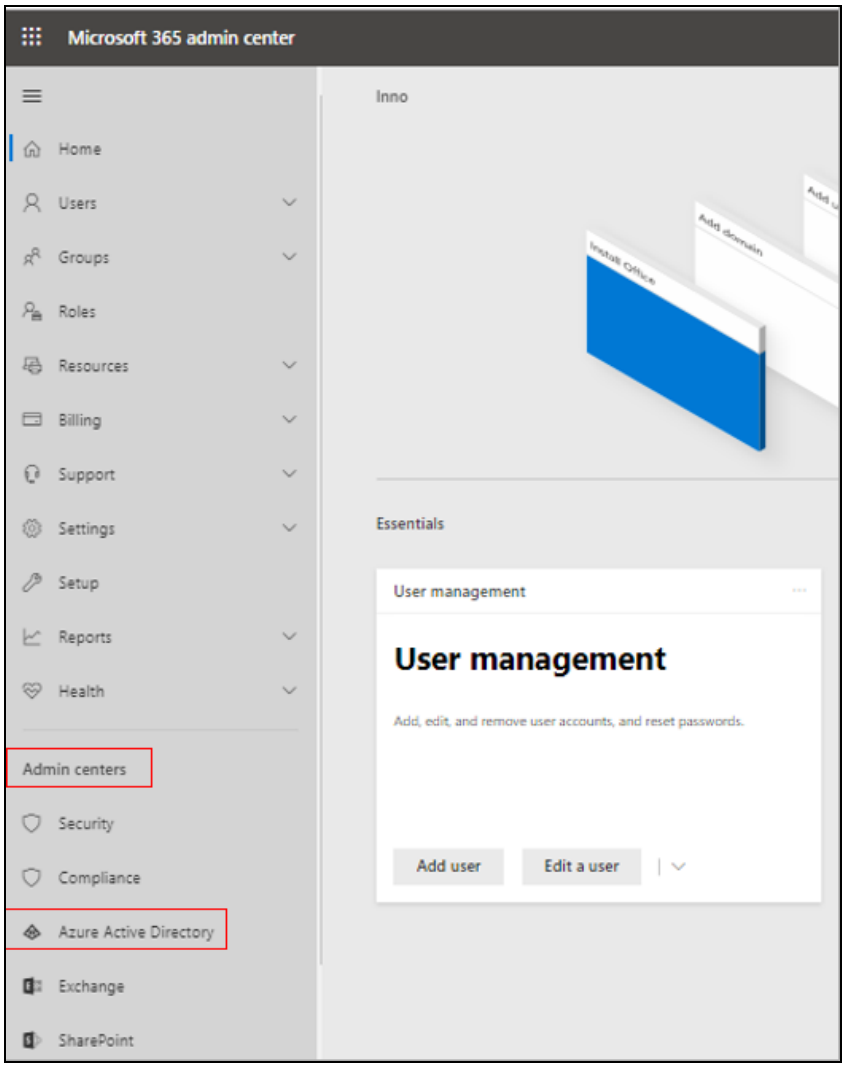


Figure 2.26: Clicking on Azure Active Directory under Admin Centers

3. Figure 2.27 then appears. Select **Azure Active Directory** from the list of **FAVORITES** in the left-most panel of Figure 2.27. Then, from the **App Registrations** list for Azure Active Directory, select **App registrations** to register the Microsoft Graph app.

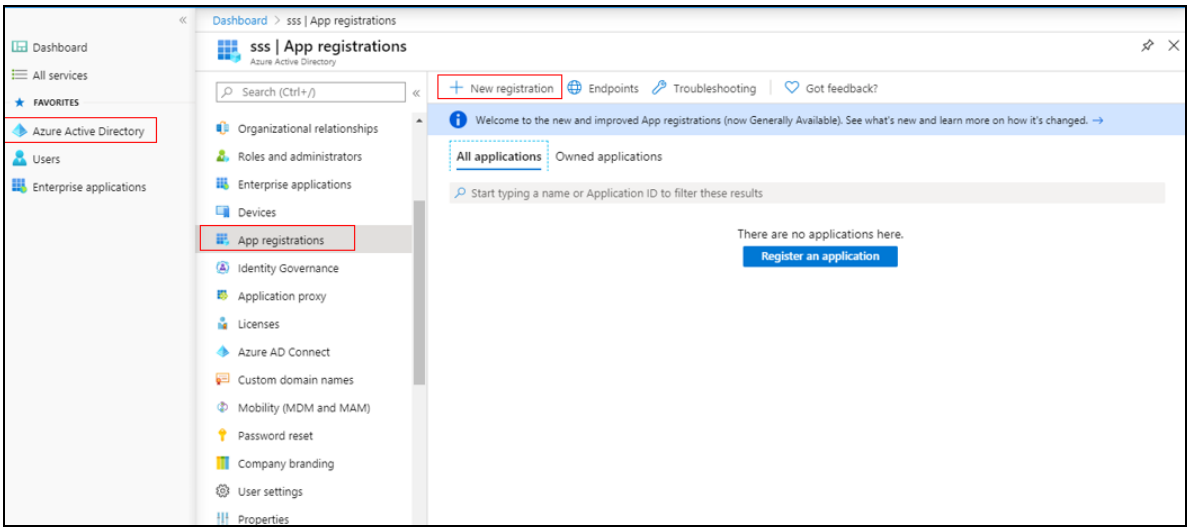


Figure 2.27: Selecting the App registrations option to register a new app on Azure AD

4. Figure 2.28 then appears, using which you can register the Microsoft Graph app. In the **Name** text box, specify the display name of the app you intend to register. **Make sure you copy this name to notepad**. Then, from the drop-down in the **Redirect URI** section, select **Web**. In the text box adjacent to the drop-down, specify the URL to which the authentication response needs to be returned after successfully authenticating users to the new app. Make sure that this URI ends with 'my-sharepoint' - eg., *https://myapp.com/my-sharepoint*. Finally, click the **Register** button in Figure 2.28 to register Microsoft Graph on Azure AD.

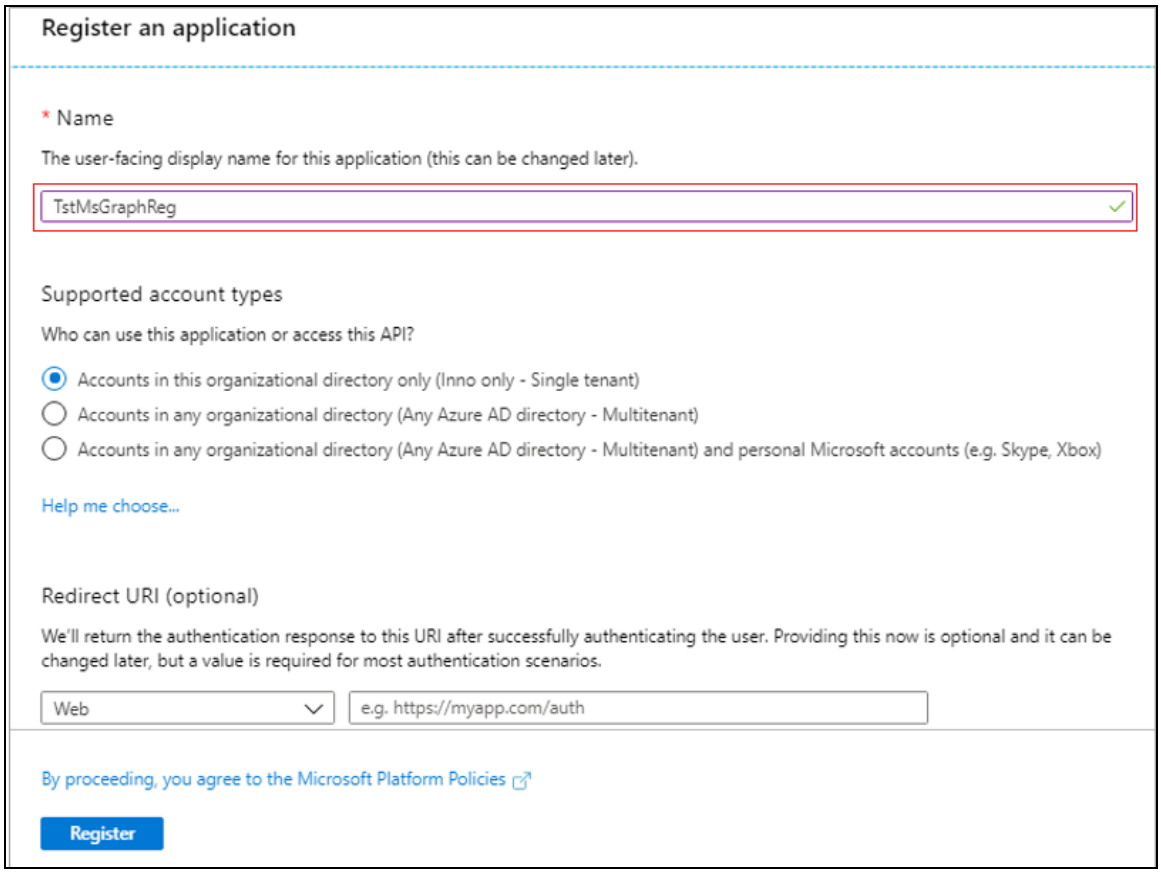


Figure 2.28: Registering the Microsoft Graph app on Azure AD

5. Upon successful app registration, Figure 2.29 will appear displaying a message to that effect. Additionally, Figure 2.29 will display the **Application (client) ID** that is auto-generated and auto-assigned to the Microsoft Graph app. **Make sure you copy this ID also to notepad**.

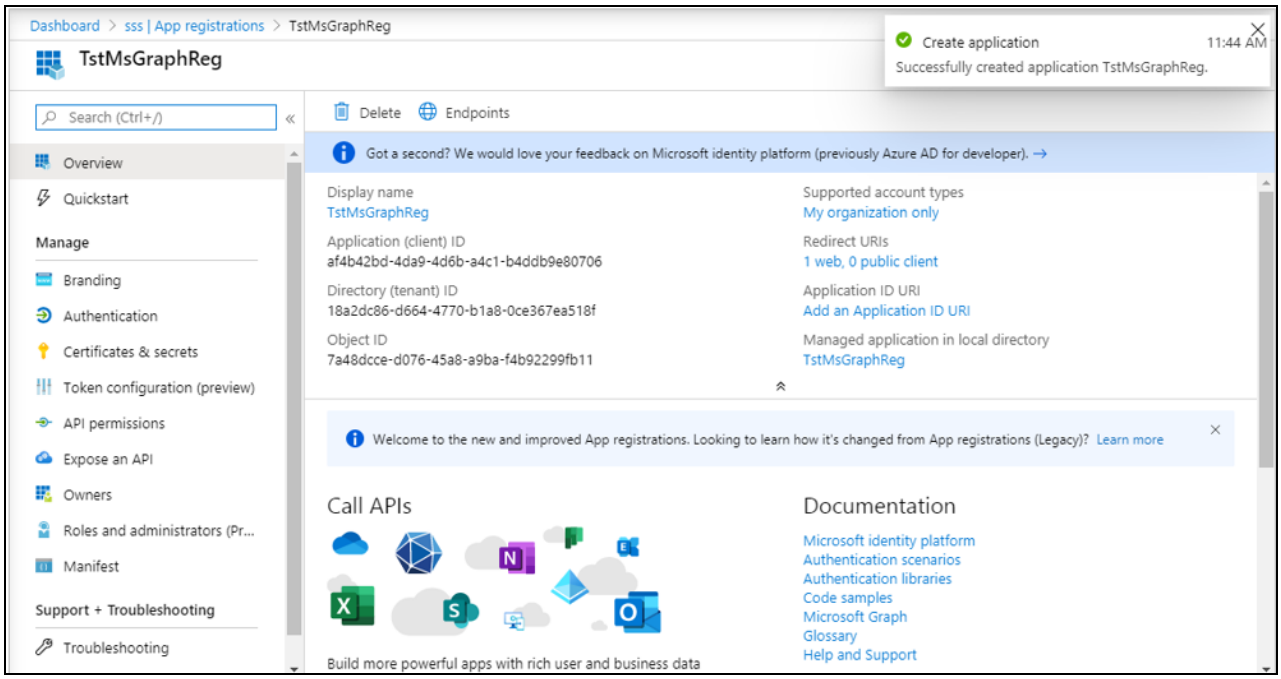


Figure 2.29: Viewing and making a note of the Application ID of the Microsoft Graph app

6. Next, proceed to create a secret for the new app. To achieve this, click on the **Certificates & Secrets** option under Manage in the left panel of Figure 2.29. Figure 2.30 will then appear. Now, click on the **New client secret** button in the **Client Secrets** section in the right panel of Figure 2.30.

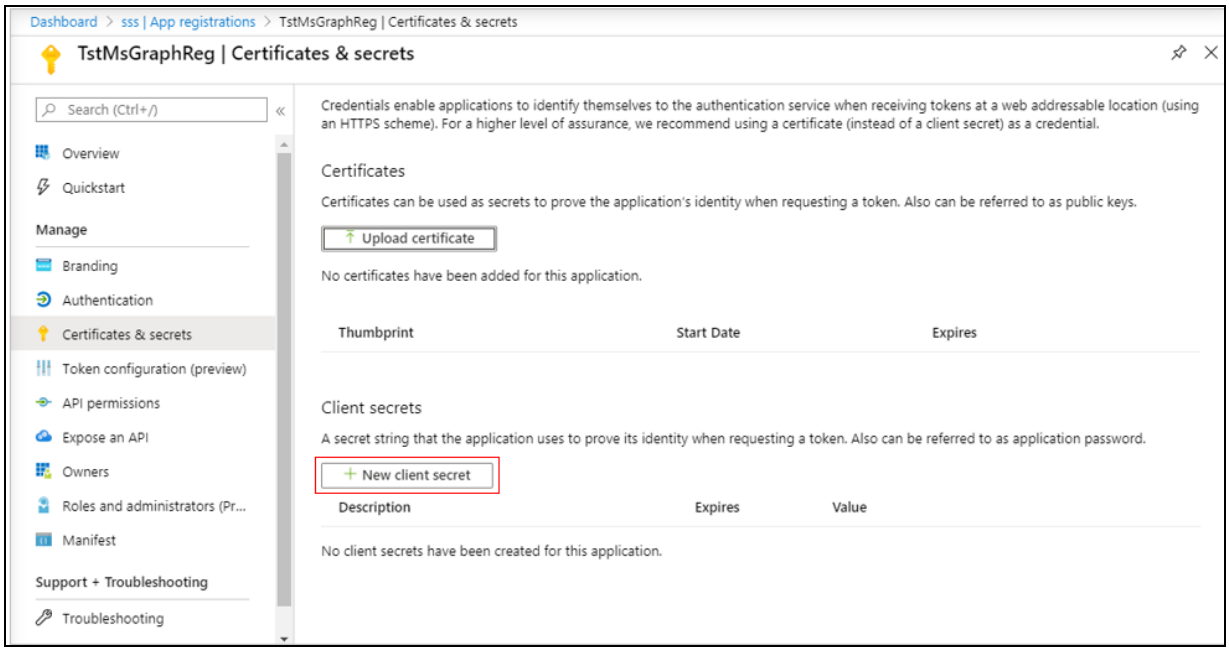


Figure 2.30: Clicking on the New client secret button

7. When Figure 2.31 appears, provide a **Description** for the new secret, set it to **Never** expire, and click the **Add** button to add the new secret.

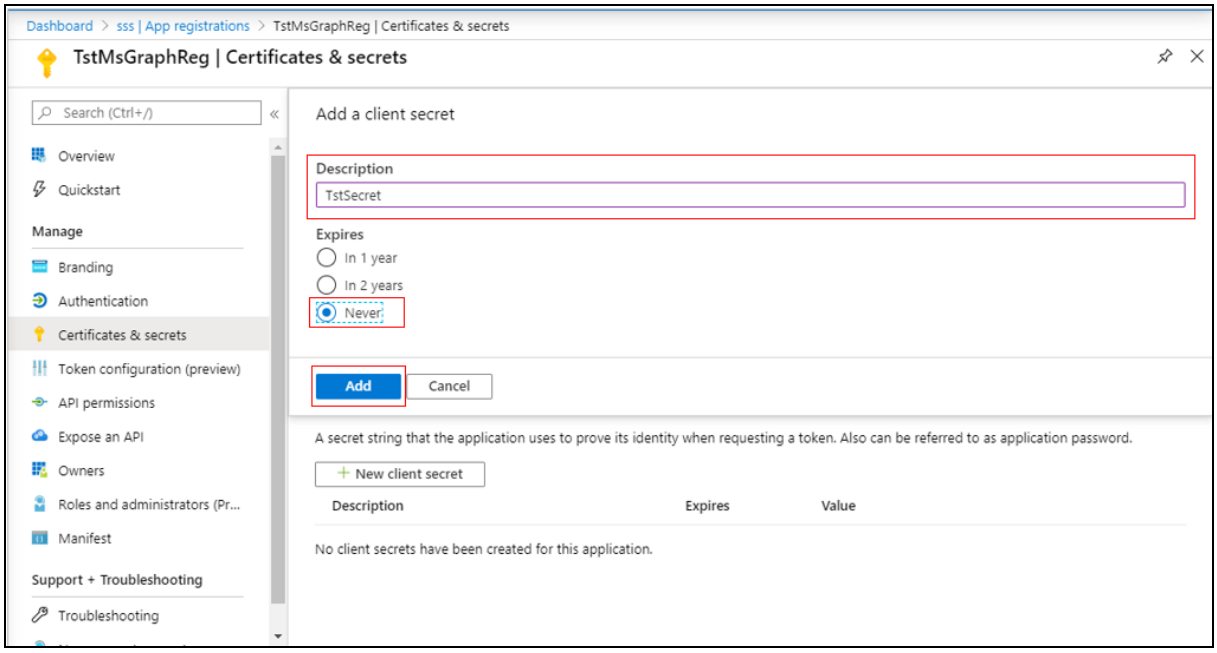


Figure 2.31: Creating a new secret for the Microsoft Graph App

8. Once the new secret is successfully created, a key will be generated for it, as depicted by Figure

2.32. **Make a note of this key in notepad**.

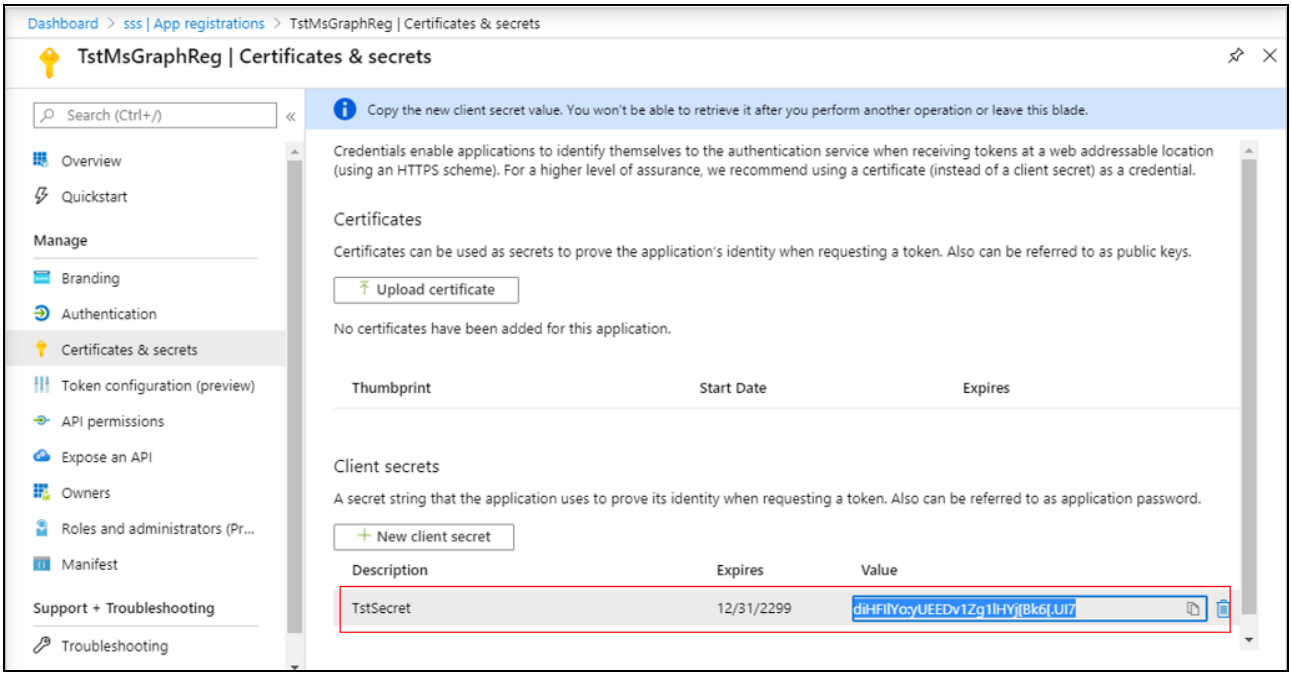


Figure 2.32: The key that is generated and assigned to the client secret of the Microsoft Graph app

9. Next, proceed to grant permissions to the Microsoft Graph app, so it can pull the desired metrics. For this, click on the **API permissions** option under **Manage** in the left panel of Figure 2.32. This will invoke Figure 2.33. In the right panel of Figure 2.33, click on the **Add a permission** button.

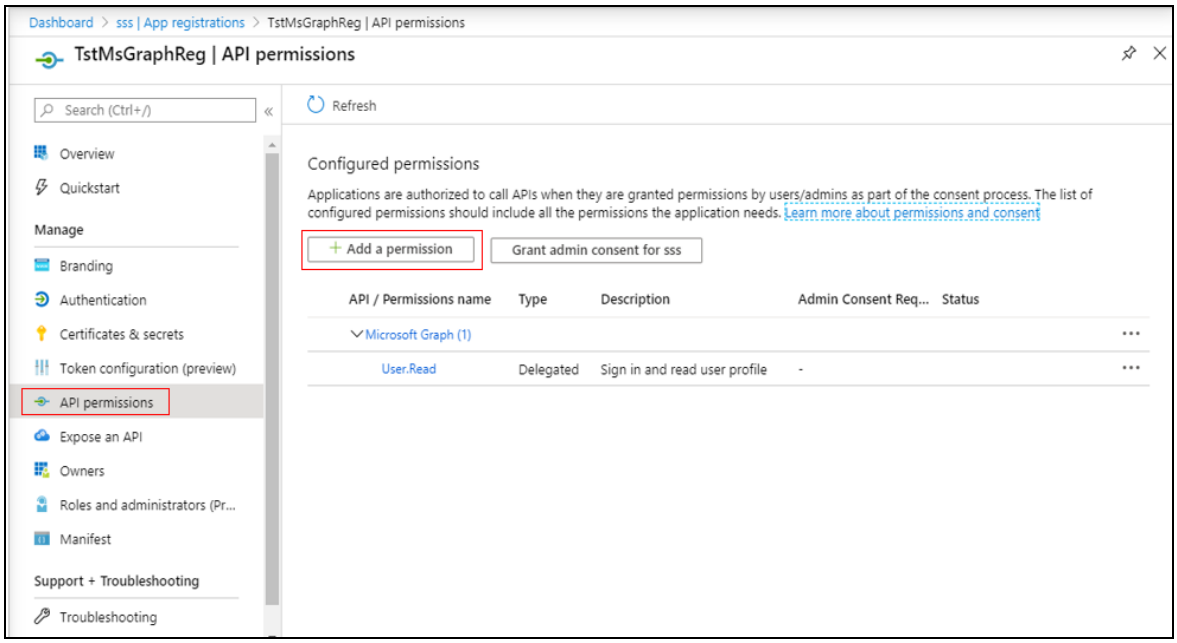


Figure 2.33: Clicking on the Add a permission button

10. Then, click on **Office 365 Management APIs** in the **Request API Permissions** window that appears (see Figure 2.34).

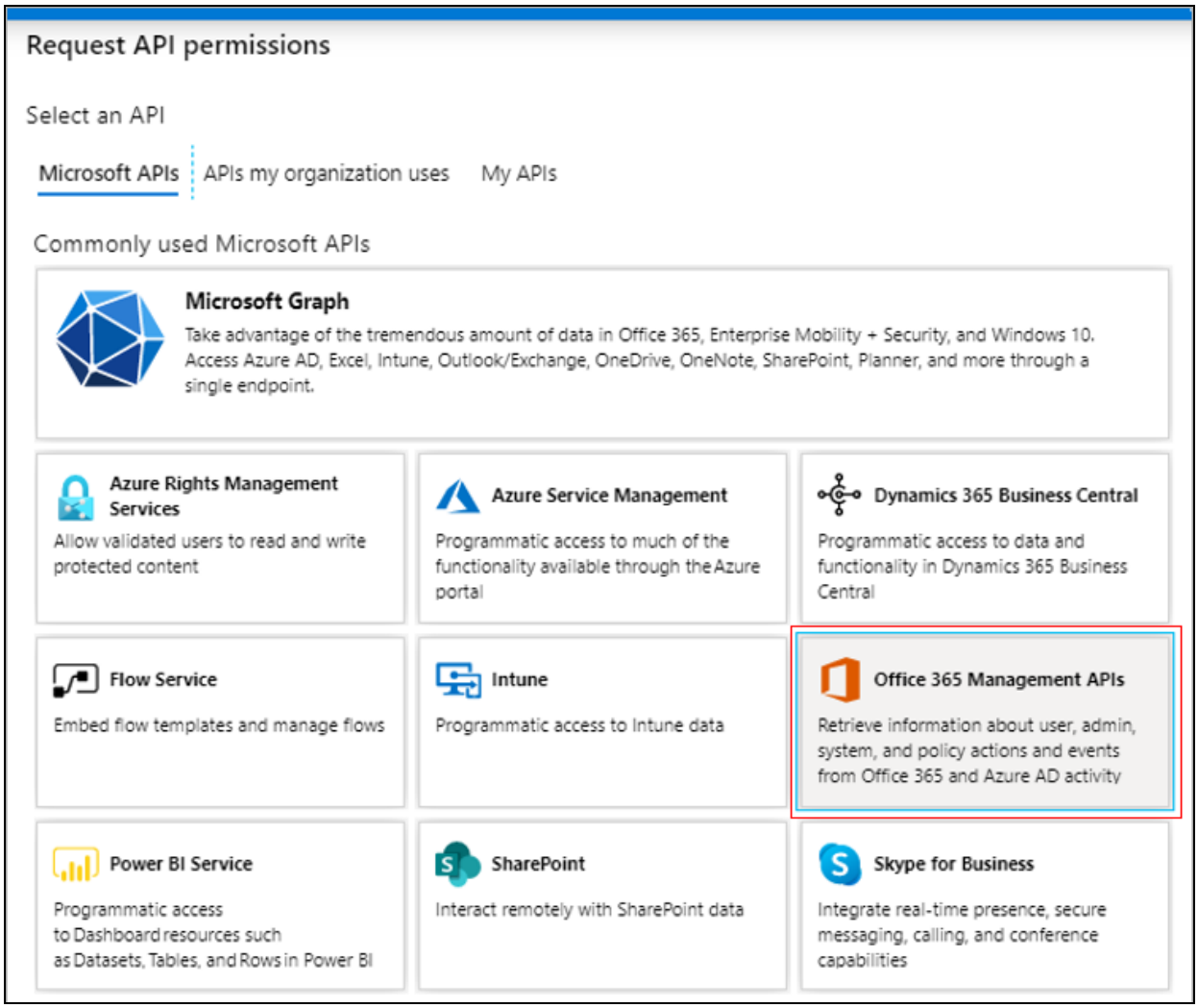


Figure 2.34: Selecting the Office 365 Management APIs option

11. When Figure 2.35 appears, click on **Application permissions**. Then, when the **Permission** tree appears below, expand the **ServiceHealth** node and select the **ServiceHealth.Read** option to assign that permission to the Microsoft Graph app. This will allow the Microsoft Graph app to read the service health information for your organization. Finally, click on **Add permissions** to add the chosen permission.

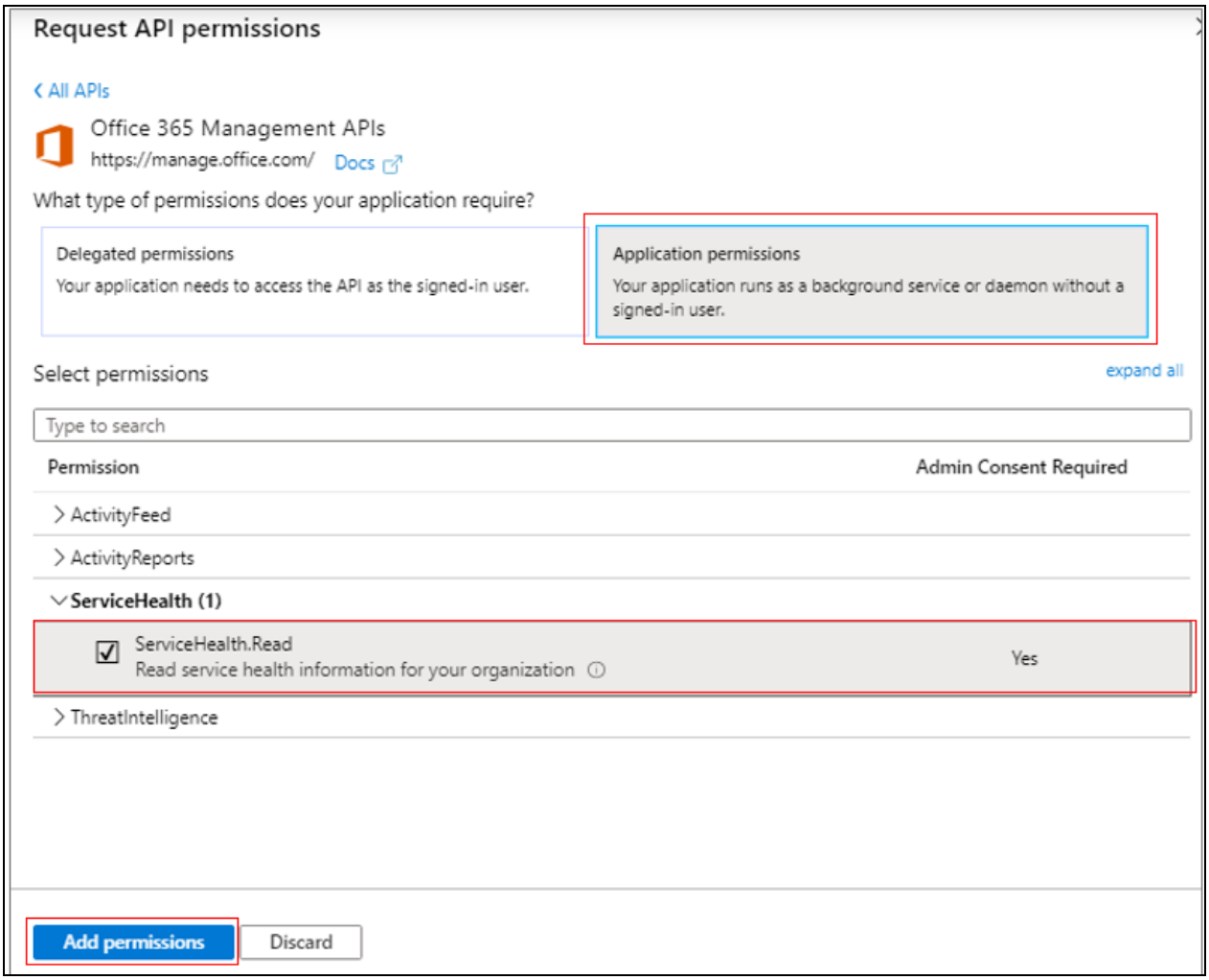


Figure 2.35: Granting permission to the Microsoft Graph app to read service health

12. When Figure 2.36 appears, click on the **Add a permission** button again.

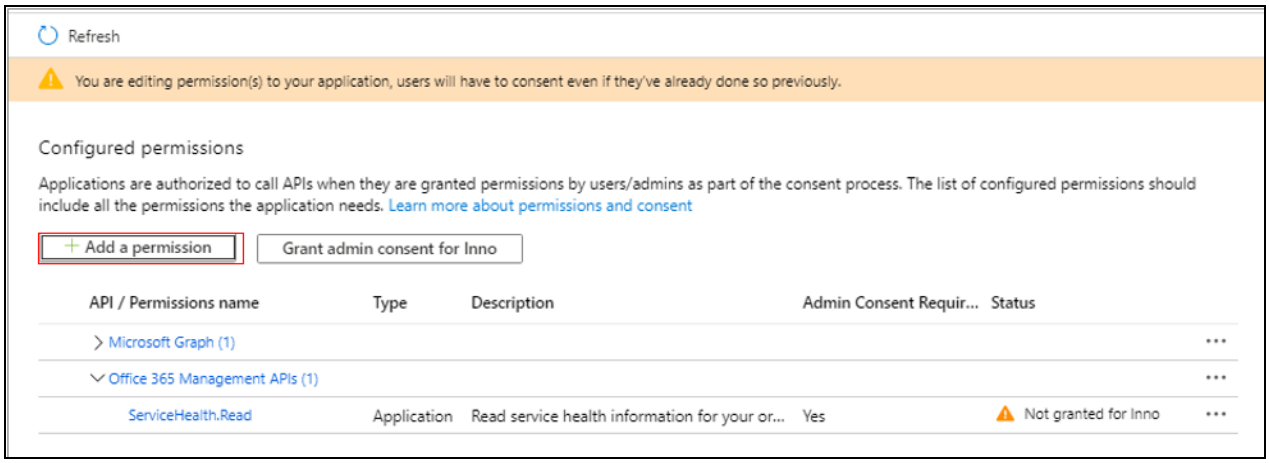


Figure 2.36: Clicking on the Add a permission button again to add permission to read from and write to user files

13. From Figure 2.37 that then appears, select the **SharePoint** option.

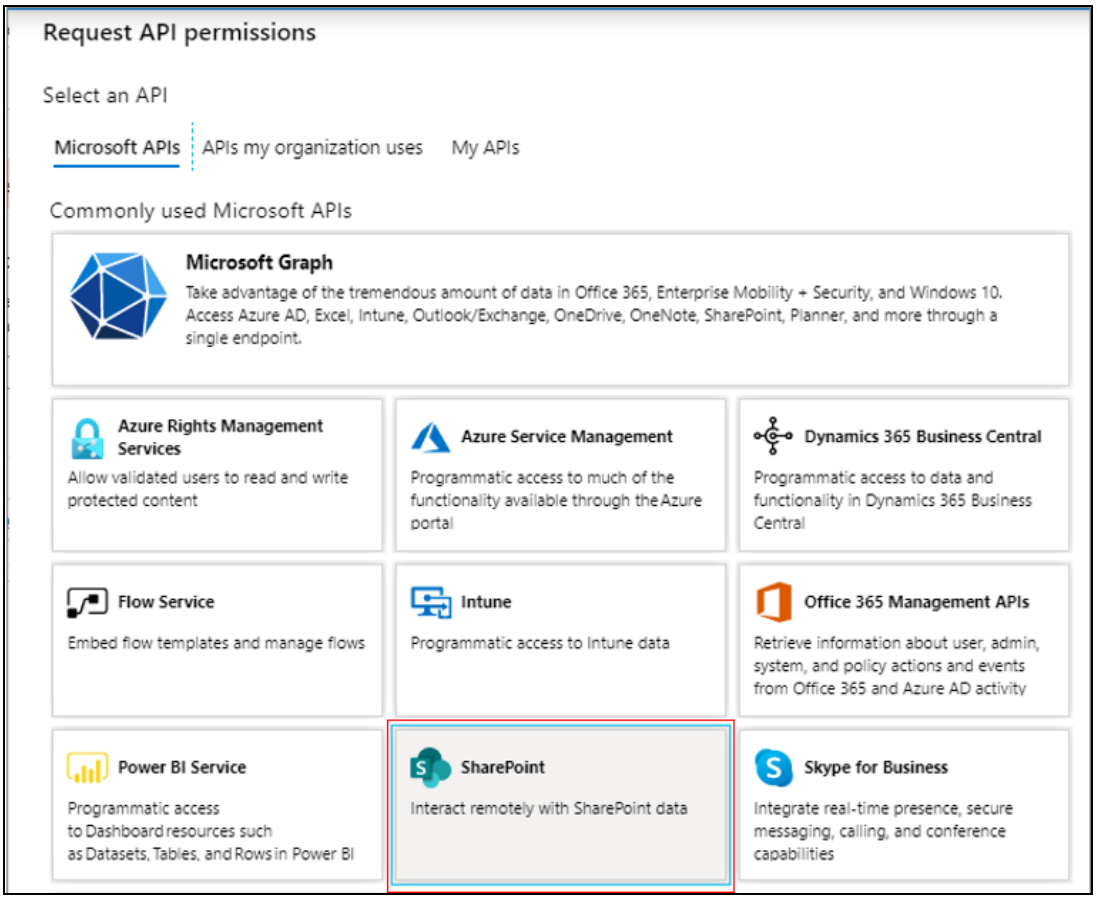


Figure 2.37: Selecting the SharePoint option

14. Then, select the **Delegated permissions** option from Figure 2.38, expand the **MyFiles** node in the **Permission** tree, and check the **MyFiles.Read** and **MyFiles.Write** check boxes within. Doing so will allow the Microsoft Graph app to read from and write to user files. As before, click the **Add permissions** button to add the chosen permissions to the Microsoft Graph app.

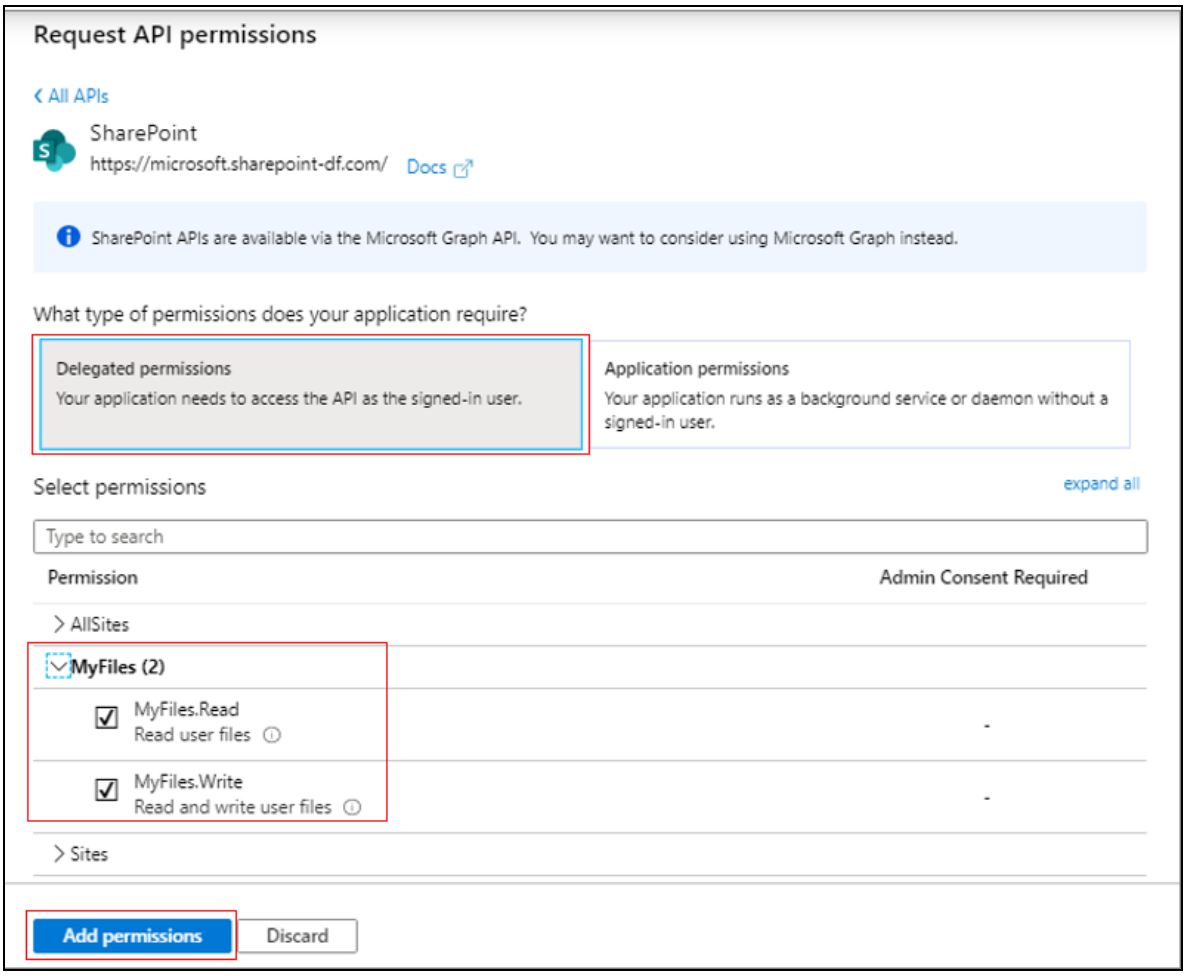


Figure 2.38: Granting permission to Microsoft Graph app to read from and write to user files

15. You will now return to Figure 2.36. Once again, click on the **Add a permission** button therein to grant another permission to Microsoft Graph. When Figure 2.37 appears, select the **SharePoint** option yet again. Next, as depicted by Figure 2.39, select **Application permissions**, expand the **Sites** node in the **Permission** tree, and select the **Sites.Read.All** check box. Doing so will allow the Microsoft Graph app to read items in all site collections. Click on **Add permissions** in Figure 2.39 to add the chosen permission to Microsoft Graph app.

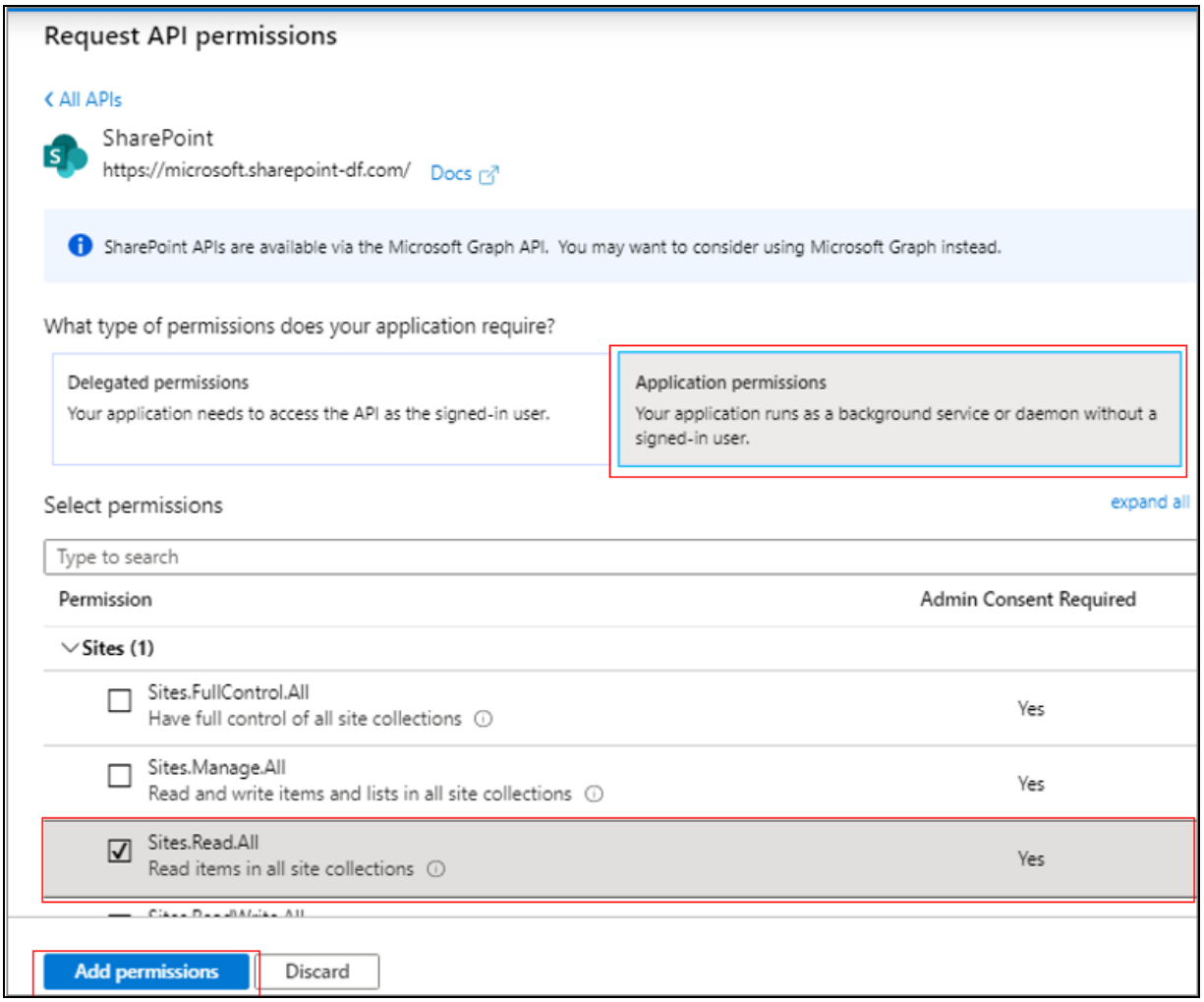


Figure 2.39: Granting permission to Microsoft Graph app to read items in all site collections

16. You will once again return to Figure 2.36. Click on the **Add a permission** button therein. When Figure 2.40 appears, select the **Azure Active Directory Graph** option.

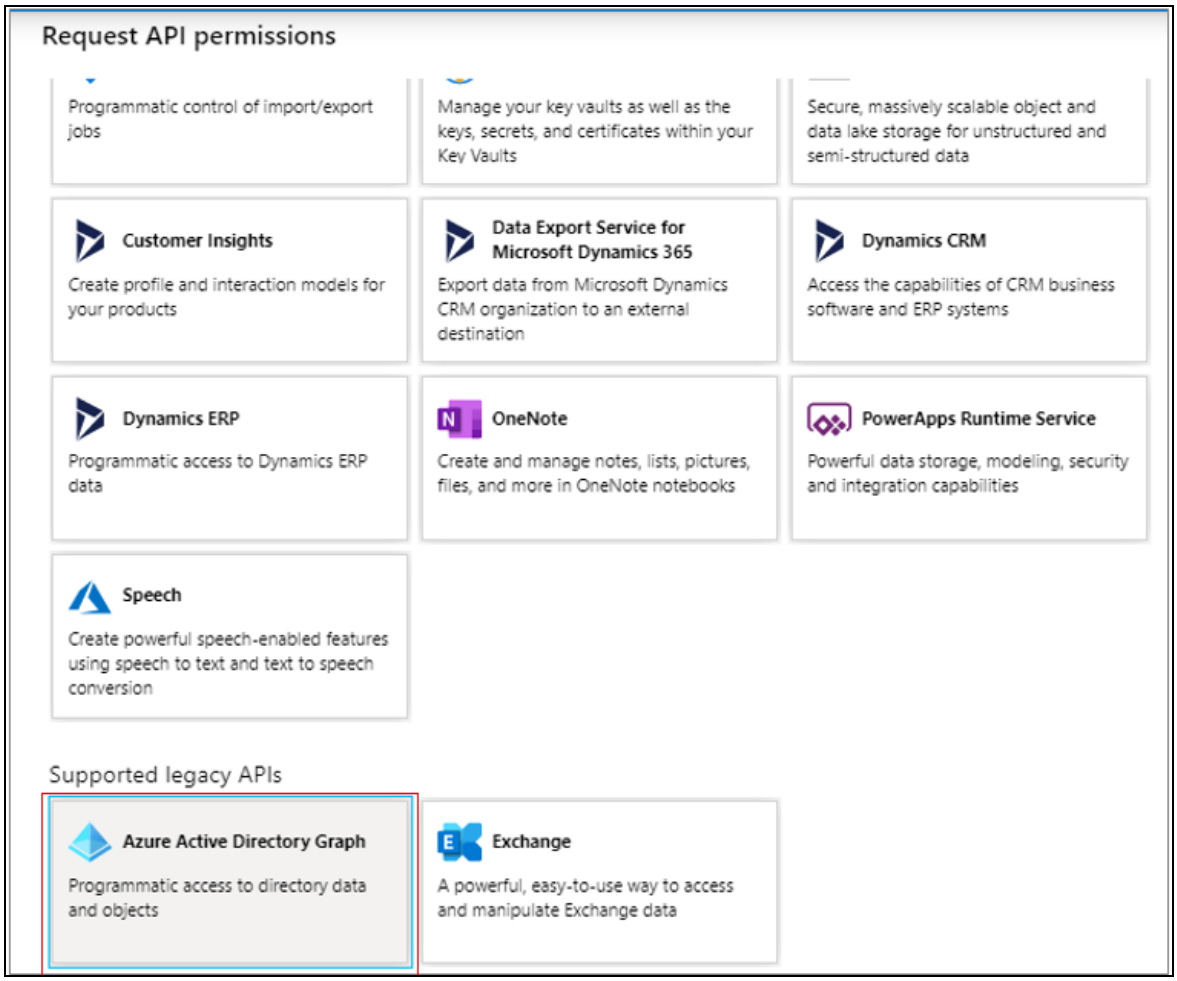


Figure 2.40: Selecting the Azure Active Directory Graph option

17. From Figure 2.41, select **Delegated Permissions**. Then, expand the **User** node in the **Permission** tree, and select the **User.Read** check box. This will allow the Microsoft Graph app to sign in and read the user profile. As before, click the **Add permissions** button to grant the chosen permission to the Microsoft Graph app.

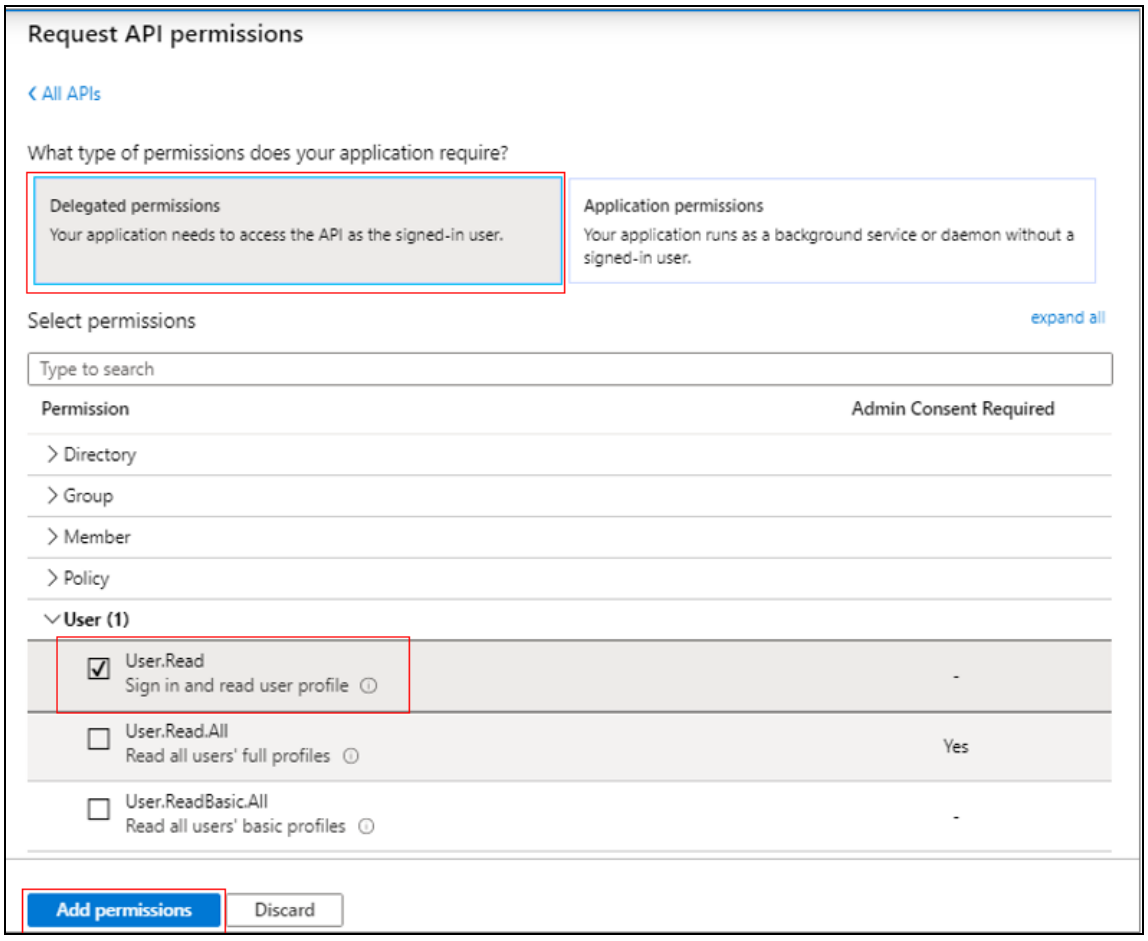


Figure 2.41: Granting the Microsoft Graph app permission to sign in and read user profile

18. As soon as you return to Figure 2.36, click the **Add a permission** button yet again. This time, click on the **APIs my organization uses** tab page in the **Request API permissions** window of Figure 2.37. Scroll down the list of APIs that appears until the **Microsoft Graph** API comes into view. Choose this API.

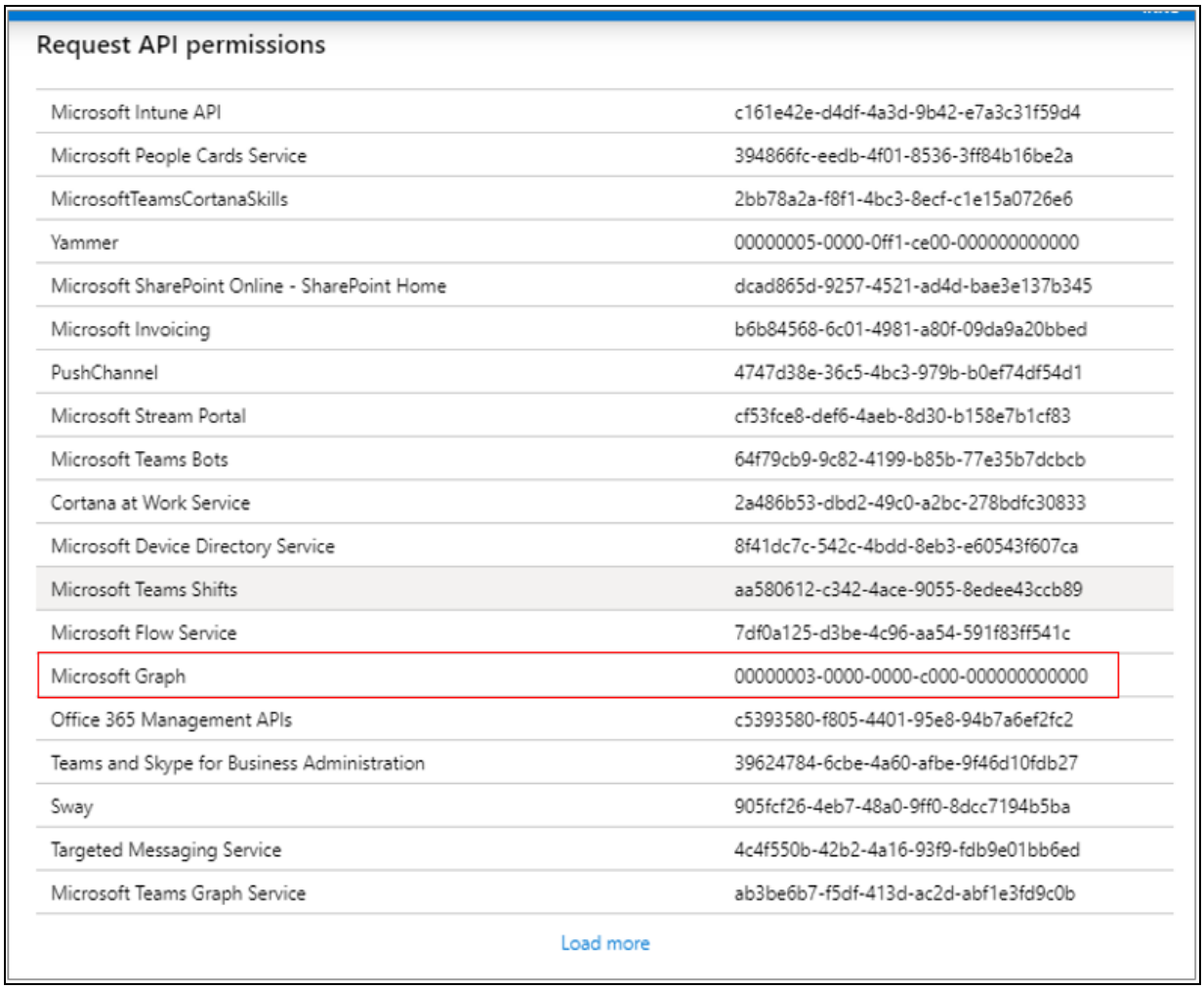


Figure 2.42: Choosing the Microsoft Graph API

19. Next, expand the **Group** node in the **Permission** tree, and select the **Group.Read.All** check box within. This will allow the Microsoft Graph app to read all groups.

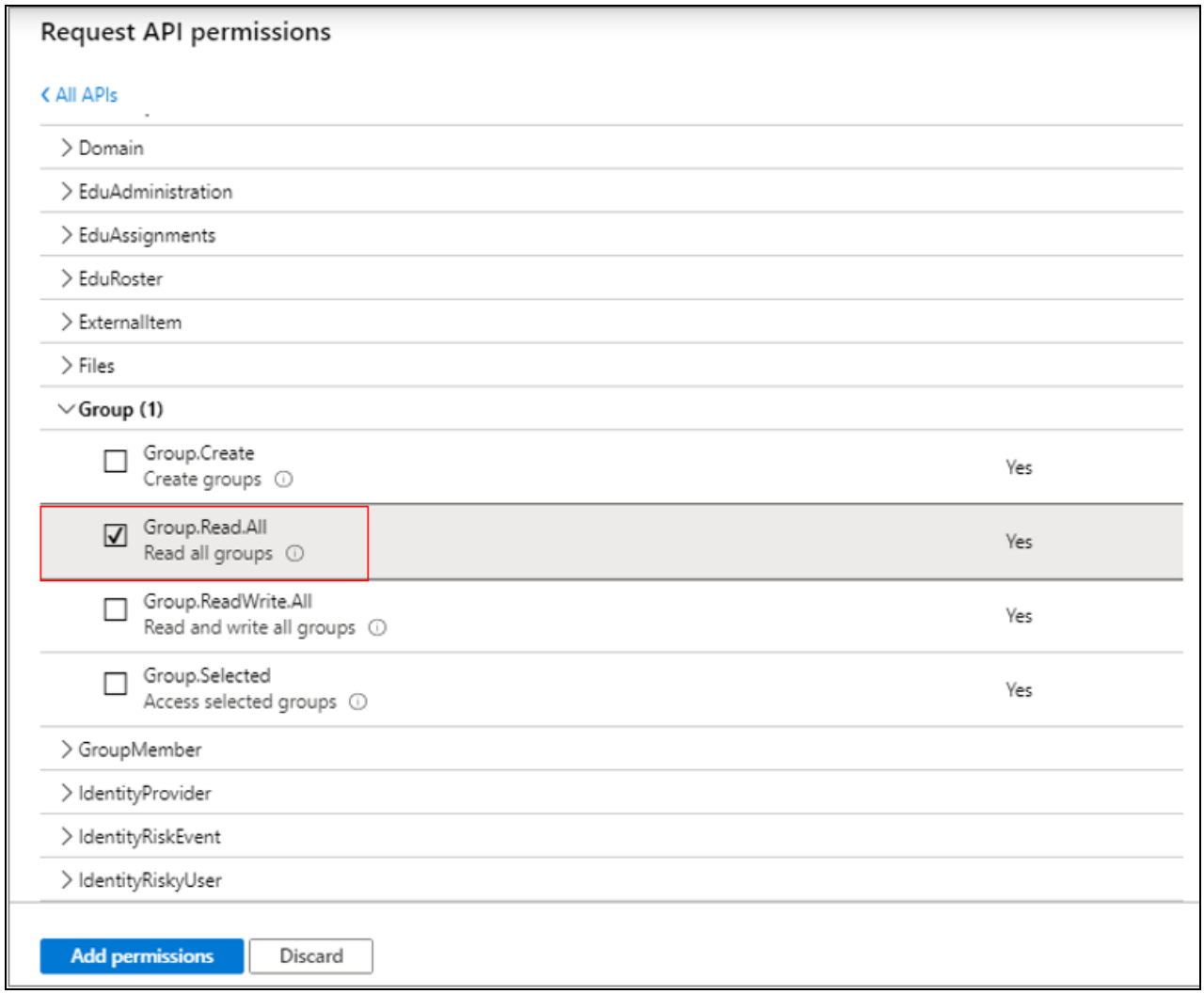


Figure 2.43: Granting the Microsoft Graph app permission to read all groups

20. Next, expand the **User** node in the **Permission** tree, and select the **User.Read.All** check box within. This will enable the Microsoft Graph app to read the full profile of all users.

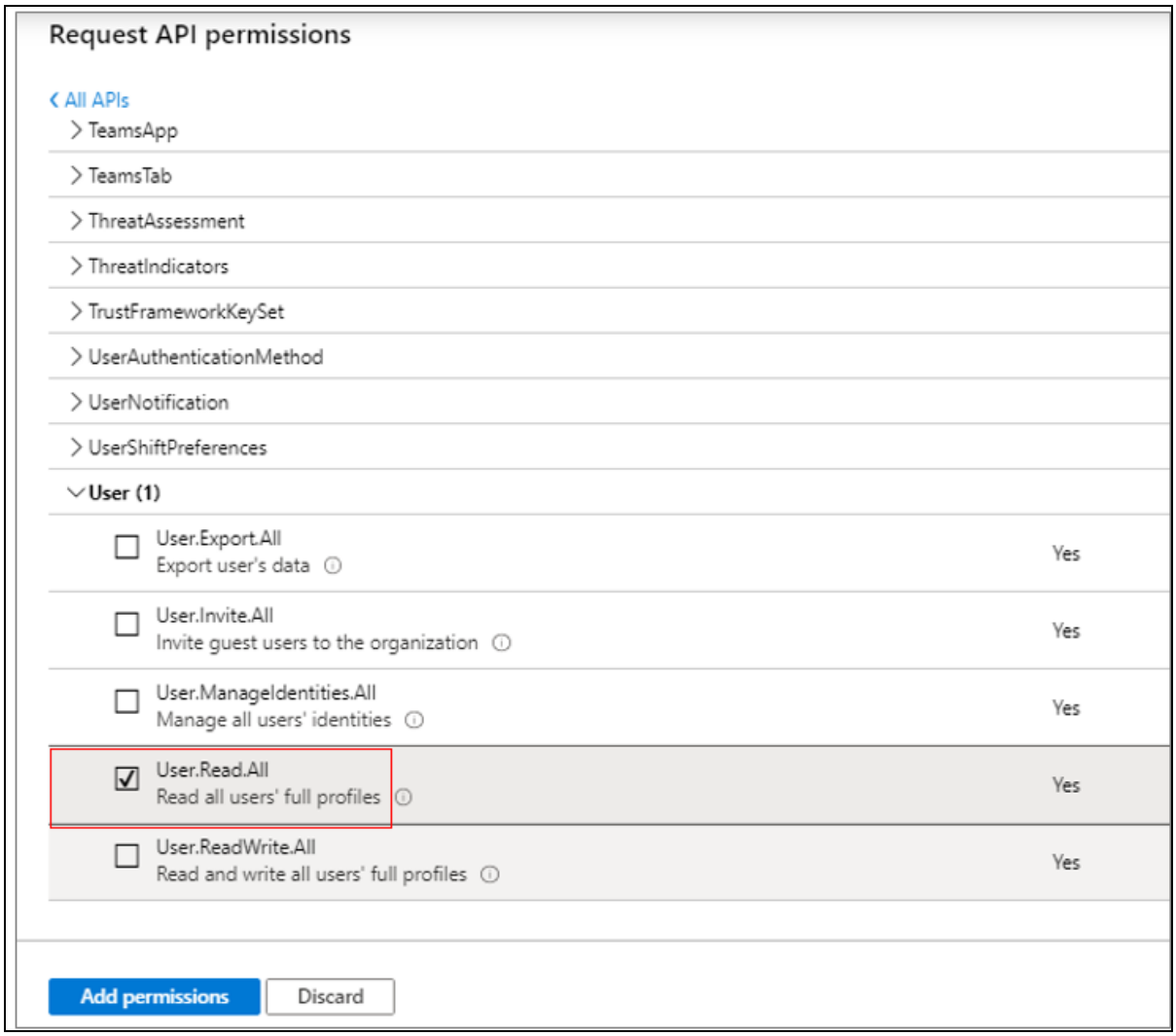


Figure 2.44: Granting the Microsoft Graph app permission to read full profile of all users

21. Next, expand the **Reports** node in the **Permission** tree, and select the **Reports.Read.All** check box within. This will permit the Microsoft Graph app to read all usage reports.

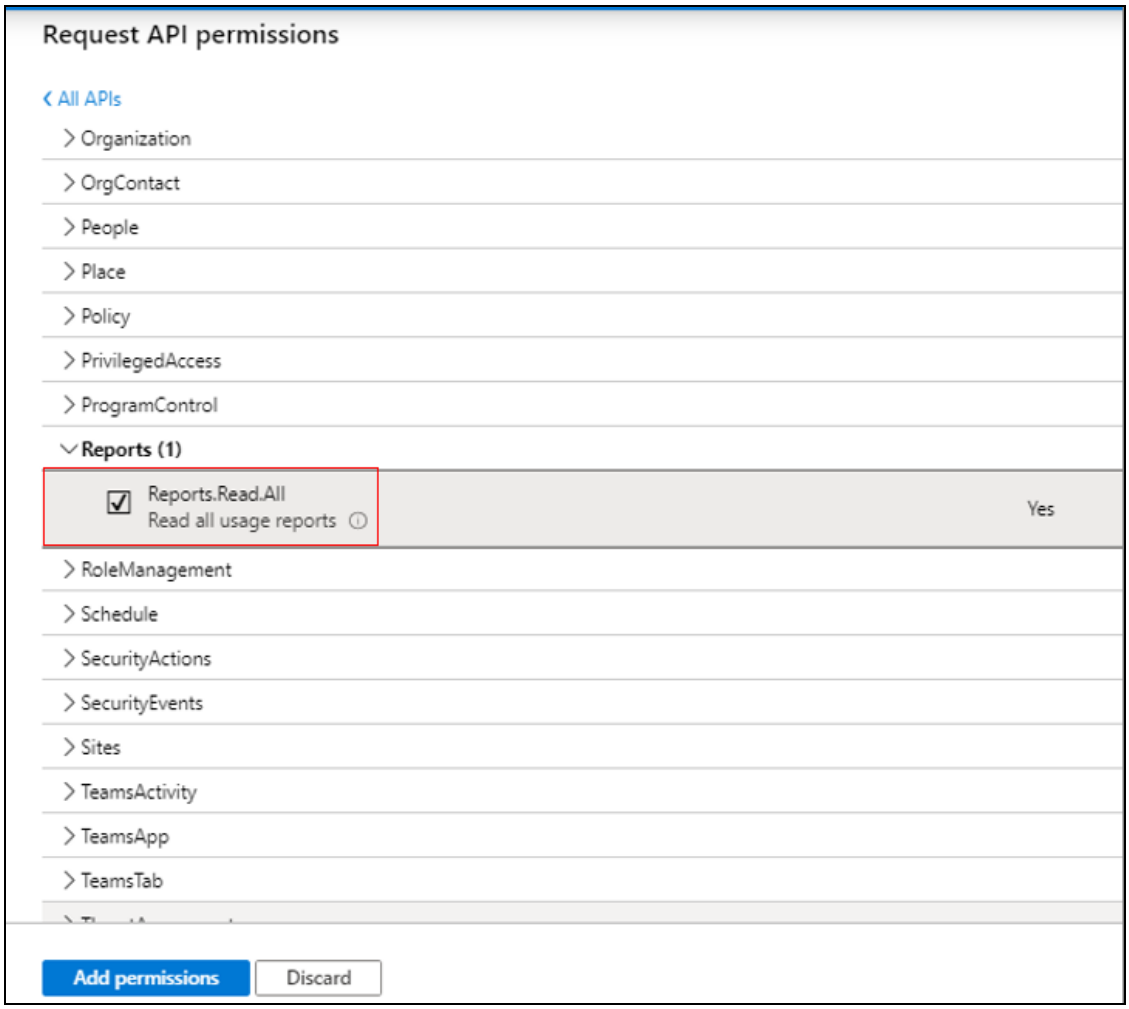


Figure 2.45: Granting permission to the Microsoft Graph app to read all usage reports

22. Finally, click the **Add permissions** button in Figure 2.45 to add all the chosen permissions to the Microsoft Graph app. When Figure 2.46 appears, click the **Grant admin consent for <user>** button therein to grant admin consent for the user.

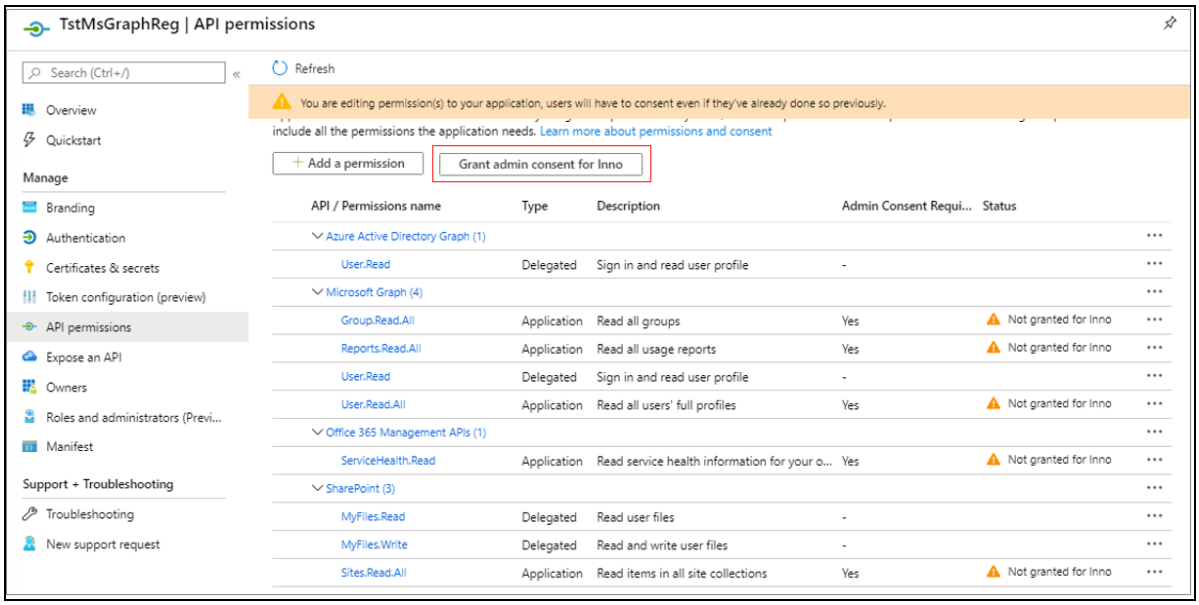


Figure 2.46: Granting admin consent to the user

23. Next, proceed to create a .dat file to which the details of the Microsoft Graph app - i.e., the app name, its client ID, and client secret - will be written. At run time, the eG agent reads the .dat file to know which app should be used for pulling metrics from Office 365. To create the .dat file, first, login to the eG agent host, Then, using Powershell ISE, execute the **CreateGraphDat.ps1** command from the <EG_INSTALL_DIR>\lib\O365 directory. Upon successful command execution, the dialog box depicted by Figure 2.47 will appear.

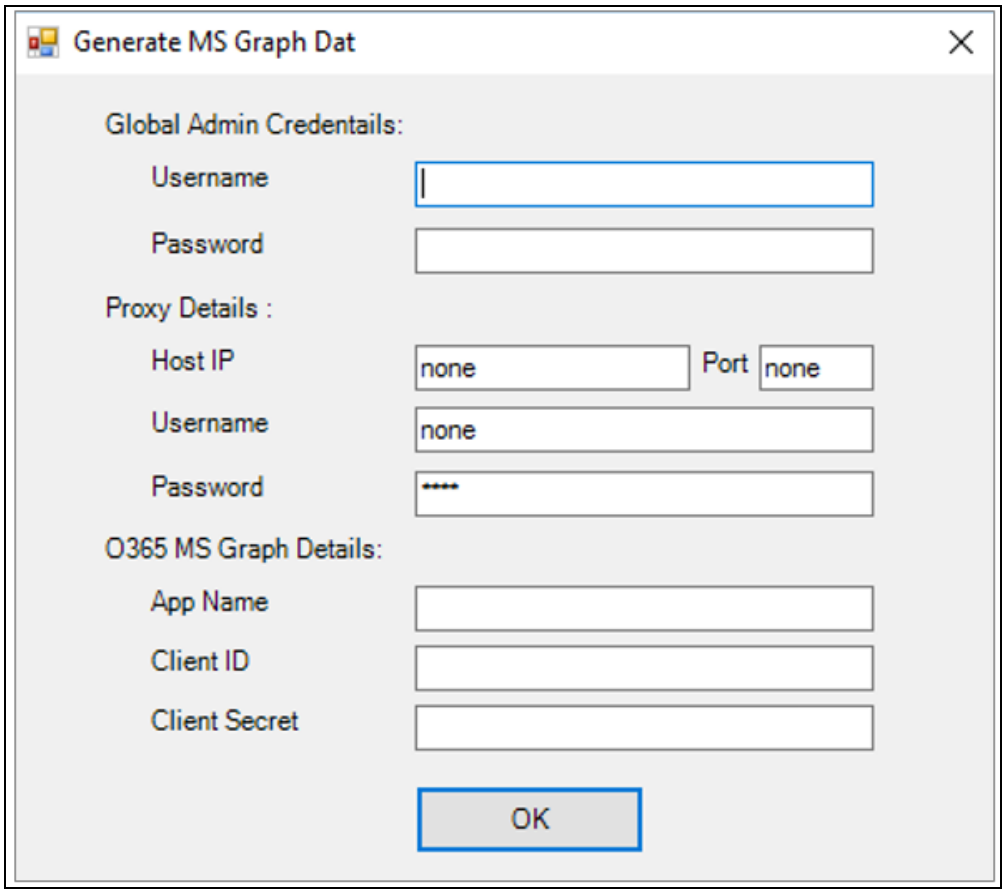


Figure 2.47: Generating MS Graph Dat

24. In Figure 2.47, specify the **Username** and **Password** of the global administrator. If the eG agent will be communicating with Office 365 via a Proxy server, then configure the **Host IP** and **Port** number of the Proxy server. If the Proxy server requires authentication, then provide a valid **Username** and **Password** for the Proxy user. Then, in the **O365 MS Graph Details** section, mention the **App name**. This should be the same name you gave the app in step 4 above. Then, specify the **Client ID** and **Client secret** for the app. The **Client ID** should be the **Application (client) ID** you made a note of in step 5 above (see Figure 2.29). The **Client secret** should be the key that is generated and assigned to the client secret in step 8 above (see Figure 2.32). Finally, click the **OK** button.

25. If the MS Graph Dat file is created successfully, a message to that effect will appear.

Chapter 3: How to Monitor Microsoft Office 365 Using eG Enterprise?

Once the pre-requisites for monitoring Office 365 are fulfilled, follow the broad steps outlined below to manage and then monitor Microsoft Office 365 using eG Enterprise:

1. Add a Microsoft Office 365 component using the eG admin interface.
2. Configure tests for the managed Microsoft Office 365 component.

3.1 Adding a Microsoft Office 365 Component

eG Enterprise cannot auto-discover a Microsoft Office 365 component. This is why, you need to manually add the component to the eG Enterprise system to monitor it. Every 'tenant' in the target Office 365 deployment should be added as a separate Microsoft Office 365 component in the eG Enterprise. The steps for manually adding a Microsoft Office 365 tenant are detailed below:

1. Login to the eG admin interface as a user with administrative privileges.
2. Follow the Infrastructure -> Components -> Add/Modify Component menu sequence in the Admin tile menu.
3. From the page that appears, select *Microsoft Office 365* as the **Component type** and click the **Add New Component** button.
4. Figure 3.1 will then appear.

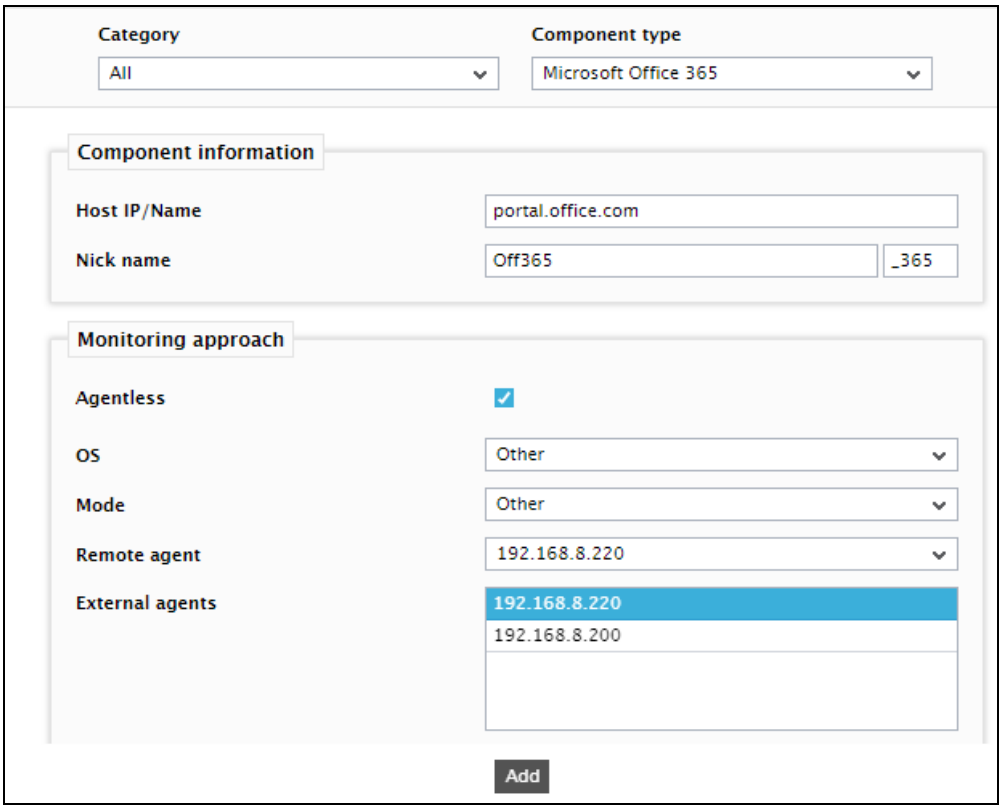


Figure 3.1: Adding a Microsoft Office 365 component

5. In Figure 3.1, by default, portal.office.com will be displayed as the **Host IP/Name** of the target Microsoft Office 365 component. If the host name of the Office 365 tenant you want to monitor is different in your environment, then modify this specification.
6. Provide a unique **Nick Name** for the Office 365 component being added. Note that any nick name you specify here will be automatically suffixed with the string, *_365*.
7. Since Office 365 is by default monitored in an agentless manner, the **Agentless** flag will be enabled. Let the default settings remain in the **OS** and **Mode** selection boxes.
8. Next, select the **Remote agent** and **External agent** that will monitor the target Office 365 component.
9. Finally, click the **Add** button to add the component to the eG Enterprise system.
10. eG Enterprise allows you the flexibility to automatically manage a SharePoint Online, Exchange Online, Skype for Business Online, Microsoft Teams, and/or a Microsoft OneDrive for Business component, when adding an Office 365 component. This is why, when clicking the **Add** button in Figure 3.1, you will be immediately prompted to manage the above-mentioned components using the same nick name as the Office 365 component (see Figure 3.2). Select the components you want to add by checking the corresponding check boxes

in Figure 3.2and click the **OK** button. If you do not want to add any other component than Office 365, then click **OK** without selecting any of the check boxes.

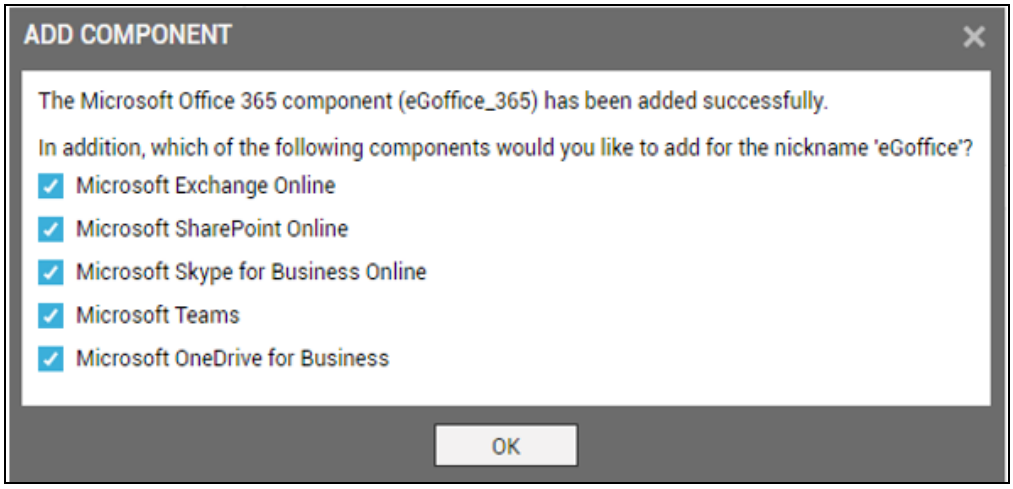


Figure 3.2: A message prompting you to add other Office 365 components

Note:

- When Office 365 components are so added, eG Enterprise automatically appends a unique suffix to the nick name of each component. This means that every component will have the same nick name, but with a different suffix. These suffixes are listed in the table below:

Component Type	Suffix
Microsoft Office 365	_365
Microsoft Exchange Online	_exo
Microsoft SharePoint Online	_spo
Microsoft Teams	_mtm
Microsoft Skype for Business Online	_sbo
Microsoft OneDrive for Business	_odb

For instance, say you are adding a component of type *Office 365* with the nick name *eGOffice*. Assume that when adding this component you choose to add a Microsoft Exchange Online component as well. At the end of this exercise, the following components will be added to the eG Enterprise system:

Component Type	Nick name
Microsoft Office 365	eGOffice_365
Microsoft Exchange Online	eGOffice_exo

- Whether you add the chosen components using different nick names, or using the same nick name as that of the Microsoft Office 365 component, each component you add will consume a separate Premium Monitor license.
- In a SaaS deployment of eG Enterprise, an administrator has to make sure that all Office 365 components of a single tenant are managed in eG Enterprise using the same nick name - i.e., are managed using step 10 above. For instance, tenant A should use a common nick name - say, *O365* - to manage all Office 365 components in their environment. Likewise, tenant B should use one nick name, say *Office* , for managing their entire Office infrastructure. At no point of time should the tenants change the nick name of one/more Office 365 components in their environment.

  This is required because the Office 365 Dashboard in the eG monitoring console groups metrics and visuals using the nick name you choose. To receive meaningful, tenant-specific insights into the performance of the Office 365 infrastructure, the aforesaid 'nick naming conventions' need to be followed.

3.2 Configuring Tests for the Microsoft Office 365 Component

After adding a Microsoft Office 365 component, click the Sign out button at the right, top corner of the eG admin interface to exit that interface. Doing so will invoke the list of tests that need to be manually configured for the managed Office 365 component.

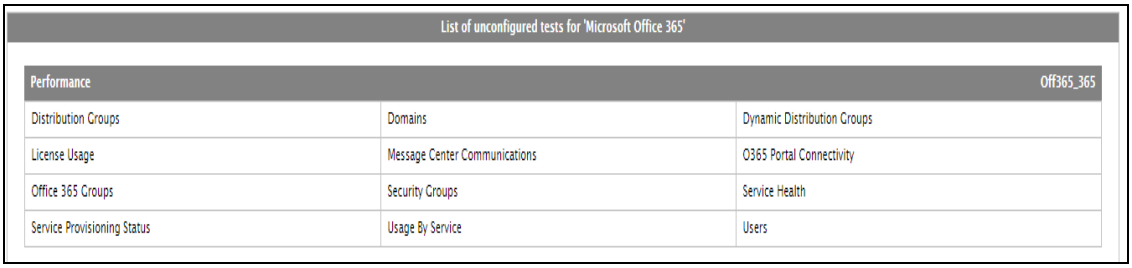


Figure 3.3: List of tests to be manually configured for Microsoft Office 365

Click on any of the tests in Figure 3.3 to configure it. Say, you want to configure the Distribution Groups test. Clicking on that test in Figure 3.3 will open Figure 3.4.

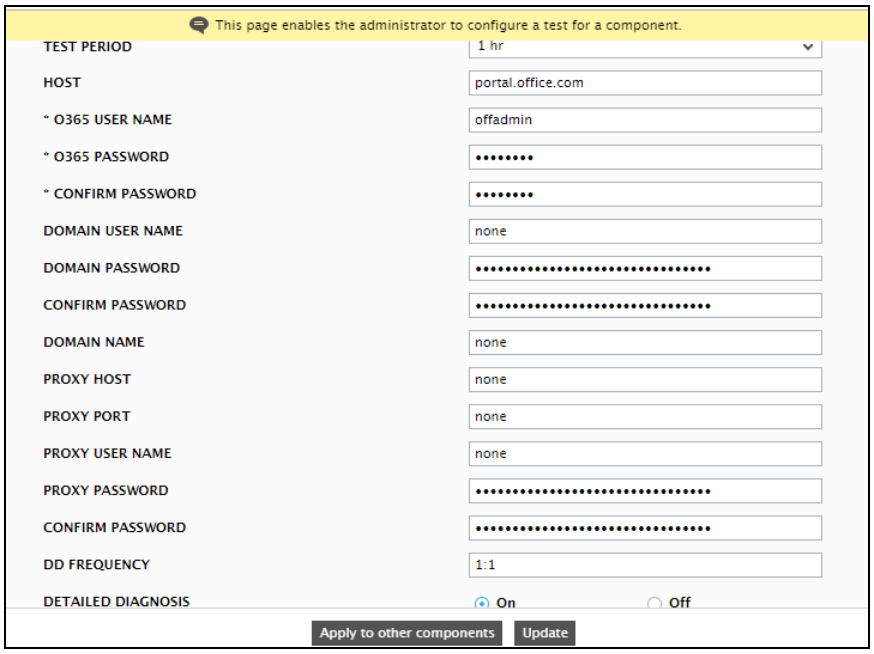


Figure 3.4: Configuring the Distribution Groups test

With the help of the Distribution Groups test, administrators can easily and efficiently audit distribution groups. For each DG type (Universal and SecurityEnabled), this test reports the count and details of new, deleted, and modified groups of that type. Additionally, empty groups and orphaned groups are also brought to the attention of administrators. This way, administrators can identify groups that may have to be assigned new owners and groups that are still awaiting members.

To know what parameters this test takes and how to configure it, refer to the Section **4.3.1** topic. Once the test is configured, click the **Update** button in Figure 3.4 to save the test configuration. Finally, sign out of the eG admin interface.

Chapter 4: Monitoring Microsoft Office 365

To monitor the managed Microsoft Office 365, login to the eG management console as a user with monitoring privileges.

Browse the **Components At-A-Glance** section of the Monitor Home page that appears, and locate the *Microsoft Office 365* component type. Click on the bar that corresponds to this component type. This will lead you to the **Layers** tab page, where you can view the monitoring model for Microsoft Office 365 (see Figure 4.1).

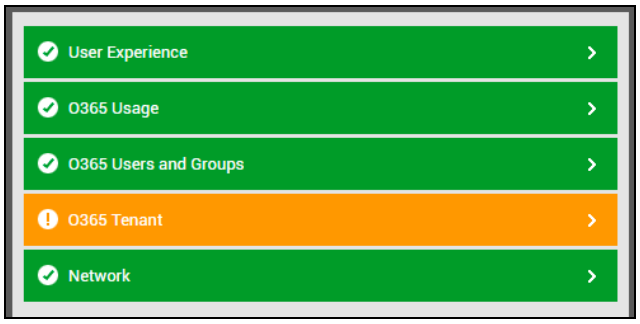


Figure 4.1: Layer model for the Microsoft Office 365 component

Each layer of Figure 4.1 is mapped to tests that report on a wide variety of KPIs such as availability, service health, resource usage, and operational health of Office 365. Using these metrics, administrators can find quick and accurate answers to the following performance queries:

- Is HTTP/S connection to the Office 365 portal available? Was any latency noticed in the connection?
- Is network connection to Office 365 available? If so, how quickly is it responding to network requests?
- Were any groups modified recently? Were they distribution groups, dynamic distribution groups, Office 365 groups, or security groups?
- Are there any orphaned groups or empty groups? Which ones are they?
- Which is the default domain of the target Office 365 tenant? Is this domain verified? Which are the unverified domains in the monitored tenant?
- Has any Office 365 product run out of licenses or is about to? Is so, which one is it?
- Is any product's license nearing expiry?

- Which products are being used on a trial license?
- Was any announcement posted on the message center recently? If so, what is it?
- Are all Office 365 services functioning optimally? Is any service in a degraded state presently? If so, which one?
- Is any service experiencing a service incident? What type of an incident is it?
- Is any service under maintenance currently?
- Which service is pending provisioning?
- Which service has a high workload? What type of operations are imposing a heavy load on the service? Who is performing such operations?
- Are there any unlicensed users on Office 365? If so, who are they?
- Which users have been denied sign-in rights?
- Which users were deleted recently?

This chapter will elaborate on each layer of Figure 4.1, the tests mapped to it, and the measures it reports.

4.1 The Network Layer

Using the test mapped to this layer, you can determine whether/not the target Microsoft Office 365 component is available over the network, and if so, how quickly it responds to network requests. Flaky/latent network connections to Office 365 thus come to light.

Figure 4.2: The test mapped to the Network layer

4.1.1 SaaS Network Connectivity Test

If your Office 365 users complain that they are unable to access the cloud services, you may want to check the quality of the network link to the Office 365 portal. A flaky or latent network connection can sometimes deny users access to their critical Office 365 services, adversely impacting their overall cloud experience. To avoid this, periodically run the **SaaS Network Connectivity** test, and check the health of the network connection to the Office 365 portal.

This is an external test that emulates a network-level ping to the portal and reports whether/not network connectivity to the portal is available, and if so, how responsive the portal is to network requests. In the process, the test reveals any break or slowness in network connection to the portal.

Target of the test : Office 365

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Office 365 portal being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
Packet Size	The size of packets used for the test (in bytes)
Packet Count	The number of packets to be transmitted during the test
Timeout	How long after transmission should a packet be deemed lost (in seconds)
Packet Interval	Represents the interval (in milliseconds) between successive packet transmissions during the execution of the network test for a specific target.
Targets	By default, this is set to portal.office.com. This test will emulate a network-level ping to this target only.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability

Parameters	Description
	• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Avg network delay	Indicates the average delay between transmission of packet to the portal and receipt of the response to the packet at the source.	Seconds	An increase in network latency could result from misconfiguration of the router(s) along the path, network congestion, retransmissions at the network, etc.
Min network delay	The minimum time between transmission of a packet and receipt of the response back from the portal.	Seconds	A significant increase in the minimum round-trip time is often a sure sign of network congestion.
Packet loss	Indicates the percentage of packets lost during transmission from source to portal and back.	Percent	Packet loss is often caused by network buffer overflows at a network router or by packet corruptions over the network. The detailed diagnosis for this measure provides a listing of routers that are on the path from the external agent to target portal, and the delays on each hop. This information can be used to diagnose the hop(s) that could be causing excessive packet loss/delays.
Network availability	Indicates whether the network connection to the portal is available or not	Percent	A value of 100 indicates that the portal is connected over the network. The value 0 indicates that the portal is not connected. Typically, the value 100 corresponds to a *Packet loss* of 0.

4.2 The O365 Tenant Layer

- Determine the health of each Office 365 service;
- Know which domains are in the monitored Office 365 tenant and determine the status, authentication type, and capabilities of each domain;
- Pinpoint Office 365 products for which licenses have been suspended, and those that may be running out of licenses;
- Capture the count and details of services , which are pending provisioning

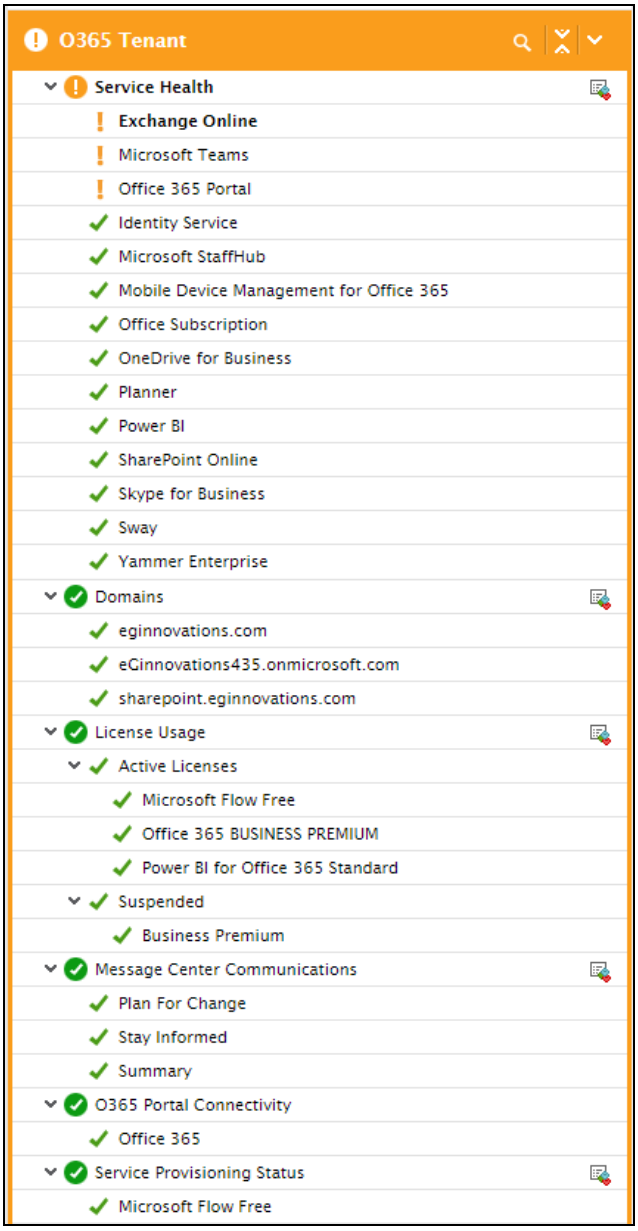


Figure 4.3: The tests mapped to the O365 Tenant layer

4.2.1 Service Health Test

If Office 365 users experience issues with cloud services, then administrators must be able to rapidly and accurately identify the problematic cloud service well-before the users complain. The **Service Health** test helps administrators with this! For each service offered by Office 365, this test reports the status of the service in real-time, thus enabling administrators to instantly spot that service that is experiencing a performance degradation. The test additionally reveals if any service incidents are occurring, and elaborately describes such incidents vide detailed diagnostics. If a service has been stopped as part of a planned maintenance activity, then this test indicates the same by reporting the count of maintenance events each service is currently experiencing.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each service offered by the monitored Office 365 tenant

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test

Parameters	Description
	with the name of this initial domain. Therefore, configure the **O365 DOMAIN** parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the **DOMAIN** text box, specify the name of the Windows domain to which the eG agent host belongs. In the **DOMAIN USER NAME** text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the **DOMAIN PASSWORD** text box and confirm that password by retyping it in the **CONFIRM PASSWORD** text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and **PROXY PORT** parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the **PROXY USER NAME** and **PROXY PASSWORD** text boxes. Confirm that password by retyping it in the **CONFIRM PASSWORD** text box. If the Proxy server does not require authentication, then specify *none* against the **PROXY USER NAME**, **PROXY PASSWORD**, and **CONFIRM PASSWORD** text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *2:1*. This indicates that, by default, detailed measures will be generated at the end of every second test execution cycle during normal operations, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.

Parameters	Description
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Service status	Indicates the current health status of this service		If the service is not experiencing any service incidents currently. , then this measure will report the value Healthy. On the other hand, if even one service incident is occurring on the service, then this measure will report the value Service Degraded. The numeric values that correspond to these measure values are discussed in the table below: **Measure Value** / **Numeric Value**: Healthy / 1; Service degraded / 0 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate current health status of a service. In the graph of this measure however, the same is indicated using the numeric equivalents

Measurement	Description	Measurement Unit	Interpretation
			only.
Service incidents	Indicates the number of service incidents that are currently occurring on this service.	Number	Unplanned service incidents occur when one of the services in the Office 365 suite is unavailable or unresponsive Use the detailed diagnosis of this measure to know the complete details of the service incidents.
Maintenance events	Indicates the number of maintenance events currently occurring on this service.	Number	Planned maintenance is regular Microsoft-initiated service updates to the infrastructure and software applications. Microsoft typically plans maintenance for times when service usage is historically at its lowest based on regional time zones.

The detailed diagnosis of the *Service incidents* measure reveals the complete details of the problems impacting service availability and responsiveness. The details include when the incident occurred, a brief description of the incident, and the tenant and feature affected by the incident. This information greatly aids troubleshooting.

Details of Service Incidents

ID	TITLE	AFFECTED TENANT COUNT	SERVICE NAME	START TIME	END TIME	LAST UPDATED	MESSAGE	FEATURE NAME
Jul 31, 2018 12:24:32								
SP143558	SP143558	9886817	SharePoint Online	6/12/2018 8:26:00 AM	-	7/28/2018 12:28:04 AM	Title: Can`t play videos from Microsoft Stream or Office 365 Video. User Impact: Users are unable to play videos from Microsoft Stream or Office 365 video when using a specific browser configuration. Next update by: Friday, August 10, 2018, at 8:00 PM UTC	SharePoint Features

Figure 4.4: The detailed diagnosis of the Service incidents measure

4.2.2 Service Provisioning Status Test

Typically, a service passes through many stages before it is successfully provisioned to a user. Knowing which service is in which stage of provisioning is essential, as that will reveal to you which services have been in a particular stage for too long a time. You may then want to closely investigate and determine the reason for the delay in provisioning. This is where the **Service Provisioning Status** test helps!

This test auto-discovers all the Office 365 products you have purchased - eg., Office 365 Business Premium, Office 365 Business, Microsoft Flow Free. When you subscribe to a product, you actually

sign up for a specific set of applications and services . The test tracks the provisioning status of each of the services offered by every product you have bought and reports the count of services that are in different stages of provisioning. This way, the test reveals to you if any service that you have subscribed for is pending provisioning. The detailed diagnosis of this test will point you to those specific services that are pending provisioning.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for Office 365 product that you have subscribed for

First-level descriptor: Product name

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account.

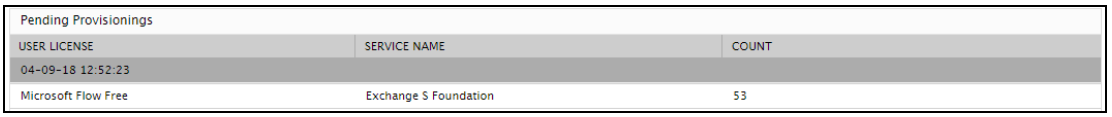
Parameters	Description
	2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the

Parameters	Description
	On option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Pending activations	Indicates the number of services offered by this product that are pending activation.	Number	PendingActivation basically means work load is available for user/tenant but need to backfill/provision.
Pending provisionings	Indicates the number of services offered by this product that are pending provisioning.	Number	PendingProvisioning means that the service will be provisioned when user start using it (just in time provisioning). To know which services are pending provisioning, use the detailed diagnosis of this measure.
Pending inputs	Indicates the number of services offered by this product that are pending inputs.	Number	PendingInput means the license assignment info has not been synced to the corresponding service's data store. Typically, after the provisioning starts, it will go to PendingInput or Success depending on the results.
Success	Indicates the number of services offered by this product that have been successfully provisioned.	Number	Typically, after the provisioning starts, it will go to PendingInput or Success depending on the results. The Success state signifies that the whole provisioning is complete.
Disabled	Indicates the number of services offered by this product that are in a Disabled state presently.	Number	A service is said to be Disabled if the license is not assigned to the user.

The detailed diagnosis of the *Pending provisionings* measure reveals which license is pending provisioning. You may want to check the detailed diagnostics periodically to figure out if any service has been in the Pending Provisioning state for too long. Such services can be subjected to deeper investigation.



Pending Provisionings

USER LICENSE	SERVICE NAME	COUNT
04-09-18 12:52:23		
Microsoft Flow Free	Exchange S Foundation	53

Figure 4.5: The detailed diagnosis of the Pending provisioning measure

4.2.3 License Usage Test

When you buy an Office 365 subscription, you specify the number of licenses that you need, based on how many people you have in your organization. The validity and usage of these licenses needs to be tracked closely, so that any potential license shortage / expiry can be proactively detected and prevented. This is because, without adequate licenses, your users will not be able to use the Office 365 product, or the applications/services they have subscribed for under that product. This is where the License Usage test helps!

This test auto-discovers the Office 365 products you have subscribed to and groups the products on the basis of the license type - active or suspended. Product licenses that have been purchased and are available for assignment to users are grouped under 'Active licenses'. Product licenses that are not available for assignment to users are grouped under 'Suspended licenses'.

For each product under these categories, the test reports the count of licenses purchased, assigned to users, and yet to be assigned to users. On the basis of these usage values, the test also auto-computes and reports the overall license usage percentage, thus proactively alerting to any potential license shortage. The test also reports the count of licenses that will expire shortly, and thus gives you a heads up on impending license expiry.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each Office 365 product that you have subscribed for

First-level descriptor: License type - Active or Suspended

Second-level descriptor: Office 365 product

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not

Parameters	Description
	disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and **PROXY PORT** parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Licensed users	Indicates the number of users who have been assigned this product's license.	Number	This indicates how many licenses of a product have been consumed.
Purchased units	Indicates the number of licenses of this product that have been purchased.	Number	
Warning units	Indicates the number of licenses of this product that you have not renewed, and that will expire after the 30-day grace period.	Number	A high value for this measure is indicative of a potential license shortage, as many licenses may expire at the end of 30 days. You may want to renew the licenses that are nearing expiry to bring this count down and to ensure that sufficient licenses are always available.
Remaining units	Indicates the number of licenses of this product that are yet to be assigned to users.	Number	The value of this measure is the difference between the value of the Purchased units and the Licensed users measure. A high value is ideal for this measure. Compare the value of this measure across products to know which product's licenses have been over-utilized and are nearing exhaustion.
Days to expire	Indicates the number of days within which this product's licenses will expire.	Number	Lower the value of this measure, sooner a product's licenses will expire. If this value is very low, it implies that license will expire very soon. To continue using the product, you will have to renew the license. Use the detailed diagnosis of this measure to know when exactly the license is expected to expire.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>License usage</td><td>Indicates the percent usage of the licenses of this product.</td><td>Percent</td><td>A value close to 100% indicates that users of this product may soon run out of licenses. You may want to plan for purchasing additional licenses of this product in this case.</td></tr>
<tr><td>Is this a trial license?</td><td>Indicates whether/not this product's license is a trial license</td><td></td><td>If a product's license is a trial license, then the value of this measure will be Yes. If not, then this measure will report the value No.

The numeric values that correspond to these measure values are as follows:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>2</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate whether/not a license is a trial license. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
</table>

The detailed diagnosis of the *Days to expire* measure reveals when the license is expected to expire.

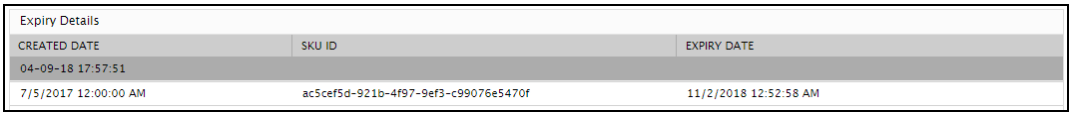


Figure 4.6: The detailed diagnosis of the Days to expire measure

4.2.4 Message Center Communications Test

To keep track of upcoming feature releases or issues, you have to go to Message center in Office 365. That's where official announcements are posted about new and changed features to enable you to take a proactive approach to change management. Each post gives you a high-level overview

of a planned change and how it may affect your users, and links out to more detailed information to help you prepare. It is therefore imperative that you are instantly alerted to every new message that is posted in the Message Center. This is exactly what the **Message Center Communications** test does!

This test reports the count of active communications in the message center. Every time this count gets incremented, the test automatically alerts you to the same, thus quickly turning your attention to new announcements in the message center. Detailed diagnostics provided by this test provide the complete details of these new communications, so that you can figure out what change has been planned and can prepare for it.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 tenant being monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain

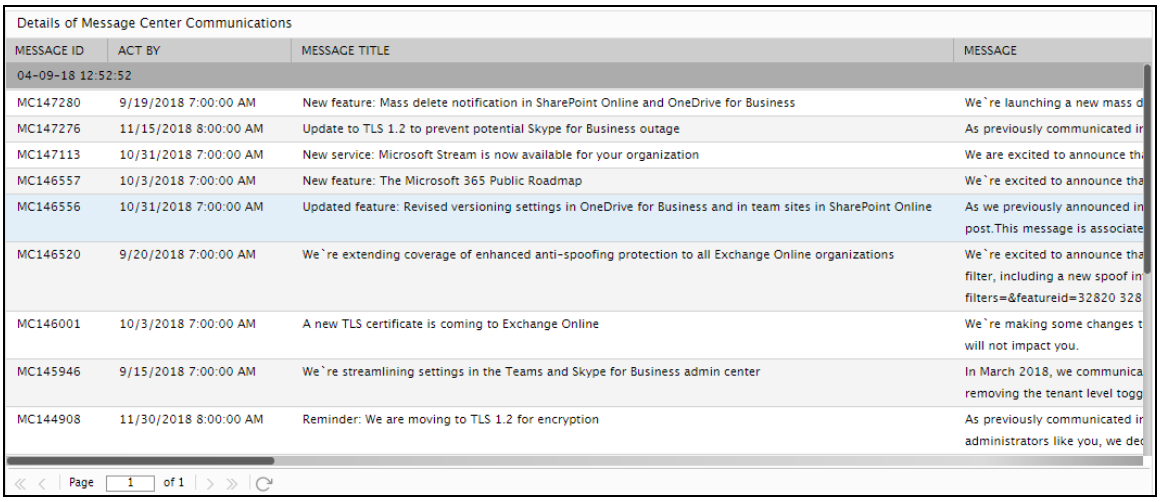
Parameters	Description
	name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and **PROXY PORT** parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.

Parameters	Description
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active message center communications	Indicates the count of communications in the message center that are currently active.	Number	A non-zero value for this measure indicates that a new announcement has been posted in the message center. In such a situation, you can use the detailed diagnosis of this measure to view the complete details of the new communications.

Using the detailed diagnosis of the *Active message center communications* measure, you can quickly understand what new changes have been planned. This knowledge will help you instantly analyze the impact of that change on your business operations and on your users. The detailed diagnosis also reveals if you need to take any action on the new announcement. This way, you can plan your future tasks.


Details of Message Center Communications

MESSAGE ID	ACT BY	MESSAGE TITLE	MESSAGE
04-09-18 12:52:52			
MC147280	9/19/2018 7:00:00 AM	New feature: Mass delete notification in SharePoint Online and OneDrive for Business	We`re launching a new mass d
MC147276	11/15/2018 8:00:00 AM	Update to TLS 1.2 to prevent potential Skype for Business outage	As previously communicated ir
MC147113	10/31/2018 7:00:00 AM	New service: Microsoft Stream is now available for your organization	We are excited to announce tha
MC146557	10/3/2018 7:00:00 AM	New feature: The Microsoft 365 Public Roadmap	We`re excited to announce tha
MC146556	10/31/2018 7:00:00 AM	Updated feature: Revised versioning settings in OneDrive for Business and in team sites in SharePoint Online	As we previously announced in post.This message is associate
MC146520	9/20/2018 7:00:00 AM	We`re extending coverage of enhanced anti-spoofing protection to all Exchange Online organizations	We`re excited to announce tha filter, including a new spoof in filters=&featureid=32820 328
MC146001	10/3/2018 7:00:00 AM	A new TLS certificate is coming to Exchange Online	We`re making some changes t will not impact you.
MC145946	9/15/2018 7:00:00 AM	We`re streamlining settings in the Teams and Skype for Business admin center	In March 2018, we communica removing the tenant level togg
MC144908	11/30/2018 8:00:00 AM	Reminder: We are moving to TLS 1.2 for encryption	As previously communicated ir administrators like you, we dec

Page 1 of 1

Figure 4.7: The detailed diagnosis of the Active message center communications measure

4.2.5 Domains Test

A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as yourbusiness.com or stateuniversity.edu.

Using a custom domain like "rob@contoso.com" with Office 365 can help build credibility and recognition for your brand.

To know what are the different domains in the monitored tenant and to determine the status, capabilities, and configuration of each domain, use the **Domains** test.

This test auto-discovers the domains in the monitored tenant and reports the type, status, capabilities, and verification method configured for each domain. Additionally, the test reveals the initial domain given for use by Office 365 and also its default domain setting. You can also use this test to know which domains are configured with root domains.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each domain in the Office 365 tenant being monitored

First-level descriptor: Domain name

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not

Parameters	Description
	disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and **PROXY PORT** parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Authentication</td><td>Indicates the authentication type of the domain.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Managed</td><td>1</td></tr><tr><td>Federated</td><td>2</td></tr></table>
By default, any domain that is added to Office 365 is set as a Managed Domain by default. Managed domain is the normal domain in Office 365 online (Azure AD), which uses standard authentication. Federated Domain Is a domain that Is enabled for a Single Sign-On and configured to use Microsoft Active Directory Federation (ADFS).
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the authentication type of a domain. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Total capabilities</td><td>Indicates the number of capabilities configured for this domain.</td><td>Number</td><td>A domain can be assigned any of the following capabilities: These can be SharePoint, Email, or OfficeCommunicationsOnline. A domain with SharePoint capability cannot be used for other capabilities.
Use the detailed diagnosis of this measure to know which capabilities have been enabled for the domain.</td></tr>
<tr><td>Is default?</td><td>Indicates whether/not</td><td></td><td>The values that this measure can report</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>this domain has been set as the default domain.</td><td></td><td>and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>True</td><td>1</td></tr><tr><td>False</td><td>2</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate whether/not a domain is set as the default domain. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Is initial?</td><td>Indicates whether/not this domain is the initial domain given for use by Office 365.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>True</td><td>1</td></tr><tr><td>False</td><td>2</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate whether/not a domain is the initial domain that Office 365 has given for use. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Status</td><td>Indicates whether this domain is verified or unverified.</td><td></td><td>Before you set up Office 365 to use a custom domain name, you have to make sure that you own the domain. Otherwise, anyone could use any domain name they wanted to. For example, someone could</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>use your domain name with Office 365 and say they were you! Verification is the process that proves to Office 365 that you own your domain.

If a domain is verified, then the value of this measure will be Verified. For an unverified domain, the value of this measure will be Unverified.

The numeric values that correspond to these measure values are listed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Verified</td><td>1</td></tr><tr><td>Unverified</td><td>2</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate the domain status. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Verification method</td><td>Indicates the verification method using which the domain has been verified.</td><td></td><td>Before you set up Office 365 to use a custom domain name, you have to make sure that you own the domain. Otherwise, anyone could use any domain name they wanted to. For example, someone could use your domain name with Office 365 and say they were you! Verification is the process that proves to Office 365 that you own your domain.

In Office 365 domain verification was traditionally only available through DNS record validation. When adding a domain</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>to Office 365 a domain verification text record or mx record was provided. This record would be added to your external DNS provider and after replication and global availability our queries would detect the presence of the record. When the record was detected the domain would be verified. Other verification methods also exist - eg., email validation.

If this domain was verified using DNS record validation, then the value of this measure will be DnsRecord. On the other hand, if any alternative verification method was used, then this measure will report the value Others.

The numeric values that correspond to these measure values are listed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>DnsRecord</td><td>1</td></tr><tr><td>Others</td><td>2</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate the verification method. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Is root domain?</td><td>Indicates whether/not this domain is a root domain.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>2</td></tr></table> **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate whether/not a domain is the root domain. In the graph of this measure however, the same is indicated using the numeric equivalents only.

The detailed diagnosis of the *Total capabilities* measure reveals the capabilities assigned to the monitored domain.

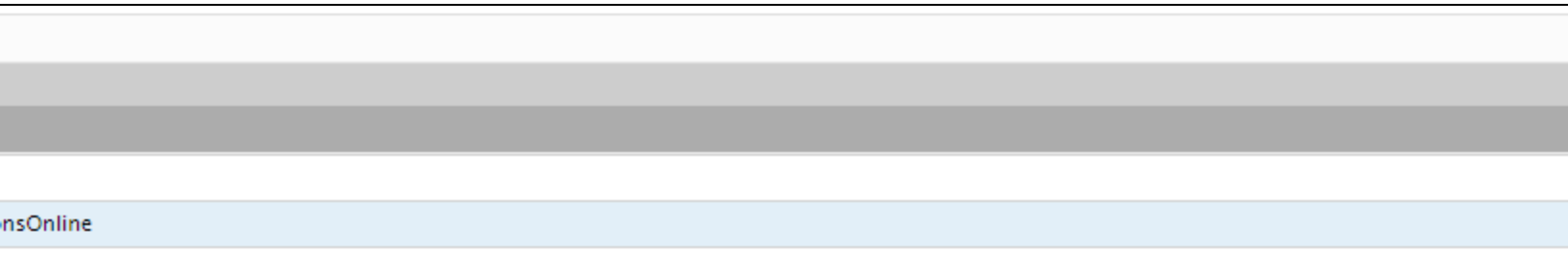


Figure 4.8: The detailed diagnosis of the Total capabilities measure

4.2.6 API Logon Status Test

Where Office 365 is used, users need to be able to quickly and easily login to Office 365, so that they have on-demand access to the wide variety of services it offers - eg., Exchange Online, SharePoint Online, etc. If users are unable to login to Office 365 when in need, their productivity is bound to get badly hit. Frequent logon issues may also force users to question the reliability of this cloud-based service. To ensure 'happy users', administrators should promptly capture logon issues, isolate its root cause, and rapidly initiate measures to address it. This is where the API Logon Status test helps!

This test emulates a user logging into Office 365 via the Office 365 REST API. The emulated logon process is as outlined below:

1. The eG agent uses the Office 365 login credentials configured for the eG tests to login to the REST API.
2. Once Azure AD successfully validates the credentials, the authentication step completes.
3. After successful authentication, the eG agent hits the SharePoint URL of the monitored Office 365 domain to complete the login.

The test reports the success/failure of each step of the emulated logon process. Additionally, the test also measures the time taken to complete every step. This way, the test enables administrators to proactively detect problems in a typical user logon to Office 365 and also pinpoints the exact step of the logon process where the bottleneck lies - in authentication? or when the domain-specific URL is hit?

This test is disabled by default. To enable the test, follow the Agents -> Tests -> Enable/Disable in the Admin tile menu, select *Microsoft Office 365* as the **Component type**, select *API Logon Status* test from the **DISABLED TESTS** list, and click the << button to enable it.

Note:

Before enabling this test, make sure that the SharePoint Online Management Shell is installed and is running on the eG agent host. To download the SharePoint Online Management Shell installable, use the following link: https://www.microsoft.com/en-in/download/details.aspx?id=35588

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes

Parameters	Description
	using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and **PROXY PORT** parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify none against the Proxy User Name, Proxy

Parameters	Description
	Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Authentication status	Indicates whether/not the login credentials were validated by Azure AD.		If the login credentials are successfully validated by Azure AD, then this measure will report the value *Success*. The value *Failed* is reported if authentication fails. The numeric values that correspond to these measure values are as follows: **Measure Value** / **Numeric Value** Success / 1 Failed / 0 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the authentication status. In the graph of this measure however, the same is indicated using the numeric equivalents only.
Authentication time	Indicates the time taken for the login credentials to be validated.	Seconds	An abnormally high value is a cause cor concern, as it indicates that authentication is slow. If you suspect issues in the API logon process, then compare the value of this measure with that of the Login time measure to know where exactly the logon process is bottlenecked - is it during authentication - i.e., when login

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>credentials are validated by Azure AD? or is it at login - i.e., when the domain-specific URL is hit?</td></tr>
<tr><td>Login status</td><td>Indicates whether/not the SharePoint URL that this test hit returned a valid response page.</td><td></td><td>If this measure reports the value Success, it means that the test was able to connect to the SharePoint URL of the domain, successfully. On the other hand, if this measure reports the value Failed, it implies that the test could not connect to the SharePoint URL of the domain.

The numeric values that correspond to these measure values are as follows:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Success</td><td>1</td></tr><tr><td>Failed</td><td>0</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate the login status. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Login time</td><td>Indicates the time taken to connect to the SharePoint URL of the monitored domain.</td><td>Seconds</td><td>An abnormally high value is a cause cor concern, as it indicates that it is taking an unusually long time to connect to the SharePoint URL.

If the Total login time reports an abnormally high value, then compare the value of this measure with that of the Authentication time measure to know where exactly the logon process is bottlenecked - is it at authentication - i.e., when login credentials are</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			validated by Azure AD? or is it at login - i.e., when the domain-specific URL is hit?
Total login time	Indicates the total time taken to complete the API logon process.	Seconds	A very high value for this measure indicates a bottleneck in the API logon process. Under such circumstances, compare the value of the Authentication time and Login time measures to know what is delaying API logon - authentication? or connecting to the SharePoint URL?

4.3 The O365 Users and Groups Layer

To audit distribution groups, dynamic distribution groups, Office 365 groups, and security groups, use the tests mapped to this layer. Using the Users test associated with this layer, you can also identify unlicensed and deleted users, and those who do not have sign-in rights.

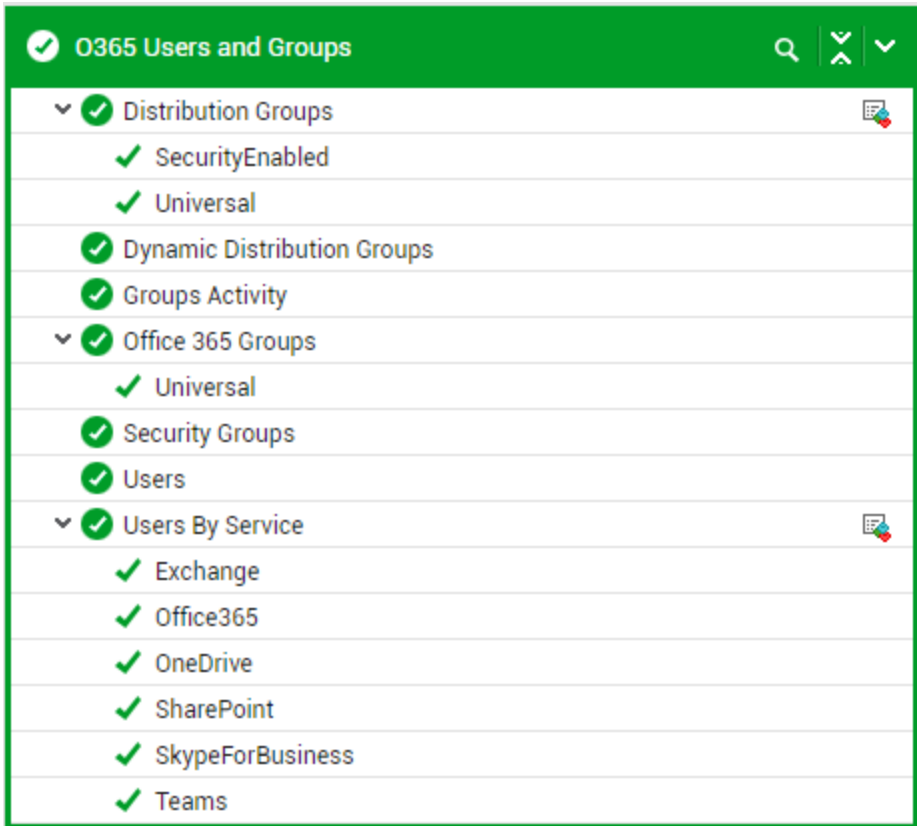


Figure 4.9: The tests mapped to the O365 Users and Groups layer

4.3.1 Distribution Groups

A Distribution Group (DG) is a group that contains two or more people, has an email address and appears in the Global Address List (GAL) for a company. Internal and External users can send emails to the DG and it will go to all members of the DG.

Typically, a Universal Distribution Group is a distribution group that is created only to serve as an email distribution group in Exchange. A security-enabled distribution group (or security group) on the other hand is created so that you can assign permissions to a large group of users instead of assigning permissions to individual users one at a time.

With the help of the **Distribution Groups** test, administrators can easily and efficiently audit distribution groups. For each DG type (Universal and SecurityEnabled), this test reports the count and details of new, deleted, and modified groups of that type. Additionally, empty groups and orphaned groups are also brought to the attention of administrators. This way, administrators can identify groups that may have to be assigned new owners and groups that are still awaiting members.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each DG type in the Office 365 tenant being monitored

First-level descriptor: DG type - this can be Universal or SecurityEnabled

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.

Parameters	Description
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these

Parameters	Description
	parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *6:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Modified groups	Indicates the number of groups of this type that were modified during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which groups were modified and when.
Newly created groups	Indicates the number of groups of this type that were newly created during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which groups were created, when.
Soft deleted groups	Indicates the number of groups of this type that have been soft-deleted.	Number	If you have deleted an Office 365 group, by default it's retained for 30 days. This 30-day period is called "soft-delete" because you can still restore the group. After 30 days, the group and associated content is

Measurement	Description	Measurement Unit	Interpretation
			permanently deleted and cannot be restored. During the "soft-delete" period if a user tries to access the site they will get a 403 forbidden message. After this period if the user tries to access the site they will get a 404 not found message. Use the detailed diagnosis of this measure to know which groups were soft-deleted and when.
Total groups	Indicates the total number of groups of this type.	Number	
Orphaned groups	Indicates the number of groups of this type that are orphaned/ownerless.	Number	If a group owner leaves your company the group could find itself without an owner. Such a group is called an Orphaned group. The content in the group is unaffected by this - the content belongs to the group and isn't tied to the owner's account. But not having a group owner means there's nobody with permissions to manage the group. Use the detailed diagnosis of this measure to know which groups are orphaned / ownerless.
Empty groups	Indicates the number of groups of this type that are empty currently.	Number	Use the detailed diagnosis of this measure to identify the empty groups. If any group is found to be empty for too long a time, you may want to delete such a group.

The detailed diagnosis of the *Modified groups* measure reveals the names of the groups that were modified recently, when such groups were created, and when the modification occurred. This enables administrators easily track changes to groups. Also, the current status of each group is revealed, so that administrators can accurately pinpoint inactive groups.

Details of Modified groups

DISPLAY NAME	EMAIL	ALIAS NAME	STATUS	GROUP MEMBER COUNT	CHANGED
04-09-18 12:52:29					
Bridgewater Associates - eG PoC	bridgewaterassociates-egpoc@eginnovations.com	bridgewaterassociates-egpoc	Active	4	9/2/2018 4:18:21 AM
Excellus - eG PoC	Excellus-eGPoC@eginnovations.com	Excellus-eGPoC	Active	5	9/2/2018 5:47:05 AM

Figure 4.10: The detailed diagnosis of the Modified groups measure reported by the Distribution Groups test

The detailed diagnosis of the *Empty groups* measure reveals the names of the empty groups, when such groups were created, whether/not the group configuration changed recently and if so when, and the current status of the groups. If an empty group is found to be inactive as well, you may want to delete the group.

Details of Empty groups

DISPLAY NAME	EMAIL	ALIAS NAME	STATUS	CHANGED	CREATED
04-09-18 12:52:29					
Service Health Widget	ServiceHealthWidget@eginnovations.com	ServiceHealthWidget	Active	3/7/2018 2:05:47 PM	11/10/2017 12:55:25 AM
Customer Inventory	CustomerInventory@eginnovations.com	CustomerInventory	Active	4/19/2018 6:13:18 PM	11/10/2017 12:55:28 AM

Figure 4.11: The detailed diagnosis of the Empty groups measure reported by the Distribution Groups test

4.3.2 Dynamic Distribution Groups Test

A dynamic distribution group is created dynamically when an email is being sent to the particular group based on some pre-defined rules or conditions. When configuring such a group, you need to choose the type of recipients who need to be automatically added as members of the group, and also define the other rules that govern membership. The group will be dynamically created with members who are of the recipient type chosen and who fulfill the defined rules .

Since these groups are auto-created, administrators may, on a daily basis, have to manually check whether any new dynamic distribution group has been created or not. Likewise, since the group configuration may also change dynamically, administrators will also need to keep reviewing the configuration periodically to capture modifications. For similar reasons, empty groups may also go undetected by administrators. To enable administrators to easily and efficiently manage dynamic distribution groups, it will be good practice to periodically run the **Dynamic Distribution Groups** test.

This test promptly alerts administrators when a new dynamic distribution group is created, modified, or deleted. Furthermore, the test also notifies administrators if any dynamic distribution group is found to be empty or orphaned. To know which dynamic distribution groups were newly created, modified, deleted, orphaned, or empty, you can use the detailed statistics reported by this test.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not

Parameters	Description
	disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Modified groups	Indicates the number of dynamic distribution groups that were modified during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which groups were modified and when.
Newly created groups	Indicates the number of groups that were newly created during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which groups were created, when.
Soft deleted groups	Indicates the number of groups that have been soft-deleted.	Number	If you have deleted an Office 365 group, by default it's retained for 30 days. This 30-day period is called "soft-delete" because you can still restore the group. After 30 days, the group and associated content is permanently deleted and cannot be restored. During the "soft-delete" period if a user tries to access the site they will get a 403 forbidden message. After this period if the user tries to access the site they will get a 404 not found message. Use the detailed diagnosis of this measure to know which groups were soft-deleted and when.
Total groups	Indicates the total number of dynamic distribution groups.	Number	
Orphaned groups	Indicates the number of groups that are orphaned/ownerless.	Number	If a group owner leaves your company the group could find itself without an owner. Such a group is called an Orphaned group. The content in the group is unaffected by this - the content belongs to the group and isn't

Measurement	Description	Measurement Unit	Interpretation
			tied to the owner's account. But not having a group owner means there's nobody with permissions to manage the group. Use the detailed diagnosis of this measure to know which groups are orphaned / ownerless.
Empty groups	Indicates the number of groups that are empty currently.	Number	Use the detailed diagnosis of this measure to identify the empty groups. If any group is found to be empty for too long a time, you may want to delete such a group.

The detailed diagnosis of the *Modified groups* measure reveals the names of the groups that were modified recently, when such groups were created, and when the modification occurred. This enables administrators easily track changes to groups. Also, the current status of each group is revealed, so that administrators can accurately pinpoint inactive groups.

Details of Modified groups

DISPLAY NAME	EMAIL	ALIAS NAME	STATUS	GROUP MEMBER COUNT	CHANGED
04-09-18 12:52:29					
Bridgewater Associates - eG PoC	bridgewaterassociates-egpoc@eginnovations.com	bridgewaterassociates-egpoc	Active	4	9/2/2018 4:18:21 AM
Excellus - eG PoC	Excellus-eGPoC@eginnovations.com	Excellus-eGPoC	Active	5	9/2/2018 5:47:05 AM

Figure 4.12: The detailed diagnosis of the Modified groups measure reported by the Dynamic Distribution Groups test

The detailed diagnosis of the *Empty groups* measure reveals the names of the empty groups, when such groups were created, whether/not the group configuration changed recently and if so when, and the current status of the groups. If an empty group is found to be inactive as well, you may want to delete the group.

Details of Empty groups

DISPLAY NAME	EMAIL	ALIAS NAME	STATUS	CHANGED	CREATED
04-09-18 12:52:29					
Service Health Widget	ServiceHealthWidget@eginnovations.com	ServiceHealthWidget	Active	3/7/2018 2:05:47 PM	11/10/2017 12:55:25 AM
Customer Inventory	CustomerInventory@eginnovations.com	CustomerInventory	Active	4/19/2018 6:13:18 PM	11/10/2017 12:55:28 AM

Figure 4.13: The detailed diagnosis of the Empty groups measure reported by the Dynamic Distribution Groups test

4.3.3 Office 365 Groups Test

An Office 365 Group is a way to centralize membership for multiple Microsoft products in one place, and apply policies at the project or team level instead of each product. Using Office 365 groups, you can create a shared space to communicate, collaborate, and schedule events with colleagues on a shared task, project, or resource.

To instantly capture newly created groups, track changes to groups, and be alerted to deleted, orphaned, and empty groups, use the Office 365 Groups test. This test auto-discovers the different types of Office 365 groups in the monitored tenant. For each type, the test reports the count of new, modified, soft-deleted, orphaned, and empty groups of that type. Detailed diagnostics of this test reveals which groups were created newly, modified recently, soft-deleted, orphaned, or empty. Moreover, the number of private and public groups of each type is reported along with detailed metrics revealing the names of the private and public groups. This information thus enables administrators to easily and efficiently manage Office 365 groups.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each type of Office 365 group in the tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that

Parameters	Description
	appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and **PROXY PORT** parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.

Parameters	Description
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Modified groups	Indicates the number of groups of this type that were modified during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which groups were modified and when.
Newly created groups	Indicates the number of groups of this type that were newly created during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which groups were created, when.
Soft deleted groups	Indicates the number of groups of this type that have been soft-deleted.	Number	If you have deleted an Office 365 group, by default it's retained for 30 days. This 30-day period is called "soft-delete" because you can still restore the group. After 30 days, the group and associated content is permanently deleted and cannot be restored.

Measurement	Description	Measurement Unit	Interpretation
			During the "soft-delete" period if a user tries to access the site they will get a 403 forbidden message. After this period if the user tries to access the site they will get a 404 not found message. Use the detailed diagnosis of this measure to know which groups were soft-deleted and when.
Total groups	Indicates the total number of this type.	Number	
Public groups	Indicates the number of public groups of this type.	Number	Anyone can see the content and conversations of a Public group. What is more, anyone can join such a group, without approval from a group owner
Private groups	Indicates the number of private groups of this type.	Number	In case of private groups, only members can see the content of those groups and joining such a group requires approval from a group owner.
Orphaned groups	Indicates the number of groups of this type that are orphaned/ownerless.	Number	If a group owner leaves your company the group could find itself without an owner. Such a group is called an Orphaned group. The content in the group is unaffected by this - the content belongs to the group and isn't tied to the owner's account. But not having a group owner means there's nobody with permissions to manage the group. Use the detailed diagnosis of this measure to know which groups are orphaned / ownerless.
Empty groups	Indicates the number of groups of this type that are empty currently.	Number	Use the detailed diagnosis of this measure to identify the empty groups. If any group is found to be empty for too long a time, you may want to

Measurement	Description	Measurement Unit	Interpretation
			delete such a group.
Groups with external members	Indicates the number of groups of this type with external members.	Number	By default, owners and/or members of a group can invite external guests to join the group. An external guest is someone whose account and credentials are controlled outside of the Office 365 tenant. Such external guests/members cannot browse groups; instead, they can only access groups via the invitation mail. By default, these external guests can access files and OneNote within the group of which they are members. Use the detailed diagnosis of this measure to know which groups have external guests.

The detailed diagnosis of the *Modified groups* measure reveals the names of the groups that were modified recently, when such groups were created, and when the modification occurred. This enables administrators easily track changes to groups. Also, the current status of each group is revealed, so that administrators can accurately pinpoint inactive groups.

Details of Modified groups

DISPLAY NAME	EMAIL	ALIAS NAME	STATUS	GROUP MEMBER COUNT	CHANGED
04-09-18 12:52:29					
Bridgewater Associates - eG PoC	bridgewaterassociates-egpoc@eginnovations.com	bridgewaterassociates-egpoc	Active	4	9/2/2018 4:18:21 AM
Excellus - eG PoC	Excellus-eGPoC@eginnovations.com	Excellus-eGPoC	Active	5	9/2/2018 5:47:05 AM

Figure 4.14: The detailed diagnosis of the Modified groups measure reported by the Office 365 Groups test

The detailed diagnosis of the *Empty groups* measure reveals the names of the empty groups, when such groups were created, whether/not the group configuration changed recently and if so when, and the current status of the groups. If an empty group is found to be inactive as well, you may want to delete the group.

Details of Empty groups

DISPLAY NAME	EMAIL	ALIAS NAME	STATUS	CHANGED	CREATED
04-09-18 12:52:29					
Service Health Widget	ServiceHealthWidget@eginnovations.com	ServiceHealthWidget	Active	3/7/2018 2:05:47 PM	11/10/2017 12:55:25 AM
Customer Inventory	CustomerInventory@eginnovations.com	CustomerInventory	Active	4/19/2018 6:13:18 PM	11/10/2017 12:55:28 AM

Figure 4.15: The detailed diagnosis of the Empty groups measure reported by the Office 365 Groups test

4.3.4 Security Groups Test

A security-enabled distribution group (or security group) is created so that you can assign permissions to a large group of users instead of assigning permissions to individual users one at a time.

Use the **Security Groups** test to periodically take stock of security groups that are created newly. With the help of this test, soft-deleted, orphaned, and empty groups can also be identified. This way, you can easily and efficiently maintain the inventory of security groups.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following:

Parameters	Description
	1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *6:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be

Parameters	Description
	configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Newly created groups	Indicates the number of groups that were newly created during the last measurement period.	Number	Use the detailed diagnosis of this measure o know which groups were created.
Soft deleted groups	Indicates the number of groups that have been soft-deleted.	Number	If you have deleted an Office 365 group, by default it's retained for 30 days. This 30-day period is called "soft-delete" because you can still restore the group. After 30 days, the group and associated content is permanently deleted and cannot be restored. During the "soft-delete" period if a user tries to access the site they will get a 403 forbidden message. After this period if the user tries to access the site they will get a 404 not found message. Use the detailed diagnosis of this measure to know which groups were soft-deleted.
Total groups	Indicates the total number of security groups.	Number	

Measurement	Description	Measurement Unit	Interpretation
Orphaned groups	Indicates the number of groups that are orphaned/ownerless.	Number	If a group owner leaves your company the group could find itself without an owner. Such a group is called an Orphaned group. The content in the group is unaffected by this - the content belongs to the group and isn't tied to the owner's account. But not having a group owner means there's nobody with permissions to manage the group. Use the detailed diagnosis of this measure to know which groups are orphaned / ownerless.
Empty groups	Indicates the number of groups that are empty currently.	Number	Use the detailed diagnosis of this measure to identify the empty groups.

The detailed diagnosis of the *Orphaned groups* measure reveals the names of the security groups that do not have an owner. The number of members in each group is also reported as part of the detailed metrics.

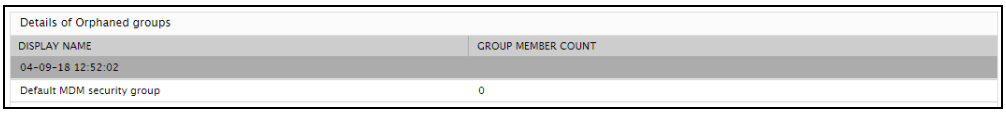


Figure 4.16: The detailed diagnosis of the Orphaned groups measure reported by the Security Groups test

The detailed diagnosis of the *Empty groups* measure reveals the names of the empty group.

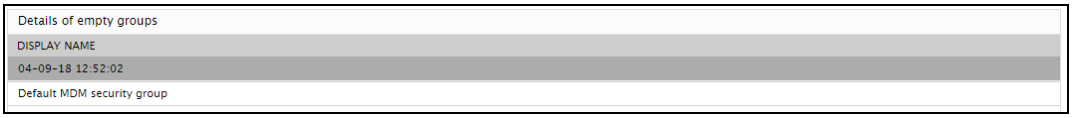


Figure 4.17: The detailed diagnosis of the Empty groups measure reported by the Security Groups test

4.3.5 Groups Activity Test

An Office 365 Group is a way to centralize membership for multiple Microsoft products in one place, and apply policies at the project or team level instead of each product. Using Office 365 groups, you

can create a shared space to communicate, collaborate, and schedule events with colleagues on a shared task, project, or resource.

Typically, members of a group communicate with each other over emails and using social networking platforms such as yammer. To disseminate information and collaborate on a project, they use SharePoint files. More often than not, administrators may want to track the level of communication / collaboration activity across groups, so they can determine whether/not adequate shared resources (eg., mailbox storage, site storage etc.) are available to the groups to handle the load. This is where the Groups Activity test helps!

This test monitors the yammer, email, and file activity across groups, and reports how much load these activities impose on mailbox storage and SharePoint site storage. This way, administrators can rapidly figure out if groups require additional storage space to handle the load. If the groups are utilizing mailbox and/or site storage abnormally, you can use the detailed diagnosis reported by the test to identify the top storage consumers - i.e., the groups that are using up a lot of storage space owing to high level of email/file activity.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that

Parameters	Description
	appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.

Parameters	Description
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Yammer liked messages	Indicates the number of messages on yammer that were liked by group members.	Number	
Yammer posted messages	Indicates the number of messages posted to yammer by group members.	Number	
Yammer read messages	Indicates the number of messages posted to yammer that were read by group members.	Number	
Mailbox storage used by groups	Indicates the amount of mailbox storage space used by groups.	GB	A consistent increase in the value of this measure is indicative of a steady increase in mailbox storage usage,

Measurement	Description	Measurement Unit	Interpretation
			probably caused by excessive mail activity across groups. In the event that the value of this measure is abnormally high, use the detailed diagnosis of this measure to identify which groups are draining mailbox storage.
Mailbox items in group	Indicates the total number of items in the mailboxes of group members.	Number	A consistent increase in the value of this measure is indicative of a steady increase in email activity in the groups. If the value of this measure is abnormally high, use the detailed diagnosis of this measure to identify which groups with many items in their mailbox, and who owns these groups.
Mails received	Indicates the number of emails received across groups.	Number	Use the detailed diagnosis of this measure to identify which groups received the maximum number of mails.
SharePoint files	Indicates the number of SharePoint files used by group members.	Number	Use the detailed diagnosis of this measure to identify which groups use the maximum number of SharePoint files.
SharePoint site storage usedU	Indicates the total amount of site storage space used by groups.	GB	A consistent increase in the value of this measure is indicative of a steady increase in site storage usage, probably caused by by the creation of many SharePoint files or a few/more large-sized SharePoint files by group members. In the event that the value of this measure is abnormally high, use the detailed diagnosis of this measure to identify which groups are hogging site storage.

Measurement	Description	Measurement Unit	Interpretation
SharePoint active files	Indicates the total number of SharePoint files actively used by group members.	Number	Use the detailed diagnosis of this measure to know which groups are actively using the maximum number of SharePoint files.

The detailed diagnosis of the *Mailbox storage used* by groups measure reveals the top-10 groups consuming the maximum mailbox storage space. This will point administrators to those groups that are contributing to the excessive usage of mailbox storage.

Top 10 Groups by Mailbox Storage

GROUP DISPLAY NAME	OWNER DISPLAY NAME	LAST ACTIVITY DATE	GROUP TYPE	MAILBOX STORAGE USED (MB)
Mar 17, 2020 15:01:38				
Postsales-eu	raja@eginnovations.com	2020-03-14	Private	2584.65
KrishTeam	george.barbosa@eginnovations.com	2020-03-13	Private	1500.85
Test	maheson.ramasamy@eginnovations.com	2020-03-13	Private	1417.77
PreSales-eu	raja@eginnovations.com	2020-03-13	Private	419.5
kbz	srinivas@eginnovations.com	2020-03-13	Private	210.73
CreativeServices	-	2020-03-13	Private	184.71
Travelers-eGPoC	Kirk.Simon@eginnovations.com	2020-03-06	Private	104.78
EY-eGDeployment	george.barbosa@eginnovations.com	2020-03-12	Private	88.53
SterlingTS-eGPOC	deepak.pr@eginnovations.com	2020-03-06	Private	81.08
StateStreet-eGPoC	george.barbosa@eginnovations.com	2020-03-05	Private	70.32

Figure 4.18: The detailed diagnosis of the Mailbox storage used by groups measure

The detailed diagnosis of the *Mailbox items in groups* measure reveals the top-10 groups, in terms of the count of items in their mailbox. With the help of these detailed metrics, administrators can quickly identify which groups are draining mailbox storage by adding many items to it.

Top 10 Groups by Mailbox Items

GROUP DISPLAY NAME	OWNER DISPLAY NAME	LAST ACTIVITY DATE	GROUP TYPE	MAILBOX ITEMS (NUMBER)
Mar 17, 2020 15:01:38				
Test	maheson.ramasamy@eginnovations.com	2020-03-13	Private	22971
Postsales-eu	raja@eginnovations.com	2020-03-14	Private	10093
KrishTeam	george.barbosa@eginnovations.com	2020-03-13	Private	9419
kbz	srinivas@eginnovations.com	2020-03-13	Private	2644
PreSales-eu	raja@eginnovations.com	2020-03-13	Private	2253
egHelpdesk	karthikg@eginnovations.com	2020-03-13	Private	1345
Training&HowToVideos	John.Worthington@eginnovations.com	2020-03-12	Public	997
EY-eGDeployment	george.barbosa@eginnovations.com	2020-03-12	Private	884
KindSnacks-eGPoC	Kirk.Simon@eginnovations.com	2020-02-10	Private	818
L1Support	Karthik.S@eginnovations.com	2020-03-04	Private	774

Figure 4.19: The detailed diagnosis of the Mailbox items in groups measure

The detailed diagnosis of the *Mails received* measure reveals the top-10 groups, in terms of mails received. If mailbox storage usage is unusually high across groups, then you can use these detailed

metrics to identify which group received and stored the maximum number of mails in the mailbox storage, thereby causing excessive consumption of storage space.

Top 10 Groups by Number of Mails Received

GROUP DISPLAY NAME	OWNER DISPLAY NAME	LAST ACTIVITY DATE	GROUP TYPE	EMAILS RECEIVED (NUMBER)
Mar 17, 2020 15:01:38				
Postsales-eu	raja@eginnovations.com	2020-03-14	Private	159
egHelpdesk	karthikg@eginnovations.com	2020-03-13	Private	28
CreativeServices	-	2020-03-13	Private	23
PreSales-eu	raja@eginnovations.com	2020-03-13	Private	21
KrishTeam	george.barbosa@eginnovations.com	2020-03-13	Private	20
saassupport	Randhir.M@eginnovations.com	2020-03-14	Private	18
anzcloud	sean@eginnovations.com	2020-03-14	Private	7
CloudSupportServices	krishk@eginnovations.com	2020-03-13	Private	6
BBVA-eGPoC	george.barbosa@eginnovations.com	2020-03-13	Private	6
Humana-eGPOC	Kirk.Simon@eginnovations.com	2020-03-12	Private	5

Figure 4.20: The detailed diagnosis of the Mails received measure

The detailed diagnosis of the *SharePoint files* measure lists the top-10 groups, with the maximum number of SharePoint files. If there is abnormal usage of site storage, then you can use these detailed metrics to identify the group that could be contributing to this by storing many SharePoint files.

Top 10 Groups by Number of SharePoint Files

GROUP DISPLAY NAME	OWNER DISPLAY NAME	LAST ACTIVITY DATE	GROUP TYPE	SHAREPOINT FILES (NUMBER)
Mar 17, 2020 15:01:38				
Product-BI-Tracking	chitra@eginnovations.com	2020-03-13	Private	5501
eGJavaAPMTeam	ramesh@eginnovations.com	2020-03-13	Private	774
eG_Cloud_Providence	karthikg@eginnovations.com	2020-03-11	Private	636
KrishTeam	george.barbosa@eginnovations.com	2020-03-13	Private	465
EY-eGDeployment	george.barbosa@eginnovations.com	2020-03-12	Private	457
Postsales-eu	raja@eginnovations.com	2020-03-14	Private	258
eG_Cloud_eGcs11	karthikg@eginnovations.com	2020-03-14	Private	183
eG_Cloud_eGcs21	karthikg@eginnovations.com	2020-03-14	Private	161
eG_Cloud_EGONTP	karthikg@eginnovations.com	2020-03-14	Private	157
eG_Cloud_APAC	karthikg@eginnovations.com	2020-03-14	Private	156

Figure 4.21: The detailed diagnosis of the SharePoint files measure

The detailed diagnosis of the *SharePoint site storage used* measure lists the top-10 groups consuming the maximum space in site storage. If groups appear to be using site storage excessively, then these detailed statistics will point you to the precise group that is responsible for the anomaly.

Top 10 Groups by SharePoint Storage Size

GROUP DISPLAY NAME	OWNER DISPLAY NAME	LAST ACTIVITY DATE	GROUP TYPE	SHAREPOINT SITE STORAGE USED (MB)
Mar 17, 2020 15:01:38				
eGJavaAPMTeam	ramesh@eginnovations.com	2020-03-13	Private	43587.58
KrishTeam	george.barbosa@eginnovations.com	2020-03-13	Private	34274.06
EY-eGDeployment	george.barbosa@eginnovations.com	2020-03-12	Private	26018.18
MSK-eGCloudEval	Kirk.Simon@eginnovations.com	2020-03-02	Private	14170.99
Training&HowToVideos	John.Worthington@eginnovations.com	2020-03-12	Public	4249.27
USWebinars	John.Worthington@eginnovations.com	2020-03-13	Public	4184.62
StateStreet-eGPoC	george.barbosa@eginnovations.com	2020-03-05	Private	3955.48
eGIndiaSupport	network@eGinnovations435.onmicrosoft.com	2020-03-12	Private	3045.28
AJGallagher-eGPoC	george.barbosa@eginnovations.com	2020-03-06	Private	2797.39
BASF-eGPoC	Kirk.Simon@eginnovations.com	2020-03-02	Private	2695.9

Figure 4.22: The detailed diagnosis of the SharePoint site storage used

The detailed diagnosis of the *SharePoint active files* measure lists the top-10 groups, in terms of the number of active SharePoint files. With the help of these detailed metrics, you can identify which group is responsible for abnormal storage usage.

Top 10 Groups by Number of SharePoint Files

GROUP DISPLAY NAME	OWNER DISPLAY NAME	LAST ACTIVITY DATE	GROUP TYPE	SHAREPOINT ACTIVE FILES (NUMBER)
Mar 17, 2020 15:01:38				
Marketing	Peter.Claridge@eginnovations.com	2020-03-14	Private	40
eGJavaAPMTeam	ramesh@eginnovations.com	2020-03-13	Private	19
KrishTeam	george.barbosa@eginnovations.com	2020-03-13	Private	16
Postsales-eu	raja@eginnovations.com	2020-03-14	Private	10
EY-eGDeployment	george.barbosa@eginnovations.com	2020-03-12	Private	10
Product-BI-Tracking	chitra@eginnovations.com	2020-03-13	Private	9
CommunityCarePhysicians,P.C.	John.Worthington@eginnovations.com	2020-03-12	Public	5
BBVA-eGPoC	george.barbosa@eginnovations.com	2020-03-13	Private	5
eGICATechs	Hydro.Soh@eginnovations.com	2020-03-14	Private	4
DCBBANK	Jayamurugan.S@eginnovations.com	2020-03-13	Public	3

Figure 4.23: The detailed diagnosis of the SharePoint active files measure

4.3.6 Users by Service Test

To know the most popular services offered by Office 365, you need to track the usage of each service over time. The Users by Service test makes this possible!

For each Office 365 service, this test reports the count of active and inactive users. By comparing the count of active users across services, you can identify which service is most popular.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each service offered by the Office 365 tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the

Parameters	Description
	Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active users	Indicates the number of users actively using this service.	Number	Compare the value of this measure across services to know which service is popular amongst users.
Inactive users	Indicates the number of inactive users of this service.	Number	

4.3.7 Users Test

Office 365 user accounts and Office 365 licenses do not need to have a one-to-one correspondence: it is possible to have Office 365 users who do not have an Office 365 license, and it is possible to have Office 365 licenses that have not been assigned to a user. Likewise, you can deny a licensed user sign-in rights, and can even delete a user without deleting his/her license. With so many different user configurations possible, its only natural that administrators find it hard to track the license assignment and access settings of each user. This is where the **Users** test helps. With the help of this test, administrators can quickly determine the count of unlicensed users, deleted users, and those who do not have sign-in rights. Detailed diagnostics reported by this test reveal the names of such users.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the monitored Office 365 tenant

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said

Parameters	Description
	privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that

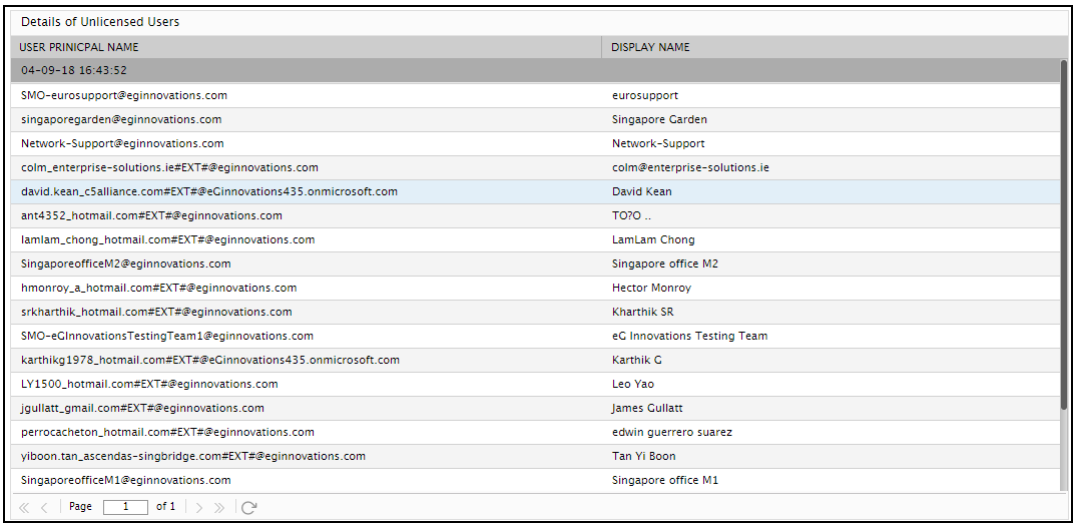
Parameters	Description
	password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Unlicensed users	Indicates the number of users who have not been assigned a license.	Number	When you create a new Office 365 user account, you don't have to assign that user a license: the new user will have a valid account, but he or she won't be able to sign in to Office 365. To know which users have not been assigned a license, use the detailed diagnosis of this measure.
Deleted users	Indicates the number of	Number	Use the detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
	users who have been removed.		measure to know which user accounts have been deleted. When deleting a user, you can choose to retain the user license or even remove the license along with the user account. The latter is cost-effective as you do not have to continue paying for an unused license. Alternatively, you can even assign the deleted license to another user, thus leveraging your existing investments in Office 365.
Users with non-expiring passwords	Indicates the number of users whose password has been set to never expire.	Number	Use the detailed diagnosis to know which users have been configured with passwords that never expire.
Users with password nearing expiry	Indicates the number of users whose password is about to expire.	Number	This measure will be reported only if the test is run by the administrator who has *Global Administrative* privileges.
Sign-in denied users	Indicates the number of users whose sign-in status has been blocked.	Number	To know which users have been denied sign-in rights, use the detailed diagnosis of this measure.
Sign-in allowed users	Indicates the number of users whose sign-in status has been blocked.	Number	

The detailed diagnosis of the *Unlicensed users* measure reveals the principal name and display name of each of the unlicensed users. This way, you can quickly identify which users have yet to be assigned a license.



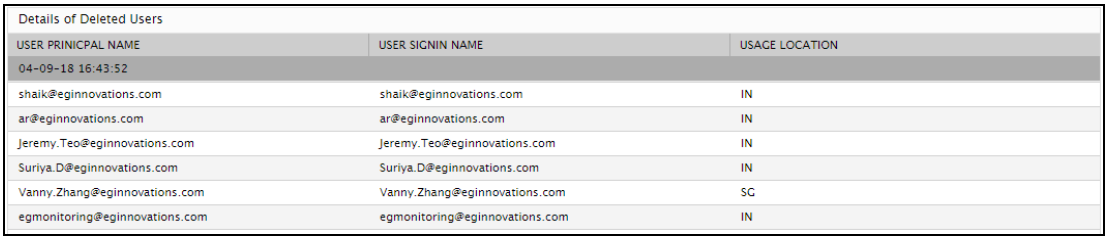
Details of Unlicensed Users

USER PRINICPAL NAME	DISPLAY NAME
04-09-18 16:43:52	
SMO-eurosupport@eginnovations.com	eurosupport
singaporegarden@eginnovations.com	Singapore Carden
Network-Support@eginnovations.com	Network-Support
colm_enterprise-solutions.ie#EXT#@eginnovations.com	colm@enterprise-solutions.ie
david.kean_c5alliance.com#EXT#@eGinnovations435.onmicrosoft.com	David Kean
ant4352_hotmail.com#EXT#@eginnovations.com	TO?O ..
lamlam_chong_hotmail.com#EXT#@eginnovations.com	LamLam Chong
SingaporeofficeM2@eginnovations.com	Singapore office M2
hmonroy_a_hotmail.com#EXT#@eginnovations.com	Hector Monroy
srkharthik_hotmail.com#EXT#@eginnovations.com	Kharthik SR
SMO-eGInnovationsTestingTeam1@eginnovations.com	eG Innovations Testing Team
karthikg1978_hotmail.com#EXT#@eGinnovations435.onmicrosoft.com	Karthik G
LY1500_hotmail.com#EXT#@eginnovations.com	Leo Yao
jgullatt_gmail.com#EXT#@eginnovations.com	James Gullatt
perrocacheton_hotmail.com#EXT#@eginnovations.com	edwin guerrero suarez
yiboon.tan_ascendas-singbridge.com#EXT#@eginnovations.com	Tan Yi Boon
SingaporeofficeM1@eginnovations.com	Singapore office M1

Page 1 of 1

Figure 4.24: The detailed diagnosis of the Unlicensed users measure

Using the detailed diagnosis of the *Deleted users* measure, you can at-a-glance identify the users who have been deleted and the locations from which they have been deleted.

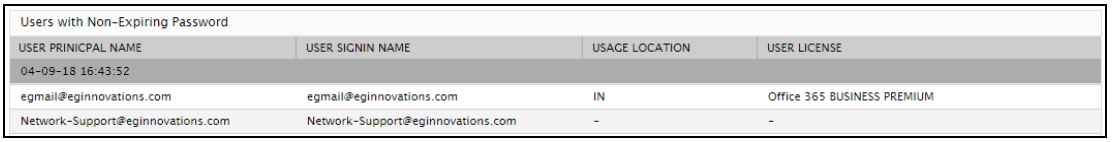


Details of Deleted Users

USER PRINICPAL NAME	USER SIGNIN NAME	USAGE LOCATION
04-09-18 16:43:52		
shaik@eginnovations.com	shaik@eginnovations.com	IN
ar@eginnovations.com	ar@eginnovations.com	IN
Jeremy.Teo@eginnovations.com	Jeremy.Teo@eginnovations.com	IN
Suriya.D@eginnovations.com	Suriya.D@eginnovations.com	IN
Vanny.Zhang@eginnovations.com	Vanny.Zhang@eginnovations.com	SG
egmonitoring@eginnovations.com	egmonitoring@eginnovations.com	IN

Figure 4.25: The detailed diagnosis of the Deleted users measure

The detailed diagnosis of the Users with non-expiring passwords measure reveals the principal name and sign-in name of the users who have been configured with non-expiring passwords. Additionally, the detailed metrics reveal the location of the user and the Office 365 product to which he/she has been assigned a license.



Users with Non-Expiring Password

USER PRINICPAL NAME	USER SIGNIN NAME	USAGE LOCATION	USER LICENSE
04-09-18 16:43:52			
egmail@eginnovations.com	egmail@eginnovations.com	IN	Office 365 BUSINESS PREMIUM
Network-Support@eginnovations.com	Network-Support@eginnovations.com	-	-

Figure 4.26: The detailed diagnosis of the Users with Non-Expiring Passwords measure

4.4 The Office 365 Usage Layer

To measure the usage of each Office 365 service, use the Usage by Service test mapped to this layer.

Figure 4.27: The test mapped to the O365 Usage layer

4.4.1 Audit Activities by Service Test

Office 365 offers subscription plans that include access to Office applications plus other productivity services that are enabled over the Internet (cloud services). To know which of these services are popular amidst users, administrators need to measure the workload of each service. In other words, administrators have to know how many users are accessing and how many operations are being performed on each service. The **Audit Activities by Service** test provides administrators with this insight!

This test auto-discovers the services offered by your Office 365 subscription. For each service, the test then reports the number of unique operations performed on the service, and the number of unique users using the service. Using these metrics, administrators can gauge the overall workload of each service and accurately identify the popular/most used service. With the help of the detailed diagnostics of this test, you can also identify that operation which has imposed maximum load on the service. Detailed metrics also reveal the users who used the service.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each service offered by your Office 365 subscription

First-level Descriptor: Service Name

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against

Parameters	Description
Confirm Password	O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively.

Parameters	Description
	If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total operations	Indicates the total number of operations performed on this service.	Number	This is a good indicator of the workload on the service. Compare the value of this measure across services to know which service is used the most.
Unique operations	Indicates the number of unique operations	Number	Use the detailed diagnosis of this measure to know which operations

Measurement	Description	Measurement Unit	Interpretation
	performed on this service.		were performed on the service and how many times.
Unique users	Indicates the number of unique users of this service.	Number	Compare the value of this measure across service to know which service is the most popular with users. Use the detailed diagnosis of this measure to know which users are using the service.
Unique client IPs	Indicates the number of unique clients from which users accessed this service.	Number	Use the detailed diagnosis of this measure to know the clients used and the users who are accessing the service from each client. The operations performed by the users and the number of times for which each operation was performed are also reported as part of detailed diagnostics.

The detailed diagnosis of the *Total operations* and *Unique operations* measures lists the operations performed on a service and the number of times for which each operation was performed. This way, you can identify the operation that imposed the maximum load on the service.

User Activity Details

OPERATION CATEGORY	OPERATION	NUMBER OF OPERATIONS
04-09-18 15:08:57		
UserLoggedIn	UserLoggedIn	8
UserLoginFailed	UserLoginFailed	1

Figure 4.28: The detailed diagnosis of the Unique operations measure

The detailed diagnosis of the *Unique users* measure lists the top-10 users of a service, in terms of the operational load they imposed on that service. For each user, the detailed diagnostics reveal the client from which the user accessed the service, the operations performed by the user, and the number of times (in square braces) each operation was performed. This way, you will be able to identify which user imposed the maximum load on the service and through which operation.

Top 10 Users by Number of Operations

USER	CLIENT IPS	NUMBER OF OPERATIONS
04-09-18 15:08:57		
satheesh@eginnovations.com	61.12.78.30	UserLoggedIn [1]
egmail@eginnovations.com	174.143.94.198, 61.12.78.30	UserLoggedIn [7]
tanch@eginnovations.com	113.128.132.176	UserLoginFailed [1]

Figure 4.29: The detailed diagnosis of the Unique users measure

Using the detailed diagnosis of the *Unique client IPs* measure, you can view the top-10 client IPs, in terms of the workload generated by the users accessing the service from those IPs. For each IP, the detailed metrics reveal the users accessing the service from that IP, the operations performed by the users when accessing from that IP, and the number of times (in square braces) each operation was performed. This way, you will be able to identify the client IP that generated the maximum workload for a service.

Top 10 Client IPs by Number of Operations

CLIENT IP	USERS	NUMBER OF OPERATIONS
04-09-18 15:08:57		
113.128.132.176	tanch@eginnovations.com	UserLoginFailed [1]
174.143.94.198	egmail@eginnovations.com	UserLoggedIn [1]
61.12.78.30	satheesh@eginnovations.com, egmail@eginnovations.com	UserLoggedIn [7]

Figure 4.30: The detailed diagnosis of the Unique client IPs measure

4.4.2 User-Logins-Test

Use this test to track user logins to Office 365, and rapidly capture login failures.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 tenant being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It

Parameters	Description
	typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for

Parameters	Description
	this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time the test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Successful logins	Indicates the number of successful logins to Office 365.	Number	
Failed logins	Indicates the number of logins to Office 365 that failed.	Number	Use the detailed diagnosis of this measure to know which login attempts failed.

Using the detailed diagnosis of the *Failed logins* measure you can accurately determine when the login failure occurred, which user's login attempt failed, from which client the user attempted to login, and to which service.

Details of Failed logins

LOG TIME	CLIENTIP	USERID	SERVICE
Mar 17, 2020 16:43:51			
3/17/2020 10:00:36 AM	95.53.192.44	joyce.lee@eginnovations.com	AzureActiveDirectory

Figure 4.31: The detailed diagnosis of the Failed logins measure

4.5 The User Experience Layer

The test mapped to this layer periodically checks the accessibility of the Office 365 portal and the time taken for access, and reports abnormalities (if any).

Figure 4.32: The test mapped to the User Experience layer

4.5.1 O365 Portal Connectivity Test

If the Office 365 portal is unavailable / inaccessible, then users will not be able to use the Microsoft Office suite and other critical services (Exchange server, Skype for Business, SharePoint, etc.) on the cloud, until such time the connection to the portal is restored. The lack of HTTP/S connectivity, even for a brief while, can severely hamper business correspondence, affect user productivity, and ultimately hit revenues. To avoid this, administrators should continuously track the connectivity to the portal, so that they promptly detect any break/slowness in connectivity, and proactively initiate corrective measures. This is where the **O365 Portal Connectivity** test helps!

This test emulates an HTTP connection to the portal URL, portal.office.com. In the process, the test reports whether the portal is accessible or not, and if so, how long it takes to connect to the portal. This way, the test proactively reveals poor connectivity to the portal, and thus enables administrators to initiate remedial measures before users complain.

Target of the test : Office 365

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Office 365 portal being monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
O365 User Name, O365 Password, and Confirm Password	For execution, this test requires the privileges of an O365 user who is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box.

Parameters	Description
	While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.2.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the *O365 Domain* parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that

Parameters	Description
	password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify *none* against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Connection status	Indicates whether/not the portal is accessible over HTTP/S.		If HTTP/S connectivity to the portal is available, then this measure will report the value *Success*. If the connectivity is unavailable, then this measure will report the value *Failed*. The numeric values that correspond to these measure values are as follows: **Measure Value** / **Numeric Value** Success / 1 Failed / 0 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate whether/not the portal is accessible. In the graph of this measure however, the same is indicated using the numeric equivalents only.
Time taken to connect	Indicates the average time taken to connect to the portal.	Seconds	An abnormally high value is a cause for concern, as it indicates that it is taking too long to connect to the portal over HTTP/S. To ensure a high quality experience for Office 365 users, you need to investigate why connectivity is slow and fix it.

Chapter 5: Troubleshooting Office 365 Monitoring

If the eG agent is unable to report metrics on Office 365 performance, then you may want to check whether/not the Microsoft Azure Active Directory Module for Windows PowerShell and the Microsoft Online Services Sign-in Assistant for IT Professionals RTW are properly installed on the eG agent host. To perform this check, do the following:

1. On the eG agent host, click Start, and search for Windows Powershell ISE. Once it is found, run Windows Powershell ISE in the elevated mode.
2. First, check if the PackageManagement module is installed properly. For that, type *Install-Module*, and see if the auto-complete feature of Windows automatically lists the command you were about to type (see Figure 5.1).

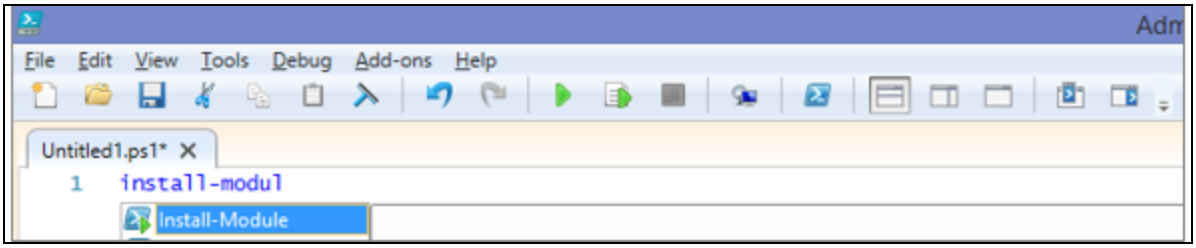


Figure 5.1: Checking if the PackageManagement module has been installed properly

3. If the command auto-completes, it means that the PackageManagement module has been installed properly. If the command does not auto-complete, then you can conclude that the PackageManagement module has not been installed on the eG agent host. In this case, first install this module on the eG agent host. You can download the installable from the URL: https://download.microsoft.com/download/C/4/1/C41378D4- 7F41- 4BBE- 9D0D-0E4F98585C61/PackageManagement_x64.msi
4. If you find that the PackageManagement module has been installed properly, proceed to check if the Microsoft Azure Active Directory Module for Windows PowerShell and the Microsoft Online Services Sign-in Assistant for IT Professionals RTW are properly installed on the eG agent host. To perform this check, with the Windows Powershell ISE in the elevated mode, type the following commands one after another:

   Connect-MSolService

   Get-MsolDomain

   Get-MsolGroup

5. If these commands auto-complete - i.e., if Windows lists these commands even before you type them fully - you can conclude that the Microsoft Azure Active Directory Module for Windows PowerShell and the Microsoft Online Services Sign-in Assistant for IT Professionals RTW are properly installed on the eG agent host. On the other hand, if the commands do not auto-complete, then you must proceed to install both the aforesaid modules on the eG agent host. To know how to install, refer to the Section **2.1**.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.