Monitoring Microsoft Exchange Online

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

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 three specialized monitoring models - one each for Microsoft Office 365, and two of the most popular cloud-based services it offers, namely - Microsoft Exchange Online and Microsoft SharePoint Online.

Microsoft Exchange Online is a hosted messaging application that provides organizations with access to the full-featured version of Exchange Server. It includes access to email, calendars, contacts and tasks for any endpoint device.

This document discussion focuses only on the Microsoft Exchange Online monitoring model that eG Enterprise provides. With the help of this document discussion, you will be able to understand how eG Enterprise monitors Microsoft Exchange Online, and how one can manage and monitor the performance of Exchange Online using eG Enterprise.

1.1 Licensing

Every *Microsoft Exchange Online* component you manage consumes a Premium Monitor license in eG Enterprise.

Chapter 2: How Does eG Enterprise Monitor Microsoft Exchange Online?

eG Enterprise monitors Microsoft Exchange Online 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 Exchange Online. To ensure that the eG agent is able to run these cmdlets, the pre-requisites detailed in the Pre-requisites for Monitoring Microsoft Exchange Online topic are to be fulfilled.

2.1 Pre-requisites for Monitoring Exchange Online

Before attempting to monitor Microsoft Exchange Online, make sure that the following pre-requisites are fulfilled:

- The eG agent should be deployed on a remote host running one of the following Windows versions:
  - Windows 10
  - Windows 8.1
  - Windows Server 2016
  - Windows Server 2012 or Windows Server 2012 R2
  - Windows 7 Service Pack 1 (SP1)
  - Windows Server 2008 R2 SP1
- The Windows system hosting the remote agent should have internet connection.
- .NET 4.5 (or above) should pre-exist on the eG agent host.
- Windows Management Framework (WMF) 5.1 should be installed on the eG agent host
- Typically, to pull metrics, the eG agent should first be able to connect to the O365 cloud via powershell. To enable this connection, 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:
  1. 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
  2. Once the PackageManagement and PowerShellGet modules are successfully installed, open Windows PowerShell ISE in elevated mode on the eG agent host.
  3. Then, run the cmdlet depicted by 2.1.

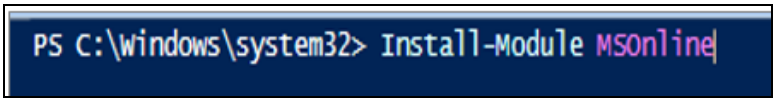


Figure 2.1: Installing the Microsoft Azure Active Directory Module for Windows PowerShell

- To enable the eG agent to monitor the Exchange Online service health, you need to ensure that the O365 Service Communications module pre-exists on the eG agent host. To install this module, do the following:
  - Go to the URL: https://github.com/mattmcnabb/O365ServiceCommunications
  - When Figure 2.2 appears, click on the **Clone or Download** button (highlighted in Figure 2.2) therein to download the module.

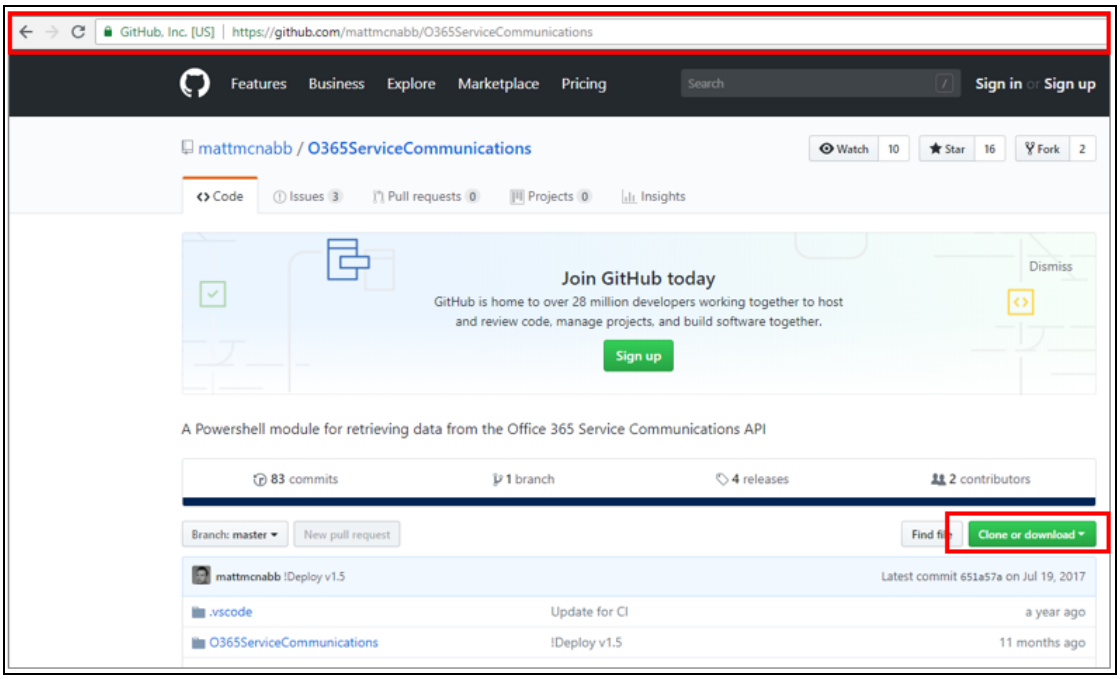


Figure 2.2: Clicking on the Clone or Download button

- Figure 2.3 then appears. Click the **Download ZIP** button in Figure 2.3.

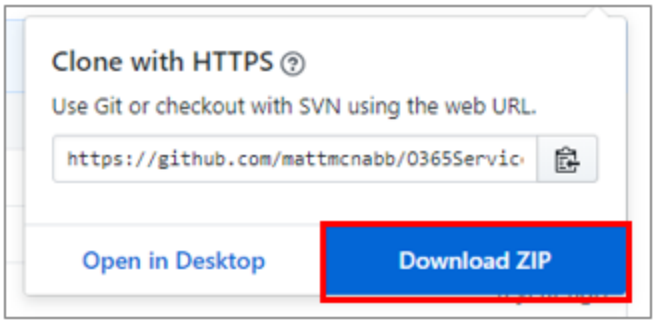


Figure 2.3: Clicking on the Download ZIP button

- Download the zip file to any location on the eG agent host. Next, unzip the downloaded file to extract its contents. From the extracted contents, copy only the **O365ServiceCommunications** folder to the <Windows_ PowerShell_ Install_ Drive>\Windows\System32\WindowsPowerShell\v1.0\Modules\ directory.
- Finally, right-click the **O365ServiceCommunications** folder, select Properties from the shortcut menu, and unblock the folder. If any of the files inside the folder are blocked, then right-click on that file, select Properties, and unblock that file. Likewise, unblock every file that is blocked.

- To monitor Microsoft Exchange Online, the eG agent requires the privileges of a user who has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs, View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. For this purpose, each test the eG agent runs on Exchange Online should be configured with the credentials of a user who has been assigned the aforesaid role and permissions.
  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 configure the eG tests with the credentials of that user. 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 **2.1.1** topic.

2.1.1 Creating a New User in the Office 365 Portal

To monitor Microsoft Exchange Online, the eG agent has to be configured with the credentials of a user who has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 2.4 will then appear.

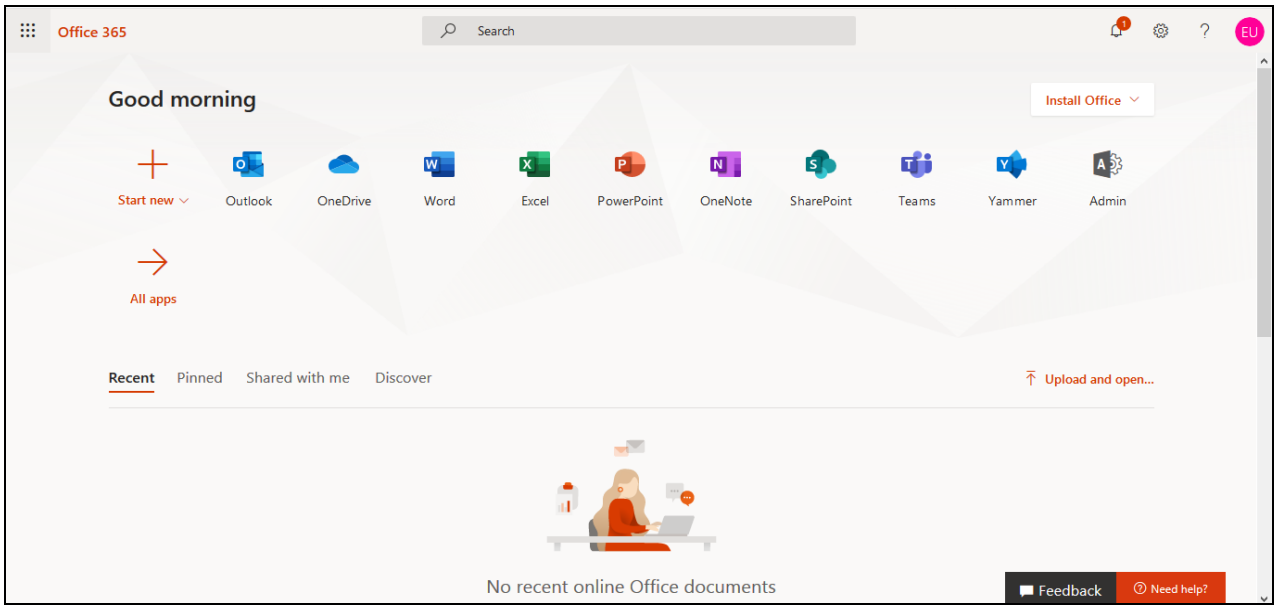


Figure 2.4: Welcome page of the Office 365 portal

4. Click on **Admin** under **Apps** (in Figure 2.4). The Microsoft Office 365 Admin Center will then appear. Expand the **Users** drop-down list and click on **Active users** (see Figure 2.5).

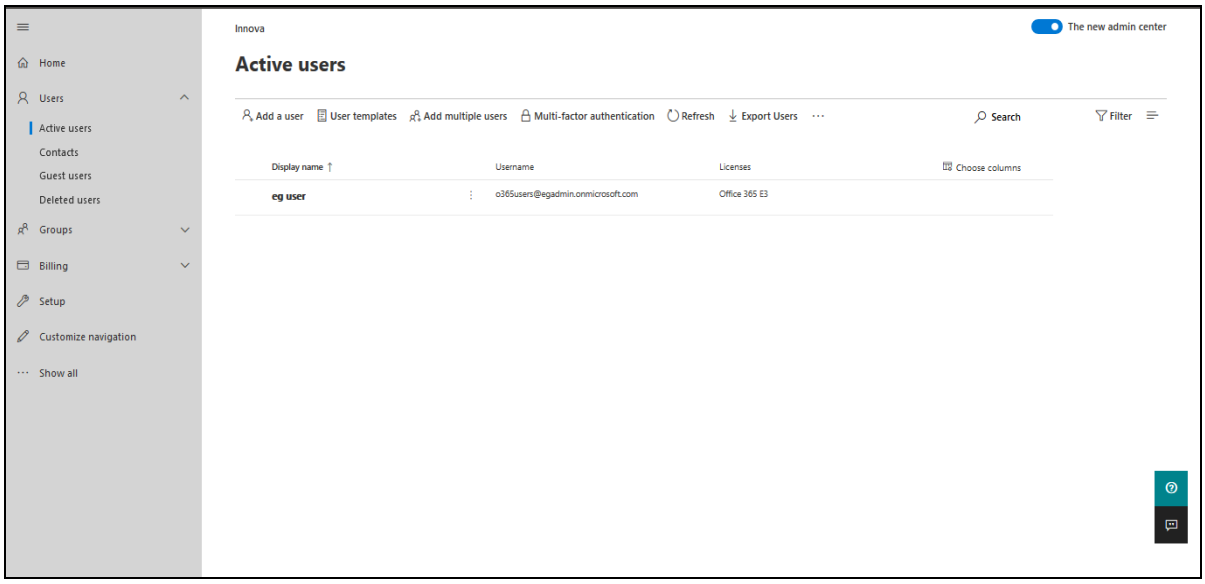


Figure 2.5: The Microsoft Office 365 Admin Center

5. To create a new user, click on the **Add a user** link in Figure 2.5.
6. Figure 2.6 will then appear.

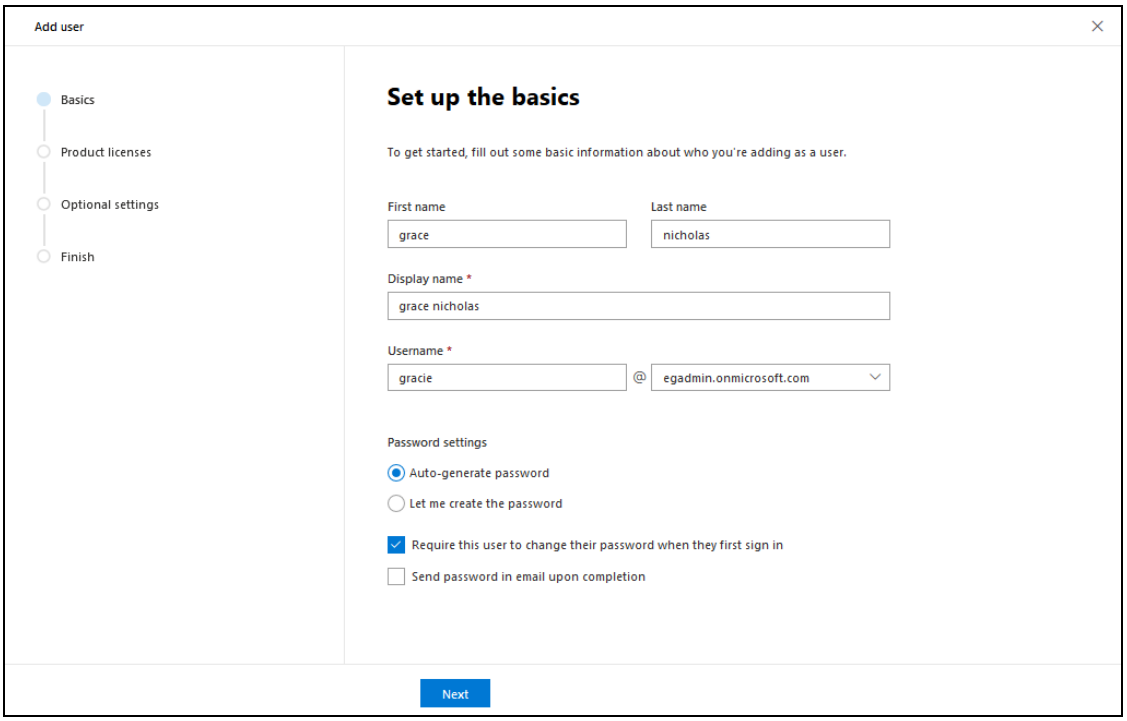


Figure 2.6: Adding a new user

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.

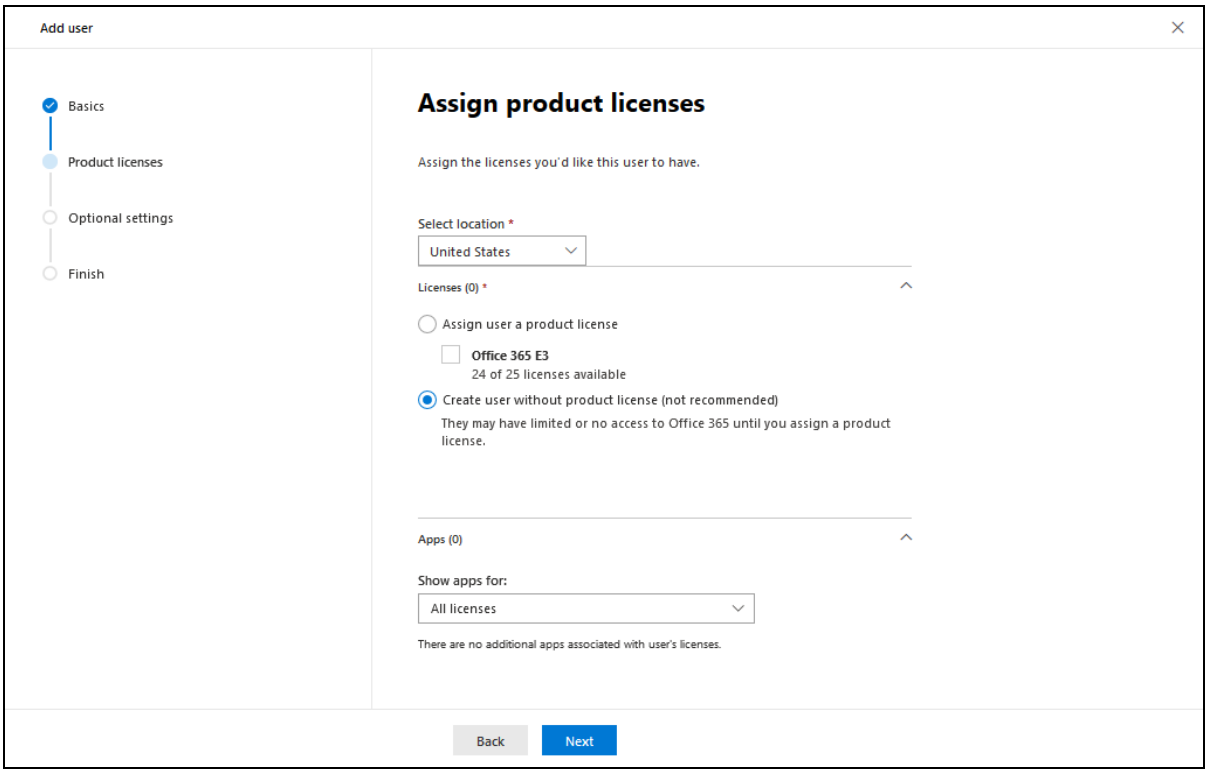


Figure 2.7: Choosing the geographic location of the new user

8. Then, select the geographic **Location** of the new user. Turn *On* the **Create user without product license** flag in Figure 2.7.
9. Clicking the **Next** button in Figure 2.7 will reveal Figure 2.8. Here, select the **Admin center access** option.

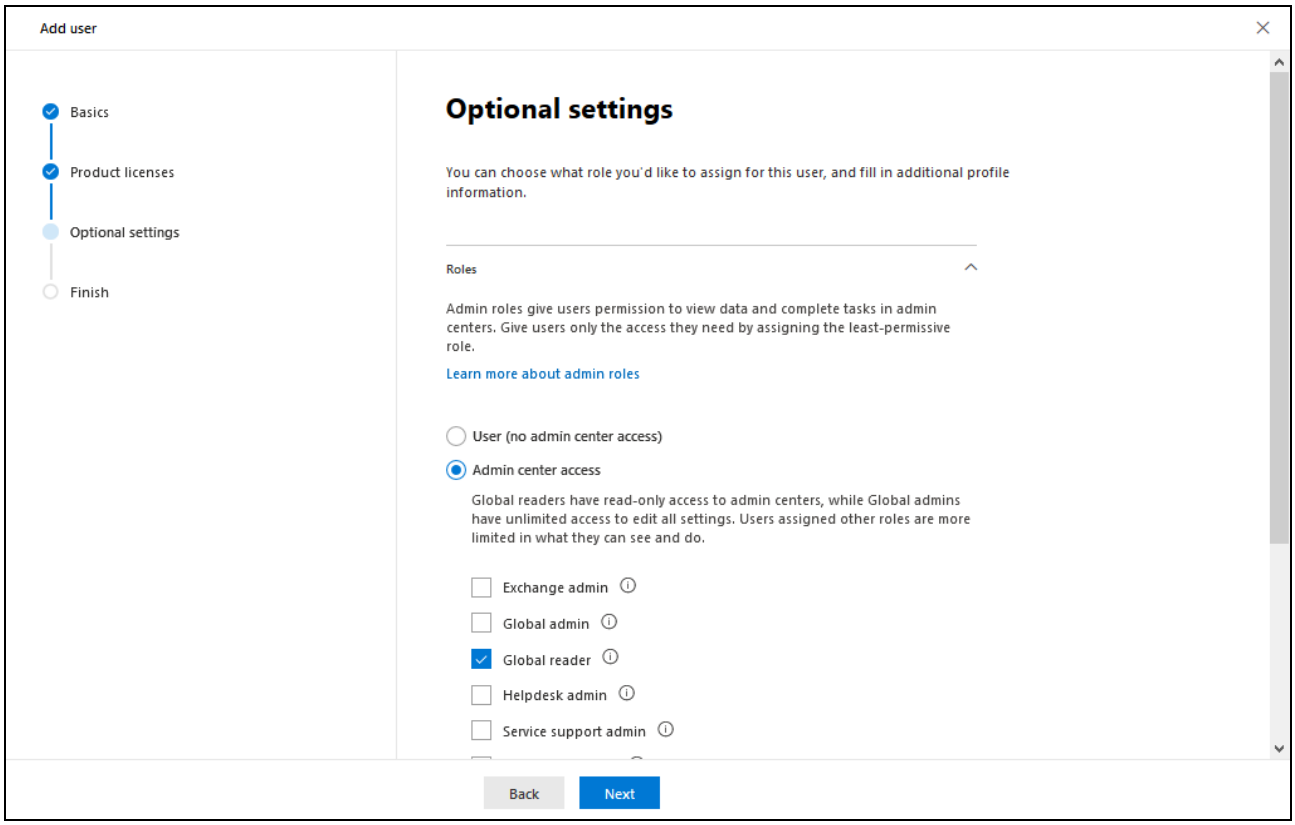


Figure 2.8: Selecting the Admin center access

10. For the purpose of monitoring, the new user should be assigned the **Global reader** role. Select this role from Figure 2.8.

11. Click the **Next** button in Figure 2.8 to review your selection which appears in Figure 2.9.

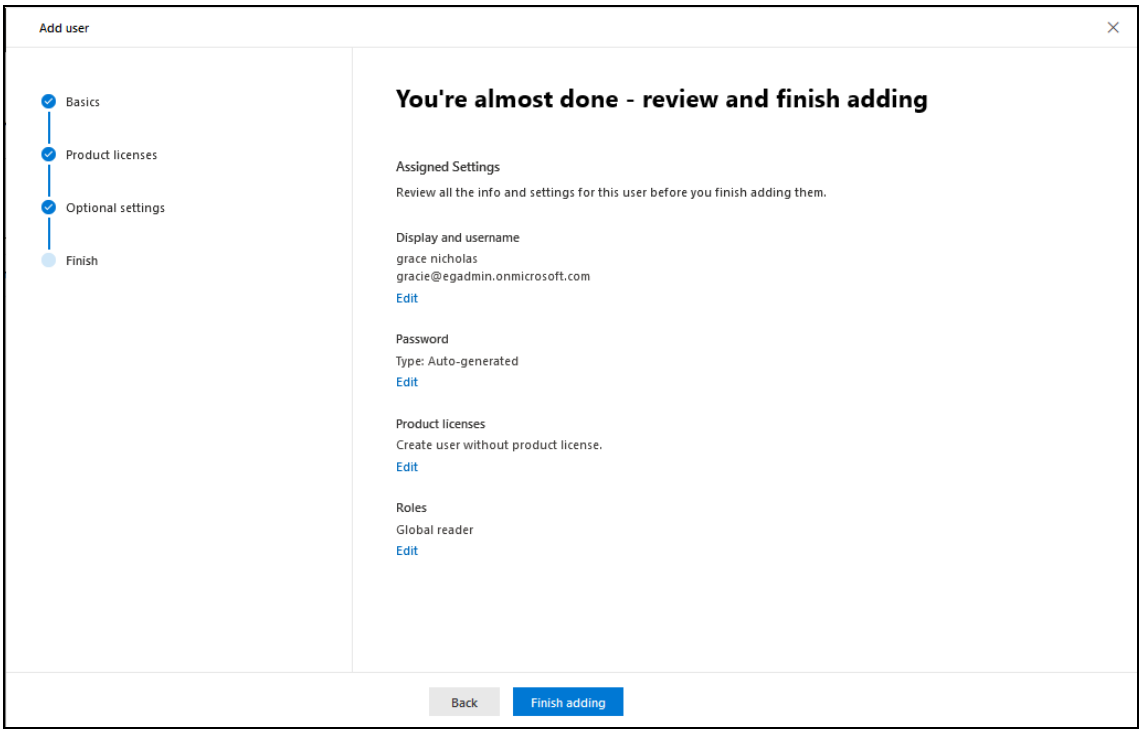


Figure 2.9: Reviewing your selection

12. Finally, click the **Finish adding** button in Figure 2.9 to add the new user. Figure 2.10 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 2.10, as this is what you need to configure against the **OFFICE 365 USER** and **OFFICE 365 PASSWORD** parameters of the eG tests.

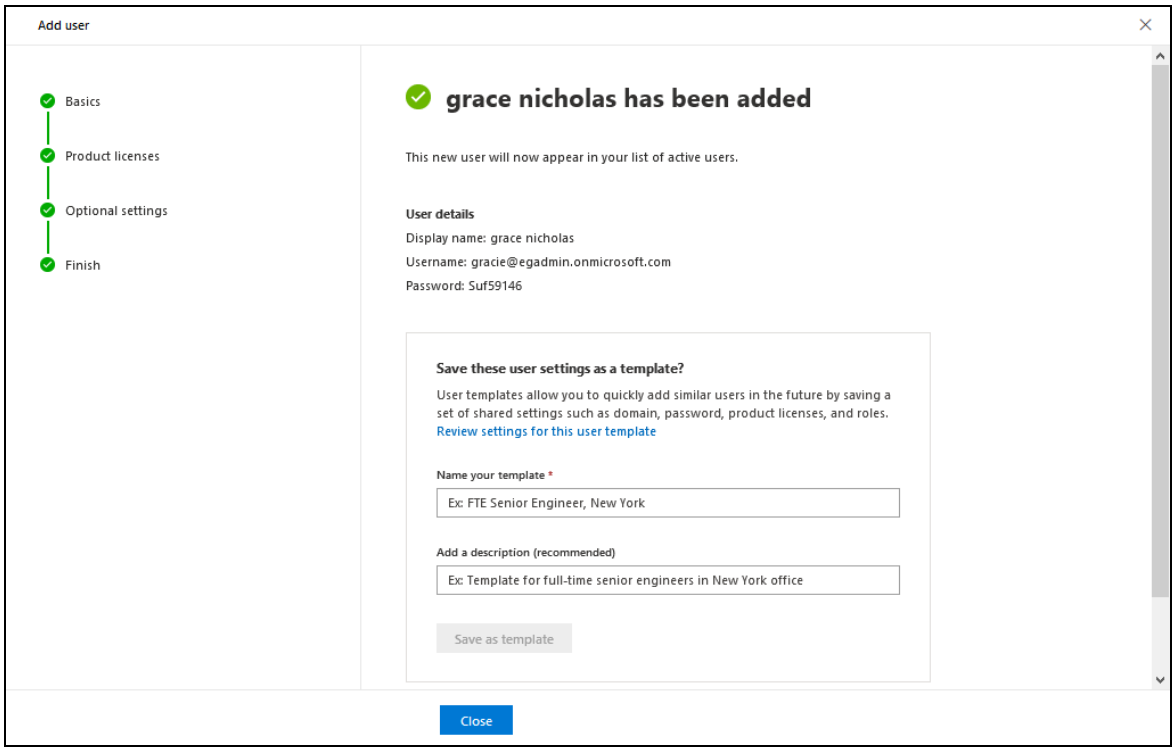


Figure 2.10: Message confirming the successful addition of a user

13. Next, proceed to assign the **View- Only Audit Logs**, **View- Only Recipients, Mail Recipients**, and **Mail Import Export** permissions to the new user. For that, first click on the Admin Center tool in the tool bar depicted by Figure 2.11. From the menu that pops up, click on **Exchange**.

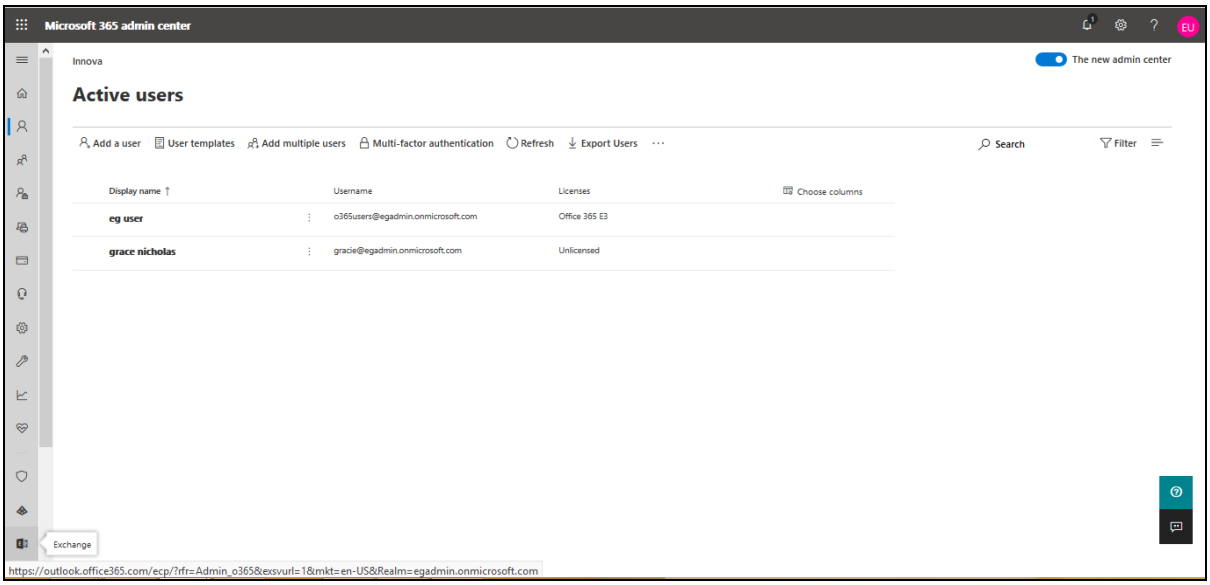


Figure 2.11: Connecting to the Exchange Admin Center

14. Figure 2.12 will then appear.

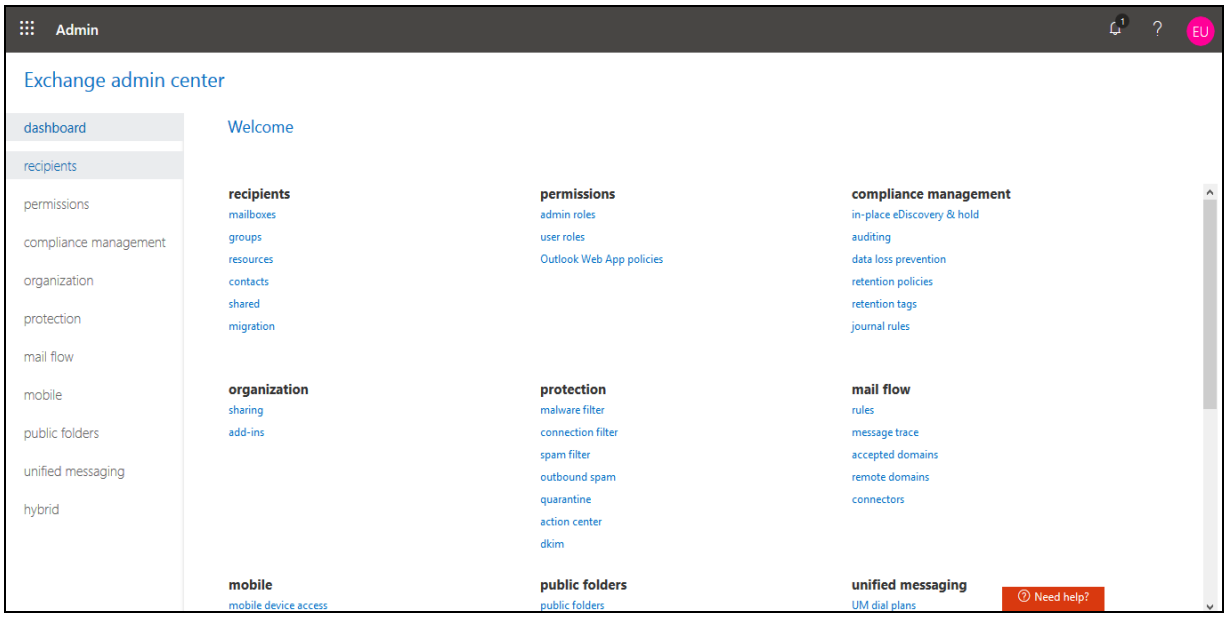


Figure 2.12: The Exchange Admin Center

15. From the list of options in the left panel of Figure 2.12, select **permissions**. Figure 2.13 will then appear listing the **admin** role groups that pre-exist.

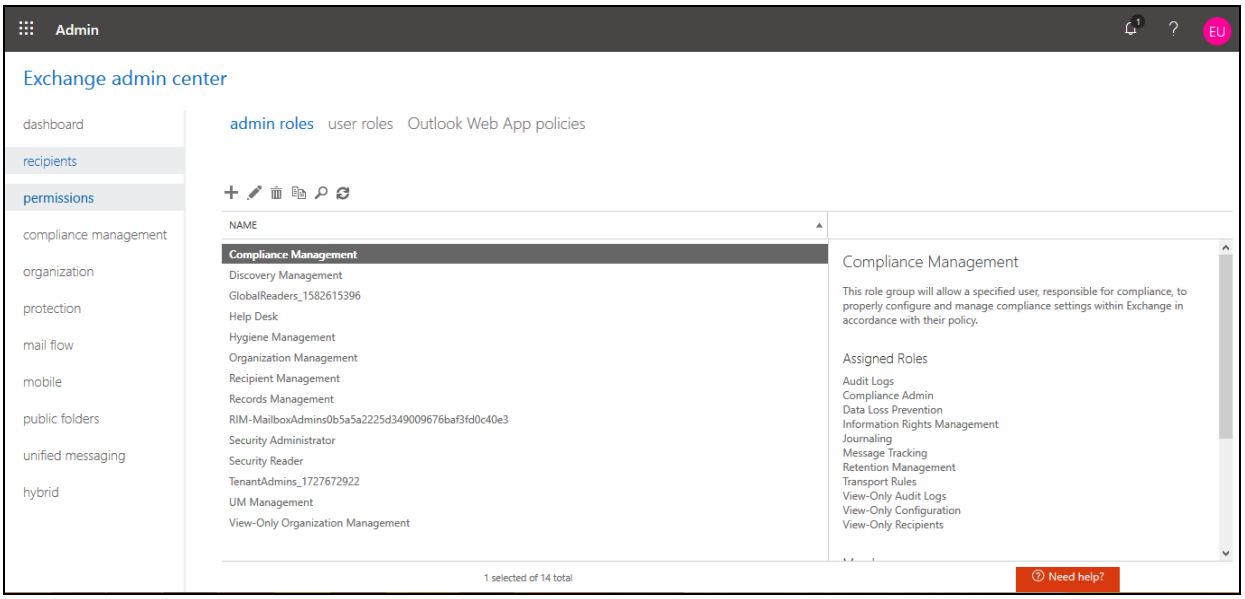


Figure 2.13: Clicking on the permissions option to view the admin role groups

16. Let us now proceed to create a role group that includes the **View-Only Audit Logs, View-Only Recipients, Mail Recipients, and Mail Import Export permissions**. For that, click on the + button on top of the list of admin role groups (see Figure 2.13). Figure 2.14 will then appear.

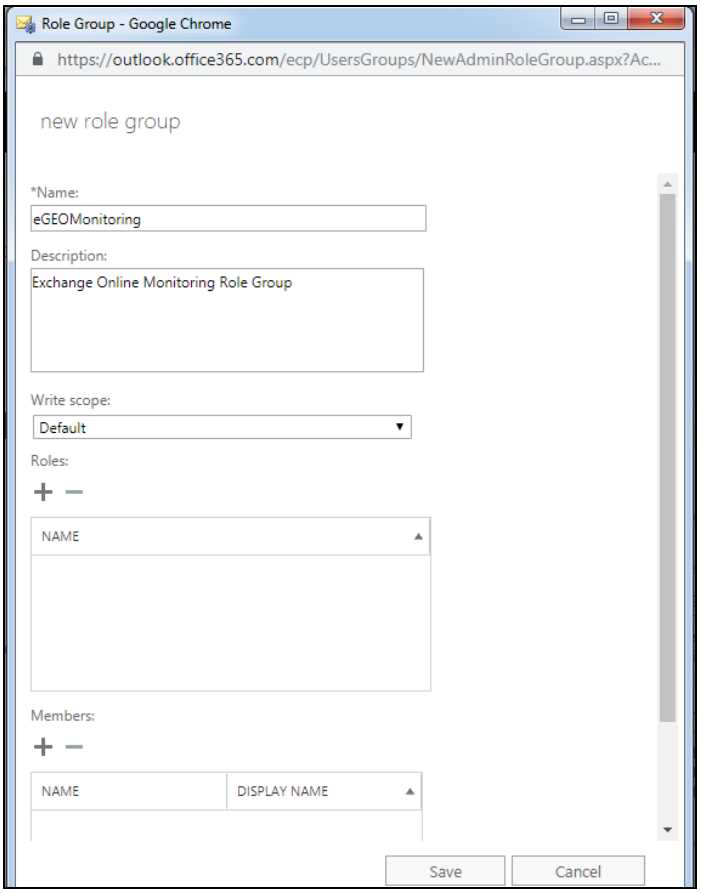


Figure 2.14: Adding a new role group

17. Provide a unique **Name** and **Description** for the new role group (see Figure 2.14). Then, click on the + button in the **Roles** section of Figure 2.14. Figure 2.15 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, View-Only Recipients, Mail Recipients, and Mail Import Export permissions** and click the **add ->** button to add the permissions. Then, click **OK** to save the changes.

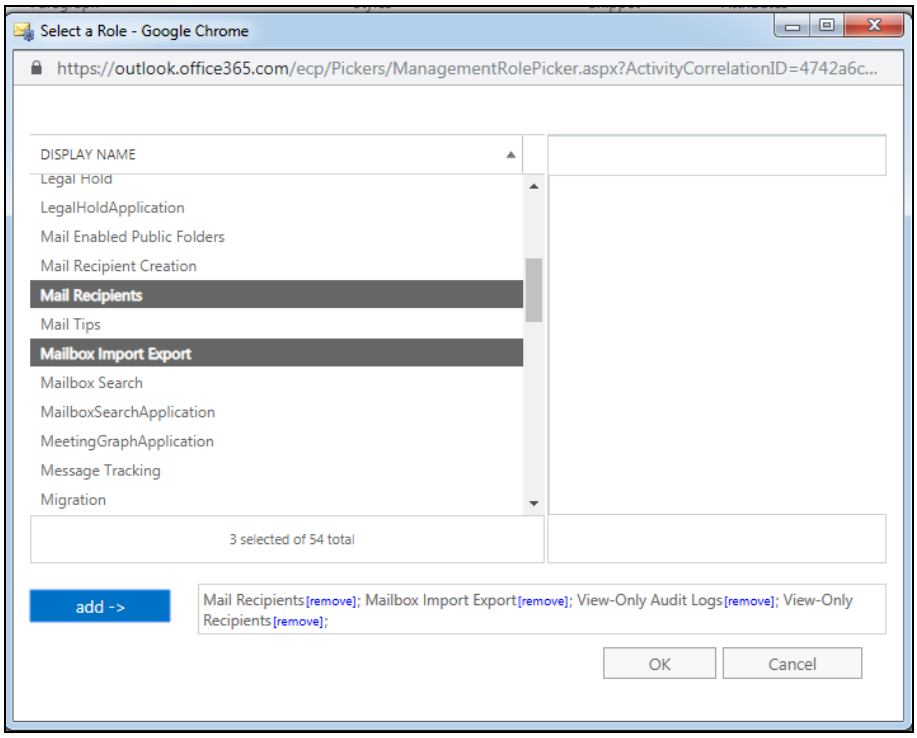


Figure 2.15: Adding the permissions to the new role

18. Figure 2.16 will then appear. Next, proceed to assign the new role group (that includes the three permissions) to the user you created previously. For that, click on the + button in the **Members** section of Figure 2.16.

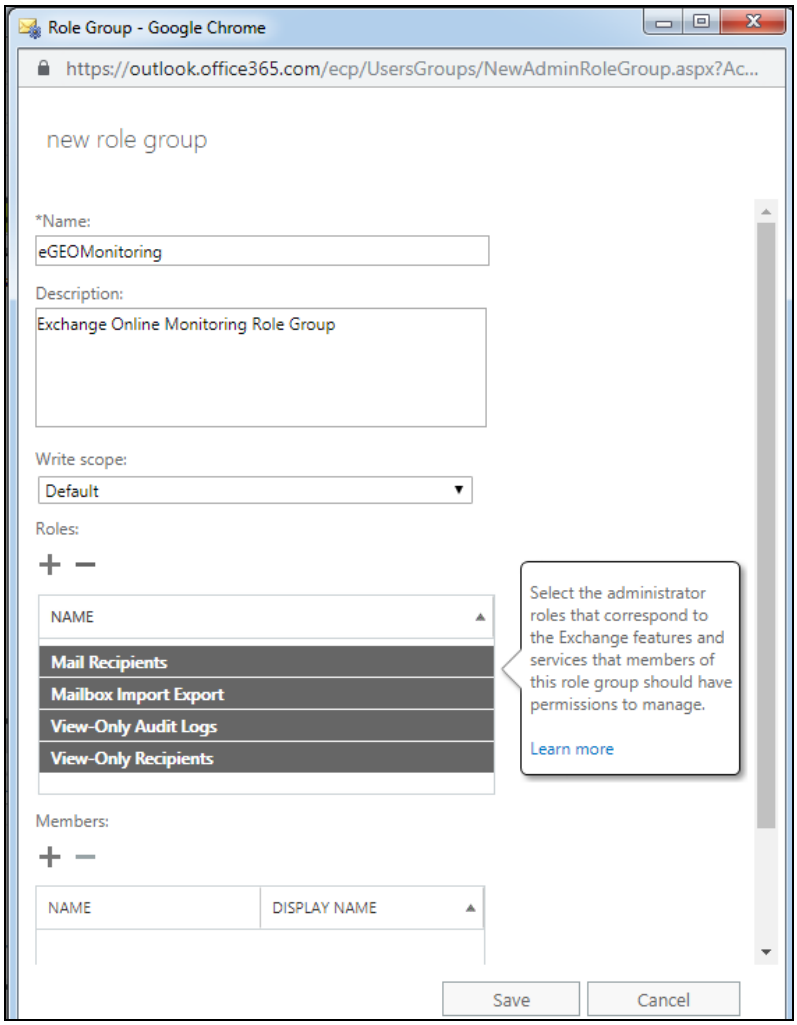


Figure 2.16: Clicking on the '+' icon in the Members section

19. Figure 2.17 will then appear. From the list of user names displayed in Figure 2.17, select the name of the user you created for monitoring purposes and click the **add ->** button. Then, click **OK**.

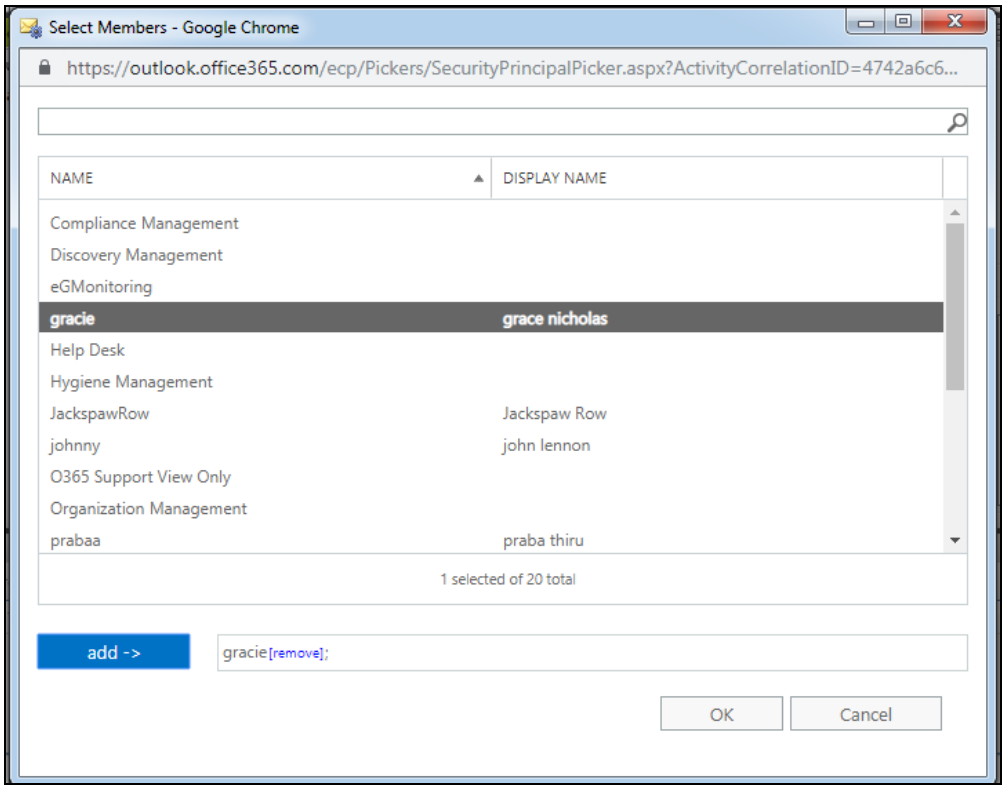


Figure 2.17: Assigning the role group to a user

20. When Figure 2.18 appears, click the **Save** button to save the new role group definition.

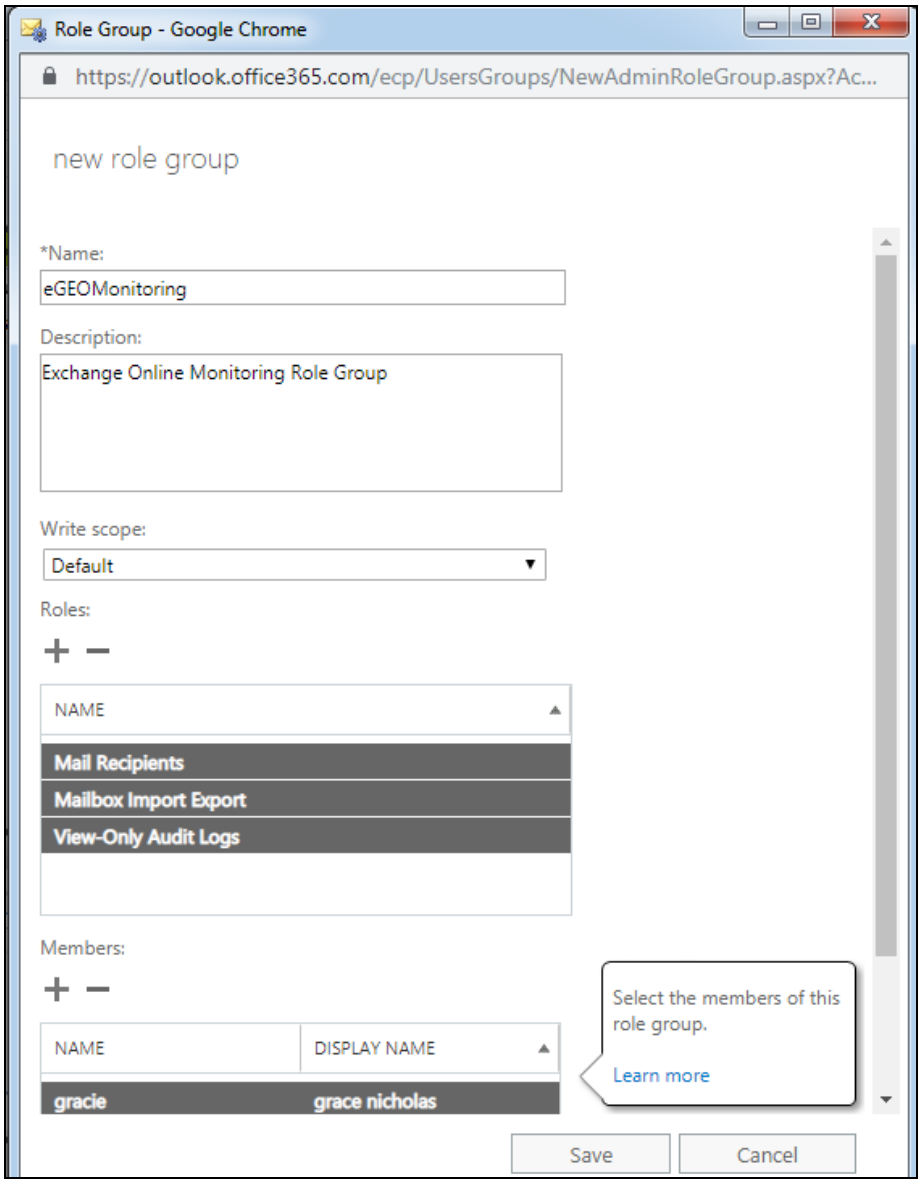


Figure 2.18: Saving the new role group

2.1.2 Installing 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 2.19).

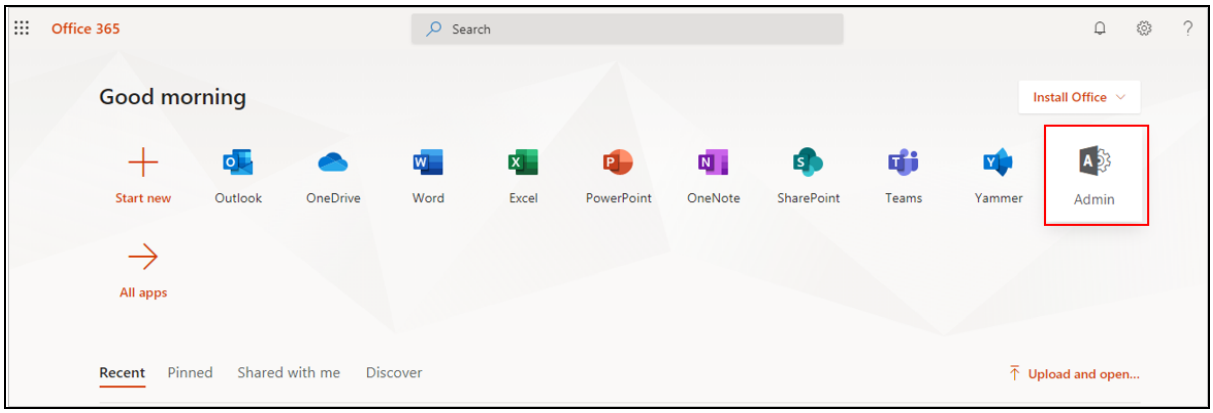


Figure 2.19: Clicking on Admin option in Office 365 portal

2. When Figure 2.20 appears, browse the left panel of Figure 2.20 for the **Admin Centers** node. Expand the node and select the **Azure Active Directory** sub-node within.

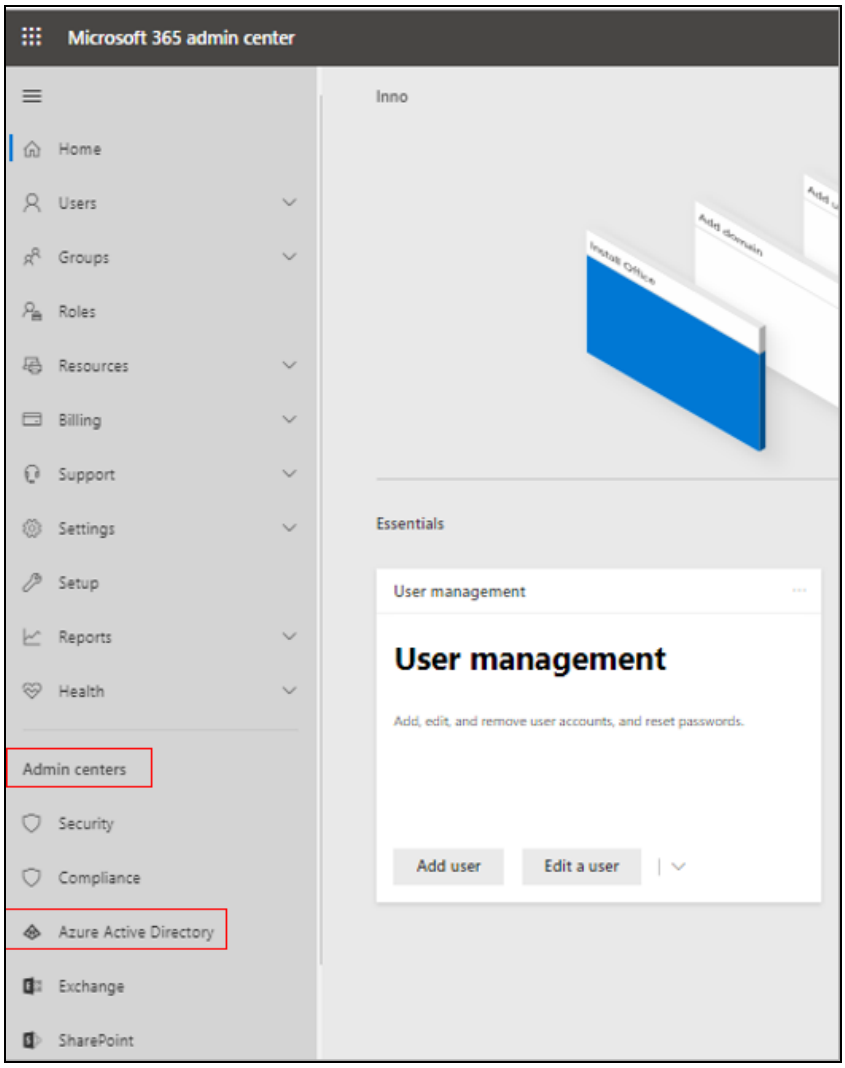


Figure 2.20: Clicking on Azure Active Directory under Admin Centers

3. Figure 2.21 then appears. Select **Azure Active Directory** from the list of **FAVORITES** in the left-most panel of Figure 2.21. Then, from the **App Registrations** list for Azure Active Directory, select **App registrations** to register the Microsoft Graph app.

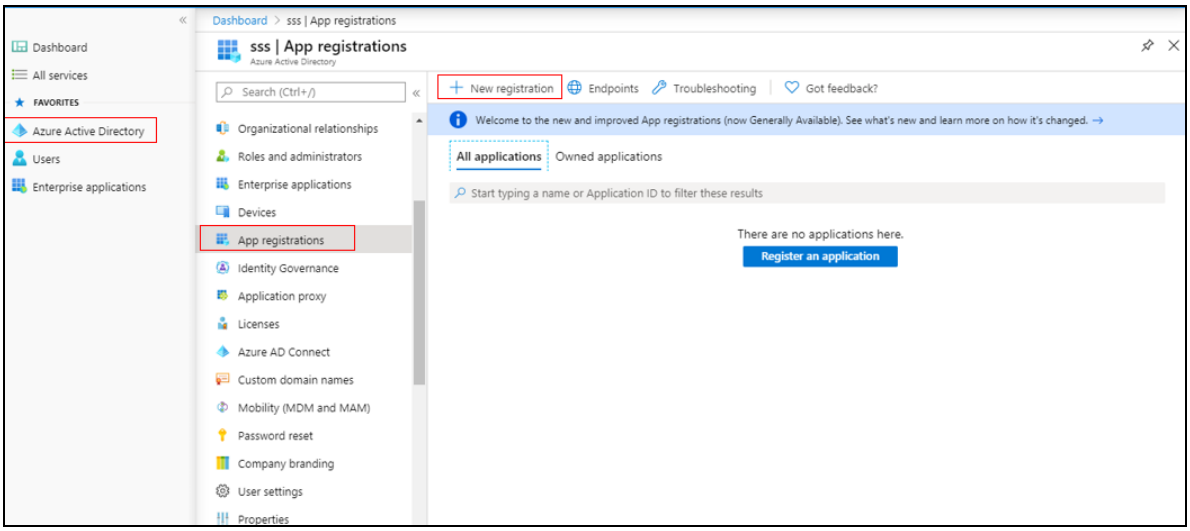


Figure 2.21: Selecting the App registrations option to register a new app on Azure AD

4. Figure 2.22 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 2.22 to register Microsoft Graph on Azure AD.

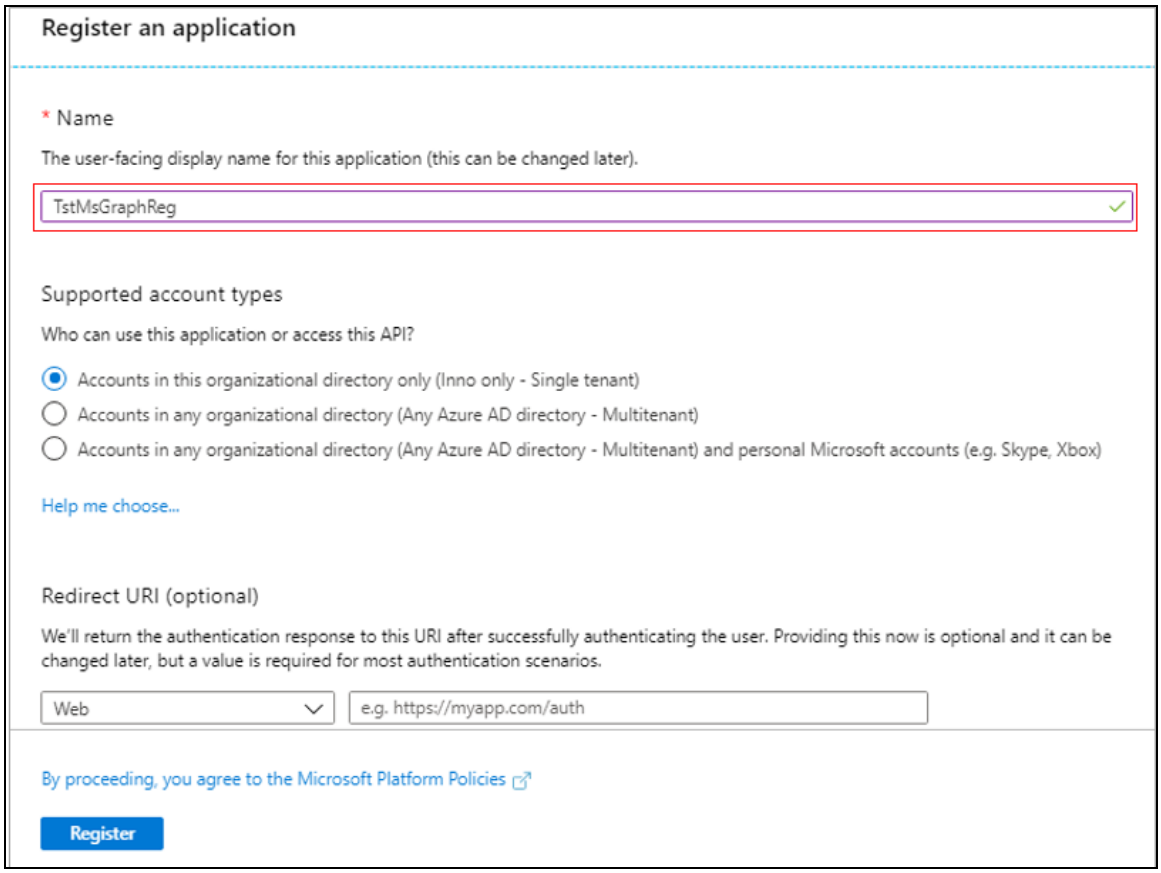


Figure 2.22: Registering the Microsoft Graph app on Azure AD

5. Upon successful app registration, Figure 2.23 will appear displaying a message to that effect. Additionally, Figure 2.23 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**.

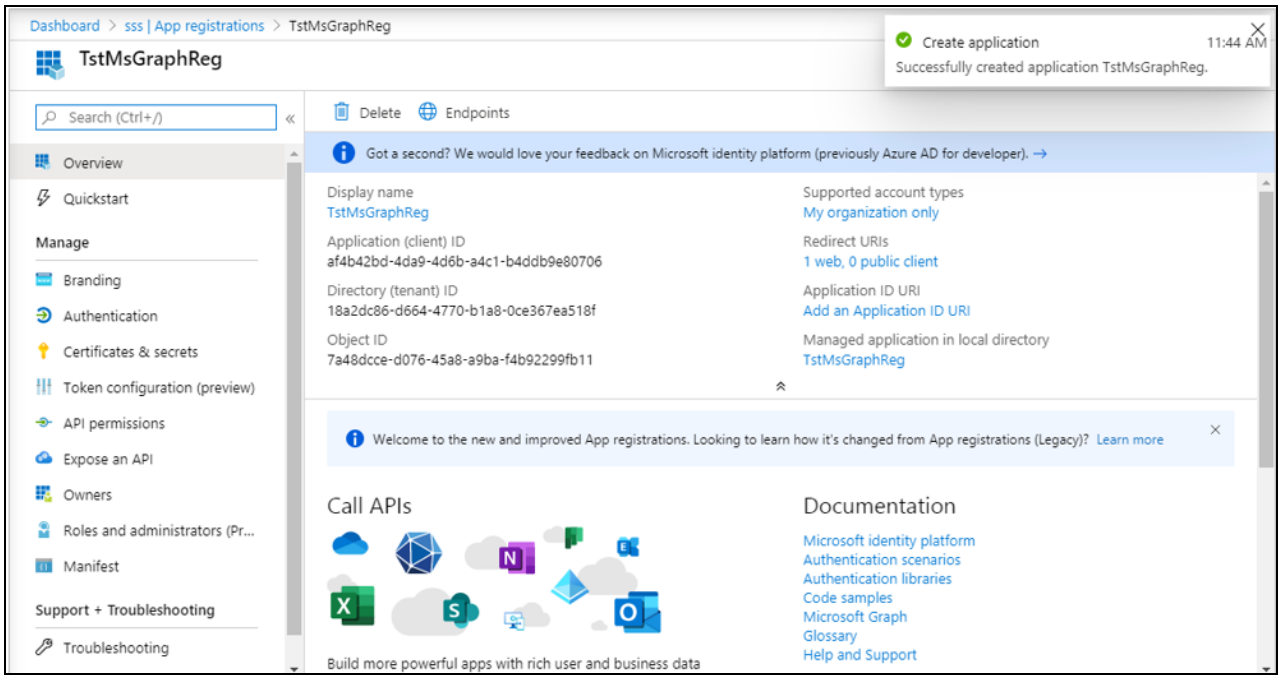


Figure 2.23: Viewing and making a note of the Application ID of the Microsoft Graph app

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 2.23. Figure 2.24 will then appear. Now, click on the **New client secret** button in the **Client Secrets** section in the right panel of Figure 2.24.

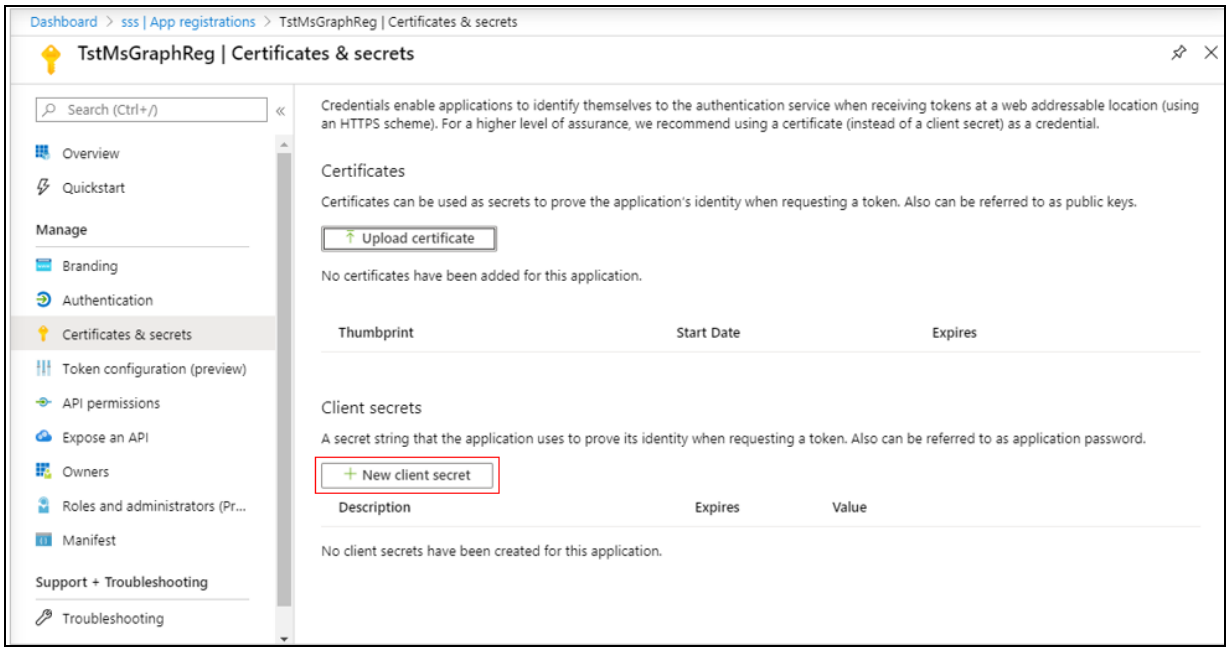


Figure 2.24: Clicking on the New client secret button

7. When Figure 2.25 appears, provide a **Description** for the new secret, set it to **Never** expire, and click the **Add** button to add the new secret.

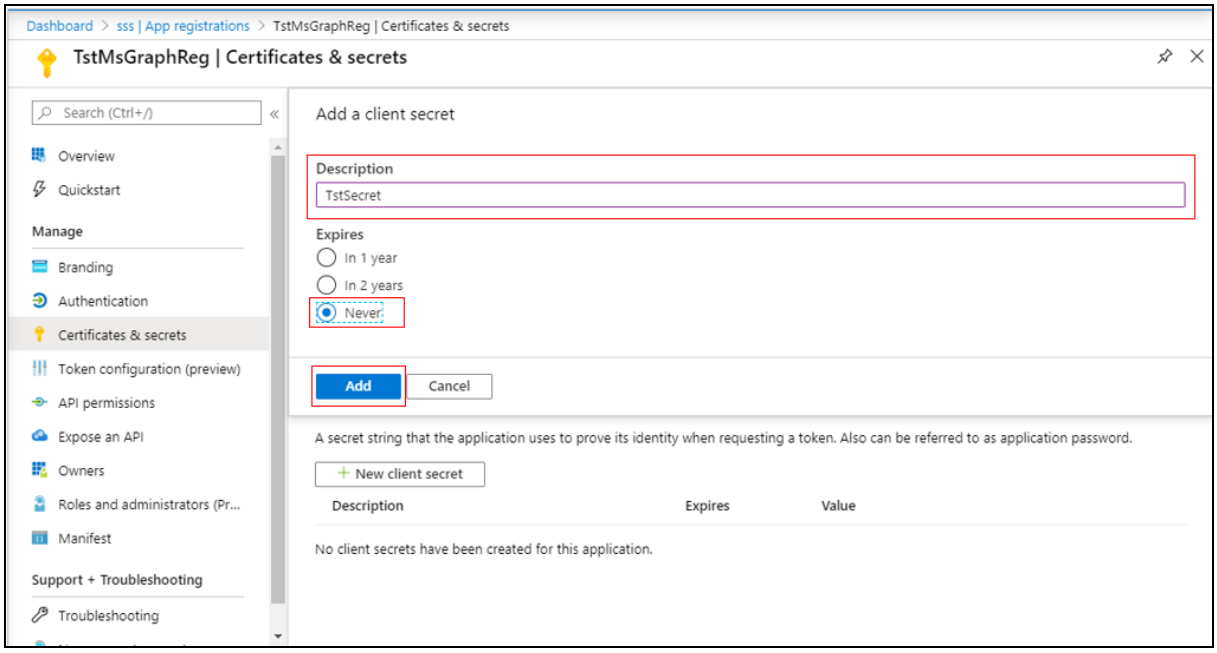


Figure 2.25: Creating a new secret for the Microsoft Graph App

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

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

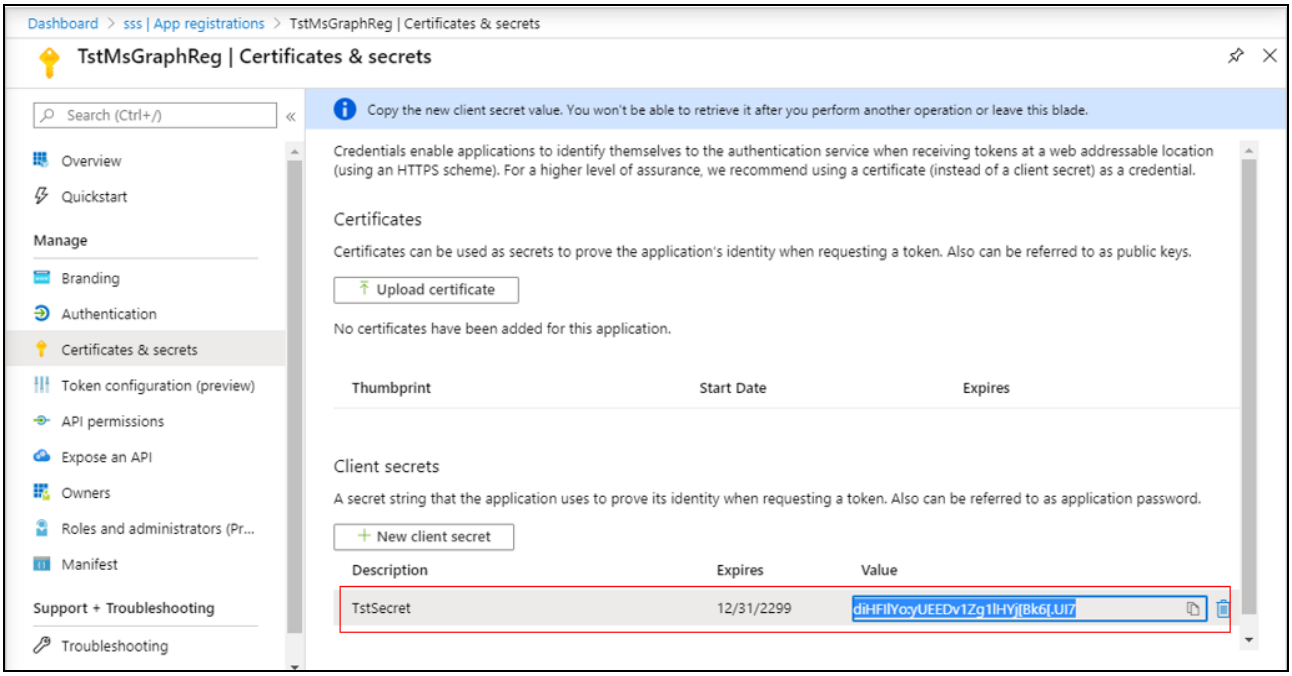


Figure 2.26: The key that is generated and assigned to the client secret of the Microsoft Graph app

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 2.26. This will invoke Figure 2.27. In the right panel of Figure 2.27, click on the **Add a permission** button.

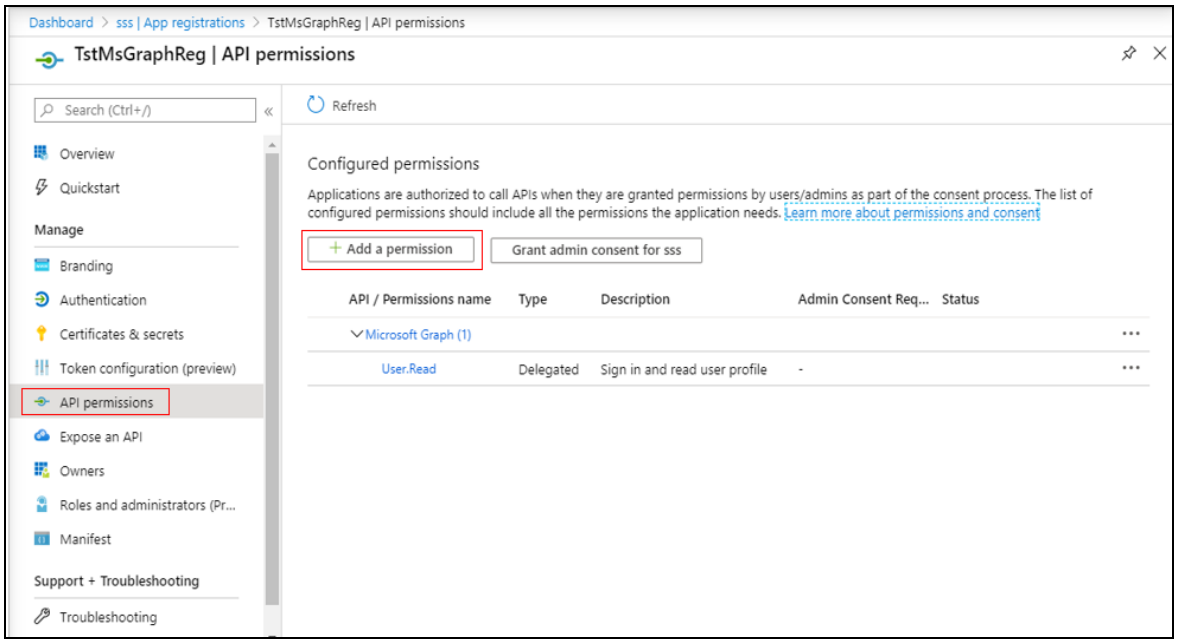


Figure 2.27: Clicking on the Add a permission button

10. Then, click on **Office 365 Management APIs** in the **Request API Permissions** window that appears (see Figure 2.28).

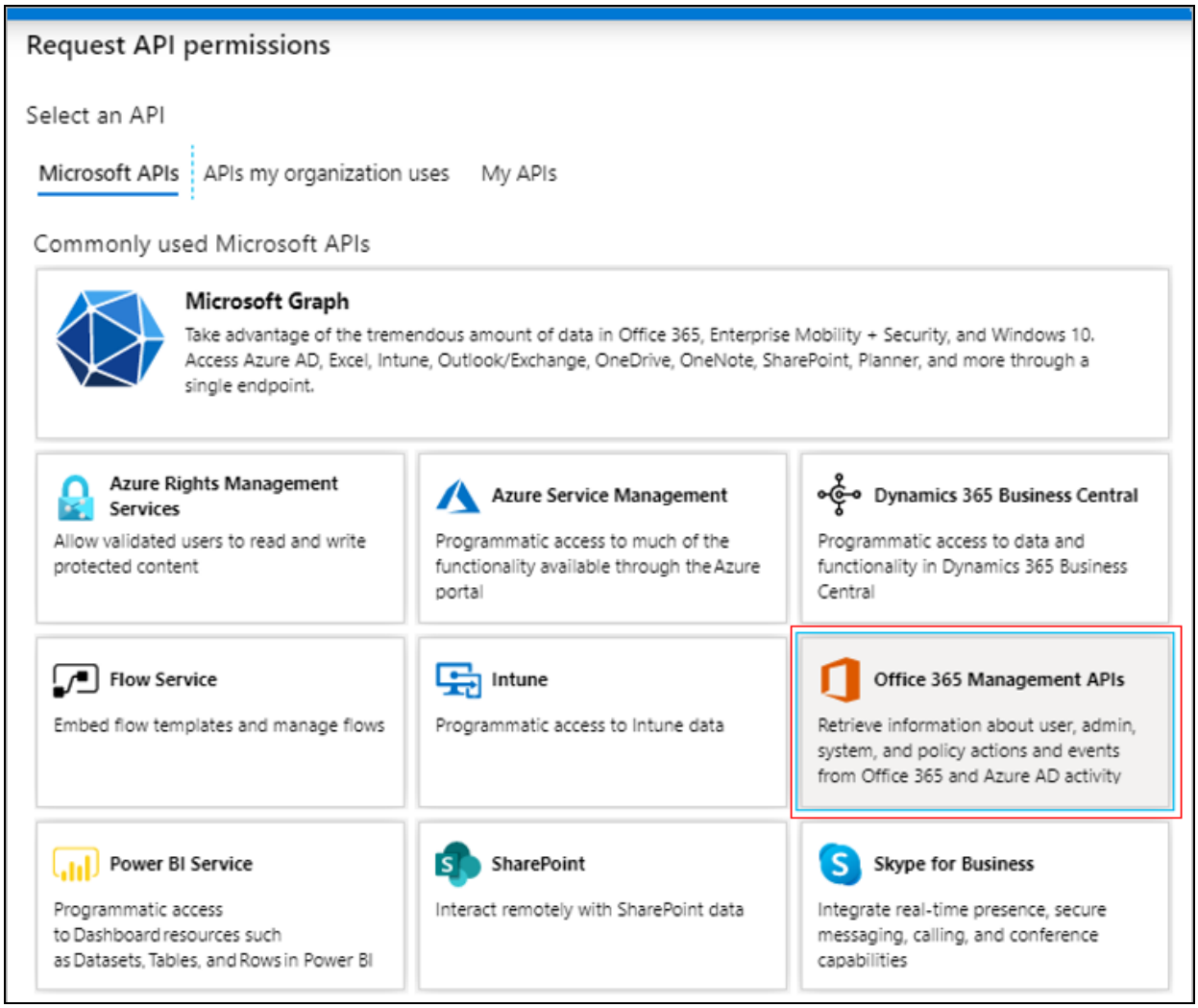


Figure 2.28: Selecting the Office 365 Management APIs option

11. When Figure 2.29 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.

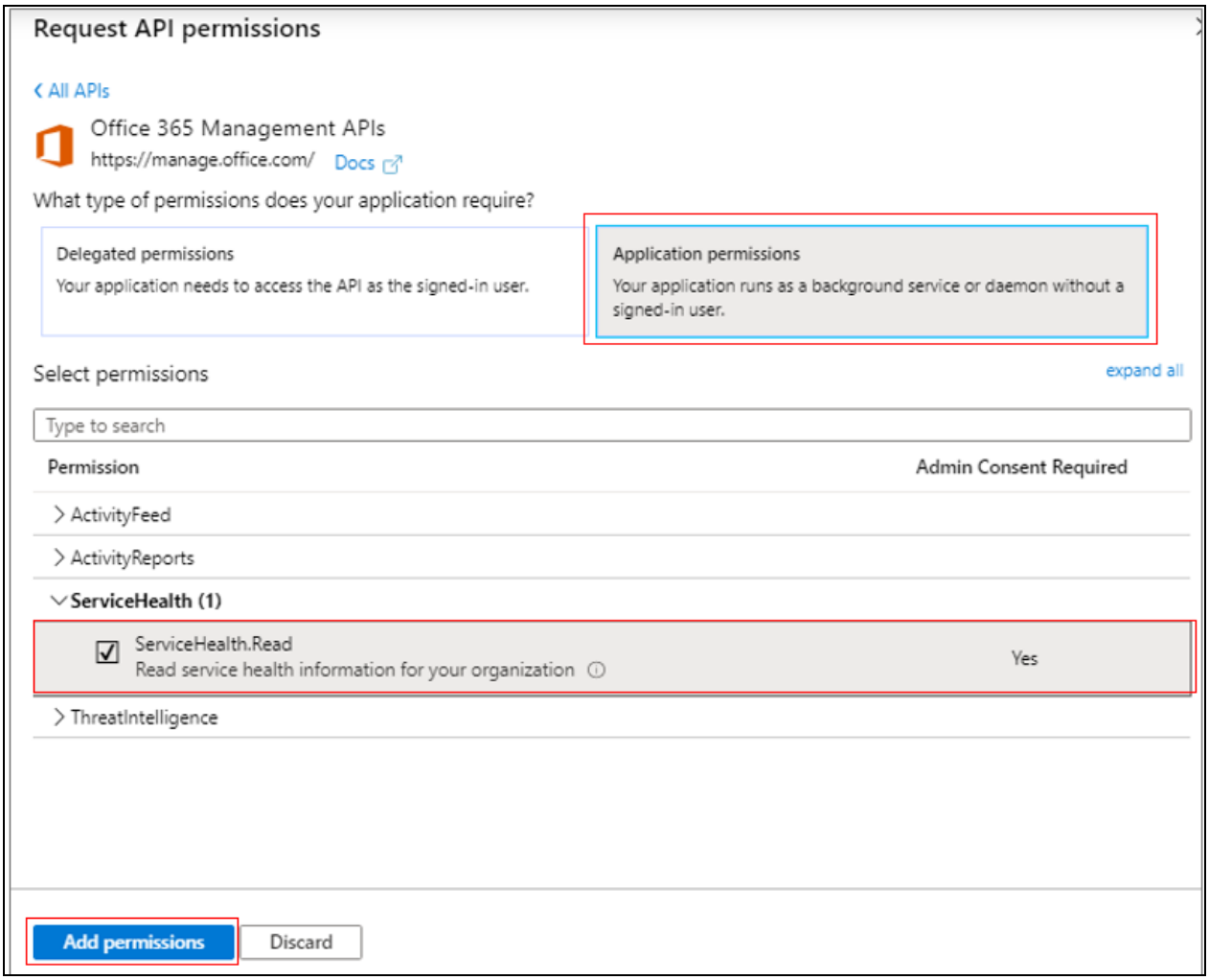


Figure 2.29: Granting permission to the Microsoft Graph app to read service health

12. When Figure 2.30 appears, click on the **Add a permission** button again.

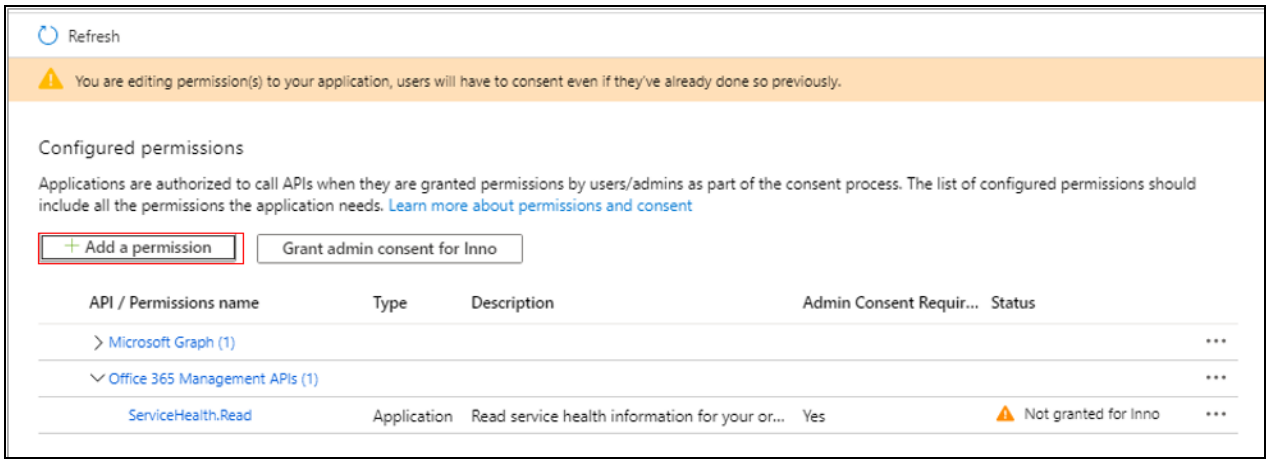


Figure 2.30: Clicking on the Add a permission button again to add permission to read from and write to user files

13. From Figure 2.31 that then appears, select the **SharePoint** option.

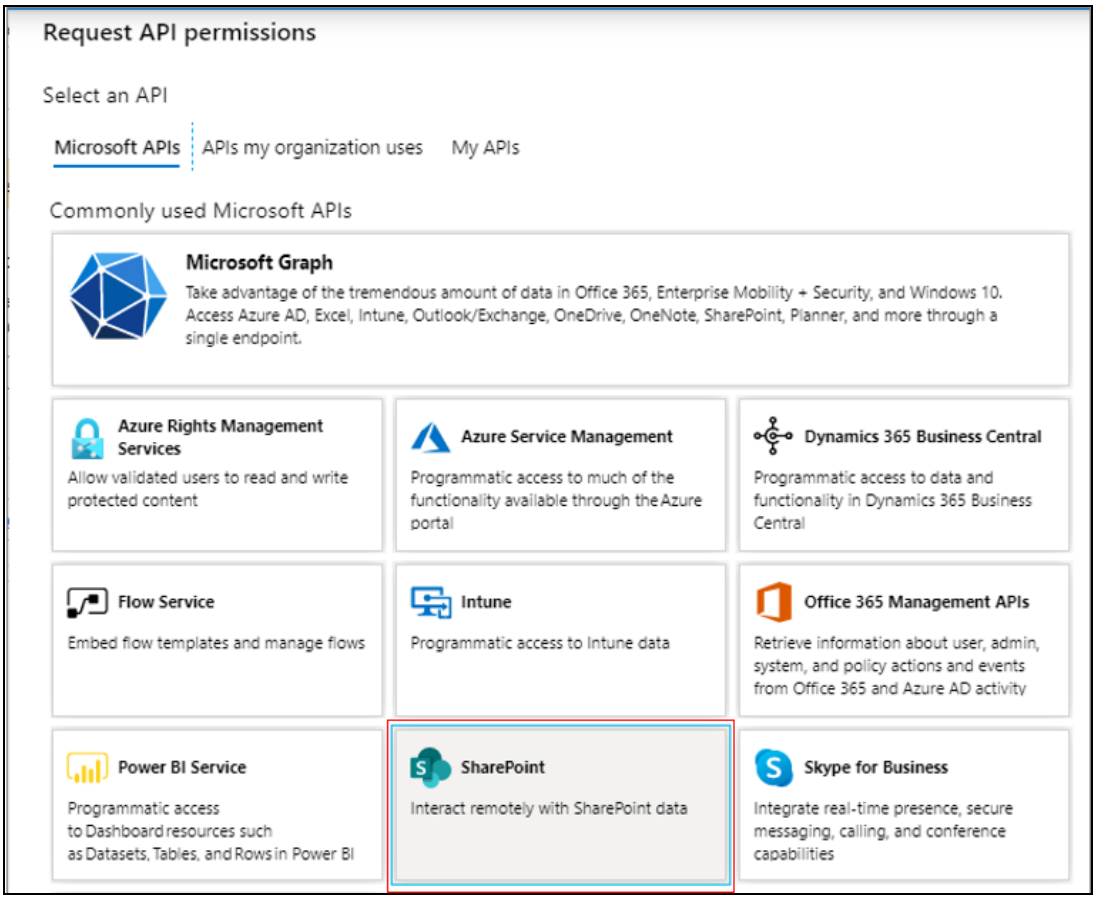


Figure 2.31: Selecting the SharePoint option

14. Then, select the **Delegated permissions** option from Figure 2.32, 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.

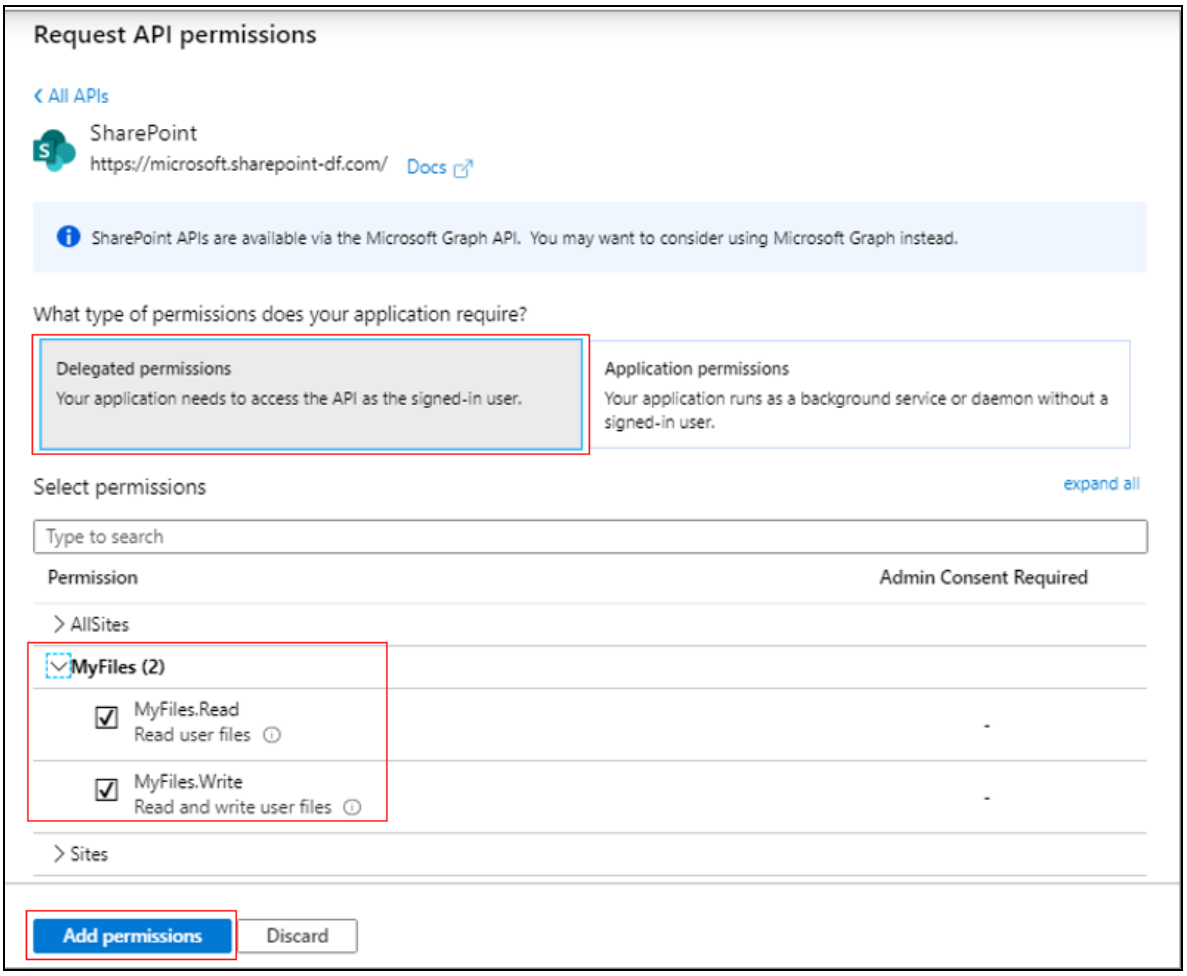


Figure 2.32: Granting permission to Microsoft Graph app to read from and write to user files

15. You will now return to Figure 2.30. Once again, click on the **Add a permission** button therein to grant another permission to Microsoft Graph. When Figure 2.31 appears, select the **SharePoint** option yet again. Next, as depicted by Figure 2.33, 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 2.33 to add the chosen permission to Microsoft Graph app.

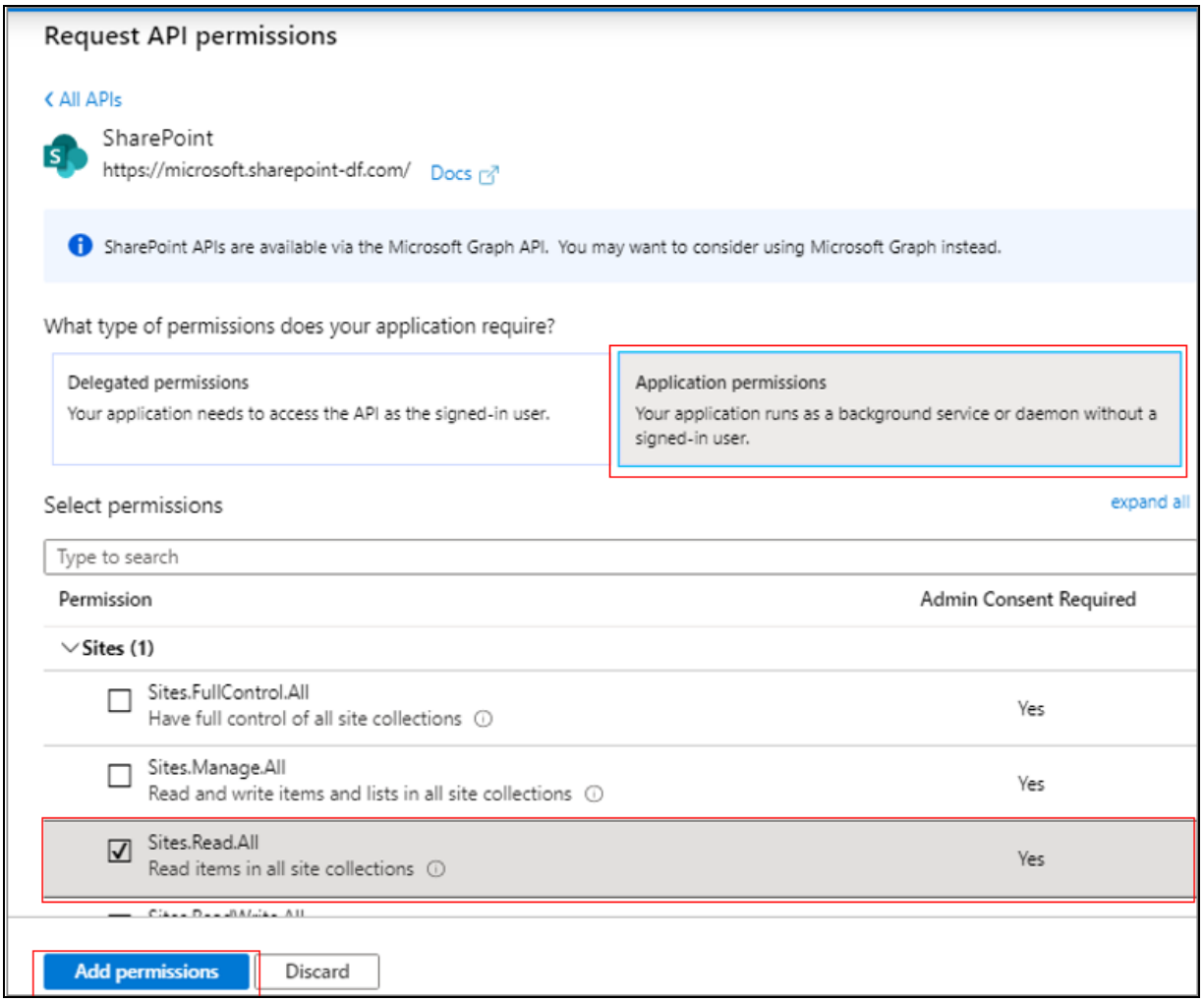


Figure 2.33: Granting permission to Microsoft Graph app to read items in all site collections

16. You will once again return to Figure 2.30. Click on the **Add a permission** button therein. When Figure 2.34 appears, select the **Azure Active Directory Graph** option.

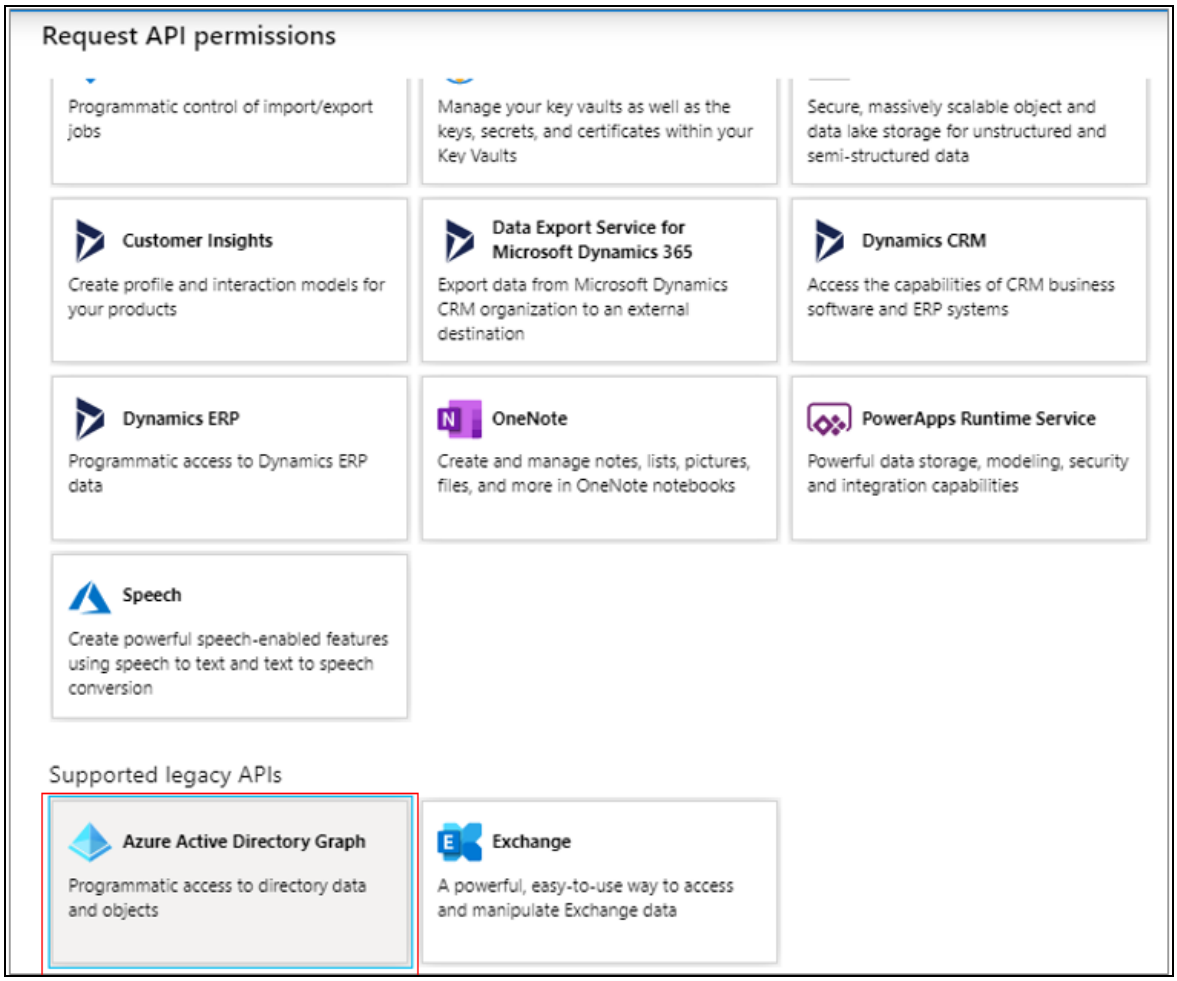


Figure 2.34: Selecting the Azure Active Directory Graph option

17. From Figure 2.35, 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.

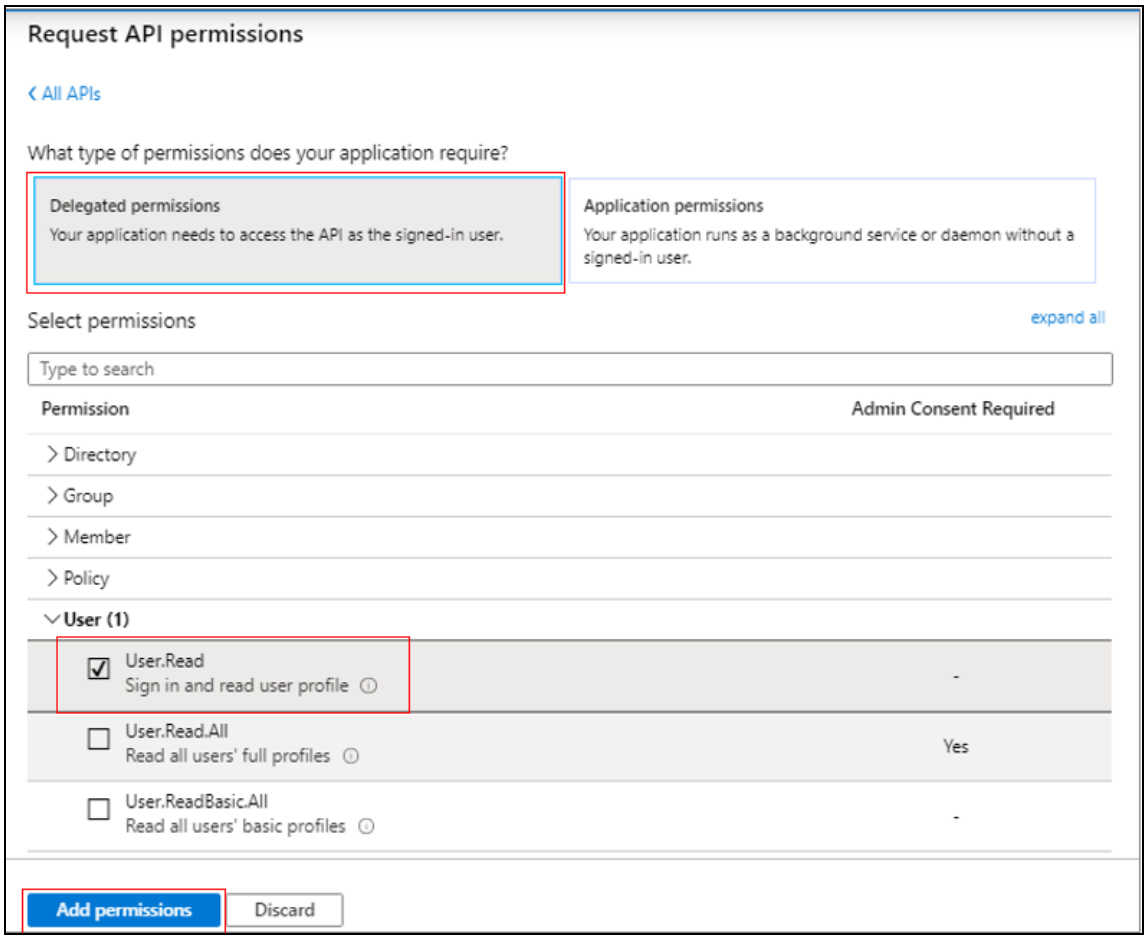


Figure 2.35: Granting the Microsoft Graph app permission to sign in and read user profile

18. As soon as you return to Figure 2.30, 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 2.31. Scroll down the list of APIs that appears until the **Microsoft Graph** API comes into view. Choose this API.

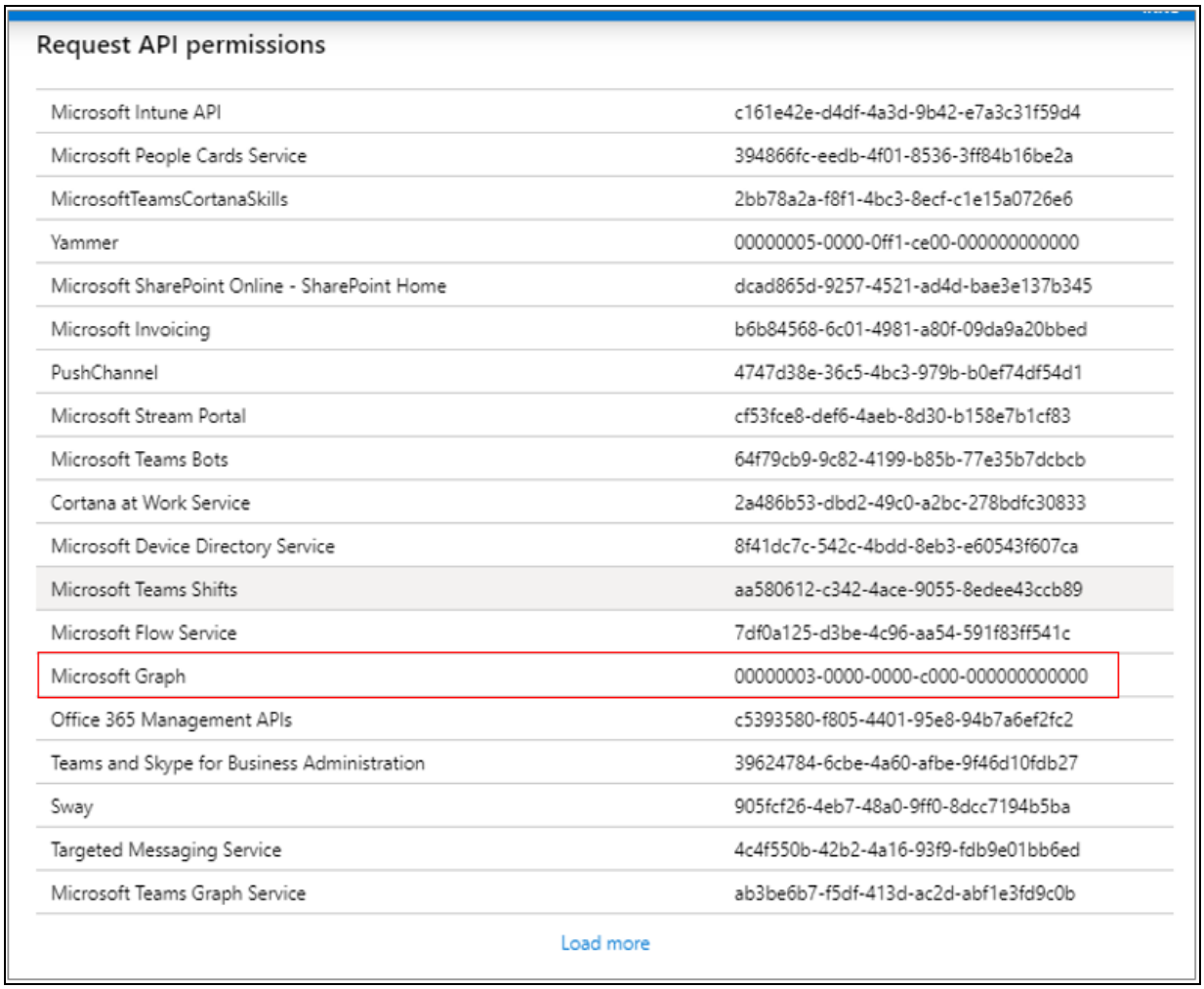


Figure 2.36: Choosing the Microsoft Graph API

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.

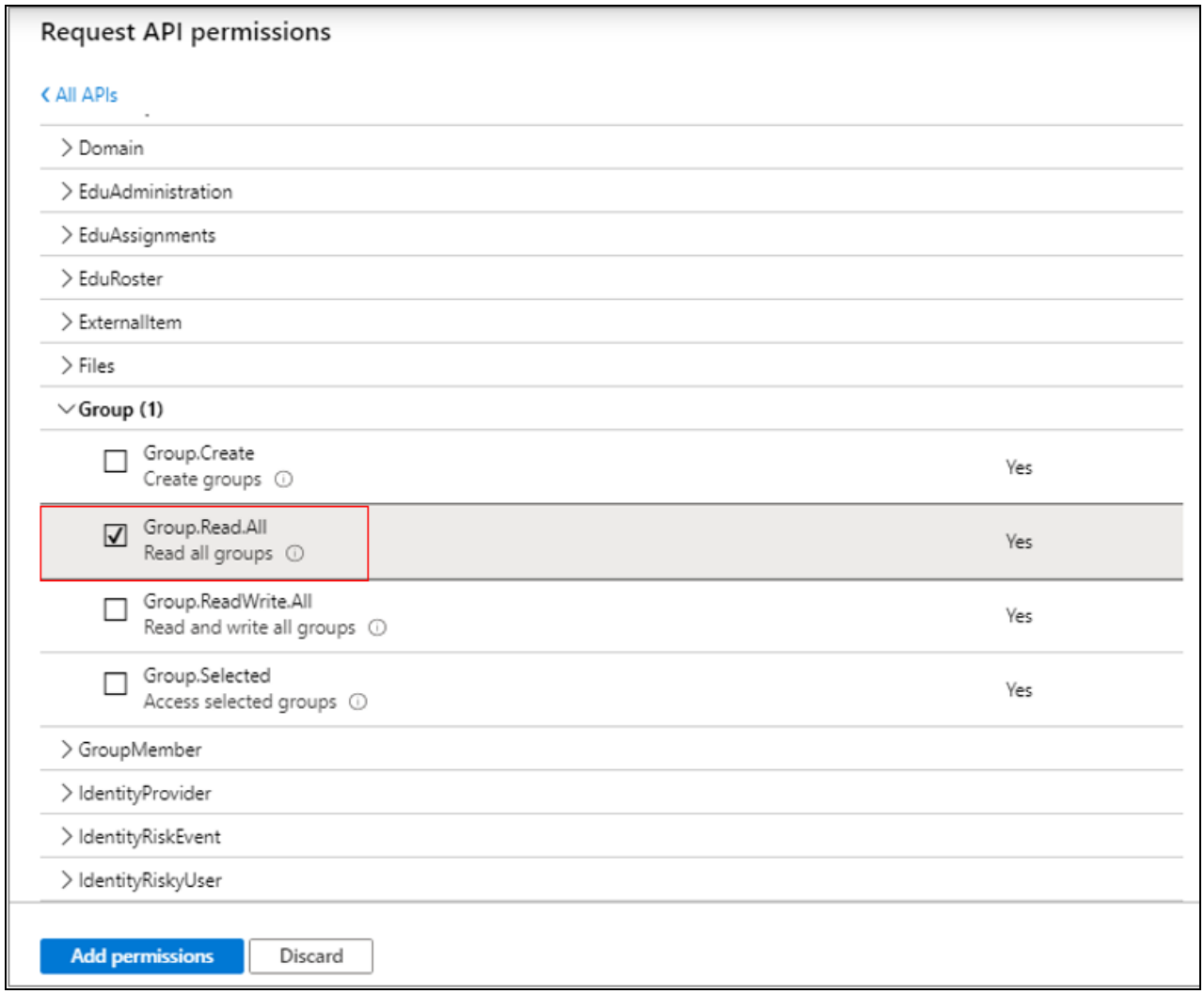


Figure 2.37: Granting the Microsoft Graph app permission to read all groups

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.

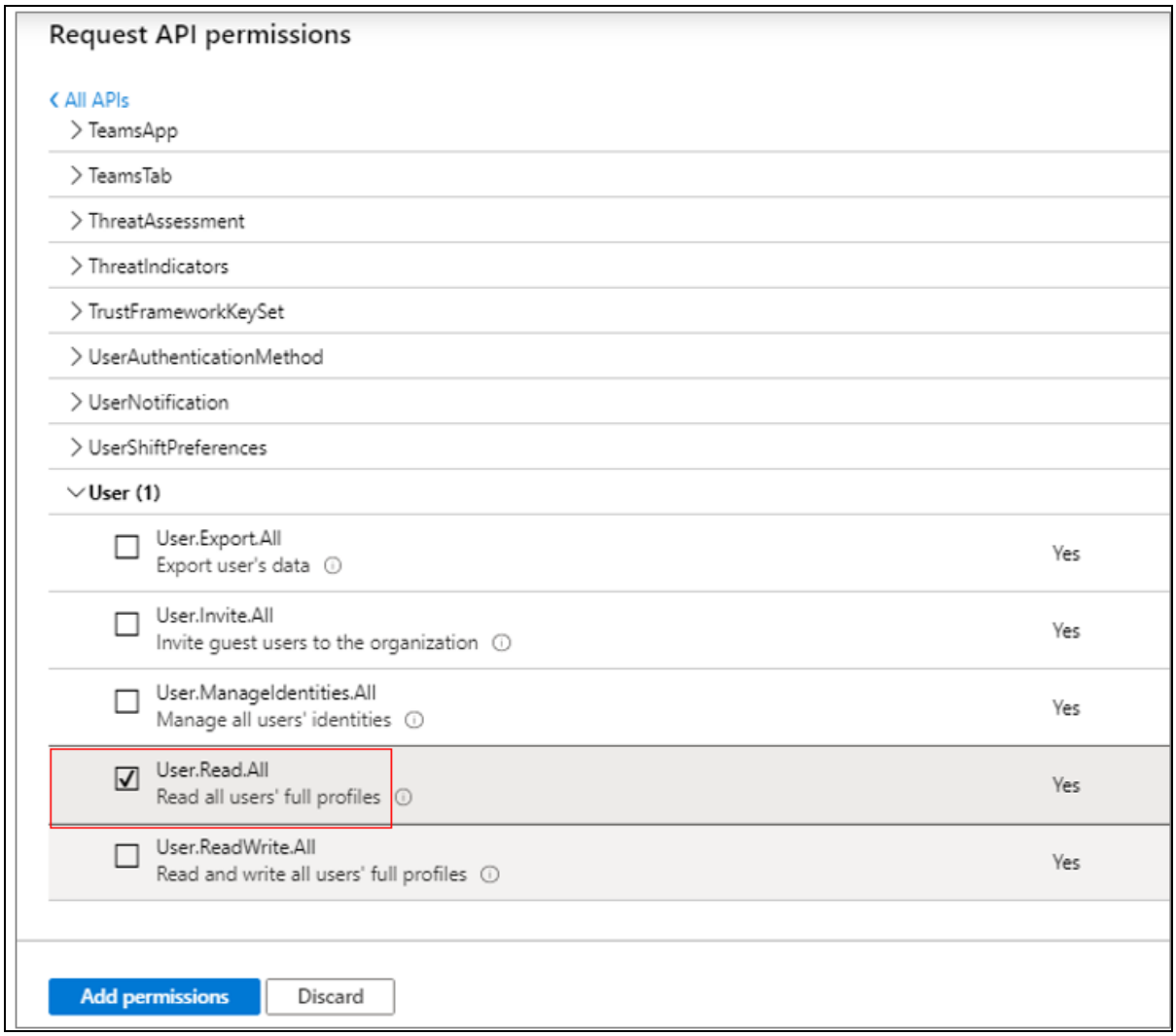


Figure 2.38: Granting the Microsoft Graph app permission to read full profile of all users

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.

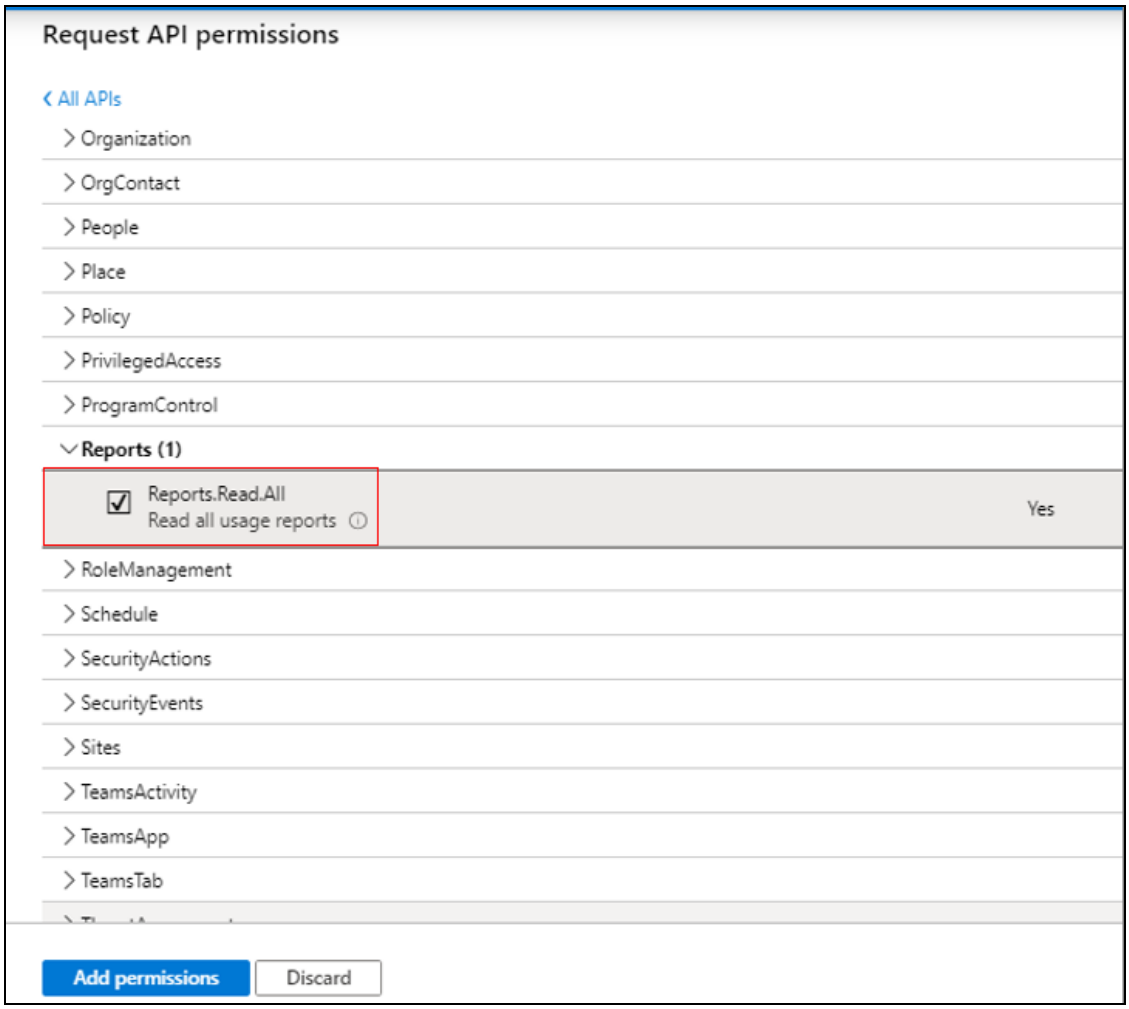


Figure 2.39: Granting permission to the Microsoft Graph app to read all usage reports

22. Finally, click the **Add permissions** button in Figure 2.39 to add all the chosen permissions to the Microsoft Graph app. When Figure 2.40 appears, click the **Grant admin consent for <user>** button therein to grant admin consent for the user.

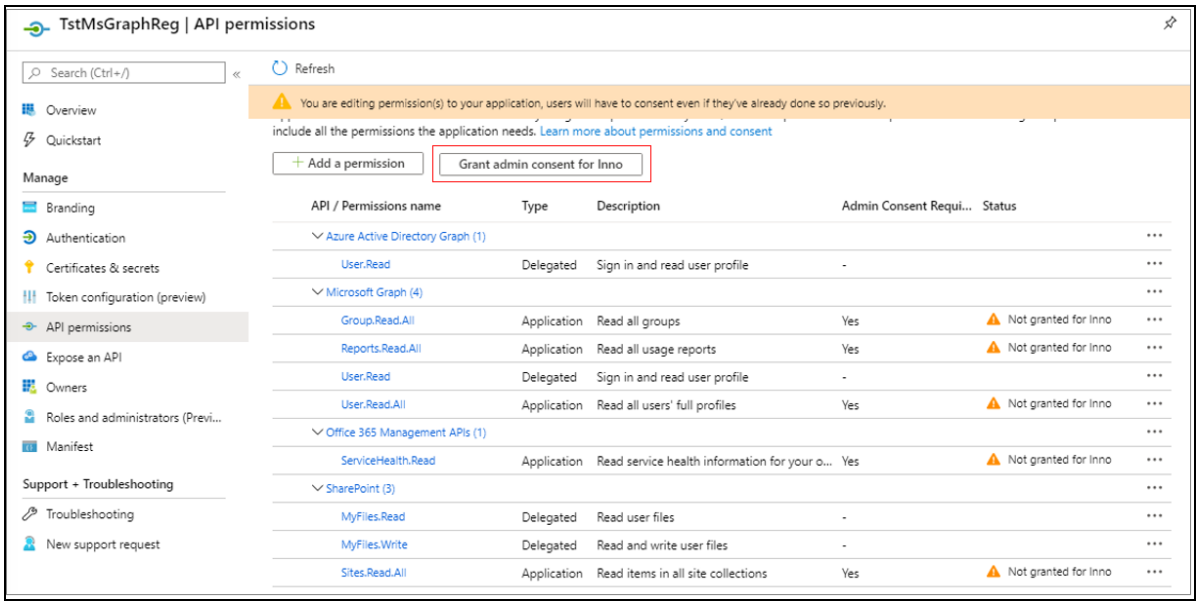


Figure 2.40: Granting admin consent to the user

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 2.41 will appear.

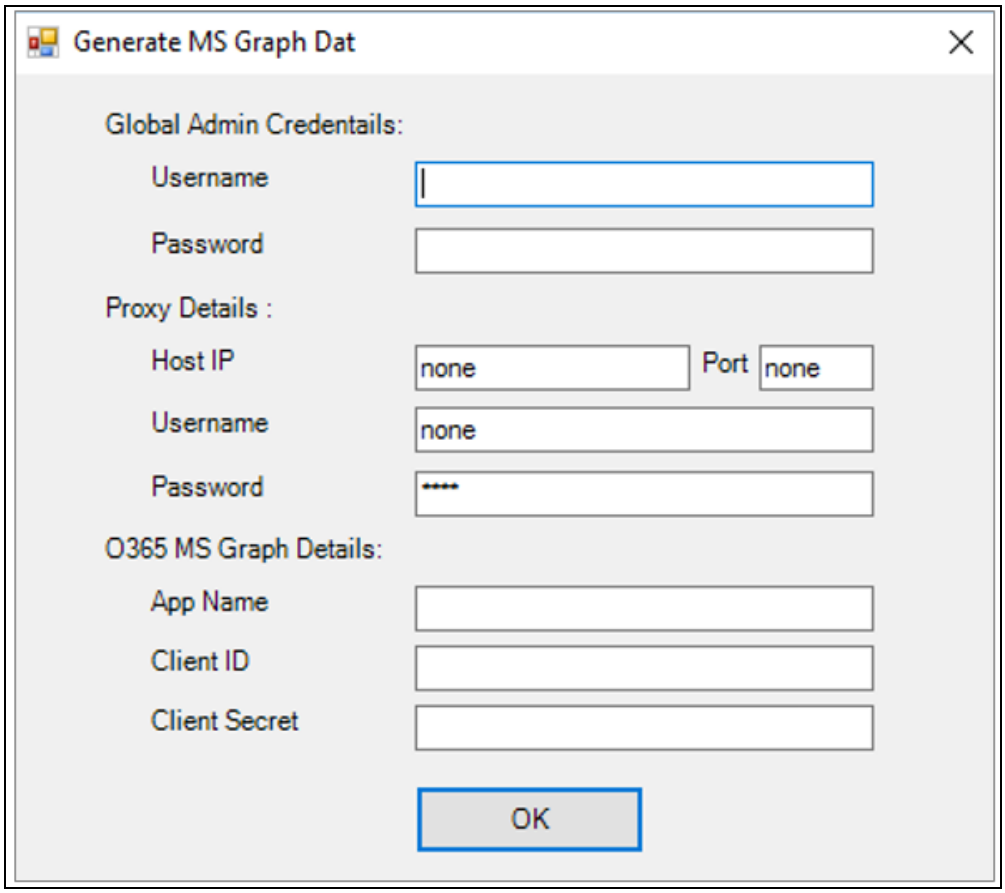


Figure 2.41: Generating MS Graph Dat

24. In Figure 2.41, 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 2.23). The **Client secret** should be the key that is generated and assigned to the client secret in step 8 above (see Figure 2.26). Finally, click the **OK** button.

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

2.1.3 Using Powershell Scripts to Fulfill Requirements for Monitoring Exchange Online

To ensure that pre-requisites 5, 6, and 7 discussed in Section **2.1** are fulfilled without a glitch, eG Enterprise provides proprietary 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 Exchange Online
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; • Creates 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 2.42 will appear.

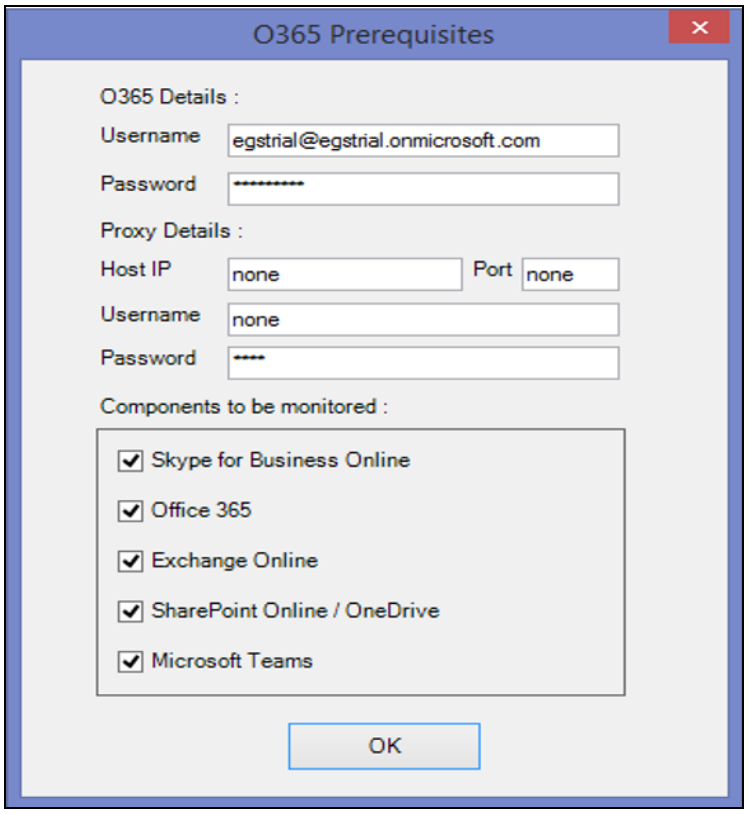


Figure 2.42: Selecting the components for which modules/packages should be automatically downloaded and installed

Specify the following in Figure 2.42:

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 2.42). 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 Exchange Online, select the **Exchange Online** check box.
5. Then, click the **OK** button. If the **Exchange Online** 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**;

If you run the **O365SetRolesAndpermissions.ps1** script from the <EG_AGENT_INSTALL_DIR>\lib directory, then the dialog box shown by Figure 2.43 will appear:

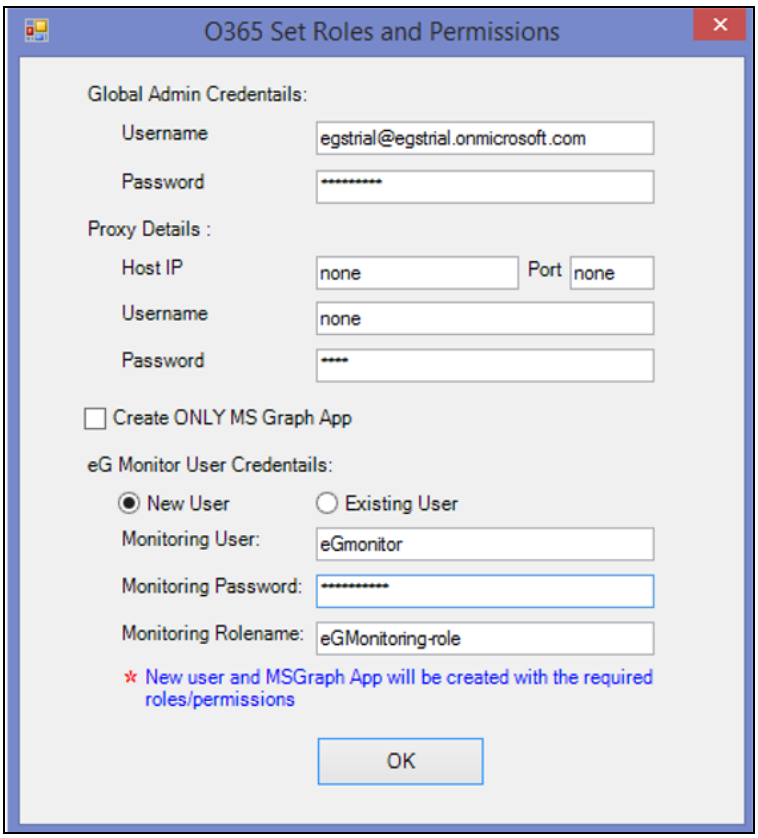


Figure 2.43: Automatically creating a new user with the required permissions

Specify the following in Figure 2.43:

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 2.43. 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 2.44). 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.

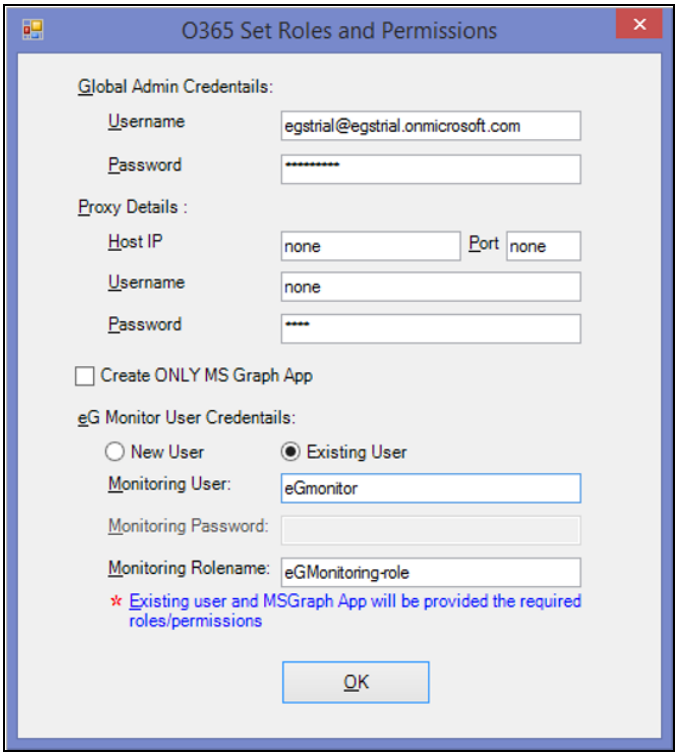


Figure 2.44: Using an existing user for monitoring purposes

6. Finally, click the **OK** button in Figure 2.44. 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 **Global reader**, **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions required for monitoring Exchange Online. 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 **Global reader**, **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions required for monitoring Exchange Online. 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 installed on Microsoft Azure Active Directory with all the required permissions.

7. If you already have an Office 365 user with the **Global reader**, **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** 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 2.45. Then, click the **OK** button.

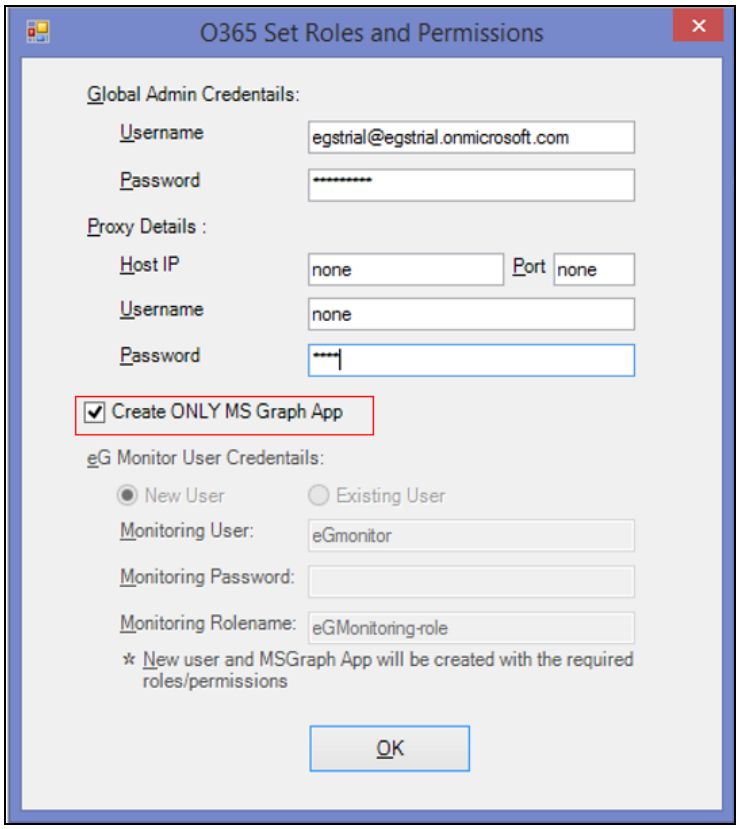


Figure 2.45: Choosing to only install the Microsoft Graph App

Chapter 3: How to Monitor Microsoft Exchange Online Using eG Enterprise?

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

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

Steps 1 and 2 above are discussed elaborately in the following topics:

Section **3.1**

Section **3.2**

3.1 Adding a Microsoft Exchange Online Component

eG Enterprise cannot auto-discover a Microsoft Exchange Online component. This is why, you need to manually add the component to the eG Enterprise system to monitor it. The steps for manually adding a Microsoft Exchange Online component 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 Exchange Online* as the **Component type** and click the **Add New Component** button.
4. Figure 3.1 will then appear.

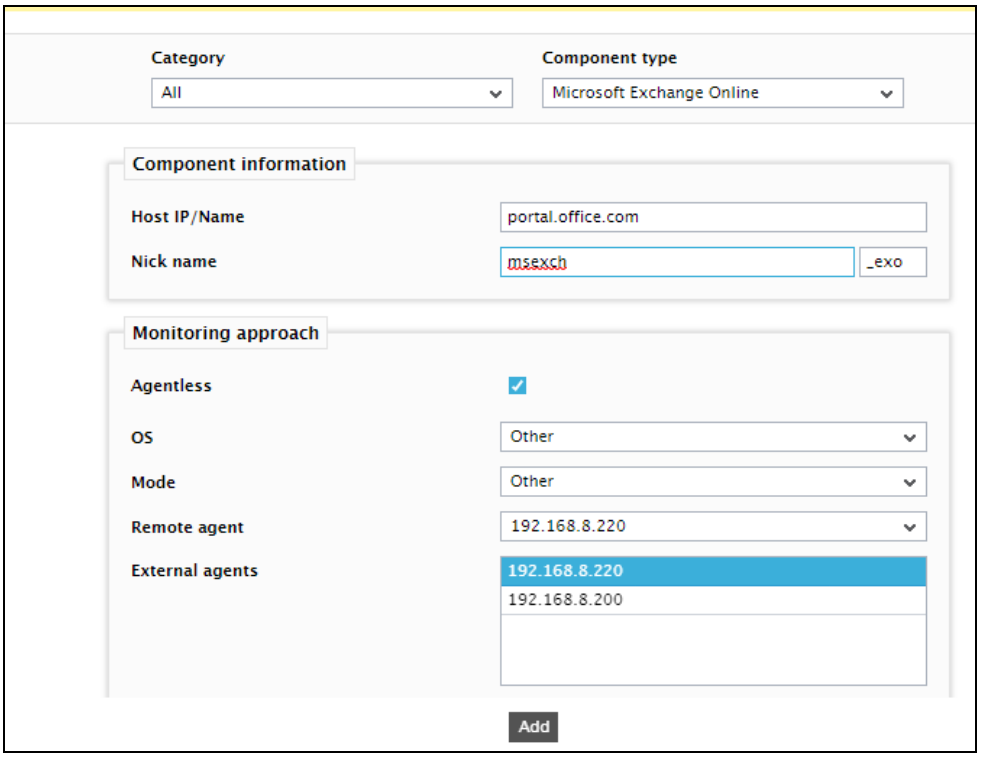


Figure 3.1: Adding a Microsoft Exchange Online component

5. In Figure 3.1, by default, portal.office.com will be displayed as the **Host IP/Name** of the target Microsoft Exchange Online component. If the host name of the Exchange Online component you want to monitor is different in your environment, then modify this specification.
6. Provide a unique **Nick Name** for the Exchange Online component being added. Note that any nick name you specify here will be automatically suffixed with the string, *_exo*.
7. Since Exchange Online 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 Exchange Online 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, Office 365, Skype for Business Online, Microsoft Teams, and/or a Microsoft OneDrive for Business component, when adding an Exchange Online component. This is why, when clicking the **Add** button in Figure 3.1, you will be immediately prompted to manage the above-mentioned component using the same nick name as the Exchange Online 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 Exchange

Online, then click **OK** without selecting any of the check boxes.

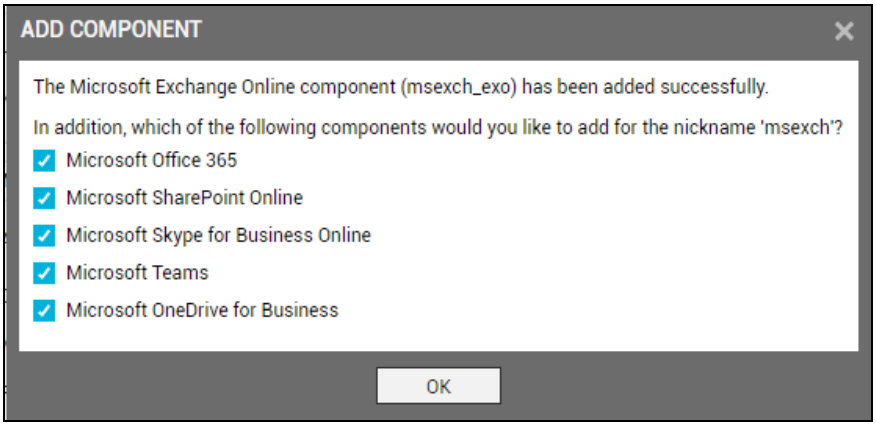


Figure 3.2: A message prompting you to add other Office 365 components

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 SharePoint Online 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 Exchange Online Component

After adding a Microsoft Exchange Online 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 Exchange Online component.

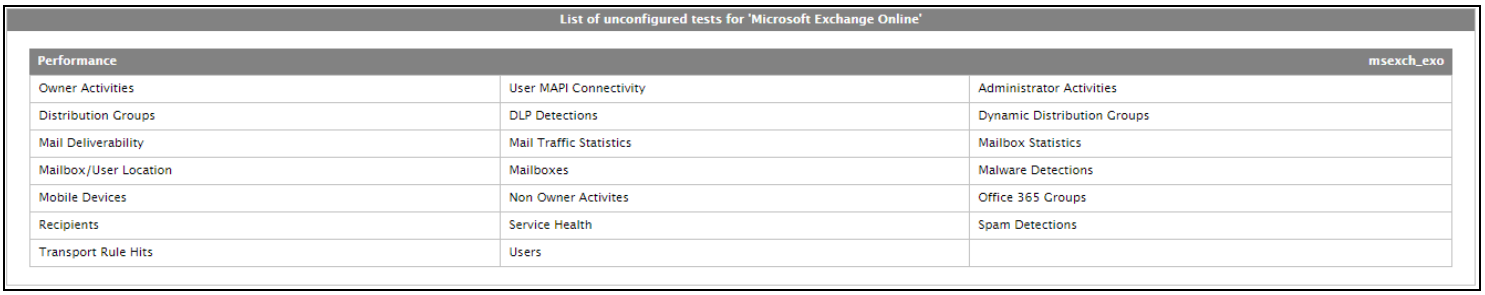


Figure 3.3: List of tests to be manually configured for Microsoft Exchange Online

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

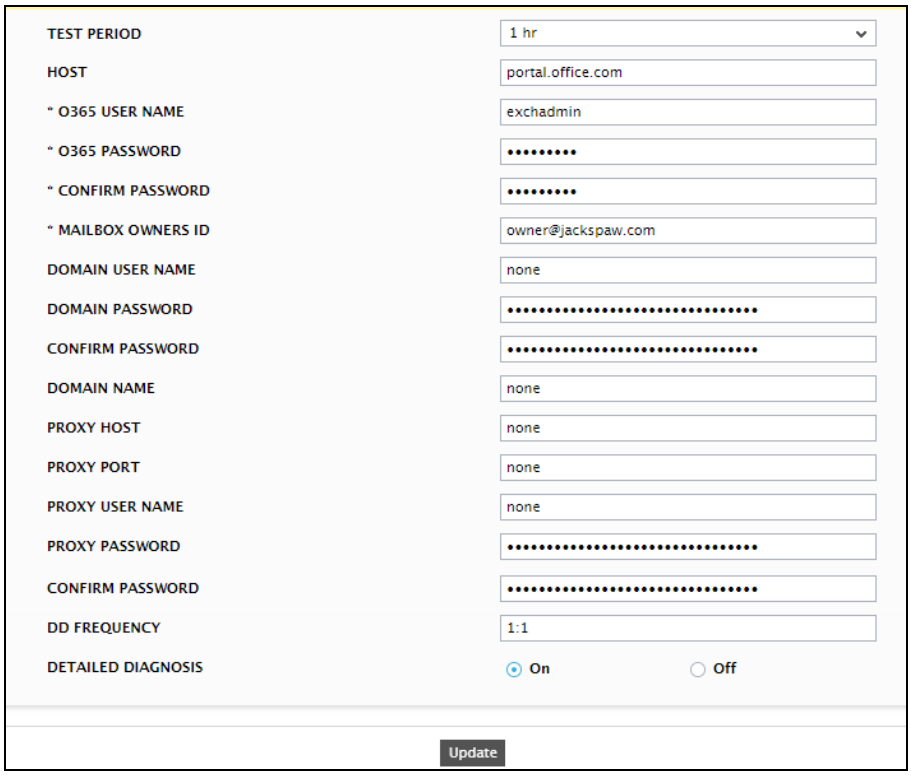


Figure 3.4: Configuring the Owner Activities test

This test helps administrators audit the activities of specific mailbox owners. To know what parameters this test takes and how to configure it, refer to the Section **4.6.3** topic. Once the test is configured, click the **Update** button in Figure 3.4 to save the test configuration. Once again, try to sign out of the eG admin interface.

You will now be prompted to configure the User MAPI Connectivity test (see Figure 3.5).

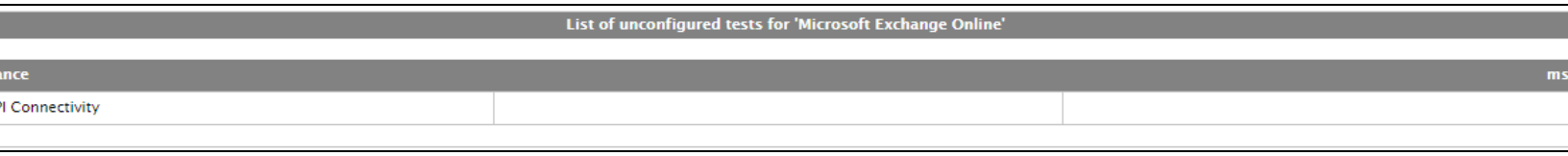


Figure 3.5: A message prompting you to configure the User MAPI Connectivity test

This test emulates a user attempting to login to his/her mailbox and retrieving a list of items in the Inbox. In the process, the test reports whether/not MAPI connectivity to that mailbox is available. If the MAPI connectivity is available, then the measure additionally reports how much time it took for the user to connect to that mailbox. This way, the test promptly alerts administrators to the unavailability of MAPI connectivity and latencies in MAPI connection to a configured user mailbox.

Click on the test inFigure 3.5 to configure it. Figure 3.6 will then appear.

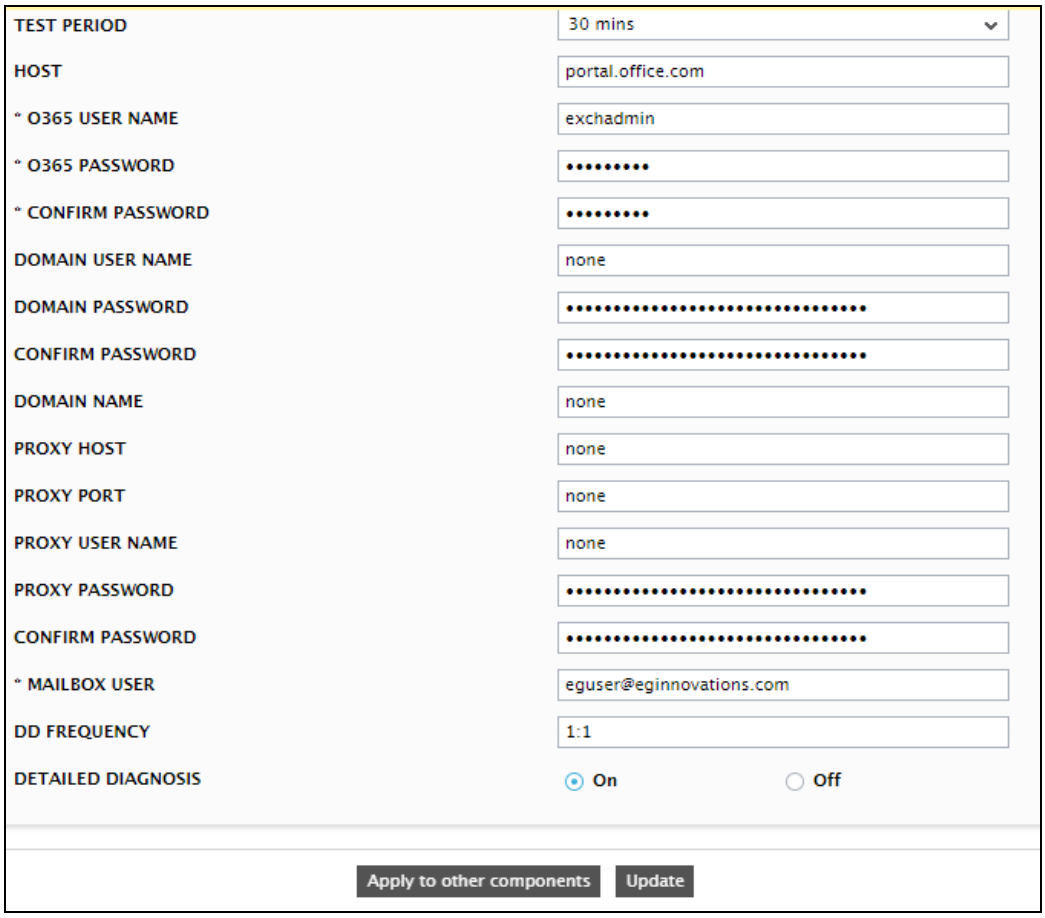


Figure 3.6: Configuring the User MAPI Connectivity test

Refer to the Section **4.7.3** topic to know how to configure this test. Once the test is configured, click the **Update** button to save the changes. Finally, sign out of the eG admin interface.

Chapter 4: Monitoring Microsoft Exchange Online

To monitor the managed Microsoft Exchange Online component, 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 Exchange Online* 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 Exchange Online (see Figure 4.1).

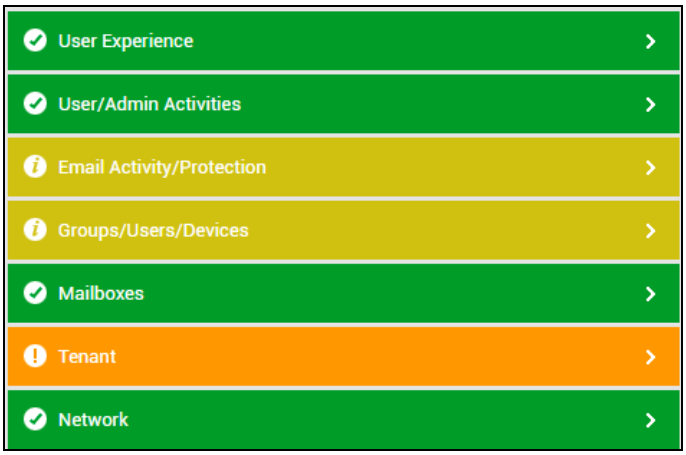


Figure 4.1: Layer model for the Microsoft Exchange Online component

Each layer of Figure 4.1 is mapped to tests that report on a wide variety of KPIs such as availability, mailbox usage, email activity, mailbox protection, and user activities of Exchange Online. Using these metrics, administrators can find quick and accurate answers to the following performance queries:

- Is Exchange Online available over the network? If so, how quickly is it responding to network requests?
- Is Exchange Online available for sending/receiving mails? If so, how quickly is Exchange Online able to send/receive mails?
- Were any email delivery failures captured? Which emails could not be delivered?
- Are too many messages pending delivery? Which mails are still to be delivered?

- Has any sudden and significant increase been noticed in the number and size of incoming mails? If so, which user has received the maximum number of mails? Which user has received mails of large sizes?
- Has any sudden and significant increase been noticed in the number and size of outgoing mails? If so, which user has sent the maximum number of mails? Which user has sent mails of large sizes?
- Is MAPI connectivity available to user mailboxes available? If so, then how long does the MAPI connection typically take? Has any latency been noticed in MAPI connections?
- Is the total size of mailboxes on Exchange Online growing abnormally? If so, which mailboxes are contributing to this growth?
- Has any mailbox's size reached the 'Prohibit send/receive' limit? If so, which one?
- Were any mailboxes soft-deleted recently? If so, which ones?
- Which mailboxes have been enabled for forwarding mails to external users?
- Which datacenter has the maximum number of mailboxes? From which geography do most mailbox users come?
- Were any DLP rules violated? If so, which rules were violated? Which DLP policy includes such rules? Which emails that violated the rules?
- Was any malware captured in incoming/outgoing mails?
- Who are the top receivers and senders of malware, in terms of the number of malware-infected mails sent/received and the malware size?
- Are too many spam mails being received/sent? Who are the top senders/receivers of spam mails, in terms of the number of spam mails sent/received and the size of spam mails?
- Do any emails match a transport rule? If so, which ones?
- Are there any users whose password is about to expire? If so, who are they?
- Who are the most inactive users of Exchange Online?
- Did any Exchange Online administrator make any configuration changes to Exchange Online recently? If so, who made what change when?
- Were any configuration changes made by mailbox owners? If so, who made what change when?

This chaptertopic will elaborate on each layer of Figure 1, the tests mapped to it, and the measures it reports, using the following sub-topics.

Section **4.1**

Section **4.2**

Section **4.3**

Section **4.4**

Section **4.5**

Section **4.6**

Section **4.7**

4.1 The Network Layer

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

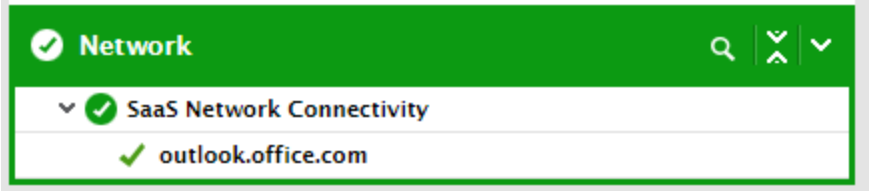


Figure 4.2: The test mapped to the Network layer

4.1.1 SaaS Network Connectivity Test

If your Exchange Online users complain of inaccessibility, you may want to check the quality of the network link to the Exchange server online. A flaky or latent network connection to the server can sometimes deny users access to their mailboxes on the cloud, adversely impacting their overall experience with Exchange Online. To avoid this, periodically run the SaaS Network Connectivity test, and check the health of the network connection to the Exchange server on the cloud.

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

Target of the test : Exchange Online

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Exchange server on the cloud

Configurable parameters for the test

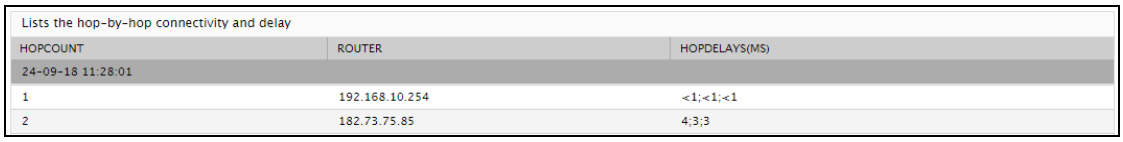
Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured. By default, this is portal.office.com
Packet Size	The size of packets used for the test (in bytes)
Packet Count	The number of packets to be transmitted during the test
Timeout	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 outlook.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 • 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	Seconds	An increase in network latency could result from misconfiguration of the

Measurement	Description	Measurement Unit	Interpretation
	transmission of packet to the server and receipt of the response to the packet at the source.		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 serverl.	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 server 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 server, 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 target server is available or not	Percent	A value of 100 indicates that the server is connected over the network. The value 0 indicates that the server is not connected. Typically, the value 100 corresponds to a *Packet loss* of 0.

The detailed diagnosis of the *Packet loss* measure provides a listing of routers that are on the path from the external agent to target server, and the delays on each hop. This information can be used to diagnose the hop(s) that could be causing excessive packet loss/delays.



Lists the hop-by-hop connectivity and delay

HOPCOUNT	ROUTER	HOPDELAYS(MS)
24-09-18 11:28:01		
1	192.168.10.254	<1;<1;<1
2	182.73.75.85	4;3;3

Figure 4.3: The detailed diagnosis of the Packet loss measure

4.2 The Tenant Layer

With the help of the tests mapped to this layer, you can:

- Quickly determine the health of the Exchange Online service;
- Verify the availability and responsiveness of Exchange Online over HTTP/S;
- Detect issues in MAPI connectivity to a user mailbox

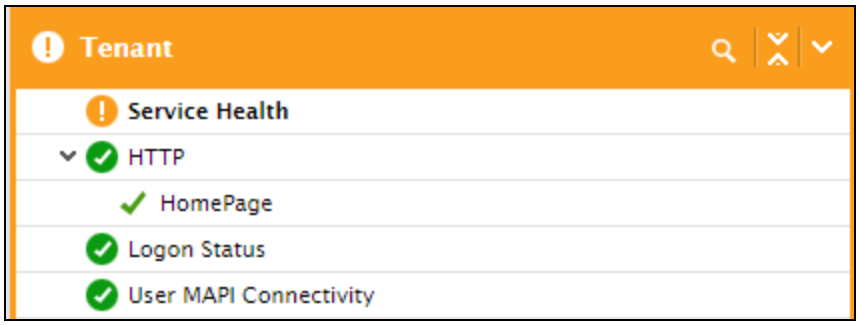


Figure 4.4: The tests mapped to the Tenant layer

4.2.1 Service Health Test

To ensure the high uptime and peak performance of Exchange Online, administrators should be able to detect issues in the Exchange Online service much before users complain. The Service Health test helps administrators with this! This test reports the status of the Exchange Online service in real-time, thus proactively alerting administrators to a service degradation. The test additionally reveals if any service incidents are occurring, and elaborately describes such incidents vide detailed diagnostics. If Exchange Online has been stopped as part of a planned maintenance activity, then this test indicates the same by reporting the count of maintenance events associated with Exchange Online.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-**

Parameters	Description
	Only Recipients, Mail Recipients, and **Mail Import Export** permissions. 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 **2.1.1**.
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 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 the Exchange Online 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

Measurement	Description	Measurement Unit	Interpretation
			status of the service. In the graph of this measure however, the same is indicated using the numeric equivalents only. You can use
Service incidents	Indicates the number of service incidents that are currently occurring.	Number	Unplanned service incidents occur when Exchange Online 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.	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
04-09-18 12:52:03							
EX146811	EX146811	19950656	Exchange Online	8/20/2018 7:11:18 PM	-	8/31/2018 10:01:16 PM	title: security and compliance port
EX147321	EX147321	11560362	Exchange Online	8/18/2018 7:00:00 AM	-	9/3/2018 7:11:11 PM	title: sent emails not saving in sha

Figure 4.5: The detailed diagnosis of the Service incidents measure

4.3 The Mailboxes Layer

This layer focuses on mailbox health. Tests mapped to this layer proactively alert administrators to the over-utilization of user mailboxes, archive mailboxes, and clutter enabled mailboxes. With the help of these tests, administrators can also audit the creation, modification, and deletion of mailboxes. The location of mailboxes and users can also be determined. Additionally, the tests also

reveal the recipient types supported by the Exchange Online organization and the count of recipients of each type.

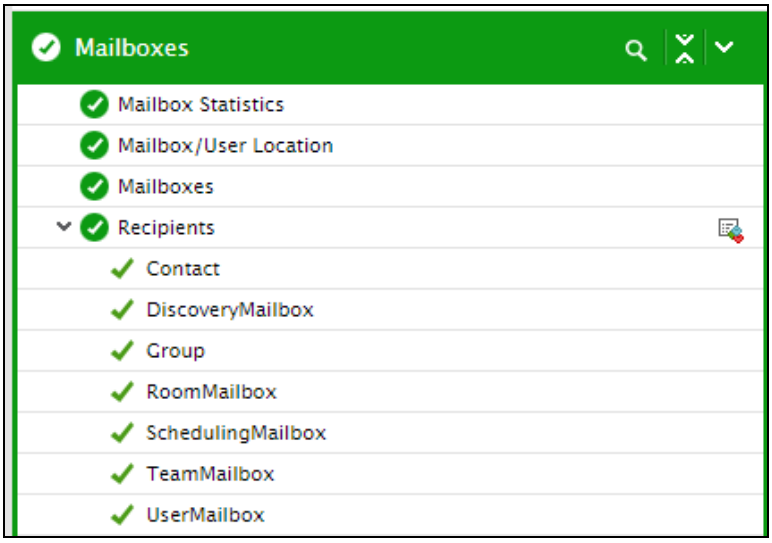


Figure 4.6: The tests mapped to the Mailboxes layer

4.3.1 Mailbox Statistics Test

Typically, the amount of mailbox storage available is determined by the mailbox type and the user's subscription license. For instance, if a user has subscribed to Office 365 Enterprise E1, then the maximum storage available to the user mailbox is 50 GB and archive mailboxes is 50 GB. On the other hand, if a user has subscribed to Office 365 Enterprise E3, then the maximum storage available to the user mailbox is 100 GB and archive mailboxes is Unlimited.

Depending upon how every type of mailbox is used, administrators can reduce the size of the mailbox either per user or globally.

If for instance, a user mailbox runs out of storage space, then that mailbox will not be able to accept any more emails. To avoid this, administrators can configure Exchange Online to send out different types of notifications, namely - Warning, Prohibit Send, and Prohibit Send/Receive - to users, depending upon the usage of their mailbox and how soon its storage space will be exhausted. Such notifications prompt users to clear up storage space, so that they can continue using their mailboxes without any interruption.

Besides the individual users, administrators also need to keep tabs on how the users use the different mailboxes - eg., user mailboxes, archive mailboxes, clutter enabled mailboxes, etc. This will help administrators capture a potential storage space crunch much before it actually occurs and

affects user productivity. Also, this may enable administrators rapidly identify users who are over-utilizing the storage space available to them. Administrators can in fact alert such users, even before Exchange Online sends out notifications! This is exactly what the Mailbox Statistics test helps administrators perform!

This test monitors the usage of the user mailboxes, and proactively alerts administrators if these mailboxes exhibit abnormal growth trends. Detailed diagnostics of this test lead administrators to those users with large-sized mailboxes, thus enabling them to accurately identify which user is over-utilizing the storage space available to them, so that they can warn such users of the impending space contention and urge them to take appropriate action. Additionally, the test also alerts administrators whenever Warning, Prohibit Send, or Prohibit Send/Receive notifications are sent out to any user. Detailed diagnostics provided by the test pinpoint the users who have received such notifications, so that administrators can intervene and ensure that such users quickly clear up storage space and do not cause mail traffic to be blocked. The usage of archive, inactive, and clutter enabled mailboxes are also monitored and administrators alerted if such mailboxes show signs of over-utilization.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
Domain, Domain	**These parameters are applicable only if the eG agent needs to communicate**

Parameters	Description
User Name, Domain Password, and Confirm Password	**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 every second 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
Total mailbox size	Indicates the total mailbox size across all user mailboxes.	Number	Use the detailed diagnosis of this measure to view the top-10 users, in terms of their mailbox size.
Mailboxes growth rate	Indicates the percentage growth in mailbox size.	Percent	This measure is computed using the following formula: *[{Total mailbox size in the current measurement period (-) Total mailbox size in the last measurement period} / Total mailbox size in the last measurement period]*100* If the value of this measure is increasing consistently and is rapidly approaching 100%, it is a clear indication that one/more users are over-utilizing their mailbox storage. To know who those users are, use the detailed diagnosis of the *Total mailbox size* measure. This will point you to the top-10 users with large-sized mailboxes.
Mailboxes exceeding warning quota	Indicates the number of user mailboxes, the storage space of which has been consumed beyond the Warning limit configured.	Number	A user receives a Warning notification by email if his/her mailbox is approaching the maximum size limit. This warning is intended to encourage users to delete unwanted mail. To know which users' mailboxes are about to run out of storage space soon, use the detailed diagnosis of this measure. THe current size of each mailbox and the Warning quota set for

Measurement	Description	Measurement Unit	Interpretation
			that mailbox is also displayed, so that administrators can understand how soon each mailbox will be running out of space.
Inactive mailboxes	Indicates the number of inactive mailboxes.	Number	When an employee leaves your organization (or goes on an extended leave of absence), you can remove their Office 365 account. The employee's mailbox data is retained for 30 days after the account is removed. During this period, you can still recover the mailbox data by undeleting the account. After 30 days, the data is permanently removed. But if your organization needs to retain mailbox content for former employees, you can turn the mailbox into an inactive mailbox by placing the mailbox on Litigation Hold or applying an Office 365 retention policy to the mailbox in the Office 365 Security & Compliance Center and then removing the corresponding Office 365 account. The contents of an inactive mailbox are retained for the duration of the Litigation Hold placed on the mailbox or the retention period of the Office 365 retention policy applied to it before the mailbox was deleted. You can still recover the corresponding user account for a 30-day period. However, after 30 days, the inactive mailbox is retained in Office 365 until the hold or retention policy is removed. By observing the variations to the *Inactive mailboxes size* measure over time, you can figure out if your inactive mailboxes are growing in size

Measurement	Description	Measurement Unit	Interpretation
			abnormally and draining valuable storage space. If this is the case, then you may want to change the hold duration of the Litigation Hold or Office 365 retention policy applied to the inactive mailbox, or completely remove the Litigation Hold or retention policy applied to that mailbox. This will ensure that the email contents are not retained for much longer, and are instead, deleted permanently. This will release storage space.
Inactive mailboxes size	Indicates the total size of inactive mailboxes.	GB	
Archive mailboxes	Indicates the number of archive mailboxes.	Number	An archive mailbox is a specialized mailbox that appears alongside the users' primary mailbox folders in Outlook or Outlook Web App. Users can drag and drop messages from .pst files into the archive, for easy online access. Users can also move email items from the primary mailbox to the archive mailbox automatically, using Archive Polices, to reduce the size and improve the performance of the primary mailbox. Users can restore items they have deleted from any email folder in their archive. When an item is deleted, it is kept in the archive's Deleted Items folder. It remains there until it is manually removed by the user, or automatically removed by retention policies. If the *Archive mailboxes size* measure reveals that the archive mailboxes are growing in abnormally in size, it could mean one or both of the following:

Measurement	Description	Measurement Unit	Interpretation
			• User mailboxes are rapidly running out of space, owing to which many emails have been moved to the archive mailboxes, thereby eroding the archive space; • The Deleted Items folder of the archive mailboxes is rapidly filling up, but is not being emptied at the same pace either manually or by the retention policy To make more space in the archive mailboxes, you may want to consider manually removing emails from the mailboxes or their Deleted Items folder, or change the retention policy of the Deleted Items folder.
Archive mailboxes size	Indicates the total size of archive mailboxes.	GB	
Clutter enabled mailboxes	Indicates the number of clutter-enabled mailboxes.	Number	The idea of the Clutter feature is to take “low-priority” emails and automatically move them out of your inbox into another folder. The thought is if there is a particular type of email you rarely read, but isn’t junk/spam, the message will be filed away into a folder where you can review it later. In order to achieve this goal, Exchange Online needs to be able to watch your behavior for a period of time before it can be “trained” on what to identify as clutter. Clutter is now enabled by default for all mailboxes. Users can disable Clutter themselves via “Options” within OWA. Otherwise, administrators can disable Clutter via PowerShell with the “Set-

Measurement	Description	Measurement Unit	Interpretation
			Clutter" cmdlet.
Clutter disabled mailboxes	Indicates the number of clutter-disabled mailboxes	Number	
Mailboxes exceeding prohibit send quota	Indicates the number of user mailboxes, the storage space of which has been consumed beyond the Prohibit send limit configured.	Number	A user receives a prohibit-send notification email when the mailbox size limit is reached. The user cannot send new messages until enough email is deleted to bring the mailbox below the size limit.. To know which users' mailboxes have reached their prohibit-send limit, use the detailed diagnosis of this measure. THe current size of each mailbox and the Prohibit Send quota set for that mailbox is also displayed, so that administrators can understand why the Prohibit-send notification was sent. Administrators can then urge the concerned users to quickly clear up space in their mailboxes by either manually deleting mails or moving mails to archive mailboxes.
Mailboxes exceeding prohibit send/receive quota	Indicates the number of user mailboxes, the storage space of which has been consumed beyond the Prohibit send/receive limit configured.	Number	A user receives a prohibit send/receive notification email when the mailbox size limit is reached. Subsequently, Exchange Online rejects any incoming mail when the mailbox size limit is reached, and sends a non-delivery report (NDR) to the sender. The sender has the option to try resending the mail later. To receive messages again, the user must delete email until the mailbox is below the size limit. To know which users' mailboxes have reached their prohibit send/receive limit, use the detailed diagnosis of this measure. The current size of each mailbox and the Prohibit Send/Receive

Measurement	Description	Measurement Unit	Interpretation
			quota set for that mailbox is also displayed, so that administrators can understand why the Prohibit Send/Receive notification was sent.

The detailed diagnosis of the *Total mailbox size* measure lists the top-10 users, in terms of their mailbox size. This will enable administrators identify those users whose mailboxes are growing abnormally in size. A quick glance at the detailed metrics also points administrators to those users whose mailboxes may run out of space very shortly - i.e., mailboxes that may be approaching the Warning quote configured. Before a Warning notification is sent to such users, administrators themselves may alert such users of the potential storage space crunch and prompt them to act fast. Likewise, the detailed metrics may also reveal the users whose mailboxes have already reached their maximum storage limit. Administrators can urge such users to clean up unnecessary mails from their mailboxes and free up storage space, so that Exchange Online does not prohibit such mailboxes from sending or receiving mails.

Top 10 Users with Large Mailboxes

DISPLAY NAME	NUMBER OF ITEMS	MAILBOX SIZE (GB)	WARNING QUOTA (GB)	PROHIBIT SEND QUOTA (GB)	PROHIBIT SEND/RECEIVE QUOTA (GB)
04-09-18 02:47:26					
Raja Kannan	327651	46.3862	49	49.5	50
Sreenivasan R	205096	37.0319	49	49.5	50
Timothy Sim	131186	35.2677	49	49.5	50
Antony Nirmal	129504	28.6978	49	49.5	50
Srinivas Ramanathan	160061	26.9016	49	49.5	50
Narendhran Kannappan	93845	25.5509	49	49.5	50
Kalaiarasi Rajendran	96307	24.5881	49	49.5	50
Kesavan Krishnan	90550	24.3933	49	49.5	50
Karthik Canesan	187607	23.7804	49	49.5	50
Parthipan Kathiresan	124240	23.1322	49	49.5	50

Figure 4.7: The detailed diagnosis of the Total mailbox size measure

4.3.2 Mailbox/User Location Test

Your Office 365 data can be spread out across multiple datacenters in a given geolocation. Administrators therefore, may often want to know where the Exchange Online users come from and where their mailboxes are located. The Mailbox/User Location test helps administrators track the location of their users and mailboxes!

This test periodically reports the count of mailbox datacenters, mailbox locations, and mailbox users. Detailed diagnosis of the test reveals the mailbox distribution by location and user distribution by geography. This way, the test enables administrators determine the location of their users and mailboxes.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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**,

Parameters	Description
	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
Mailbox datacenters	Indicates the total number of mailbox datacenters	Number	
Unique mailbox locations	Indicates the number of unique mailbox locations.	Number	Use the detailed diagnosis of this measure to view the distinct mailbox locations and the count of mailboxes in each location. This way, you can identify the location that hosts the maximum number of mailboxes.
Unique user locations	Indicates the count of unique user locations.	Number	Use the detailed diagnosis of this measure to view the distinct user

Measurement	Description	Measurement Unit	Interpretation
			locations and the count of users connecting to Exchange Online from each location. This way, administrators can identify which location most Exchange Online users are coming from.

The detailed diagnosis of the *Unique mailbox locations* measure lists the distinct mailbox locations and the count of mailboxes in each location. This way, you can identify the location that hosts the maximum number of mailboxes.

	MAILBOXES COUNT
	35
	13
	1
	1
	48
	57
	19
ysia	31

Figure 4.8: The detailed diagnosis of the Unique mailbox locations measure

The detailed diagnosis of the *Unique user locations* measure lists the distinct user locations and the count of users connecting to Exchange Online from each location. This way, administrators can identify which location most Exchange Online users are coming from.

	USERS COUNT
	192
	7
	5
	4
	3
	1
	1
	1

Figure 4.9: The detailed diagnosis of the Unique user locations measure

4.3.3 Mailboxes Test

When auditing user mailboxes, an administrator would typically like to know:

- Which mailboxes were newly created, and which ones were modified / soft-deleted recently?
- Which mailboxes are on hold, and what type of hold are they on - Litigation hold? or In-place hold?
- Are any mailboxes shared? If so, which are they?
- Have any mailboxes been enabled for forwarding mails to external addresses? If so, which ones?

The Mailboxes test provides administrators with quick and accurate answers to these questions, and thus enables them to manage mailboxes better.

Target of the test : Exchange Online

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,	For execution, this test requires the privileges of an O365 user who has been assigned

Parameters	Description
O365 Password, and Confirm Password	the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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

Parameters	Description
	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 mailboxes	Indicates the total count of mailboxes on Exchange Online.	Number	
External forward enabled mailboxes	Indicates the count of mailboxes that have been enabled for forwarding mails to external email addresses.	Number	If this measure reports a non-zero value, then use the detailed diagnosis of the measure to find out which mailboxes have been configured to send emails to external addresses. Its important for administrators to closely monitor the mail traffic to/from such mailboxes. This is because, external forwarders are commonly used by hackers and bad actors to exfiltrate data from an organisation.
Shared mailboxes	Indicates the number of shared mailboxes.	Number	Shared mailboxes make it easy for a group of people in your company to monitor and send email from a common account, such as info@contoso.com or support@contoso.com. When a person in the group replies to a message sent to the shared mailbox, the email looks like

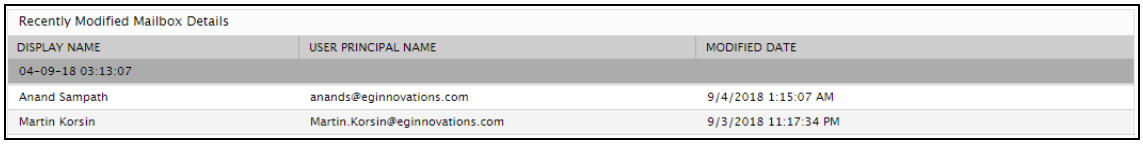
Measurement	Description	Measurement Unit	Interpretation
			it was sent by the shared mailbox, not from the individual user. To know which are the shared mailboxes, use the detailed diagnosis of this measure.
Newly created mailboxes	Indicates the number of mailboxes that were created newly.	Number	Use the detailed diagnosis of this measure to know which mailboxes were created newly.
Modified mailboxes	Indicates the number of mailboxes that were modified recently.	Number	Use the detailed diagnosis of this measure to identify the mailboxes that were changed recently.
Soft deleted mailboxes	Indicates the number of mailboxes that were soft deleted.	Number	A soft-deleted user mailbox is a mailbox that has been deleted using the Office 365 admin center or the Remove-Mailbox cmdlet in the Exchange Management Shell, and has still been in the Azure active directory (Azure AD) recycle bin for less than 30 days. A soft-deleted user mailbox is a mailbox that has been deleted in the following cases: • The user mailbox's associated Azure active directory user account is soft deleted (the Azure active directory user object is out of scope or in the recycle bin container). • The user mailbox's associated Azure active directory user account has been hard deleted but the Exchange Online mailbox is in a litigation hold or eDiscovery hold.

Measurement	Description	Measurement Unit	Interpretation
			• The user mailbox's associated Azure active directory user account has been purged within the last 30 days; which is the retention length Exchange Online will keep the mailbox in a soft deleted state before it is permanently purged and unrecoverable. Use the detailed diagnosis of this measure to identify the soft-deleted mailboxes.
Mailboxes on litigation hold	Indicates the count of mailboxes on litigation hold.	Number	Litigation Hold is one of the functionalities of eDiscovery feature in Exchange Online. Putting mailboxes, public folders or sites (e.g. OneDrive, SharePoint) on Litigation Hold prevents users from permanently deleting all or chosen content. Before the recent updates, litigation hold allowed to secure only whole mailboxes. Partial mailbox protection required using In-Place hold. Now, Litigation Hold allows you to use filters and conditions so that you can decide precisely which items to protect and which not. As the name suggests, the primary function of a Litigation Hold is to protect data in case there is a lawsuit in action, and some emails might be evidence. In fact, that is what the whole eDiscovery is there for. But you can use it, as many other companies do, as a means to backup sensitive data, just in case. Although the storage for protected items is not limited, including all mailboxes is

Measurement	Description	Measurement Unit	Interpretation
			not advisable – it will save all items, including spam emails, making future searches troublesome, to say the least. What is more, if you remove a hold, all purged data is irreversibly deleted. You can export mailboxes to PST files and store them locally. This way, you will increase your data safety. To know which mailboxes are on litigation hold, use the detailed diagnosis of this measure.
Mailboxes on inplace hold	Indicates the count of mailboxes on in-place hold.	Number	In-Place Hold essentially helps an admin determine what items to hold and the amount of time to hold them. Using the In-Place Hold feature, administrators can accomplish various tasks that focus around preserving email. Mail preservation is critical if a company is faced with litigation and needs to perform any sort of electronic discovery. Using In-Place Hold, an Exchange 2013 administrator can: • Place complete user mailboxes on hold. • Preserve mailbox items that were previously deleted. • Search for specific items via criteria such as keywords, send date, recipients and more. • Preserve items for an indefinite amount of time. • Place an actual user on hold. Use the detailed diagnosis of this

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>measure to know which mailboxes have been put on in-place hold.</td></tr>
<tr><td>All mailboxes on hold?</td><td>Indicates whether/not all mailboxes are on hold presently.</td><td></td><td>The values that this measure can report and their corresponding numeric 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>0</td></tr></table>Note:
Typically, this measure reports the Measure Values listed in the table above to indicate whether/not all mailboxes are on hold. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

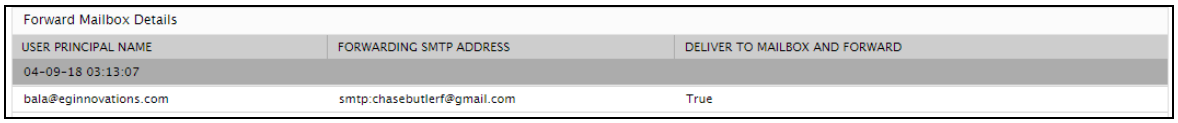
The detailed diagnosis of the *Modified mailboxes* measure lists the mailboxes that were modified and when they were modified. This way, administrators can keep track of changes to mailbox configuration.


Recently Modified Mailbox Details

DISPLAY NAME	USER PRINCIPAL NAME	MODIFIED DATE
04-09-18 03:13:07		
Anand Sampath	anands@eginnovations.com	9/4/2018 1:15:07 AM
Martin Korsin	Martin.Korsin@eginnovations.com	9/3/2018 11:17:34 PM

Figure 4.10: The detailed diagnosis of the Modified mailboxes measure

The detailed diagnosis of the *External forward enabled mailboxes* measure lists the mailboxes that have been configured to forward emails to external email addresses. The forwarding SMTP address is also revealed, so that administrators can quickly identify the external domain to which each mailbox forwards emails.


Forward Mailbox Details

USER PRINCIPAL NAME	FORWARDING SMTP ADDRESS	DELIVER TO MAILBOX AND FORWARD
04-09-18 03:13:07		
bala@eginnovations.com	smtp:chasebutlerf@gmail.com	True

Figure 4.11: The detailed diagnosis of the External forward enabled mailboxes measure

4.3.4 Recipients Test

The people and resources that send and receive messages are the core of any messaging and collaboration system. In an Exchange Online organization, these people and resources are referred to as recipients. A recipient is any mail-enabled object to which Exchange Online can deliver or route messages. Exchange includes several explicit recipient types, namely:

Recipient Type	Description
Dynamic distribution group	A distribution group that uses recipient filters and conditions to derive its membership at the time messages are sent.
Equipment mailbox	A resource mailbox that's assigned to a resource that’s not location-specific, such as a portable computer, projector, microphone, or a company car. Equipment mailboxes can be included as resources in meeting requests, providing a simple and efficient way of using resources for your users.
Linked mailbox	A mailbox that's assigned to an individual user in a separate, trusted forest.
Mail contact	A mail-enabled Active Directory contact that contains information about people or organizations that exist outside the Exchange organization. Each mail contact has an external email address. All messages sent to the mail contact are routed to this external email address.
Mail forest contact	A mail contact that represents a recipient object from another forest. Mail forest contacts are typically created by Microsoft Identity Integration Server (MIIS) synchronization.
Mail user	A mail-enabled Active Directory user that represents a user outside the Exchange organization. Each mail user has an external email address. All messages sent to the mail user are routed to this external email address.
Mail-enabled public folder	An Exchange public folder that's configured to receive messages.
Distribution groups	A distribution group is a mail-enabled Active Directory distribution group object that can be used only to distribute messages to a group of recipients.
Mail-enabled security group	A mail-enabled security group is an Active Directory universal security group object that can be used to assign access permissions to resources in Active Directory and can also be used to distribute messages.
Microsoft Exchange recipient	A special recipient object that provides a unified and well-known message sender that differentiates system-generated messages from other messages. It replaces the System Administrator sender used for system-generated messages in earlier versions of Exchange.
Room mailbox	A resource mailbox that's assigned to a meeting location, such as a

	conference room, auditorium, or training room. Room mailboxes can be included as resources in meeting requests, providing a simple and efficient way of organizing meetings for your users.
Shared mailbox	A mailbox that's not primarily associated with a single user and is generally configured to allow access for multiple users.
Site mailbox	A mailbox comprised of an Exchange mailbox to store email messages and a SharePoint site to store documents. Users can access both email messages and documents using the same client interface. For more information, see Site mailboxes.
User mailbox	A mailbox that's assigned to an individual user in your Exchange organization. It typically contains messages, calendar items, contacts, tasks, documents, and other important business data.
Office 365 mailbox	In hybrid deployments, an Office 365 mailbox consists of a mail user that exists in Active Directory on-premises and an associated cloud mailbox that exists in Exchange Online.
Linked user	A linked user is a user whose mailbox resides in a different forest than the forest in which the user resides.
Discovery mailbox	Discovery mailboxes are used as target mailboxes for In-Place eDiscovery searches in the Exchange admin center (EAC).

To know which recipient types are supported by the Exchange Online organization and the number of recipients configured for each type, administrators can use the Recipients test. For recipient types that are mailboxes, the test additionally reports the total size of mailboxes of that type and the total number of emails in those mailboxes. This way, administrators can easily manage recipients and track the growth in size of the recipient mailboxes.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each recipient type in the Exchange Online organization

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions.

Parameters	Description
	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 **2.1.1**.
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 **P**roxy 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*.

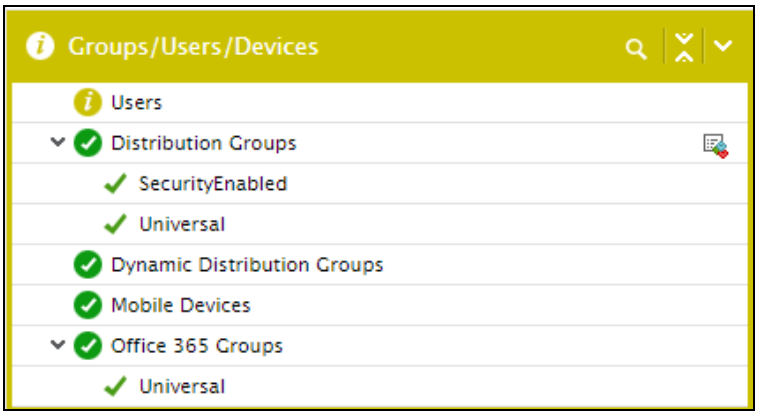
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Count	Indicates the number of recipients of this type.	Number	

Measurement	Description	Measurement Unit	Interpretation
Mailboxes size	Indicates the total size of mailboxes of this type.	Number	**This measure is reported only for recipients that are mailboxes.**
Item count	Indicates the total number of mails in mailbox recipients of this type.	Number	**This measure is reported only for recipients that are mailboxes.**

4.4 The Groups/Users/Devices Layer

Using the tests mapped to this layer, you can audit and easily manage distribution groups, dynamic distribution groups, and Office 365 groups. The tests also help audit user rights/permissions and track user password expiry. Additionally, the tests reveal the ActiveSync-enabled mobile devices and device types that are syncing their mailboxes with Exchange Online, so you can identify the most popular devices/types.



4.4.1 Distribution Groups Test

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 : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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

Parameters	Description
	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 at every sixth test execution cycle if no problems are reported, 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	Number	Use the detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
	groups of this type that were modified during the last measurement period.		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. 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.

Measurement	Description	Measurement Unit	Interpretation
			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 4.12: 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 4.13: The detailed diagnosis of the Empty groups measure reported by the Distribution Groups test

4.4.2 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 : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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
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 4.14: 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 4.15: The detailed diagnosis of the Empty groups measure reported by the Dynamic Distribution Groups test

4.4.3 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 : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
Domain, Domain	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.**

Parameters	Description
User Name, Domain Password, and Confirm Password	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 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 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 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

Measurement	Description	Measurement Unit	Interpretation
			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 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 4.16: 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 4.17: The detailed diagnosis of the Empty groups measure reported by the Office 365 Groups test

4.4.4 Users Test

User management is a critical administrative task. This is of more significance in an Exchange Online environment, which is characterized by numerous users.

There are many aspects to user management in an Exchange Online setup. Some of them are, namely - user password management, user activity management, and the management of user privileges/permissions. To manage user passwords, administrators should be able to alert users to a potential password expiry, at least a few days before it actually occurs. For that, the administrators should first track the validity of the password of each user closely. User activity management on the other hand is about tracking user logins and logouts and understanding whether/not users are actively using Exchange Online. The knowledge of active/inactive users helps administrators assess license usage and plan license procurement better. Lastly, by periodically revisiting which user has been assigned what permission in Exchange Online, an administrator is allowed the opportunity to review usage policies and if required, even reconfigure them. The Users test enables administrators to cover all these aspects of user management.

With the help of this test, administrators can find quick and accurate answers for the following management queries:

- How many users have been granted administrative rights? Who are they?
- How many users have been granted 'Send As' and/or 'Send on behalf of' permissions? Who are they?
- Are there any users for whom ActiveSync is not enabled? If so, who are they?
- Who are the most inactive users of Exchange Online? When was the last time they logged in? Are there any users who have never logged in?
- Is any user's password nearing expiry? If so, who are they?

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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*.
Inactive Period	Specify the number of days (before the current date) for which a user should not have logged into Exchange Online for him/her to be counted as an inactive user. The default value is 15 days. This means that by default, any user who has not logged in even once in the last 15 days will be counted as an inactive user.
Password Expire Period	By default, this parameter is set to 5 days. This means that the test will include all those users whose passwords will expire within 5 days in its count of users whose passwords are nearing expiry. You can change this value, if you so need.
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 every second 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
ActiveSync enabled users	Indicates the number of users for whom the Exchange ActiveSync protocol has been enabled.	Number	Exchange Online supports the Microsoft Exchange ActiveSync protocol, which synchronizes mailbox data between mobile devices and Exchange Online, so users can access their email, calendar, contacts, and tasks on the go.
Non-active sync users	Indicates the number of users for whom the Exchange ActiveSync protocol has been enabled.	Number	Use the detailed diagnosis of this measure to view the users who are not ActiveSync-enabled.
Users with 'Send as' permission	Indicates the number of users who have been granted the permission to send mails as the group to which they belong.	Number	A member of an Office 365 Group who has been granted Send as or Send on behalf permissions can send email as the group, or on behalf of the group. For example, if Allie Bellew is part of Training Office 365 Group in your organization, and has Send as permissions on the group, if she sends an email as the Office 365 Group, it will look like the Training department from your organization sent the email. The Send on Behalf permission lets a user send email on behalf of an Office 365 Group. For example, if Donald Forster is a part of the Marketing Office 365 Group, and has Send on Behalf permissions, any email he sends to the group will look like it was sent by **Donald Forster on behalf of Marketing Team**.

Measurement	Description	Measurement Unit	Interpretation
Users with 'Send on behalf of' permission	Indicates the number of users who have the permission to send mails on behalf of a group.	Number	Use the detailed diagnosis of each of these measures to know which users have been granted Send as and Send on behalf of permissions.
Admin users	Indicates the number of users who have been assigned the Exchange Admin role.	Number	Here are some of the key tasks an Exchange Admin can perform: • Recover deleted items in a user's mailbox • Determine how long deleted email should be retained before it's permanently deleted. • Set up mailbox features such as the mailbox sharing policy: how users can share calendar and contacts information with others outside of your organization. • Set up "Send As" and "Send on Behalf" delegates for someone's mailbox. For example, an executive may want their assistant to have the ability to send mail on their behalf. • Create shared mailboxes so a group of people can monitor and send email from a common email address. • Set up anti-spam and malware filters for the organization. • Manage Office 365 Groups To know which users have been assigned the Admin role, use the

Measurement	Description	Measurement Unit	Interpretation
			detailed diagnosis of this measure.
Active users	Indicates the number of active users of Exchange Online.	Number	By default, any user who has logged into Exchange Online at least once in the last 15 days is considered to be an 'active user'. This is governed by the **INACTIVE PERIOD** setting of this test. By default, this parameter is set to 15 days.
Inactive users	Indicates the number of inactive users of Exchange Online.	Number	By default, any user who has not logged into Exchange Online even once in the last 15 days is considered to be an 'inactive user'. This is governed by the **INACTIVE PERIOD** setting of this test. By default, this parameter is set to 15 days. Use the detailed diagnosis of this measure to know who are the inactive users.
Never logged in users	Indicates the number of users who have never logged into Exchange Online.	Number	Use the detailed diagnosis of this measure to know which users have never logged in.
Users password nearing expiry	Indicates the number of users whose password is nearing expiry.	Number	By default, if a user's password is expected to expire in 5 days or less, then that user will be counted as a user whose password is nearing expiry. This computation is governed by the **PASSWORD EXPIRE PERIOD** configured for this test. By default, this parameter is set to 5. Use the detailed diagnosis of this measure to know who are the users whose password is about to expire.

The detailed diagnosis of the *Non-active sync users* measure lists the users who are not ActiveSync-enabled. The last time each such user logged into Exchange Online is also displayed.

Non-Activesync users

SIGN NAME	LAST LOGIN TIME
04-09-18 17:05:57	
egmail@eginnovations.com	9/4/2018 10:49:05 AM

Figure 4.18: The detailed diagnosis of the Non-active sync users measure

The detailed diagnosis of the *Inactive users* measure lists the users who are inactive, and the last date/time they logged into Exchange Online.

Inactive users

SIGN NAME	LAST LOGIN TIME
04-09-18 17:05:57	
Neeharika@eginnovations.com	07/11/2018 15:29:12

Figure 4.19: The detailed diagnosis of the Inactive users measure

Use the detailed diagnosis of the *Users with 'Send as' permission* measure to view the list of users who have been granted the permission to send mail as the Office 365 group to which they belong.

List of Users with 'Send As' Permission

IDENTITY	TRUSTEE	ACCESSCONTROLTYPE	ISINHERITED	INHERITANCETYPE	ISVALID
04-09-18 17:05:57					
eG Network	kharthik@eginnovations.com	Allow	False	None	True
eG Network	Parthasarathi.PM@eginnovations.com	Allow	False	None	True
eG Network	S-1-5-21-4016215872-4056554821-1302376290-14382566	Allow	False	None	True
eG Network	egmail@eginnovations.com	Allow	False	None	True
eG Network	manikandan@eginnovations.com	Allow	False	None	True
eG Network	karthikg@eginnovations.com	Allow	False	None	True
hr	sreeni@eginnovations.com	Allow	False	None	True
nandakumar	egmail@eginnovations.com	Allow	False	None	True
network	karthikg@eginnovations.com	Allow	False	None	True

Figure 4.20: The detailed diagnosis of the Users with 'Send as' permission measure

Use the detailed diagnosis of the *Users with 'Send on behalf of' permission* measure to view the users who have the right to send mails on behalf of the Office 365 group to which they belong.

List of Users with 'Send On Behalf Of' Permission

DISPLAY NAME	USER PRINCIPALNAME	PRIMARY SMTPADDRESS	GRANT SENDONBEHALFTO
04-09-18 17:05:57			
Renne Bots	renne.bots@eginnovations.com	renne.bots@eginnovations.com	wingyiu.lee
Wing Yiu Lee	wingyiu.lee@eginnovations.com	wingyiu.lee@eginnovations.com	renne.bots chrisvdberg

Figure 4.21: The detailed diagnosis of the Users with 'Send on behalf of' permission measure

4.4.5 Mobile Devices Test

Exchange Online supports the Microsoft Exchange ActiveSync protocol, which synchronizes mailbox data between mobile devices and Exchange Online, so users can access their email,

calendar, contacts, and tasks on the go.

With many organizations these days encouraging their employees to bring their own mobile devices to work, it has become super-imperative for administrators to keep track of which mobile devices are accessing Exchange Online and syncing with the mailboxes hosted on it, and what are the most popular devices. This information is critical, as they help administrators understand the type of devices that frequently interact with Exchange Online, so that they can accordingly define access policies, DLP policies, and anti-malware protection policies to protect the mailboxes and data hosted online. This is where the Mobile Devices test helps!

This test captures and reports the count and details of ActiveSync-enabled mobile devices and device types that are syncing with mailboxes hosted on Exchange Online. With the help of this information, administrators can quickly identify devices that are popular and the configuration (OS, OS language, mail client) of such devices, so that access policies can be prudently defined.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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

Parameters	Description
	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 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
Unique user agents	Indicates the number of mobile device user agents accessing Exchange Online.	Number	The User-Agent header contains a line of text that can be used to identify a mobile device. Using the detailed diagnosis of this measure, you can view the top-20 user-agent strings, in terms of the number of mobile devices supporting those strings. From the user-agent strings, you will be able to figure out the type of mobile devices interacting with Exchange Online.
Unique device types	Indicates the number of mobile device types that are syncing with Exchange Online.	Number	Use the detailed diagnosis of this measure to view the top-20 mobile device types, in terms of the number of mobile devices of that type accessing Exchange Online.
Unique operating systems	Indicates the number of mobile operating systems accessing Exchange Online.	Number	Use the detailed diagnosis of this measure to view the top-20 mobile operating systems, in terms of the number of mobile devices running those operating systems.
Unique clients	Indicates the number of mail clients that are interacting with Exchange Online.	Number	Use the detailed diagnosis of this measure to view the top-20 mail clients, in terms of the number of mobile devices supporting those clients.
Unique device OS languages	Indicates the number of unique device OS languages in use in the mobile devices that are interacting with Exchange Online.	Number	Use the detailed diagnosis of this measure to view the top-20 OS languages, in terms of the number of mobile devices that have been configured with those languages.

Measurement	Description	Measurement Unit	Interpretation
Total devices	Indicates total number of mobile devices syncing with mailboxes on Exchange Online.	Number	This is a good indicator of the device load on Exchange Online.

The detailed diagnosis of the *Unique user agents* measure lists the top-20 user-agent strings, in terms of the number of mobile devices supporting those strings. From the user-agent strings, you will be able to figure out the type of mobile devices interacting with Exchange Online. From the device count, you can instantly identify the most popular device type.

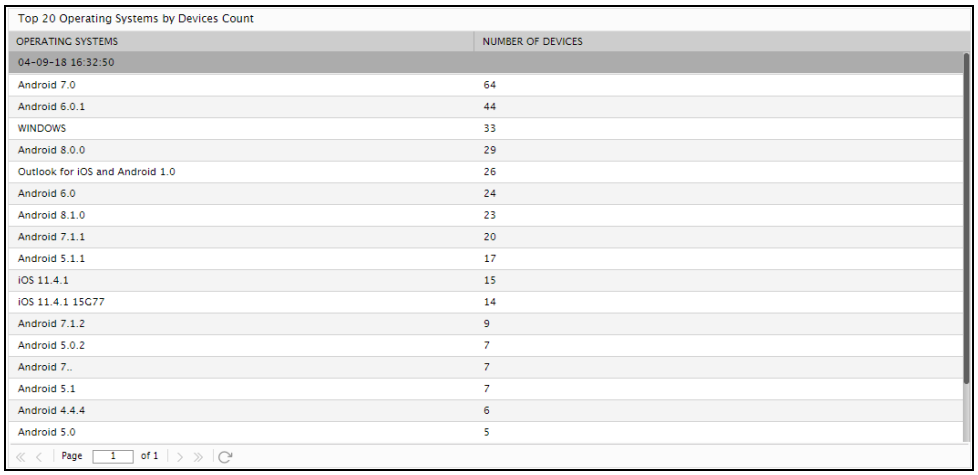
Top 20 User Agents by Devices Count

USER AGENT	NUMBER OF DEVICES
04-09-18 16:32:50	
Outlook-Android/2.0	194
Outlook-iOS/2.0	39
microsoft.windowscommunicationsapps	33
Outlook-iOS-Android/1.0	26
MOWA / 15.01.0396.034	6
Android-Mail/8.8.12.210495220.release	5
MSFT-WIN-3/10.0.14393	4
Android/5.0.2-EAS-2.0	4
Android/4.4.4-EAS-2.0	3
Apple-iPhone8C2/1507.77	3
MSFT-WP/8.10.14234	3
MSFT-WIN-3/10.0.10586	3
Android/6.0.1-EAS-1.3	3
Apple-iPhone10C6/1507.77	2
Apple-iPhone9C1/1507.77	2
Android/5.1.1-EAS-1.3	2
Android/8.1.0-EAS-2.0	2

Page 1 of 1

Figure 4.22: The detailed diagnosis of the Unique user agents measure

The detailed diagnosis of the *Unique operating systems* measure lists the top-20 mobile operating systems, in terms of the number of mobile devices running those operating systems. This will reveal to you that operating system that runs on the maximum number of mobile devices which are interacting with Exchange Online.



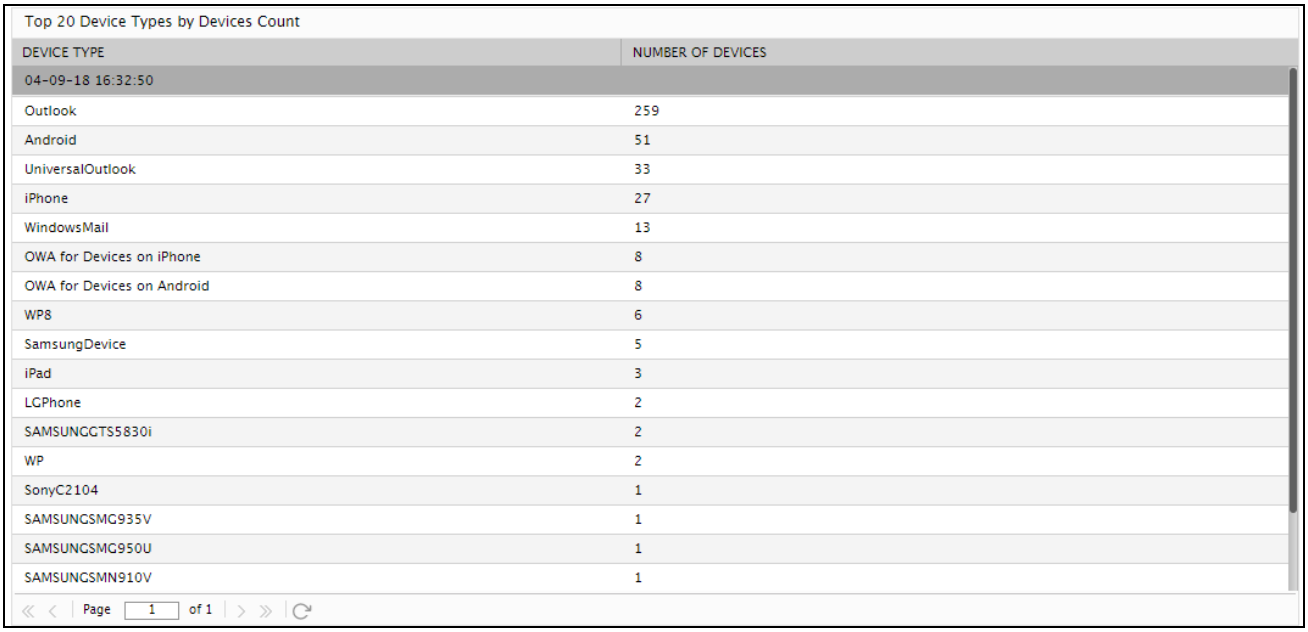
Top 20 Operating Systems by Devices Count

OPERATING SYSTEMS	NUMBER OF DEVICES
04-09-18 16:32:50	
Android 7.0	64
Android 6.0.1	44
WINDOWS	33
Android 8.0.0	29
Outlook for iOS and Android 1.0	26
Android 6.0	24
Android 8.1.0	23
Android 7.1.1	20
Android 5.1.1	17
iOS 11.4.1	15
iOS 11.4.1 15G77	14
Android 7.1.2	9
Android 5.0.2	7
Android 7..	7
Android 5.1	7
Android 4.4.4	6
Android 5.0	5

Page 1 of 1

Figure 4.23: The detailed diagnosis of the Unique operating systems measure

Use the detailed diagnosis of the *Unique device types* measure to view the top-20 mobile device types, in terms of the number of mobile devices of that type accessing Exchange Online. With the help of these detailed metrics, you can quickly identify the device type that is most popular.



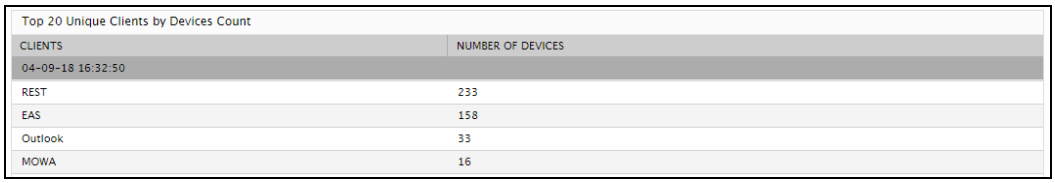
Top 20 Device Types by Devices Count

DEVICE TYPE	NUMBER OF DEVICES
04-09-18 16:32:50	
Outlook	259
Android	51
UniversalOutlook	33
iPhone	27
WindowsMail	13
OWA for Devices on iPhone	8
OWA for Devices on Android	8
WP8	6
SamsungDevice	5
iPad	3
LGPhone	2
SAMSUNGGTS5830i	2
WP	2
SonyC2104	1
SAMSUNGSMG935V	1
SAMSUNGSMG950U	1
SAMSUNGSMN910V	1

Page 1 of 1

Figure 4.24: The detailed diagnosis of the Unique device types measure

Use the detailed diagnosis of the *Unique clients* measure to view the top-20 mail clients, in terms of the number of mobile devices supporting those clients.

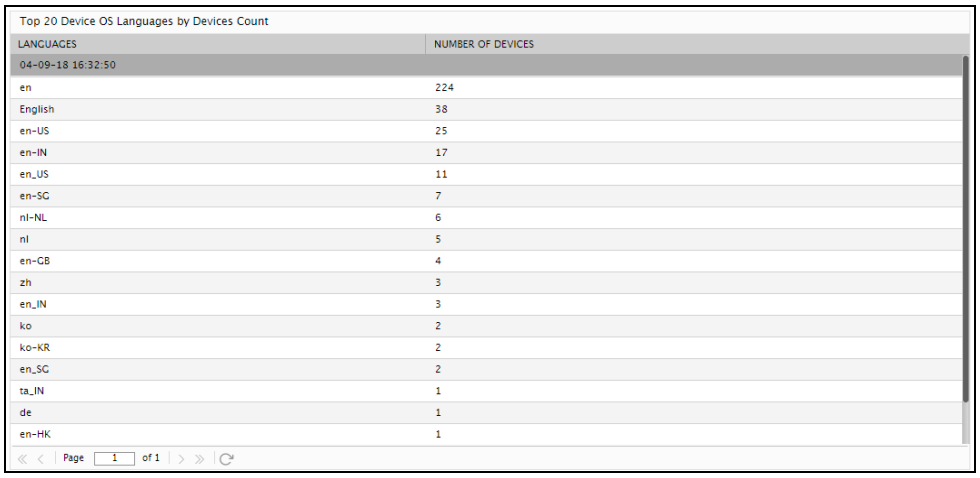


Top 20 Unique Clients by Devices Count

CLIENTS	NUMBER OF DEVICES
04-09-18 16:32:50	
REST	233
EAS	158
Outlook	33
MOWA	16

Figure 4.25: The detailed diagnosis of the Unique clients measure

Use the detailed diagnosis of the *Unique device OS languages* measure to view the top-20 OS languages, in terms of the number of mobile devices that have been configured with those languages.



Top 20 Device OS Languages by Devices Count

LANGUAGES	NUMBER OF DEVICES
04-09-18 16:32:50	
en	224
English	38
en-US	25
en-IN	17
en_US	11
en-SG	7
nl-NL	6
nl	5
en-GB	4
zh	3
en_IN	3
ko	2
ko-KR	2
en_SG	2
ta_IN	1
de	1
en-HK	1

Page 1 of 1

Figure 4.26: The detailed diagnosis of the Unique device OS languages measure

4.4.6 User Connections by Email App Test

If Exchange Online is overloaded with user connections, administrators may want to know which email app is drawing the maximum number of users. Administrators can use the User Connections by Email App test for this!

This test automatically discovers the email apps on Exchange Online and reports the count of unique users for each app.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each email app

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 Creating a New User in the Office 365 Portal.
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*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Unique users	Indicates the number of unique users for this app.	Number	Compare the value of this measure across email apps to know which app is imposing the maximum connection load on Exchange Online.

4.4.7 Users by Outlook Versions Test

At any given point in time, administrators may want to know how many users are using the different versions of Outlook deployed on Exchange Online. This is useful to understand how many users will be impacted if Outlook is upgraded from one version to another. The Users by Outlook Versions test provides this insight to administrators!

This test reports the count of unique users for every Outlook version on Exchange Online.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each version of Outlook

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 Creating a New User in the Office 365 Portal.

Parameters	Description
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*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Unique users	Indicates the number of unique users for this version of Outlook.	Number	

4.5 The Email Activity/Protection Layer

Incoming and outgoing emails can be tracked and delivery failures promptly captured using the tests mapped to this layer. The tests also proactively alert administrators to non-availability of Exchange Online for sending/receiving mails and slowness in mail delivery. Additionally, the tests also turn on the spotlight on spam mails, malware, and DLP violations, thereby revealing to administrators how

well-insulated user mailboxes are from malicious attacks. Transport rules and mails that conform to those rules are also highlighted by the tests, so as to enable review and reconfiguration (if required) of rules.

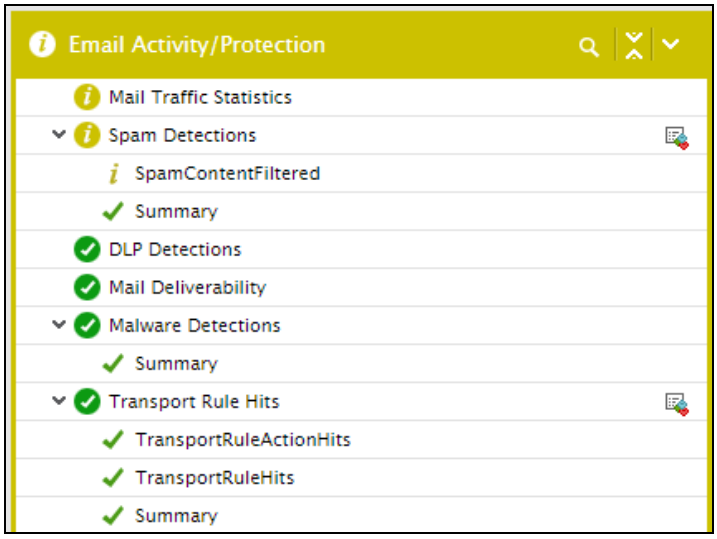


Figure 4.27: The tests mapped to the Email Activity/Protection layer

4.5.1 DLP Detections Test

To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy in the Office 365 Security & Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365.

A DLP policy contains a few basic things:

- Where to protect the content - locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites.
- When and how to protect the content by enforcing rules comprised of:
  - Conditions the content must match before the rule is enforced -- for example, look only for content containing Social Security numbers that's been shared with people outside your organization.
  - Actions that you want the rule to take automatically when content matching the conditions is found -- for example, block access to the document and send both the user and compliance officer an email notification.

You can use a rule to meet a specific protection requirement, and then use a DLP policy to group together common protection requirements, such as all of the rules needed to comply with a specific regulation.

Whenever a DLP rule applied to Exchange Online is violated, an administrator should be instantly notified of the violation, with details of the rule/policy that was violated and the email sender/receiver who violated it. Administrators can easily and efficiently investigate DLP violations when they have access to this information. This is exactly the kind of assistance the DLP Detections test provides to administrators!

This test monitors the email traffic over Exchange Online, instantly captures traffic that violates any of the DLP rules that apply to the Exchange Online location, and promptly alerts administrators to such violations. Detailed diagnostics reported by the test provide the complete details of each violation, thereby enabling administrators to accurately identify the rules and policies that were violated, the emails that violated the rules and policies, and the senders and receivers responsible for the same. This information helps administrators investigate and take appropriate action against the violations.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.

Parameters	Description
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 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
DLP detections	Indicates the number of DLP rules that were violated.	Number	Ideally, the value of this measure should be 0. A non-zero value implies that one/more DLP rules have been violated. In this case, you can use the detailed diagnosis of this measure to know which emails violated the rules, which rules were violated, which policies these rules belong to, and which senders and receivers violated them.
Unique senders	Indicates the number of unique senders who violated one/more DLP rules.	Number	Use the detailed diagnosis of this measure to know the senders of emails that violated a DLP rule.
Unique receivers	Indicates the number of unique receivers who violated one/more DLP rules.	Number	Use the detailed diagnosis of this measure to known who were the receivers of emails that violated one/more DLP rules.

The detailed diagnosis of the *DLP detections* measure reveals the details of those emails that violated one/more DLP rules. The subject of the email, the sender and receiver of the email, the date/time at which the email was sent, the rule that is violated, and the DLP policy that includes that rule are displayed as part of the detailed metrics. Using this information, administrators can easily investigate DLP violations.

CREATION TIME	OPERATION	BCC	CC	FROM	TO	RECIPIENT COUNT
Jul 31, 2018 15:19:15						
2018-06-05T05:33:55	DlpRuleMatch	-	-	mohanraj@Jackbill.onmicrosoft.com	jackbill93@Jackbill.onmicrosoft.com	1
2018-06-05T05:36:01	DlpRuleMatch	-	-	shankar@Jackbill.onmicrosoft.com	gopi@Jackbill.onmicrosoft.com	1
2018-06-05T05:31:46	DlpRuleMatch	-	-	karthi@Jackbill.onmicrosoft.com	manoj@Jackbill.onmicrosoft.com	1
2018-06-05T05:29:28	DlpRuleMatch	-	-	shankar@Jackbill.onmicrosoft.com	karthi@Jackbill.onmicrosoft.com	1
2018-06-05T05:29:49	DlpRuleMatch	-	-	egmonitor@Jackbill.onmicrosoft.com	mohanraj@Jackbill.onmicrosoft.com	1
2018-06-05T05:40:28	DlpRuleMatch	-	-	egmonitor@Jackbill.onmicrosoft.com	prabu@Jackbill.onmicrosoft.com	1
2018-06-05T05:42:33	DlpRuleMatch	-	-	kannan@Jackbill.onmicrosoft.com	mohanraj@Jackbill.onmicrosoft.com	1
2018-06-05T05:40:23	DlpRuleMatch	-	-	gopi@Jackbill.onmicrosoft.com	prabha@Jackbill.onmicrosoft.com	1
2018-06-05T05:36:07	DlpRuleMatch	-	-	prabha@Jackbill.onmicrosoft.com	mohanraj@Jackbill.onmicrosoft.com	1
2018-06-05T05:38:12	DlpRuleMatch	-	-	thiru@Jackbill.onmicrosoft.com	jackbill93@Jackbill.onmicrosoft.com	1

Figure 4.28: The detailed diagnosis of the DLP detections measure

To quickly identify all those email senders who violated one/more DLP rules, use the detailed diagnosis of the *Unique senders* measure.

Unique Senders
UNIQUE SENDERS
Jul 31, 2018 15:19:15
mohanraj@Jackbill.onmicrosoft.com, shankar@Jackbill.onmicrosoft.com, karthi@Jackbill.onmicrosoft.com, egmonitor@Jackbill.onmicrosoft.com, kannan@Jackbill.onmicrosoft.com,

Figure 4.29: The detailed diagnosis of the Unique senders measure reported by the DLP Detections Test

To quickly identify all those email receivers who violated one/more DLP rules, use the detailed diagnosis of the *Unique receivers* measure.

Unique Recipients
UNIQUE RECIPIENTS
Aug 02, 2018 12:36:21
jackbill93@Jackbill.onmicrosoft.com, mohanraj@Jackbill.onmicrosoft.com, egmonitor@Jackbill.onmicrosoft.com, manoj@Jackbill.onmicrosoft.com, prabu@Jackbill.onmicrosoft.com,

Figure 4.30: The detailed diagnosis of the Unique receivers measure reported by the DLP Detections Test

4.5.2 Malware Detections Test

Malware is comprised of viruses and spyware. Viruses infect other programs and data, and they spread throughout your computer looking for programs to infect. Spyware refers to malware that gathers your personal information, such as sign-in information and personal data, and sends it back to the malware author.

Mailboxes hosted in Exchange Online are vulnerable and may get infected by malware. When this happens, administrators should be able to promptly identify the malware that has attacked the mailboxes, accurately capture the files infected by it, and also isolate the senders/receivers who are sending/receiving the malware. This will help them tweak Exchange Online's built-in anti-malware protection policies, so that such policies acquire the ability to shield the mailboxes in Exchange Online from that malware. This is where the Malware Detections test helps!

This test promptly captures the different types of malware infecting the mailboxes in Exchange Online. For each malware type, the test then reports the count of inbound and outbound mails infected by the malware of that type, the count of senders sending that malware, and the count of receivers receiving it. With the help of this information, administrators can assess the severity of the malware infection and may even to choose to review and, if required, reconfigure the default anti-malware protection policies of Exchange Online.

Moreover, the detailed metrics reported by the test reveal the top senders and receivers of malware. This will point you to email traffic that you may want to track closely.

The test also reports the malware size in both incoming and outgoing mails, with detailed diagnosis pointing you to the senders/receivers who sent/received malware of large sizes. If the mailboxes of such senders/receivers exhibit abnormal growth suddenly, you may want to check these detailed metrics to see if that can be attributed to the malware size.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each malware that is infecting mailboxes

First-level descriptor: Malware

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
Domain, Domain User Name, Domain	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.**

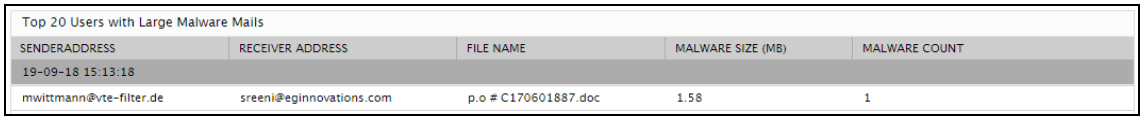
Parameters	Description
Password, and Confirm Password	In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password 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 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
Inbound malware items	Indicates the number of inbound emails carrying this malware.	Number	A high value for this measure is a cause for concern, as it indicates that incoming mail traffic is severely infected by malware. In this case, use the detailed diagnosis of this measure to view the top-20 receivers, in terms of the number of malware-infected mails they received. This information, thus points administrators to those receivers who were worst hit by malware.
Outbound malware items	Indicates the number of outbound emails carrying this malware.	Number	A high value for this measure is a cause for concern, as it indicates that outgoing mail traffic is severely infected by malware. In this case, use the detailed diagnosis of this measure to view the top-20 senders, in terms of the number of malware-infected mails they sent. This will also point you to those senders who are probably responsible for spreading the malware infection.
Inbound malware size	Indicates the total size of this malware in incoming mails.	GB	If the value of this measure is abnormally high, then use the detailed diagnosis of this measure to view the top-20 receivers, in terms of the malware size in the mails they received. If the mailbox of these receivers increase in size suddenly, then check the malware size of these receivers to see if the malware caused the abnormal mailbox growth.
Outbound malware size	Indicates the total size of this malware in outgoing mails.	GB	If the value of this measure is abnormally high, then use the detailed diagnosis of this measure to view the

Measurement	Description	Measurement Unit	Interpretation
			top-20 senders, in terms of the malware size in the mails they sent. If the mailbox size of these senders increase suddenly, then check the malware size of these senders to see if the malware caused the abnormal mailbox growth.
Unique senders	Indicates the number of unique senders of this malware.	Number	Use the detailed diagnosis of this measure to view the top-20 senders, in terms of the number of malware-infected mails they sent .
Unique receivers	Indicates the number of unique receivers of this malware.	Number	Use the detailed diagnosis of this measure to view the top-20 receivers, in terms of the number of malware-infected mails they received.

The detailed diagnosis of the *Inbound malware items* measure lists the top-20 receivers, in terms of the number of malware-infected mails they received. This will point you to that receiver who received the maximum number of malware-infected mails and was hence affected the worst by it. With the help of the detailed metrics, you can also accurately identify who sent the malware-infected mails to the top receiver, the file that was infected, and the malware size. Using this information, administrators can tell over which email communication - i.e., communication between which sender and receiver - the maximum number of malware items were trafficked; such email communication may be pulled up for closer monitoring.



Top 20 Users with Large Malware Mails

SENDERADDRESS	RECEIVER ADDRESS	FILE NAME	MALWARE SIZE (MB)	MALWARE COUNT
19-09-18 15:13:18				
mwittmann@vte-filter.de	sreeni@eginnovations.com	p.o # C170601887.doc	1.58	1

Figure 4.31: The detailed diagnosis of the Inbound malware items measure

The detailed diagnosis of the *Outbound malware items* measure lists the top-20 senders, in terms of the number of malware-infected mails they sent. This will point you to that sender who sent the maximum number of malware-infected mails, thus causing the infection to spread. With the help of the detailed metrics, you can also accurately identify who received the malware-infected mails from the top sender, the file that was infected, and the malware size. Using this information, administrators can tell over which email communication - i.e., communication between which sender

and receiver - the maximum number of malware items were trafficked; such email communication may be pulled up for closer monitoring.

SENDERADDRESS	RECEIVER ADDRESS	FILE NAME	MALWARE SIZE (MB)	MALWARE COUNT
Jul 31, 2018 12:24:53				
Mohandoss.R@eginnovations.com	nagarajan@eginnovations.com	Main.zip	0.14	1
Mohandoss.R@eginnovations.com	narendhran@eginnovations.com	Main.zip	0.14	1

Figure 4.32: The detailed diagnosis of the Outbound malware items measure

Use the detailed diagnosis of the *Unique senders* measure to view the top-20 senders, in terms of the number of malware-infected mails they sent . This will point administrators to that sender who caused a malware to spread. The total size of the malware sent by each sender is also displayed.

UNIQUE SENDERS	MALWARE COUNT	MALWARE SIZE (MB)
Jul 31, 2018 12:24:53		
Mohandoss.R@eginnovations.com	2	0.2728

Figure 4.33: The detailed diagnosis of the Unique senders measure reported by the Malware Detections test

Use the detailed diagnosis of the *Unique receivers* measure to view the top-20 receivers, in terms of the number of malware-infected mails they received. This will point administrators to that receiver who was most affected by the malware. The total size of the malware received by each receiver is also displayed.

UNIQUE SENDERS	MALWARE COUNT	MALWARE SIZE (MB)
Jul 31, 2018 12:24:53		
Mohandoss.R@eginnovations.com	2	0.2728

Figure 4.34: The detailed diagnosis of the Unique receivers measure reported by the Malware Detections test

4.5.3 Spam Detections Test

Spam is unsolicited (and typically unwanted) email messages. If spam mails are not captured promptly and filtered out, they can prove to be an unwanted distraction and can also end up unnecessarily hogging your mailbox space. This is why, its good practice to run the Spam Detections test periodically.

At configured intervals, this test scans the mail traffic over Exchange Online for spam mails. Spam mails detected are then categorized based on their nature. By default, the test captures the following spam categories:

- **SpamIPBlock:** Messages that were blocked based on sender IP
- **SpamDBEBFilter:** Messages that were blocked based on checking the recipient against the directory. This happens when a message is addressed to an unknown recipient.
- **SpamEnvelopeBlock:** Messages that were blocked based on SMTP
- **SpamContentFiltered:** Messages that passed the initial IP and SMTP filters and were filtered based on content, rules or other spam configurations.

For each spam category, the test then reports the count of spam mails of that category that were found in incoming mails and outgoing mails. This will reveal to administrators whether too many spam mails are coming in or going out of the monitored Office 365 tenant, and the most common spam type. Based on the pointers provided by these metrics, administrators can make intelligent spam filtering customizations.

Moreover, the detailed metrics reported by the test reveal the top senders and receivers of spam mails. This will point administrators to email traffic that they may want to track closely, so as to check for spams.

The test additionally reports the size of the incoming and outgoing spam mails. Detailed diagnostics accurately point administrators to users who sent/received large-sized spam mails, thus enabling administrators to analyze the impact of spam mail size on the mailbox size of those users.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each category of spam mails sent/received over Exchange Online

First-level descriptor: Spam mail category

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. Configure the credentials of such a user against O365 User Name and O365 Password

Parameters	Description
	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 **2.1.1**.
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 suite embeds an

Parameters	Description
	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
Inbound spam items	Indicates the number of incoming spam mails of this category.	Number	A high value for this measure is a cause for concern, as it indicates that many of the mails received are spam mails. In this case, use the detailed diagnosis of this measure to view the top-10 receivers, in terms of the number of spam mails they received. This information, thus points administrators to those receivers who were worst hit by spam mails.
Outbound spam items	Indicates the number of spam mails of this category that were sent.	Number	A high value for this measure is a cause for concern, as it indicates that many of the mails sent were spam mails. In this case, use the detailed diagnosis of this measure to view the top-10 senders, in terms of the number of spam mails they sent. This will also point you to those senders who are probably responsible for generating a lot of spam mails and frustrating receivers.
Inbound spam size	Indicates the total size of incoming spam mails of	GB	If the value of this measure is abnormally high, then use the detailed

Measurement	Description	Measurement Unit	Interpretation
	this category.		diagnosis of this measure to view the top-10 receivers, in terms of the size of the spam mails they received. If the mailboxes of these receivers increase in size suddenly, then check the spam mail size of these receivers to see if the spam mails caused the abnormal mailbox growth.
Outbound malware size	Indicates the total size of the outgoing spam mails of this category.	GB	If the value of this measure is abnormally high, then use the detailed diagnosis of this measure to view the top-10 senders, in terms of the size of the spam mails they sent. If the mailboxes size of these senders increase suddenly, then check the spam mail size of these senders to see if the spam mails caused the abnormal mailbox growth.
Unique senders	Indicates the number of unique senders of spam mails of this category.	Number	Use the detailed diagnosis of this measure to view the top-10 senders, in terms of the number of spam mails they sent .
Unique receivers	Indicates the number of unique receivers of spam mails of this category.	Number	Use the detailed diagnosis of this measure to view the top-10 receivers, in terms of the number of spam mails they received.

The detailed diagnosis of the *Inbound spam items* measure lists the top-10 receivers, in terms of the number of spam mails they received. This will point you to that receiver who received the maximum number of spam mails and was hence affected the worst by it. With the help of the detailed metrics, you can also accurately identify who sent the spam mails to the top receive and the size of these spam mails. Using this information, administrators can tell over which email communication - i.e., communication between which sender and receiver - the maximum number of spam mails were trafficked; such email communication may be pulled up for closer monitoring.

Top 10 Users with Large Spam Mails

SENDER ADDRESS	RECEIVER ADDRESS	SPAM SIZE (MB)	SPAM COUNT
04-09-18 18:41:57			
sandhya.tg@cii.in	sreeni@eginnovations.com	1.41	1
sandhya.tg@cii.in	ajay@eginnovations.com	1.41	1
sandhya.tg@cii.in	india-resigned@eginnovations.com	1.41	1
newsletter@indiaretailnews.com	kharthik@eginnovations.com	1	1
kamal@crimsoncloud.in	narendhran@eginnovations.com	0.3	2
kamal@crimsoncloud.in	karthick.b@eginnovations.com	0.3	2
kamal@crimsoncloud.in	sureshkumaran.sathyamurthi@eginnovations.com	0.3	2
kamal@crimsoncloud.in	supportindia@eginnovations.com	0.3	2
kamal@crimsoncloud.in	jayamurugan.s@eginnovations.com	0.3	2
newsletter@indiaretailnews.com	network@eginnovations.com	0.18	1

Figure 4.35: The detailed diagnosis of the Inbound malware items measure

The detailed diagnosis of the *Outbound spam items* measure lists the top-10 senders, in terms of the number of spam mails they sent. This will point you to that sender who sent the maximum number of spam mails. With the help of the detailed metrics, you can also accurately identify who received the spam mails from the top sender and the total size of these spam mails. Using this information, administrators can tell over which email communication - i.e., communication between which sender and receiver - the maximum number of spam mails were trafficked; such email communication may be pulled up for closer monitoring.

Top 10 Users with Large Spam Mails

SENDER ADDRESS	RECEIVER ADDRESS	SPAM SIZE (ME
04-09-18 17:46:16		
postmaster@eginnovations.com	antispam@eginnovations.com	4.92
postmaster@eginnovations.com	abdulkareem@aumbrokers.com	3.92
postmaster@eginnovations.com	jagadeesha.vishwanatha=citrix.com._.n74slac24oikcefz@0hu7lwzqdwjqfrm2.f2nmdgbcb3rd5jya.ejgl.3-6m9veau.na67.bnc.salesforce.com	0.09

Figure 4.36: The detailed diagnosis of the Outbound spam items measure

Use the detailed diagnosis of the *Unique senders* measure to view the top-10 senders, in terms of the number of spam mails they sent. This will point administrators to that sender who is responsible for unnecessarily spamming receivers, much to their frustration.

Top 10 Users with Spam Mails

SENDER ADDRESS	NO OF SPAM MAILS
04-09-18 18:41:57	
kamal@crimsoncloud.in	10
newsletter@indiaretailnews.com	5
subscriptions@smartpicture.org	4
sandhya.tg@cii.in	3
no-reply@edm.thecorporatetreasurer.com	1
sarina@i-globalearning.com	1
mx-59545445435@protection.office-365.com	1

Figure 4.37: The detailed diagnosis of the Unique senders measure reported by the Spam Detections test

Use the detailed diagnosis of the *Unique receivers* measure to view the top-10 receivers, in terms of the number of spam mails they received. This will point administrators to that receiver who was most affected by spam mails.

Top 10 Users with Spam Mails

RECEIVER ADDRESS	NO OF SPAM MAILS
04-09-18 18:41:57	
sreeni@eginnovations.com	3
sureshkumaran.sathyamurthi@eginnovations.com	2
karthick.b@eginnovations.com	2
jayamurugan.s@eginnovations.com	2
narendhran@eginnovations.com	2
supportindia@eginnovations.com	2
india-resigned@eginnovations.com	1
ajay@eginnovations.com	1
karthikg@eginnovations.com	1
manikandan@eginnovations.com	1

Figure 4.38: The detailed diagnosis of the Unique receivers measure reported by the Spam Detections test

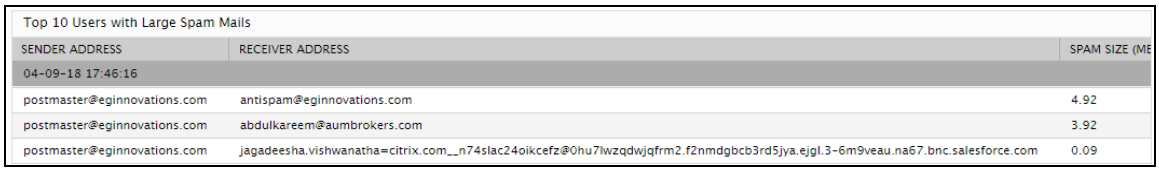
Use the detailed diagnosis of the *Inbound spam size* measure to view the top-10 receivers, in terms of the total size of the spam mails they received. This will point administrators to that receiver who has received large-sized spam mails. If that receiver's mailbox size suddenly grew at around the same time of the spam mails, you can conclude that it is owing to the spam mail size. The detailed statistics also point you to who sent such large-sized spam mails to the top receiver. This sender can be pulled up for questioning.

Top 10 Users with Large Spam Mails

SENDER ADDRESS	RECEIVER ADDRESS	SPAM SIZE (MB)	SPAM COUNT
04-09-18 18:41:57			
sandhya.tg@cii.in	sreeni@eginnovations.com	1.41	1
sandhya.tg@cii.in	ajay@eginnovations.com	1.41	1
sandhya.tg@cii.in	india-resigned@eginnovations.com	1.41	1
newsletter@indiaretailnews.com	kharthik@eginnovations.com	1	1
kamal@crimsoncloud.in	narendhran@eginnovations.com	0.3	2
kamal@crimsoncloud.in	karthick.b@eginnovations.com	0.3	2
kamal@crimsoncloud.in	sureshkumaran.sathyamurthi@eginnovations.com	0.3	2
kamal@crimsoncloud.in	supportindia@eginnovations.com	0.3	2
kamal@crimsoncloud.in	jayamurugan.s@eginnovations.com	0.3	2
newsletter@indiaretailnews.com	network@eginnovations.com	0.18	1

Figure 4.39: The detailed diagnosis of the Inbound spam size measure

Use the detailed diagnosis of the *Outbound spam size* measure to view the top-10 senders, in terms of the total size of the spam mails they sent. This will point administrators to that sender who has sent large-sized spam mails. If that sender's mailbox size suddenly grew at around the same time of the spam mails, you can conclude that it is owing to the spam mail size. The detailed statistics also point you to who received such large-sized spam mails from the top sender. This sender can be pulled up for questioning.



Top 10 Users with Large Spam Mails

SENDER ADDRESS	RECEIVER ADDRESS	SPAM SIZE (MB
04-09-18 17:46:16		
postmaster@eginnovations.com	antispam@eginnovations.com	4.92
postmaster@eginnovations.com	abdulkareem@aumbrokers.com	3.92
postmaster@eginnovations.com	jagadeesha.vishwanatha=citrix.com__n74slac24oikcefz@0hu7lwzqdwjqfrm2.f2nmdgbcb3rd5jya.ejgl.3-6m9veau.na67.bnc.salesforce.com	0.09

Figure 4.40: The detailed diagnosis of the Outbound spam size measure

4.5.4 Transport Rule Hits Test

You can use mail flow rules (also known as transport rules) to identify and take action on messages that flow through your Office 365 organization. Mail flow rules are similar to the Inbox rules that are available in Outlook and Outlook on the web. The main difference is mail flow rules take action on messages while they're in transit, and not after the message is delivered to the mailbox. Mail flow rules contain a richer set of conditions, exceptions, and actions, which provides you with the flexibility to implement many types of messaging policies.

A mail flow rule is made of conditions, exceptions, actions, and properties:

- Conditions: Conditions identify the messages that you want to apply the actions to.
- Exceptions: Exceptions, optionally identify the messages that the actions shouldn't apply to.
- Actions: Actions specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions.
- Properties: Properties specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.

All messages that flow through your organization are evaluated against the enabled mail flow rules in your organization. To know whether any of these messages match a configured rule, and if so, which rule it is, use the Transport Rule Hits test. This test evaluates incoming and outgoing messages against configured transport rules, and reports the count of messages that conform to any of the rules. Detailed diagnostics of the test reveal which messages match which rule and what action has been taken on such messages. This enables administrators to review and evaluate their rule and action configurations, and figure out if rules need to be fine-tuned.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each event type related to transport rules

First-level descriptor: Event type

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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 *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 hits	Indicates the number of messages that conform to transport rules.	Number	The value of this measure is a sum of the values of the *Inbound rule hits* and *Outbound rule hits* measures.
Inbound rule hits	Indicates the number of incoming messages that conform to transport rules.	Number	Use the detailed diagnosis of this measure to know which incoming messages matched which rule and what action was taken on them.
Outbound mail hits	Indicates the number of outgoing messages that conform to transport rules.	Number	Use the detailed diagnosis of this measure to know which outgoing messages matched which rule and what action was taken on them.
Unique senders	Indicates the total number of unique senders of messages that match	Number	

Measurement	Description	Measurement Unit	Interpretation
	one/more transport rules.		
Unique receivers	Indicates the number of unique recipients of messages that match one/more transport rules.	Number	

The detailed diagnosis of the *Inbound rule hits* measure lists the 10 messages that were received recently, which conformed to one/more transport rules. The ID of the messages, the subject of the messages, when they were sent/received, the sender and receiver of such messages, the rules that they matched, and the actions that were taken on them are revealed as part of detailed diagnosis. This will enable administrators to review and evaluate their rule and action configurations, and figure out if rules need to be fine-tuned.

Recent 10 Inbound Rule Items

DATE	DOMAIN	TRANSPORTRULE	SUBJECT	MESSAGESIZE (KB)	SENDERADDRESS	RECI
04-09-18 18:50:38						
9/3/2018 7:19:12 AM	eginnovations.com	Manish	Automatic reply: EG Innovations - APM Solution for HCL	33.76	daminder.s@hcl.com	mar
9/3/2018 7:01:36 AM	eginnovations.com	Manish	RE: EG Innovations - APM Solution for HCL	449.59	jadeesh.u@hcl.com	mar
9/3/2018 6:29:27 AM	eginnovations.com	Manish	RE: EG Innovations - APM Solution for HCL	303.51	GagandeepKohli@hcl.com	mar
9/3/2018 6:15:03 AM	eginnovations.com	Manish	RE: EG Innovations - APM Solution for HCL	297.76	GagandeepKohli@hcl.com	mar

Figure 4.41: The detailed diagnosis of the Inbound rule hits measure

The detailed diagnosis of the *Outbound rule hits* measure lists the 10 messages that were sent recently, which conformed to one/more transport rules. The ID of the messages, the subject of the messages, when they were sent/received, the sender and receiver of such messages, the rules that they matched, and the actions that were taken on them are revealed as part of detailed diagnosis. This will enable administrators to review and evaluate their rule and action configurations, and figure out if rules need to be fine-tuned.

Recent 10 Outbound Rule Items

DATE	DOMAIN	TRANSPORTRULE	SUBJECT	MESSAGESIZE (KB)	SENDERADDRESS
04-09-18 18:50:38					
9/4/2018 4:01:03 AM	eginnovations.com	Manish	RE: hcl	248.61	srinivas@eginnovations
9/3/2018 10:48:32 AM	eginnovations.com	Manish	Your leads from VMworld US 2018	44.67	gayathri.ashok@eginno
9/3/2018 10:48:32 AM	eginnovations.com	Manish	Your leads from VMworld US 2018	44.67	gayathri.ashok@eginno
9/3/2018 9:47:38 AM	eginnovations.com	Manish	Re: Leave on 6th and 7th	19.29	anands@eginnovations.
9/3/2018 9:32:38 AM	eginnovations.com	Manish	Re: Leave on 6th and 7th	14.96	anands@eginnovations.
9/3/2018 8:10:32 AM	eginnovations.com	Manish	Re: Leave on 6th and 7th	9.7	anands@eginnovations.
9/3/2018 7:28:03 AM	eginnovations.com	Manish	Welcome New Joinee Narayan.S - Software Engineer - Arun`s team	49.56	hr@eginnovations.com
9/3/2018 7:28:03 AM	eginnovations.com	Manish	Welcome New Joinee Narayan.S - Software Engineer - Arun`s team	49.56	hr@eginnovations.com
9/3/2018 7:28:03 AM	eginnovations.com	Manish	Welcome New Joinee Narayan.S - Software Engineer - Arun`s team	49.56	hr@eginnovations.com
9/3/2018 7:28:03 AM	eginnovations.com	Manish	Welcome New Joinee Narayan.S - Software Engineer - Arun`s team	49.56	hr@eginnovations.com

Figure 4.42: The detailed diagnosis of the Outbound rule hits measure

4.5.5 Mail Deliverability Test

Frequents breaks in the availability of Exchange Online and prolonged slowness in delivery of mails sent/received via Exchange Online, can adversely impact user experience with Exchange Online. To assure users of a high quality experience with Exchange Online at all times, administrators should be able to proactively detect and promptly avert the non-availability of Exchange Online and any processing slowness that it may be experiencing. This is where the Mail Deliverability test helps!

At configured intervals, this test emulates a user sending/receiving a configured number of emails (default: 1) over Exchange Online. In the process, the test verifies the availability of Exchange Online for sending and receiving the emulated mail(s), and also reports the time taken to send and receive mails. This way, the test notifies administrators of the non-availability of Exchange Online and processing bottlenecks that it may be experiencing, well before users notice and complain.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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

Parameters	Description
	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*.
Number of Messages	Specify the number of messages this test should send over Exchange Online, as part of the emulation. By default, this parameter is set to 1.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Send mail availability	Indicates whether/not Exchange Online is available to send emails.	Percent	If the value of this measure is 100%, it implies that Exchange Online is available for sending emails. The value 0 on the other hand denotes that Exchange Online is not available for sending emails.
Sent messages	Indicates the number of messages this test sent successfully over Exchange Online.	Number	If this test has been configured to send more than one email over Exchange Online (via the Number of Messages parameter), then the value of this measure will clearly indicate whether

Measurement	Description	Measurement Unit	Interpretation
			all messages were successfully sent or not, and if not, how many email transmissions failed.
Avg time to send messages	Indicates the average time taken by Exchange Online to send messages.	Seconds	Ideally, the value of this measure should be low. A high value is indicative of a bottleneck when sending messages.
Receive mail availability	Indicates whether/not Exchange Online is available to receive emails.	Percent	If the value of this measure is 100%, it implies that Exchange Online is available for receiving emails. The value 0 on the other hand denotes that Exchange Online is not available for receiving emails.
Received messages	Indicates the number of messages this test received successfully over Exchange Online.	Number	If say, this test has been configured to receive more than one email over Exchange Online (via the Number of Messages parameter), then the value of this measure will clearly indicate whether all messages were successfully received or not, and if not, how many email emails could not be received.
Avg time to receive messages	Indicates the average time taken by Exchange Online to receive messages.	Seconds	Ideally, the value of this measure should be low. A high value is indicative of a bottleneck when receiving messages.
Avg round-trip time	Indicates the average time taken to send a message over Exchange Online and receive it.	Seconds	Ideally, the value of this measure should be low. A high value is indicative of a bottleneck when receiving messages.
Max round-trip time	Indicates the maximum time taken to send a message over Exchange Online and receive it.	Seconds	

4.5.6 Mail Traffic Statistics Test

Where Exchange Online handles heavy mail traffic, it is impossible for administrators to manually track each email transmitted by Exchange Online, and to determine whether/not it has been successfully delivered to the designated recipients. In such environments therefore, administrators can periodically run the Mail Traffic Statistics test, receive deep-dive insights on the flow of mails through Exchange Online, and accurately determine the delivery status of the emails.

This test tracks the mails going in and out of the Exchange Online organization, reports the count of inbound and outbound mails, and thus reveals the level of mail traffic on Exchange Online. The test further reveals the nature of the mail traffic by reporting the count of internal and external mails. The total size of mails is also reported, with detailed diagnostics shedding light on mail activity that is suspect owing to its abnormal size. Most importantly, the test reports the count of mails in different states, thus promptly alerting administrators to delivery failures / slowness. Detailed diagnostics accurately point administrators to the exact mails that are pending delivery and the ones that could not be delivered.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the monitored Offce 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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
Domain, Domain	**These parameters are applicable only if the eG agent needs to communicate**

Parameters	Description
User Name, Domain Password, and Confirm Password	**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 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
Unique senders	Indicates the number of unique senders of emails.	Number	
Unique receivers	Indicates the number of unique receivers of emails.	Number	
Unique sender IPs	Indicates the number of unique IPs from which emails were sent.	Number	
Inbound mail items	Indicates the number of emails coming into all domains in the monitored tenant.	Number	Use the detailed diagnosis of this measure to view the top-10 recipients, in terms of the number of mails they received. This will point administrators to those recipients who have been receiving an abnormally large number of emails and is contributing to the heavy email mail traffic on Exchange Online.
Inbound mail size	Indicates the total size of emails received by the domains in the monitored tenant.	GB	Use the detailed diagnosis of this measure to view the top-10 recipients, in terms of the total size of emails they received.
Outbound mail items	Indicates the number of emails flowing out of the domains in the monitored tenant.	Number	Use the detailed diagnosis of this measure to view the top-10 senders, in terms of the number of mails they sent. This will point administrators to those senders who have been sending an abnormally large number of emails and is contributing to the heavy email mail traffic on Exchange Online.
Outbound mail size	Indicates the total size of emails sent by the domains in the monitored	GB	Use the detailed diagnosis of this measure to view the top-10 senders, in terms of the total size of emails they

Measurement	Description	Measurement Unit	Interpretation
	tenant.		sent.
Total mail items	Indicates the total number of emails sent/received by domains in the monitored tenant.	Number	This measure is the sum of the values of the *Inbound mail items* and *Outbound mail items* measures. This is a good indicator of the total mail traffic on Exchange Online. If the value of this measure is abnormally high, you can check the values of the *Inbound mail items* and *Outbound mail items* measures to know what is causing the abnormal traffic - a high volume of incoming mails? or a high volume of outgoing mails? Based on the result, you can use the detailed diagnosis of the corresponding measure to know which exact sender/receiver (as the case may be) is responsible for the abnormal email traffic.
Total mails size	Indicates the total size of emails sent/received by domains in the monitored tenant.	GB	This measure is the sum of the values of the *Inbound mail size* and *Outbound mail size* measures. If the value of this measure is abnormally high, you can check the values of the *Inbound mails size* and *Outbound mails size* measures to determine whether the size of incoming mails is more than that of outgoing mails or vice-versa. If *Inbound mails size* is abnormally high, then proceed to determine what type of incoming mails are of an abnormal size - internal mails? or external mails? For this, compare the value of the *Size of internal mails received* and *Size of external mails received* measures. Likewise, if the value of the *Outbound mail size*

Measurement	Description	Measurement Unit	Interpretation
			measure is very high, then compare the value of the *Size of internal mails sent* and *Size of external mails sent* measures to know what type of outbound mail activity is suspect owing to abnormal mail size - outgoing internal mail activity? or outgoing external mail activity? Based on the result, you can use the detailed diagnosis of the corresponding measure to know which exact sender's/receiver's (as the case may be) mail size is much higher than the rest. Such a sender's/receiver's mail activity may have to be investigated.
Internal emails sent	Indicates the number of emails sent to receivers who are in the same domain as the senders.	Number	If the *Total mail items* and *Outbound mail items* measures report an abnormally high value, then take a look at this measure to figure out if the abnormal outbound email traffic is owing to too many internal mails being sent. Use the detailed diagnosis of this measure to identify who sent the maximum number of internal mails.
Size of internal emails sent	Indicates the total size of emails sent to receivers who are in the same domain as the senders.	GB	If the *Total mails size* and *Outbound mails size* measures report abnormally high values, then take a look at this measure to figure out if there is any internal outbound email activity that is suspicious owing to its abnormal size. Use the detailed diagnosis of the *Internal emails sent* measure to identify who sent internal emails of an abnormal size. The mail activity of such senders can be investigated.
Internal emails received	Indicates the number of emails received by	Number	If the *Total mail items* and *Inbound mail items* measures report an

Measurement	Description	Measurement Unit	Interpretation
	recipients who are in the same domain as the senders.		abnormally high value, then take a look at this measure to figure out if the abnormal inbound email traffic is owing to too many internal mails being received. Use the detailed diagnosis of this measure to identify who received the maximum number of internal mails.
Size of internal emails received	Indicates the total size of emails received by recipients who are in the same domain as the senders.	GB	If the *Total mails size* and *Inbound mails size* measures report abnormally high values, then take a look at this measure to figure out if there is any internal inbound email activity that is suspicious owing to its abnormal size. Use the detailed diagnosis of the *Internal emails received* measure to identify who received internal emails of an abnormal size. The mail activity of such recipients can be investigated.
External emails sent	Indicates the number of emails sent to receivers who are in a domain different from that of the senders.	Number	If the *Total mail items* and *Outbound mail items* measures report an abnormally high value, then take a look at this measure to figure out if the abnormal outbound email traffic is owing to too many external mails being sent. Use the detailed diagnosis of this measure to identify who sent the maximum number of external mails.
Size of external emails sent	Indicates the total size of emails sent to receivers who are in a domain different from that of the senders.	GB	If the *Total mails size* and *Outbound mails size* measures report abnormally high values, then take a look at this measure to figure out if there is any external outbound email activity that is suspicious owing to its abnormal size. Use the detailed diagnosis of the *External emails sent* measure to identify who sent external emails of an abnormal size. The mail activity of such

Measurement	Description	Measurement Unit	Interpretation
			senders can be investigated.
External emails received	Indicates the number of emails received by recipients who are in a domain different from that of the senders.	Number	If the *Total mail items* and I*nbound mail items* measures report an abnormally high value, then take a look at this measure to figure out if the abnormal inbound email traffic is owing to too many external mails being received. Use the detailed diagnosis of this measure to identify who received the maximum number of external mails.
Size of external emails received	Indicates the total size of emails received by recipients who are in a domain different from that of the senders.	GB	If the *Total mails size* and *Inbound mails size* measures report abnormally high values, then take a look at this measure to figure out if there is any external inbound email activity that is suspicious owing to its abnormal size. Use the detailed diagnosis of the *External emails received* measure to identify who received external emails of an abnormal size. The mail activity of such recipients can be investigated.
Rejected or redirected	Indicates the number of emails that were rejected or redirected.	Number	If this measure reports a non-zero value, then use the detailed diagnosis of the measure to know which messages were rejected/redirected. Using this information, you can figure out if your message flow rules need to be tweaked.
Failed	Indicates the number of messages that could not be delivered.	Number	Ideally, the value of this measure should be 0. If this measure reports a non-zero value, it means that one/more messages could not be delivered. In this case, use the detailed diagnosis of this measure to identify the emails for which delivery failed. An email delivery is considered to have

Measurement	Description	Measurement Unit	Interpretation
			failed if delivery was attempted and it failed or it was not delivered as a result of actions taken by the filtering service - eg., if the message was determined to contain malware.
Pending	Indicates the number of messages that are waiting to be delivered.	Number	Typically, an email's status will be Pending if its delivery is being attempted or re-attempted. If the value of this measure increases consistently, it could hint at a processing bottleneck on Exchange Online. This may warrant further investigation. In this case, use the detailed diagnosis of this measure to identify the emails that are yet to be delivered.
Getting status	Indicates the number of emails that are in the Getting status presently.	Number	If an email is in the Getting status, it means that the email was recently received by Office 365, but no other status data is yet available. You may have to check back in a few minutes.
Delivered	Indicates the number of emails that were successfully delivered.	Number	A high value is desired for this measure.
Resolved	Indicates the number of emails that are in the RESOLVED status currently.	Number	A RESOLVED event is triggered if a message was redirected to a new recipient address based on an Active Directory look up. When this happens, the original recipient address is listed in a separate row in the message trace along with the final delivery status for the message.
Filtered as spam	Indicates the number of emails that were filtered as spam.	Number	If this measure reports a non-zero value, it means that that one/more mails have been identified as spams, and were rejected or blocked (not

Measurement	Description	Measurement Unit	Interpretation
			quarantined).
Expanded	Indicates the number of emails in the Expanded state currently.	Number	The delivery status of a message is set as Expanded, if the message was sent to a distribution group that was expanded.
Quarantined	Indicates the number of emails that have been quarantined.	Number	You can set up quarantine for incoming email messages in Office 365 where messages that have been filtered as spam, bulk mail, phishing mail, mail that contains malware, and mail that matched a specified mail flow rule can be kept for later review. As an Office 365 user, you can manage messages that were sent to quarantine instead of sent to you in one of two ways: by responding to spam notifications sent to you directly (if your admin has set this up), or by using the Security & Compliance Center.
Unknown	Indicates the number of emails for which the delivery status is Unknown presently.	Number	Ideally, the value of this measure should be 0.
Unique outbound domains	Indicates the number of unique domains that sent emails to the domains in the monitored Office 365 tenant.	Number	Use the detailed diagnosis of this measure to know the outbound domains.
Unique inbound domains	Indicates the number of unique domains that received emails from the domains in the monitored tenant.	Number	Use the detailed diagnosis of this measure to know the inbound domains.

The detailed diagnosis of the *Internal emails sent* measure reveals the top-10 senders of internal emails, in terms of the number of emails they sent. In the event of abnormally high internal email traffic on Exchange Online, you can use these detailed metrics to quickly identify the sender

responsible for such traffic. The number of internal emails received by each sender and the total size of outbound and inbound emails per sender are also reported as part of detailed metrics.

Top 10 Internal Emails Sent By Items

SENDER	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 17:55:19				
gayathri.ashok@eginnovations.com	6	21	986	4284
egmail@eginnovations.com	0	20	0	211
srinivas@eginnovations.com	19	17	2899	585
testing@eginnovations.com	0	15	0	2442
sreeni@eginnovations.com	9	15	2437	1491
Jayamurugan.S@eginnovations.com	3	15	98	491
chitra@eginnovations.com	2	14	1468	1366
webmaster@eginnovations.com	0	12	0	155
karthikg@eginnovations.com	16	12	333	356
egeurocrm@eginnovations.com	0	10	0	496

Figure 4.43: The detailed diagnosis of the Internal emails sent measure

The detailed diagnosis of the *Internal emails received* measure reveals the top-10 recipients of internal emails, in terms of the number of emails they received. In the event of abnormally high internal email traffic on Exchange Online, you can use these detailed metrics to quickly identify the receiver responsible for such traffic. The number of internal emails sent by each receiver and the total size of outbound and inbound emails per receiver are also reported as part of detailed metrics.

Top 10 Internal Emails Received By Items

RECIPIENT	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 17:55:19				
srinivas@eginnovations.com	19	17	2899	585
karthikg@eginnovations.com	16	12	333	356
kharthik@eginnovations.com	13	5	303	191
manikandan@eginnovations.com	11	1	248	48
raja@eginnovations.com	11	4	2181	126
parthasarathi.pm@eginnovations.com	11	0	248	0
vijayakumar@eginnovations.com	10	0	200	0
sreeni@eginnovations.com	9	15	2437	1491
venkateswari.j@eginnovations.com	8	8	1180	1180
madhu.barathi@eginnovations.com	7	1	985	333

Figure 4.44: The detailed diagnosis of the Internal emails received measure

The detailed diagnosis of the *External emails sent* measure reveals the top-10 senders of external emails, in terms of the number of emails they sent. In the event of abnormally high external email traffic on Exchange Online, you can use these detailed metrics to quickly identify the sender responsible for such traffic. The number of external emails received by each sender and the total size of outbound and inbound emails per sender are also reported as part of detailed metrics.

Top 10 External Emails Sent By Items

RECIPIENT	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 17:55:19				
leonard@crimsoncloud.in	28	0	1306	0
network@eginnovations435.onmicrosoft.com	8	0	155	0
karthik@karthik.com	4	0	97	0
sakthi@eginnovations435.onmicrosoft.com	2	0	339	0
kesavan@eginnovations435.onmicrosoft.com	2	0	339	0
srinivas@eginnovations435.onmicrosoft.com	2	0	339	0
kalaiarasi@eginnovations435.onmicrosoft.com	2	0	339	0
sandhya@eginnovations435.onmicrosoft.com	2	0	339	0
ydchoi@uws.co.kr	1	1	47	41
binoyp@mashreq.com	1	0	335	0

Figure 4.45: The detailed diagnosis of the External emails sent measure

The detailed diagnosis of the *External emails received* measure reveals the top-10 recipients of external emails, in terms of the number of emails they received. In the event of abnormally high external email traffic on Exchange Online, you can use these detailed metrics to quickly identify the receiver responsible for such traffic. The number of external emails sent by each receiver and the total size of outbound and inbound emails per receiver are also reported as part of detailed metrics.

Top 10 External Emails Received By Items

SENDER	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS
04-09-18 17:55:19				
info@leadmaster.com	0	24	0	2642
noreply@sf-notifications.com	0	20	0	766
googlealerts-noreply@google.com	0	12	0	885
RLI@se1.RapidLearningInstitute.net	0	10	0	353
Sandeep.Jadhav@transunion.com	0	10	0	7324
eGAlert@wda.gov.sg	0	9	0	350
MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@eGinnovations435.onmicrosoft.com	0	7	0	1198
businessoutfitters@shop.business.landsend.com	0	6	0	394
victor.mui@basf.com	0	6	0	737
info@ed-email.techtarget.com	0	5	0	127

Figure 4.46: The detailed diagnosis of the External emails received measure

The detailed diagnosis of the *Inbound mail items* measure reveals the top-10 receivers of emails, in terms of the number of emails they received. This will point administrators to that receiver who has received the maximum number of messages. In the event of abnormal mail traffic on Exchange Online, this information will help administrators identify the recipient who is probably contributing to the heavy traffic. The count of emails sent by each receiver and the total size of inbound and outbound mails per receiver are also displayed as part of detailed diagnostics.

Top 10 Receivers by Number of Mail Items

RECIPIENT	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 19:01:05				
srinivas@eginnovations.com	73	12	6731	311
karthikg@eginnovations.com	21	6	2751	640
vinod.mohan@eginnovations.com	20	11	3288	1300
sreeni@eginnovations.com	19	1	12923	46
us-resigned@eginnovations.com	17	0	984	0
gayathri.ashok@eginnovations.com	16	6	2495	155
raja@eginnovations.com	15	112	3723	2033
antony@eginnovations.com	14	61	2601	6696
hydro.soh@eginnovations.com	13	0	2048	0
kesavan@eginnovations.com	13	18	2697	433

Figure 4.47: The detailed diagnosis of the Inbound mail items measure

The detailed diagnosis of the *Inbound mails size* measure lists the top-10 email recipients, in terms of the total size of emails they received. If the total size of mails appears to be unusually high, administrators can use these detailed metrics to accurately pinpoint the recipient who has received mails of large sizes. The number of mails received and sent by each recipient and the outbound mails size is also displayed as part of detailed statistics.

Top 10 Receivers by Mails Size

RECIPIENT	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 19:01:05				
sreeni@eginnovations.com	19	1	12923	46
jim.giovinazzo@eginnovations.com	3	0	12024	0
srinivas@eginnovations.com	73	12	6731	311
karthick.b@eginnovations.com	10	24	5983	11762
narendhran@eginnovations.com	12	0	5596	0
sureshkumaran.sathyamurthi@eginnovations.com	9	6	5528	19193
raja@eginnovations.com	15	112	3723	2033
supportindia@eginnovations.com	2	0	3689	0
Jayamurugan.S@eginnovations.com	2	2	3689	53
vinod.mohan@eginnovations.com	20	11	3288	1300

Figure 4.48: The detailed diagnosis of the Inbound mails size measure

The detailed diagnosis of the *Outbound mail items* measure reveals the top-10 senders of emails, in terms of the number of emails they sent. This will point administrators to that sender who has sent the maximum number of messages. In the event of abnormal mail traffic on Exchange Online, this information will help administrators identify the sender who is probably contributing to the heavy traffic by sending too many messages. The count of emails received by each sender and the total size of inbound and outbound mails per sender are also displayed as part of detailed diagnostics.

Top 10 Senders by Number of Mail Items

SENDER	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 19:01:05				
john.worthington@eginnovations.com	12	151	1845	140202
raja@eginnovations.com	15	112	3723	2033
support@eginnovations.com	7	110	1839	2334
gandhi@eginnovations.com	8	65	1857	35616
antony@eginnovations.com	14	61	2601	6696
testing@eginnovations.com	1	43	26	11319
karthick.b@eginnovations.com	10	24	5983	11762
anands@eginnovations.com	6	23	1834	3054
kesavan@eginnovations.com	13	18	2697	433
accts@eginnovations.com	1	14	46	12109

Figure 4.49: The detailed diagnosis of the Outbound mail items measure

The detailed diagnosis of the *Outbound mails size* measure lists the top-10 email senders, in terms of the total size of emails they sent. If the total size of mails appears to be unusually high, administrators can use these detailed metrics to accurately pinpoint the sender who has sent mails of large sizes. The number of mails received and sent by each sender and the inbound mails size is also displayed as part of detailed statistics.

Top 10 Senders by Mails Size

SENDER	INBOUND ITEMS	OUTBOUND ITEMS	INBOUND ITEMS SIZE (KB)	OUTBOUND ITEMS SIZE (KB)
04-09-18 19:01:05				
john.worthington@eginnovations.com	12	151	1845	140202
gandhi@eginnovations.com	8	65	1857	35616
sureshkumaran.sathyamurthi@eginnovations.com	9	6	5528	19193
accts@eginnovations.com	1	14	46	12109
karthick.b@eginnovations.com	10	24	5983	11762
testing@eginnovations.com	1	43	26	11319
brijesh@eginnovations.com	2	3	81	7456
antony@eginnovations.com	14	61	2601	6696
renne.bots@eginnovations.com	3	9	1167	3837
anands@eginnovations.com	6	23	1834	3054

Figure 4.50: The detailed diagnosis of the Outbound mails size measure

The detailed diagnosis of the *Failed* messages measure, provides complete details of the messages that could not be delivered. The senders of such messages, the recipient of these messages, and the message subject is reported, so as to ease the troubleshooting of delivery failures.

Failed Messages

DATE	SENDER ADDRESS	RECIPIENTADDRESS	SUBJEC
04-09-18 17:55:19			
9/4/2018 12:03:28 PM	postmaster@eginnovations.com	antispam@eginnovations.com	Undeli
9/4/2018 12:03:24 PM	info@rs-flond.ch	birnbaum@eginnovations.com	Re: loa
9/4/2018 11:55:24 AM	fantasysports@dream11.com	thirumaran.m@eginnovations.com	??Feat
9/4/2018 11:54:22 AM	renne.bots@eginnovations.com	danny.freese@axaoft.nl	eG Inn
9/4/2018 11:53:13 AM	MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@eGinnovations435.onmicrosoft.com	testing@eginnovations.com	Undeli
9/4/2018 11:53:12 AM	testing@eginnovations.com	saurabh.kumar@eginnovations435.onmicrosoft.com	Bug:16
9/4/2018 11:45:19 AM	renne.bots@eginnovations.com	karin.van.ieperen@inisi.com	Berich
9/4/2018 11:30:22 AM	info@ed-email.techtarget.com	hiten@eginnovations.com	3 com

Figure 4.51: The detailed diagnosis of the Failed measure

The detailed diagnosis of the Pending measure provides the complete details of the email messages that have been attempted/re-attempted, and are awaiting delivery. The sender, receiver, and subject of such messages are reported, along with the date on which such messages were sent. This greatly aids administrators troubleshoot delivery delays.

Pending Messages

DATE	SENDERADDRESS	RECIPIENTADDRESS	SUBJECT
04-09-18 17:55:19			
9/4/2018 11:55:26 AM	postmaster@eginnovations.com	bounces+450664-913e-thirumaran.m=eginnovations.com@email.dream11.com	Undeliverable: ??Feature Update: Private C

Figure 4.52: The detailed diagnosis of the Pending measure

The detailed diagnosis of the *Unique outbound domains* measure lists the top-10 domains, in terms of the number of emails they sent. In the event of abnormal email traffic, administrators can use this information to isolate the domain that sent the maximum number of emails and contributed to the traffic.

Top 10 Domain Names By Emails Sent Items

SENDER DOMAIN NAME	NUMBER OF EMAILS SENT	SIZE OF EMAILS(KB)
04-09-18 17:55:19		
leadmaster.com	24	2642
sf-notifications.com	20	766
google.com	12	885
se1.RapidLearningInstitute.net	10	353
transunion.com	10	7324
wda.gov.sg	9	350
eGinnovations435.onmicrosoft.com	7	1198
basf.com	6	737
shop.business.landsend.com	6	394
ed-email.techtarget.com	5	127

Figure 4.53: The detailed diagnosis of the Unique outbound domains measure

The detailed diagnosis of the *Unique inbound domains* measure lists the top-10 domains, in terms of the number of emails they received. In the event of abnormal email traffic, administrators can use this information to isolate the domain that received the maximum number of emails and contributed to the traffic.

Top 10 Domain Names By Emails Received Items

RECIPIENT DOMAIN NAME	NUMBER OF EMAILS RECEIVED	SIZE OF EMAILS(KB)
04-09-18 17:55:19		
crimsoncloud.in	28	1306
eginnovations435.onmicrosoft.com	21	2258
mashreq.com	6	2008
gmail.com	5	351
karthik.com	4	97
uws.co.kr	4	188
externe.bnpparibas.com	3	881
x-pressfeeders.com	3	1014
t-systems.com	1	105
hotmail.com	1	25

Figure 4.54: The detailed diagnosis of the Unique inbound domains measure

4.6 The User/Admin Activities Layer

The tests mapped to this layer enable easy and effective audit of administrator, mailbox owner, and non-owner activities.

Figure 4.55: The tests mapped to the User/Admin Activities layer

4.6.1 Administrator Activities Test

It is important to keep track of the activities of administrators on Exchange Online, as the changes they make may impact the way Exchange Online functions and how it performs. This is why, it is good practice to periodically run the Administrator Activities test .

This test keep tabs on the activities performed by administrators on Exchange Online. In the process, the test reports the count of operations that were performed, the number of admin users who performed the operations, and the count of client IPs from which the administrators initiated these operations. Detailed diagnostics reported by the test reveal which users performed which operations from which client IPs. In the process, you can accurately identify the admin user who has imposed the maximum operational load on Exchange Online. Moreover, if you notice any sudden change in the way the Exchange Online operates or any unexpected dip in the performance of Exchange Online, you can use this test and its detailed metrics to figure out if any critical configuration change was made, and if so, what change is it and which administrator effected the change.

Note:

This test will report metrics only if Audit Logging is enabled for Exchange Online.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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
Total operations	Indicates the total number of operations performed by the administrators.	Number	Use the detailed diagnosis of this measure to know which operations were performed , who performed each operation, and when. This information enables an efficient audit of the activities of administrators.
Unique operations	Indicates the number of unique operations performed by the administrators.	Number	Use the detailed diagnosis of this measure to know which operations were performed and how many times. From this, you can identify the operation that was performed most often on Exchange Online.
Unique users	Indicates the number of unique admin users.	Number	Use the detailed diagnosis of this measure to know who are the unique users, what are the unique operations

Measurement	Description	Measurement Unit	Interpretation
			each user performed, and how many times every operation was performed. This way, you can quickly identify which user imposed the maximum operational load on Exchange Online.
Client IPs	Indicates the number of unique clients from which administrators initiated operations on Exchange Online.	Number	Use the detailed diagnosis of this measure to know the clients from which administrators operated Exchange Online. The unique operations performed from each client and the number of times every operation was performed from that client are also reported as part of detailed diagnostics.
Microsoft admins operations	Indicates the number of operations performed by Microsoft administrators.	Number	

The detailed diagnosis of the *Total operations* measure lists the operations were performed , who performed each operation, and when. This information enables an efficient audit of the activities of administrators.

All Operations

CREATION TIME	OPERATION NAME	CLIENT IP	USER ID	ORIGINATING SERVER	PARAMETERS
Jul 31, 2018 16:25:52					
2018-07-31T09:44:37	HardDelete	-	eTius@eCshareit.onmicrosoft.com	PN1PR0101MB1327 (15.20.1017.000)	-
2018-07-31T09:39:28	HardDelete	-	eTius@eCshareit.onmicrosoft.com	PN1PR0101MB1327 (15.20.1017.000)	-
2018-07-31T09:34:39	HardDelete	-	eTius@eCshareit.onmicrosoft.com	PN1PR0101MB1327 (15.20.1017.000)	-
2018-07-31T09:29:16	HardDelete	-	eTius@eCshareit.onmicrosoft.com	PN1PR0101MB1327 (15.20.1017.000)	-
2018-07-31T09:24:43	HardDelete	-	eTius@eCshareit.onmicrosoft.com	PN1PR0101MB1327 (15.20.1017.000)	-

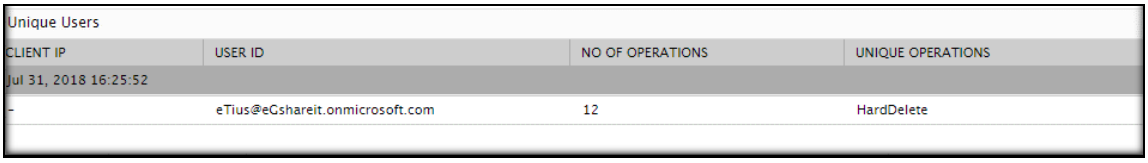
Figure 4.56: The detailed diagnosis of the Total operations measure

The detailed diagnosis of the *Unique operations* measure lists the administrative operations that were performed on Exchange Online and also reveals how many times each operation was performed. From this, you can identify the operation that was performed most often on Exchange Online.

Operations	
N NAME	NUMBER OF OPERATIONS
018 12:14:51	
d	2
e	2

Figure 4.57: The detailed diagnosis of the Unique operations measure

The detailed diagnosis of the *Unique users* measure reveals the unique users, what are the unique operations each user performed, and how many times every operation was performed. This way, you can quickly identify which user imposed the maximum operational load on Exchange Online.

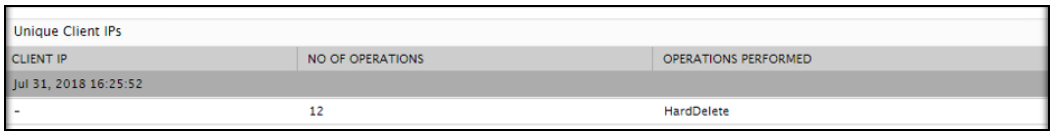


Unique Users

CLIENT IP	USER ID	NO OF OPERATIONS	UNIQUE OPERATIONS
Jul 31, 2018 16:25:52			
-	eTius@eGshareit.onmicrosoft.com	12	HardDelete

Figure 4.58: The detailed diagnosis of the Unique users measure

Using the detailed diagnosis of the *Client IPs* measure, you can identify the clients from which administrators operated Exchange Online. The unique operations performed from each client and the number of times every operation was performed from that client are also reported as part of detailed diagnostics. This way, you will be able to identify the client IP that generated the maximum workload for Exchange Online.



Unique Client IPs

CLIENT IP	NO OF OPERATIONS	OPERATIONS PERFORMED
Jul 31, 2018 16:25:52		
-	12	HardDelete

Figure 4.59: The detailed diagnosis of the Client IPs measure

4.6.2 Non Owner Activities Test

A member of an Office 365 Group who has been granted Send as or Send on behalf permissions can send email as the group, or on behalf of the group.

For example, if Allie Bellew is part of Training Office 365 Group in your organization, and has Send as permissions on the group, if she sends an email as the Office 365 Group, it will look like the Training department from your organization sent the email.

The Send on Behalf permission lets a user send email on behalf of an Office 365 Group. For example, if Donald Forster is a part of the Marketing Office 365 Group, and has Send on Behalf permissions, any email he sends to the group will look like it was sent by **Donald Forster on behalf of Marketing Team**.

To track the operations of users who are configured to Send mail as or on behalf of an Office 365 group, use the Non Owner Activities test.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every type of non-owner

First-level Descriptor: Non-owner type - this can be SendAs and/or SendOnBehalf

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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

Parameters	Description
	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
Total operations	Indicates the total number of operations performed by	Number	Use the detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
	this type of non-owners. For the **Summary** descriptor, this measure will report the total number of operations performed by all non-owners.		measure to know which users have been configured as non-owners - i.e., configured to send mail as or on behalf of an Office 365 group, what operation was performed by each user, when was the operation performed, status of the operation (whether it succeeded or failed), the client from which the operation was initiated, etc.

The detailed diagnosis of the *Total operations* measure lists the users who have been configured as non-owners - i.e., configured to send mail as or on behalf of an Office 365 group, what operation was performed by each user, when was the operation performed, status of the operation (whether it succeeded or failed), the client from which the operation was initiated, etc. This information enables an efficient audit of the activities of non-owners.

CREATION TIME	ID	OPERATION	RESULT	USER TYPE	USER ID	CLIENT IP	CLIENT INFO STRING	EXTERNAL ACCESS
Jul 31, 2018 17:37:35								
2018-07-31T11:49:34	2f7ff120-45d3-4d97-435d-08d5f6dbaf85	SendAs	Succeeded	0	rajesh@eGshareit.onmicrosoft.com	61.12.78.30	Client=OWA;Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36;	False
2018-07-31T11:49:18	ec002d63-ab07-4afb-1aa5-08d5f6dba5ae	SendAs	Succeeded	0	rajesh@eGshareit.onmicrosoft.com	61.12.78.30	Client=OWA;Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36;	False

Figure 4.60: The detailed diagnosis of the Total operations measure reported by the Non Owner Activities test

4.6.3 Owner Activities Test

If you want to audit the activities of specific mailbox owners, then use the Owner Activities Test.

This test automatically discovers the activities performed by configured mailbox owners, and reports the number of times each activity was performed, the number of unique users performing every activity, and the number of clients from which each activity was initiated. Detailed diagnostics

reported by the test reveals which of the configured mailbox owners performed the activity, when, and what was the result of the activity each time it was performed.

Target of the test : Exchange Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every activity/operation performed by a configured mailbox owner

First-level Descriptor: Operation 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 has been assigned the **Service Administrator** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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*.

Parameters	Description
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*.
Mailbox Owners ID	Configure a comma-separated list of the email IDs of mailbox owners you want to monitor - eg., andy@garcia.com,george@clooney.com
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 times this operation was performed.	Number	Use the detailed diagnosis of this measure to know which mailbox owner performed the operation, when, and what was the result of the activity each time it was performed.
Unique users	Indicates the number of unique users who performed this operation.	Number	Use the detailed diagnosis of this measure to know who are the users performing the operation.
Unique client IPs	Indicates the number of unique client IPs from which users initiated this operation.	Number	Use the detailed diagnosis of this measure to know the clients from which this operation was performed.

The detailed diagnosis of the *Total operations* measure reveals which mailbox owner performed the operation, when, and what was the result of the activity each time it was performed. With the help of this information, you can spot instances when the operation failed.

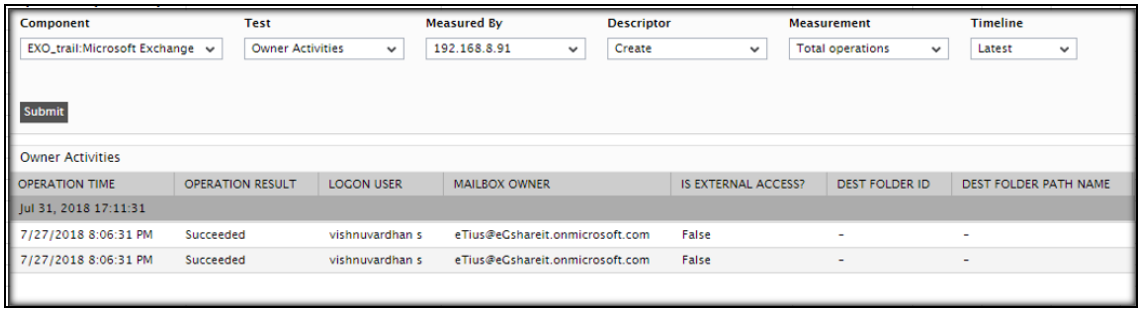


Figure 4.61: The detailed diagnosis of the Total operations measure reported by the Owner Activities test

To know the users who performed a particular operation, use the detailed diagnosis of the *Unique users* measure.

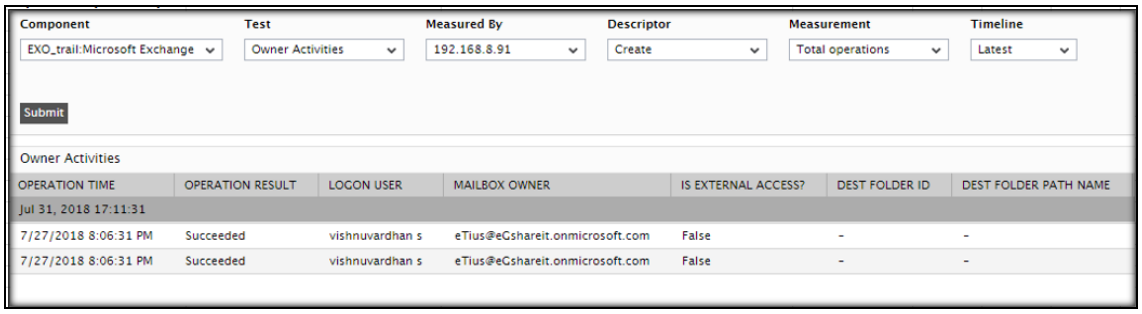


Figure 4.62: The detailed diagnosis of the Unique users measure reported by the Owner Activities test

To know the clients from which a particular operation was performed, use the detailed diagnosis of the *Unique client IPs* measure.

Figure 4.63: The detailed diagnosis of the Unique client IPs measure reported by the Owner Activities test

4.7 The User Experience Layer

The tests mapped to this layer proactively alert administrators to the non-availability of Exchange Online for sending/receiving mails and slowness in mail delivery. Using the tests, you can also verify the availability and responsiveness of Exchange Online over HTTP/S, and detect issues in MAPI connectivity to a user mailbox.

Figure 4.64: The tests mapped to the User Experience layer

4.7.1 Mail Deliverability Test

Frequents breaks in the availability of Exchange Online and prolonged slowness in delivery of mails sent/received via Exchange Online, can adversely impact user experience with Exchange Online. To assure users of a high quality experience with Exchange Online at all times, administrators should be

able to proactively detect and promptly avert the non-availability of Exchange Online and any processing slowness that it may be experiencing. This is where the Mail Deliverability test helps!

At configured intervals, this test emulates a user sending/receiving a configured number of emails (default: 1) over Exchange Online. In the process, the test verifies the availability of Exchange Online for sending and receiving the emulated mail(s), and also reports the time taken to send and receive mails. This way, the test notifies administrators of the non-availability of Exchange Online and processing bottlenecks that it may be experiencing, well before users notice and complain.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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

Parameters	Description
	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*.
Number of Messages	Specify the number of messages this test should send over Exchange Online, as part of the emulation. By default, this parameter is set to 1.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Send mail availability	Indicates whether/not Exchange Online is available to send emails.	Percent	If the value of this measure is 100%, it implies that Exchange Online is available for sending emails. The value 0 on the other hand denotes that Exchange Online is not available for sending emails.
Sent messages	Indicates the number of messages this test sent successfully over Exchange Online.	Number	If this test has been configured to send more than one email over Exchange Online (via the Number of Messages parameter), then the value of this measure will clearly indicate whether all messages were successfully sent or not, and if not, how many email transmissions failed.
Avg time to send messages	Indicates the average time taken by Exchange Online to send messages.	Seconds	Ideally, the value of this measure should be low. A high value is indicative of a bottleneck when

Measurement	Description	Measurement Unit	Interpretation
			sending messages.
Receive mail availability	Indicates whether/not Exchange Online is available to receive emails.	Percent	If the value of this measure is 100%, it implies that Exchange Online is available for receiving emails. The value 0 on the other hand denotes that Exchange Online is not available for receiving emails.
Received messages	Indicates the number of messages this test received successfully over Exchange Online.	Number	If say, this test has been configured to receive more than one email over Exchange Online (via the Number of Messages parameter), then the value of this measure will clearly indicate whether all messages were successfully received or not, and if not, how many email emails could not be received.
Avg time to receive messages	Indicates the average time taken by Exchange Online to receive messages.	Seconds	Ideally, the value of this measure should be low. A high value is indicative of a bottleneck when receiving messages.
Avg round-trip time	Indicates the average time taken to send a message over Exchange Online and receive it.	Seconds	Ideally, the value of this measure should be low. A high value is indicative of a bottleneck when receiving messages.
Max round-trip time	Indicates the maximum time taken to send a message over Exchange Online and receive it.	Seconds	

4.7.2 Logon Status Test

Where Exchange Online is used, users need to be able to quickly and easily login to Exchange Online, so that they have on-emand access to their mailboxes on the cloud. If users are unable to login to Exchange Online 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 Logon Status test helps!

This test emulates a user logging into Exchange Online 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 URL of the Exchange Domain configured for this test 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 Exchange Online* as the **Component type**, select *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 on the eG agent host. You can download the installable for the SharePoint Online Management Shell from the URL: https://www.microsoft.com/en- in/download/details.aspx?id=35588. After downloading, use the installable to install the management shell on the eG agent host.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions.

Parameters	Description
	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 **2.1.1**.
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*.
Exchange Domain	Specify the Exchange Domain this test should connect to, when emulating the API logon process.

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 credentials are validated by Azure AD? or is it at login - i.e., when the domain-specific URL is hit?
Login status	Indicates whether/not the URL that this test hit returned a valid response		If this measure reports the value Success, it means that the test was able to connect to the SharePoint

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>page.</td><td></td><td>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 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 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 validated by Azure AD? or is it at login - i.e., when the domain-specific URL is hit?</td></tr>
<tr><td>Total login time</td><td>Indicates the total time taken to complete the API logon process.</td><td>Seconds</td><td>A very high value for this measure indicates a bottleneck in the API logon</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			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 domain-specific URL?

4.7.3 User MAPI connectivity Test

If MAPI connectivity to a user mailbox is unavailable, then that user may not be able to logon to that mailbox to send/receive mails. This is why, it is important that administrators periodically verify whether/not MAPI connectivity to a user mailbox is available. This check is now possible, thanks to the **User MAPI Connectivity** Test.

This test emulates a user attempting to login to his/her mailbox and retrieving a list of items in the Inbox. In the process, the test reports whether/not MAPI connectivity to that mailbox is available. If the MAPI connectivity is available, then the measure additionally reports how much time it took for the user to connect to that mailbox. This way, the test promptly alerts administrators to the unavailability of MAPI connectivity and latencies in MAPI connection to a configured user mailbox.

Target of the test : Exchange Online

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 has been assigned the **Global reader** role and is vested with the **View-Only Audit Logs**, **View-Only Recipients, Mail Recipients**, and **Mail Import Export** permissions. 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 **2.1.1**.
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*.
Mailbox User	Specify the name of the user mailbox to which the MAPI connectivity has to be verified by this test.
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

Parameters	Description
	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
Status	Indicates whether/not MAPI connectivity is available.		The values that this measure can report and their corresponding numeric values are listed in the table below: **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 status of the MAPI connectivity. In the graph of this measure however, the same is indicated using the numeric equivalents only. Use the detailed diagnosis of this measure to know the mailbox that this test logged into, the database that was accessed in the backend, the latency that was experienced, and the errors that may have been encountered.
Connection time	Indicates the time it took	Seconds	A high value is a cause for concern as it

Measurement	Description	Measurement Unit	Interpretation
	for the MAPI connection to be established.		indicates significant latencies in connectivity.

If the MAPI connectivity fails, then you may want to check the detailed diagnosis of the *Status* measure to know which mailbox was accessed, which database server was accessed, and latencies experienced in the process. This may point administrators to the probable cause of the delay/failure of MAPI connectivity.

Chapter 5: Troubleshooting Exchange Online Monitoring

If the eG agent is unable to report metrics on Exchange Online 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).

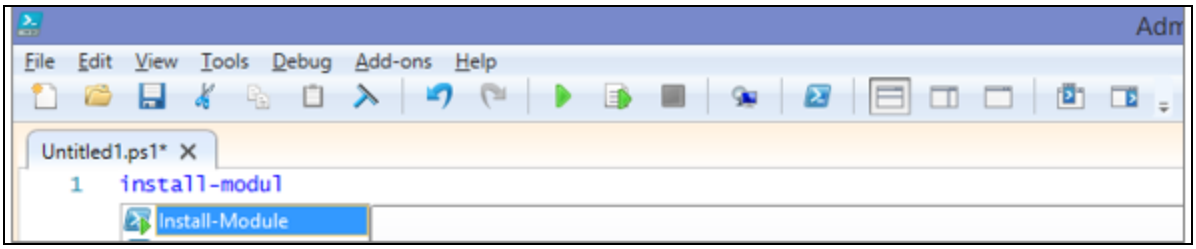


Figure 5.1: Checking if the PackageManagement module has been installed properly

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**.

If the Exchange Online - Service Health test does not report metrics, then check whether the O365 Service Communications module has been properly installed on the eG agent host.

To perform the check, with the Windows Powershell ISE in the elevated mode, type the following commands one after another:

New-SCSession

GetSCEvent

If these commands auto-complete - i.e., if Windows lists these commands even before you type them fully - you can conclude that the O365 Service Communications module has been properly installed on the eG agent host. On the other hand, if the commands do not auto-complete, then you must proceed to install this module 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.