Monitoring Microsoft SharePoint 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 SharePoint Online is a collection of cloud- and web-based technologies that makes it easy to store, share and manage digital information within an organization. SharePoint online also allows collaboration with external users, such as vendors or customers.

This document discussion focuses only on the Microsoft SharePoint 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 SharePoint Online, and how one can manage and monitor the performance of SharePoint Online using eG Enterprise.

1.1 Licensing

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

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

eG Enterprise monitors Microsoft SharePoint 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 SharePoint Online. To ensure that the eG agent is able to run these cmdlets, the pre-requisites detailed in the Section **2.1** topic are to be fulfilled.

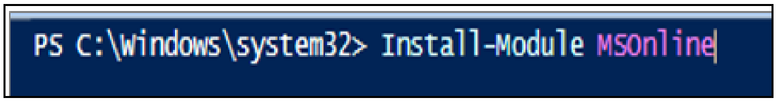
2.1 Pre-requisites for Monitoring Microsoft SharePoint Online

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

1. The eG agent should be deployed on a remote host running one of the following Windows versions:
   - Windows 10
   - Windows 8.1
   - Windows Server 2016
   - Windows Server 2012 or Windows Server 2012 R2
   - Windows Server 2008 R2 SP1
2. The Windows system hosting the remote agent should have internet connection.
3. .NET 4.5 (or above) should pre-exist on the eG agent host.
4. Windows Management Framework (WMF) 5.1.14 (or above) should be installed on the eG agent host
5. The eG agent runs Powershell cmdlets to pull a few metrics from SharePoint Online. To enable the eG agent to run these cmdlets, the following need to be installed and run on the eG agent host:
   - A 64-bit version of the **Microsoft Online Services Sign-in Assistant for IT Professionals RTW** : You can download its installable from the URL : https://download.microsoft.com/download/7/1/E/71EF1D05- A42C- 4A1F- 8162-

96494B5E615C/msoidcli_64bit.msi. After downloading, use the installable to install the sign-in assistant, and then start it.

- A 64-bit version of the **Microsoft Azure Active Directory Module for Windows PowerShell**: To install this module, do the following:
  - First, install the **PackageManagement** and **PowerShellGet** modules on the eG agent host. You can download the installable from the URL: https://download.microsoft.com/download/C/4/1/C41378D4- 7F41- 4BBE- 9D0D-0E4F98585C61/PackageManagement_x64.msi
  - Once the PackageManagement and PowerShellGet modules are successfully installed, open Windows PowerShell ISE in elevated mode on the eG agent host.
  - Then, run the cmdlet depicted by 2.1.



```
PS C:\Windows\system32> Install-Module MSOnline
```

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

6. To run PowerShell cmdlets for metrics collection, the eG agent requires the privileges of a user who has been assigned the **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. For this purpose, each test the eG agent runs on SharePoint Online should be configured with the credentials of a user who has been assigned the aforesaid roles and permission.

   While you can use the credentials of any existing O365 user with the aforesaid privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and 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 Section **2.1.1** topic.

7. To enable the eG agent to collect critical statistics on site collections, site connectivity, health score, tenant storage usage, and file operations, you need to make sure that the SharePoint Online Management Shell is installed and run 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

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

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

The steps for manually installing this app and granting the aforesaid permissions are detailed in Section **2.1.2**topic.

To ensure that pre-requistes 5, 6, 7, and 8 above are fulfilled without a glitch, eG Enterprise provides proprietary PowerShell scripts, which you can run and have these requirements automatically fulfilled. These scripts and their purposes are discussed in the table below:

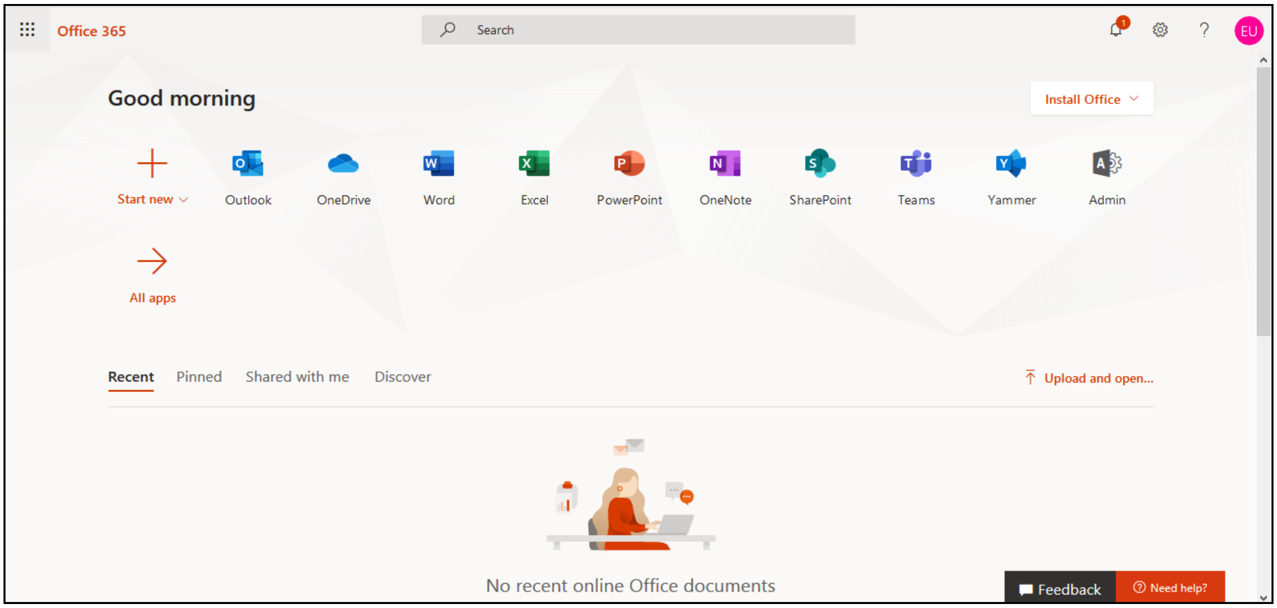
Script name	**Purpose**
O365_Step2_ModulesDwnldnInstall.ps1	Automatically installs the modules/packages required for monitoring SharePoint Online
O365SetRolesAndpermissions.ps1	• Automatically creates a user and grants that user the permission to run Powershell cmdlets • If you want to use an existing 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 it

To know how to use these scripts, refer to Section **2.1.3**topic.

2.1.1 Creating a New User in the Office 365 Portal

To monitor Microsoft SharePoint Online, the eG agent has to be configured with the credentials of a user who has been assigned the **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. While you can use the credentials of any existing O365 user with the aforesaid privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and pass the credentials of that user to the eG agent. To create a new user using the Office 365 portal and assign the required privileges to that user, follow the steps detailed below:

1. Using a browser, connect to the Office 365 portal. The default URL of the portal is: https://portal.office.com
2. Login to the portal as a user with administrator privileges.
3. Figure 2.2 will then appear.

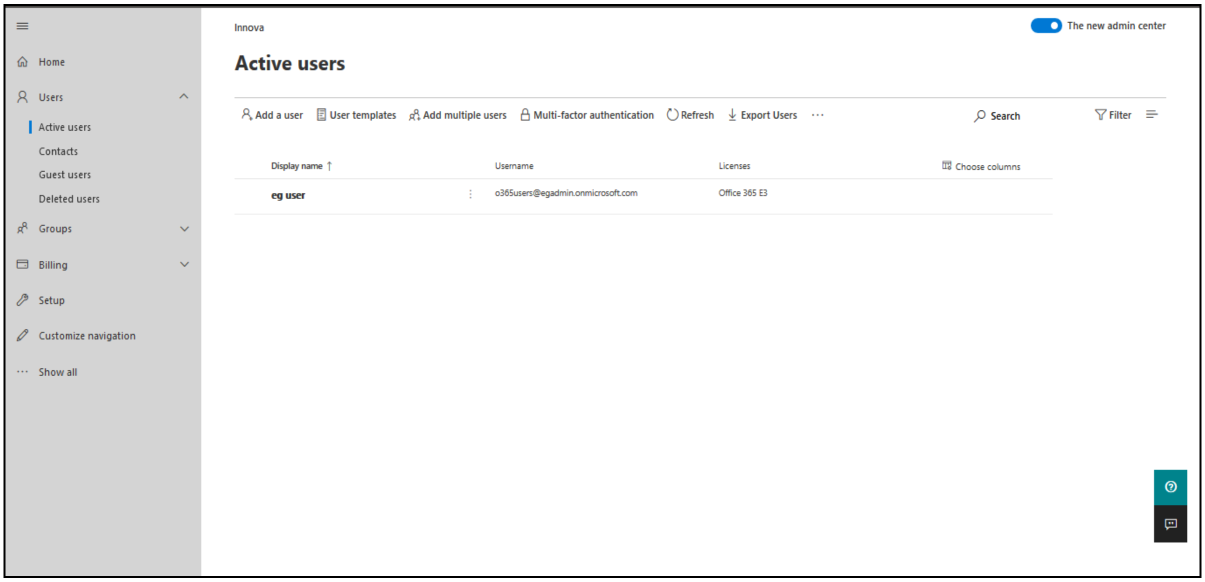


Good morning

No recent online Office documents

Figure 2.2: Welcome page of the Office 365 portal

4. Click on **Admin** under **Apps** (in Figure 2.2). The Microsoft Office 365 Admin Center will then appear (see Figure 2.3).

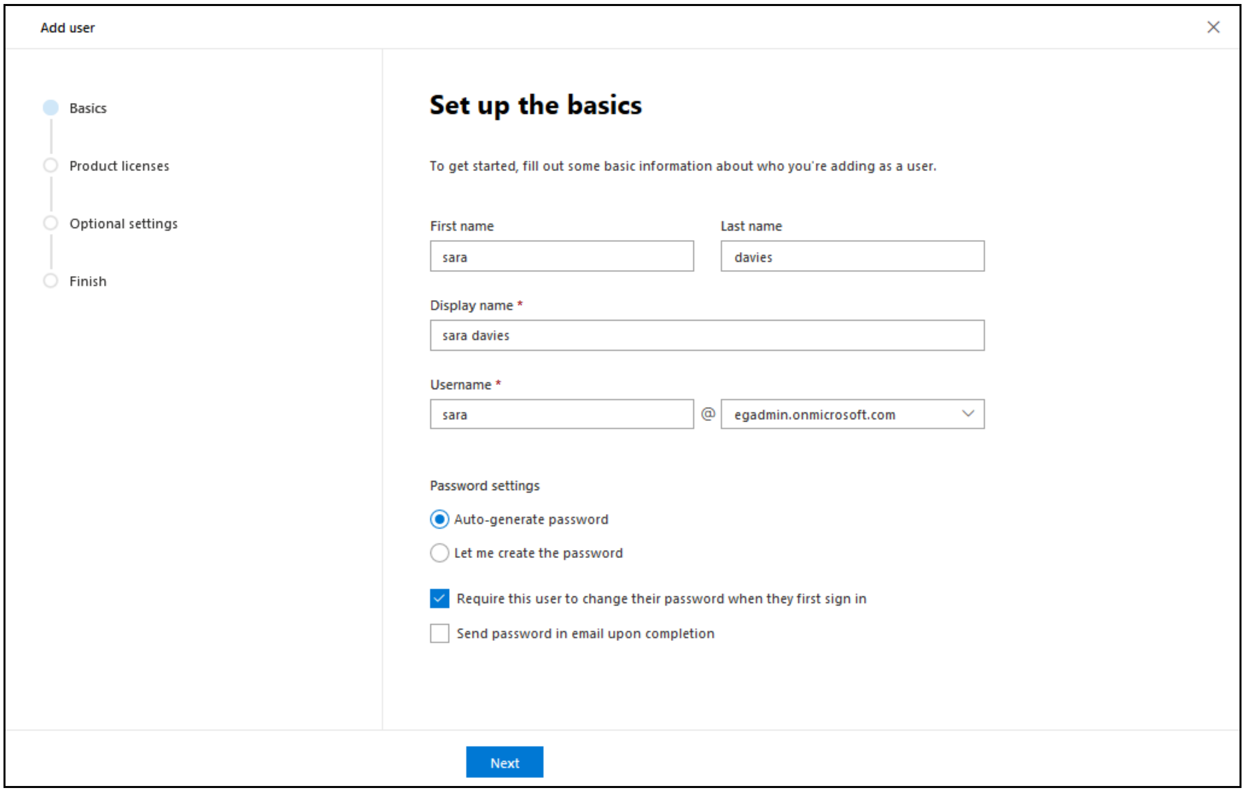


Display name ↑	Username	Licenses
eg user	o365users@egadmin.onmicrosoft.com	Office 365 E3

Figure 2.3: The Microsoft Office 365 Admin Center

5. To create a new user, click on the **Add a user** link under the **Active users** section in Figure 2.3.

6. Figure 2.4 will then appear.



Add user

Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name: sara

Last name: davies

Display name *: sara davies

Username *: sara @ egadmin.onmicrosoft.com

Password settings

● Auto-generate password

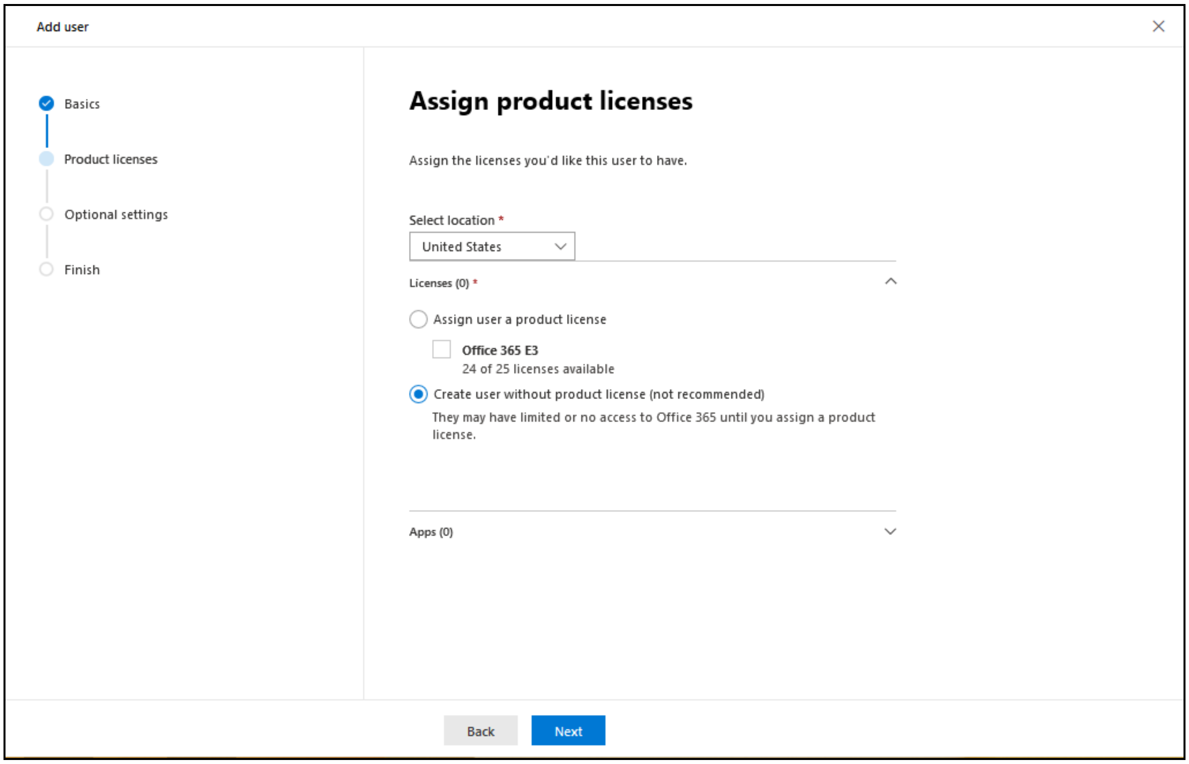
○ Let me create the password

☑ Require this user to change their password when they first sign in

□ Send password in email upon completion

Figure 2.4: 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.



Assign product licenses

Assign the licenses you'd like this user to have.

Select location * United States

Licenses (0) *

○ Assign user a product license

□ Office 365 E3
24 of 25 licenses available

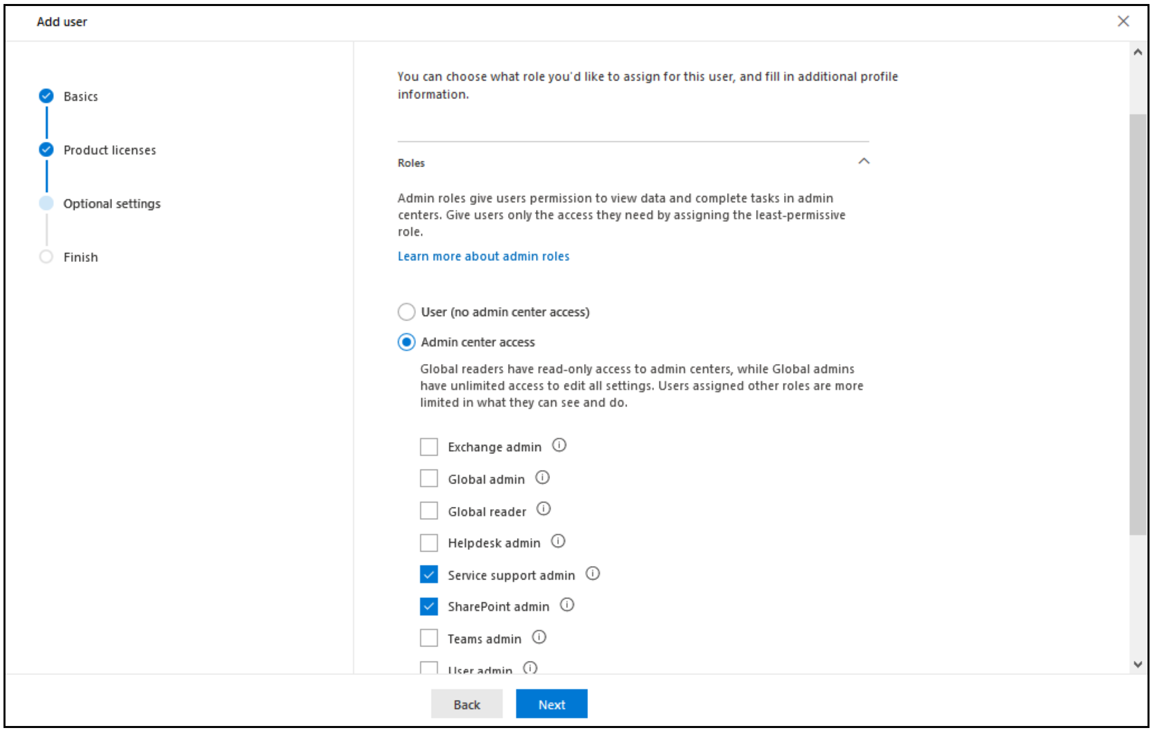
● Create user without product license (not recommended)
They may have limited or no access to Office 365 until you assign a product license.

Apps (0)

Figure 2.5: 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 2.5.

9. Clicking the **Next** button in Figure 2.5 will reveal Figure 2.6. Here, select the **Admin center access** option.



You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles

Admin roles give users permission to view data and complete tasks in admin centers. Give users only the access they need by assigning the least-permissive role.

Learn more about admin roles

○ User (no admin center access)

● Admin center access

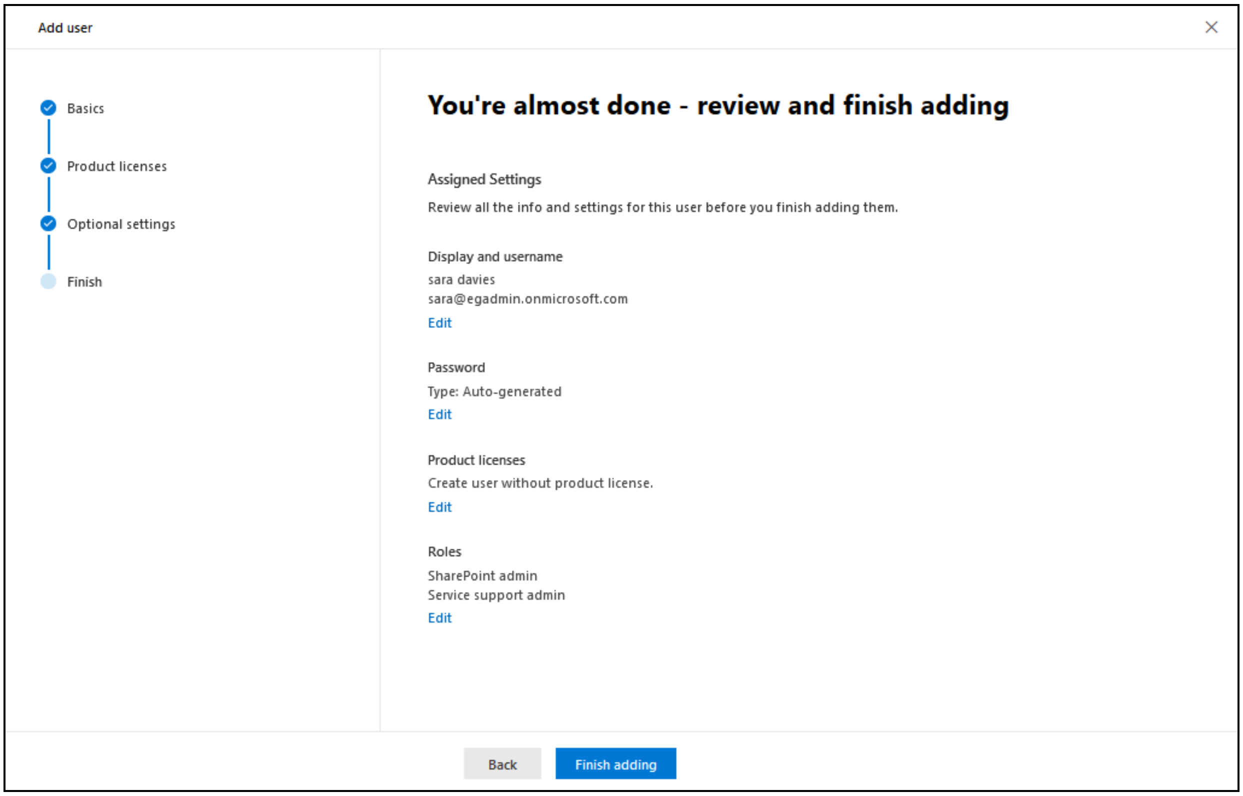
Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

- □ Exchange admin
- □ Global admin
- □ Global reader
- □ Helpdesk admin
- ☑ Service support admin
- ☑ SharePoint admin
- □ Teams admin
- □ User admin

Figure 2.6: Selecting the Admin center access

10. For the purpose of monitoring, the new user should be assigned the **Service support admin** role and the **SharePoint admin**. Select these roles from Figure 2.6.

11. Click the **Next** button in Figure 2.6 to review your selection which appears in Figure 2.7.



You're almost done - review and finish adding

Assigned Settings

Review all the info and settings for this user before you finish adding them.

Display and username
sara davies
sara@egadmin.onmicrosoft.com
Edit

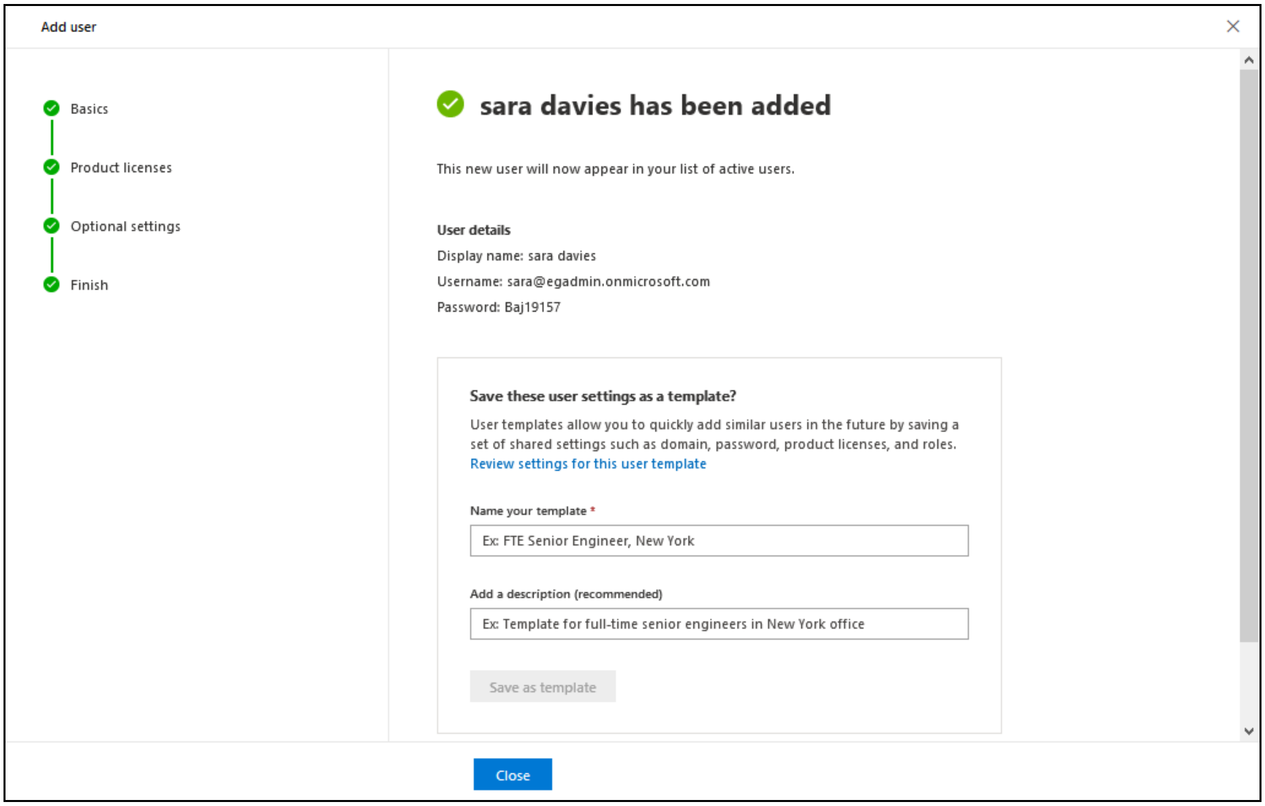
Password
Type: Auto-generated
Edit

Product licenses
Create user without product license.
Edit

Roles
SharePoint admin
Service support admin
Edit

Figure 2.7: Reviewing your selection

12. Finally, click the **Finish adding** button in Figure 2.7 to add the new user. Figure 2.8 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 2.8, as this is what you need to configure against the **O365 USER NAME** and **O365 PASSWORD** parameters of the eG tests.



sara davies has been added

This new user will now appear in your list of active users.

User details

Display name: sara davies

Username: sara@egadmin.onmicrosoft.com

Password: Baj19157

Save these user settings as a template?

User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.

Review settings for this user template

Name your template *

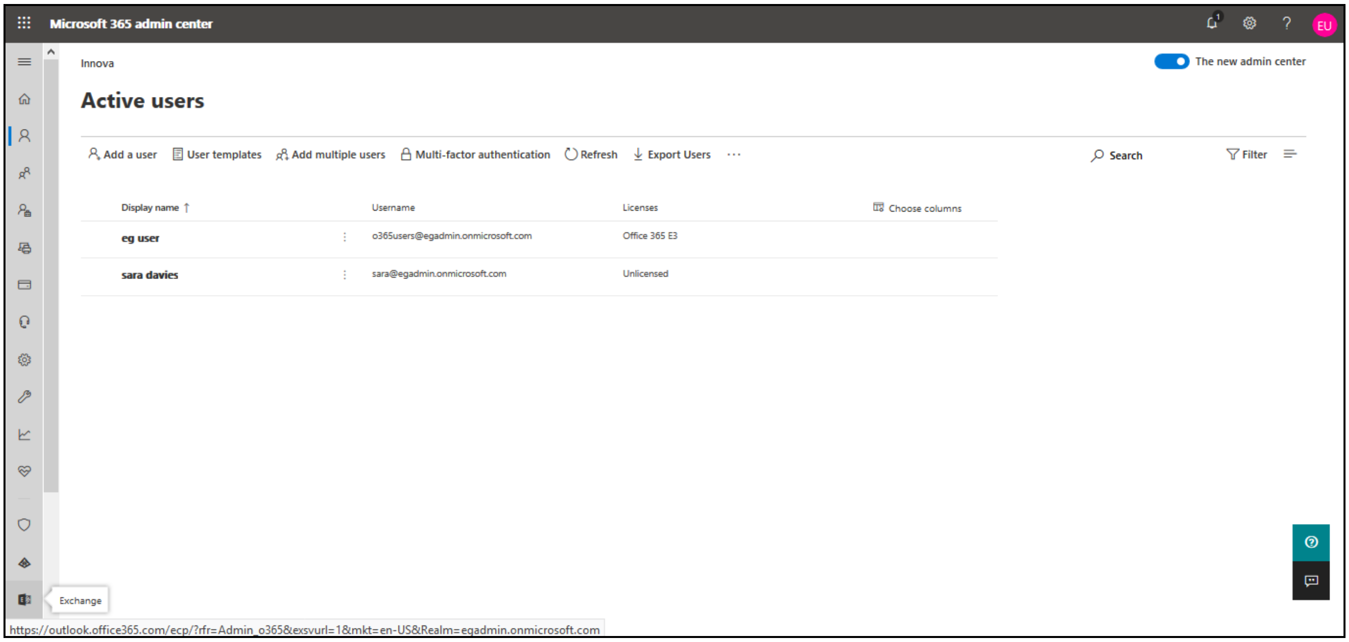
Ex: FTE Senior Engineer, New York

Add a description (recommended)

Ex: Template for full-time senior engineers in New York office

Figure 2.8: Message confirming the successful addition of a user

13. Next, proceed to assign the **View-Only Audit Logs** permission to the new user. For that, first click on the Admin Center tool in the tool bar depicted by Figure 2.9. From the menu that pops up, click on **Exchange**.


Microsoft 365 admin center
EU
Innova
The new admin center
Active users
Add a user
User templates
Add multiple users
Multi-factor authentication
Refresh
Export Users
Search
Filter
Choose columns
Exchange
https://outlook.office365.com/ecp/?rfr=Admin_o365&exsvurl=1&mkt=en-US&Realm=egadmin.onmicrosoft.com

Display name ↑	Username	Licenses
eg user	o365users@egadmin.onmicrosoft.com	Office 365 E3
sara davies	sara@egadmin.onmicrosoft.com	Unlicensed

Figure 2.9: Connecting to the Exchange Admin Center

14. Figure 2.10 will then appear.

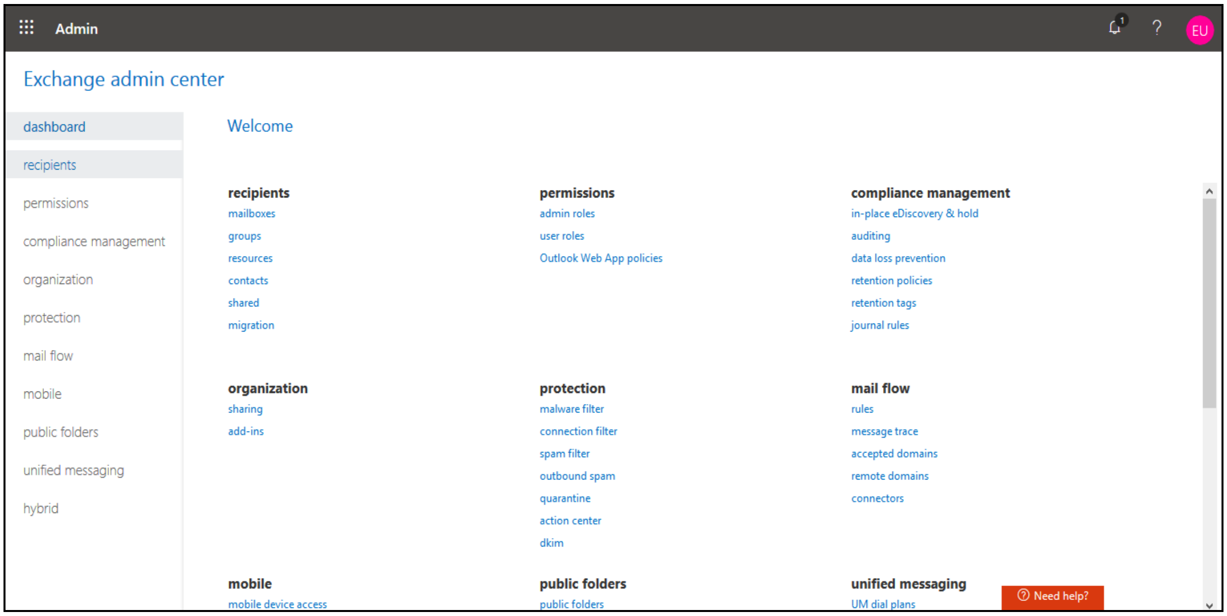
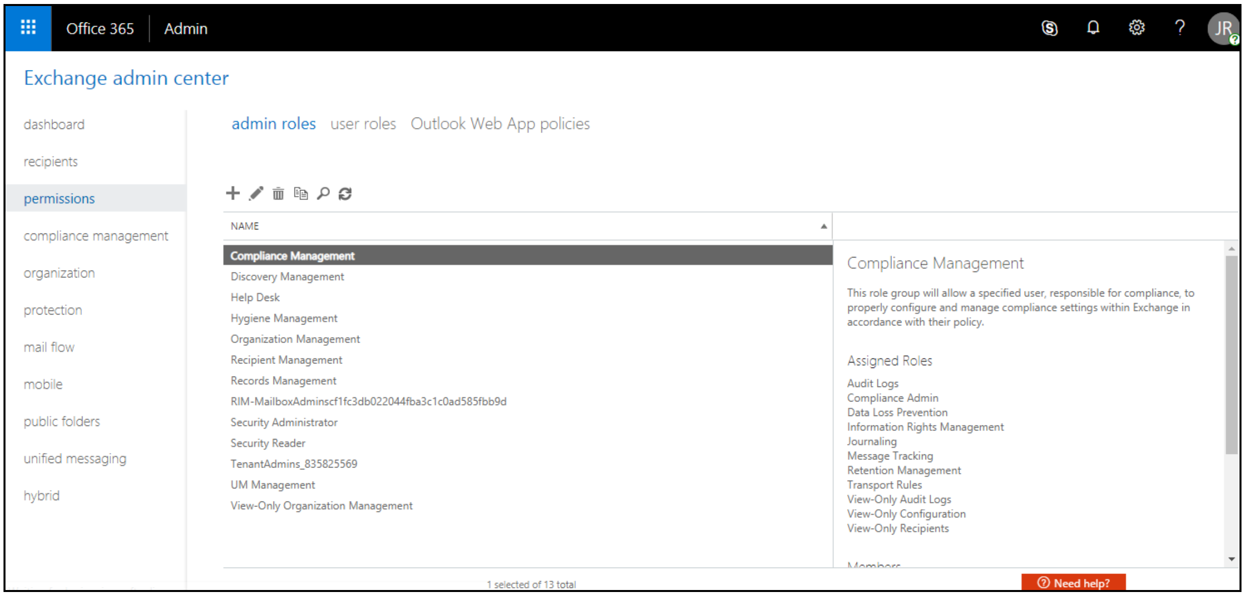


Figure 2.10: The Exchange Admin Center

15. From the list of options in the left panel of Figure 2.10, select **permissions**. Figure 2.11 will then appear listing the **admin** role groups that pre-exist.



Compliance Management
Discovery Management
Help Desk
Hygiene Management
Organization Management
Recipient Management
Records Management
RIM-MailboxAdminscf1fc3db022044fba3c1c0ad585fbb9d
Security Administrator
Security Reader
TenantAdmins_835825569
UM Management
View-Only Organization Management

1 selected of 13 total

Compliance Management

This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.

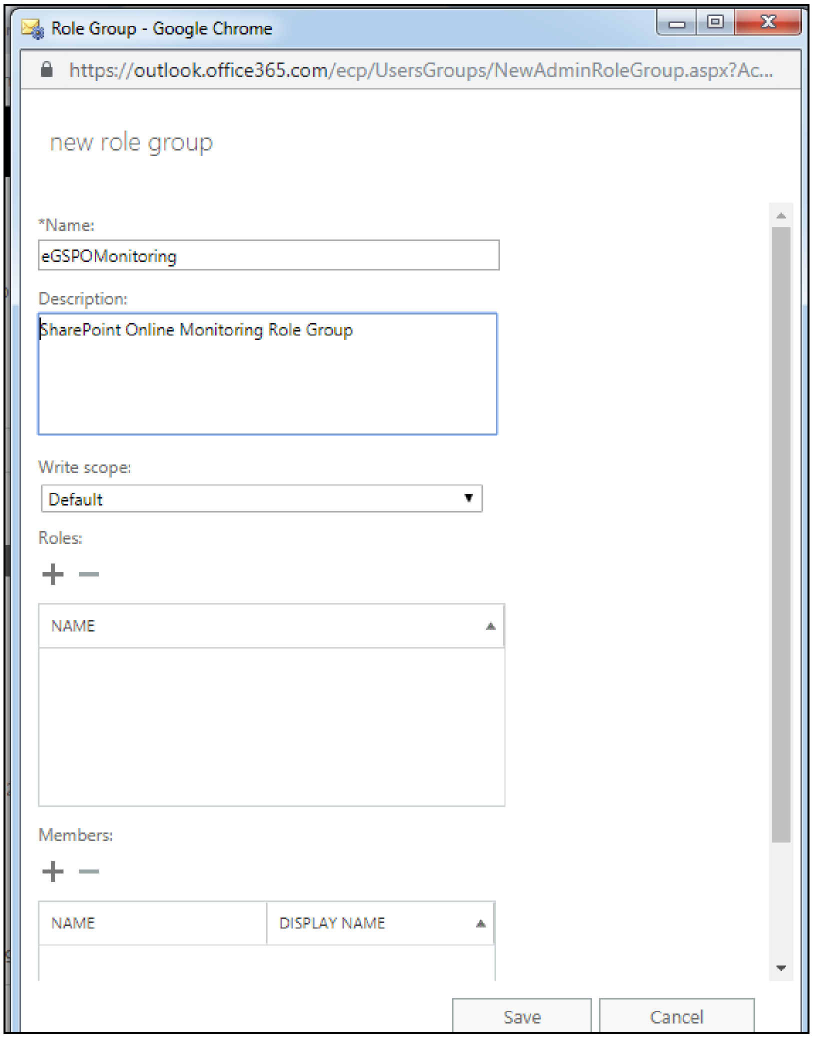
Assigned Roles

Audit Logs
Compliance Admin
Data Loss Prevention
Information Rights Management
Journaling
Message Tracking
Retention Management
Transport Rules
View-Only Audit Logs
View-Only Configuration
View-Only Recipients

Members

Figure 2.11: 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** permission. For that, click on the + button on top of the list of admin role groups (see Figure 2.11). Figure 2.12 will then appear.



Role Group - Google Chrome
https://outlook.office365.com/ecp/UsersGroups/NewAdminRoleGroup.aspx?Ac...
new role group

*Name:
eGSPOMonitoring

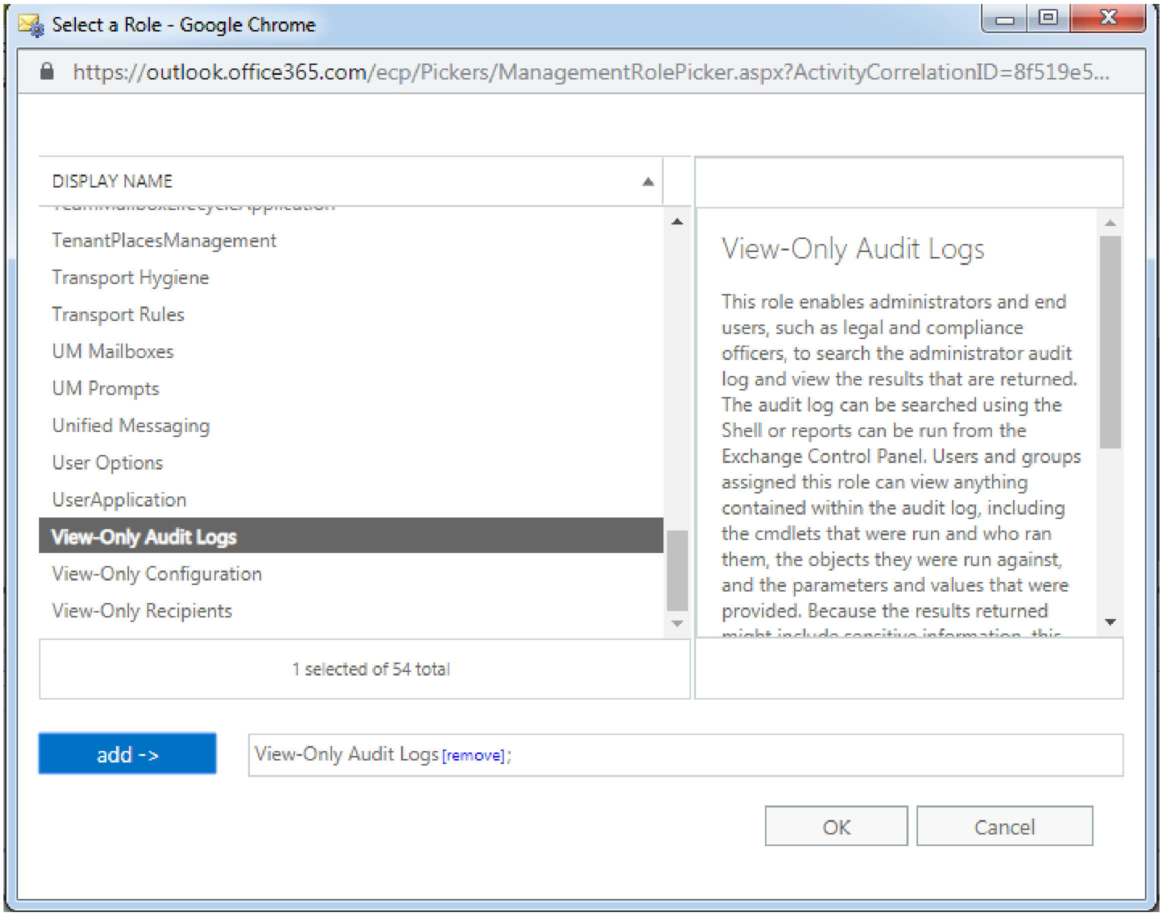
Description:
SharePoint Online Monitoring Role Group

Write scope:
Default

Roles:
+ −
NAME
Members:
+ −
NAME
DISPLAY NAME
Save
Cancel

Figure 2.12: Adding a new role group

17. Provide a unique **Name** and **Description** for the new role group (see Figure 2.12). Then, click on the + button in the **Roles** section of Figure 2.12. Figure 2.13 will then appear listing the **DISPLAY NAME**s of permissions that you want to add to the new role. From this list, select the **View-Only Audit Logs** permission and click the **add ->** button to add the permission. Then, click **OK** to save the changes.



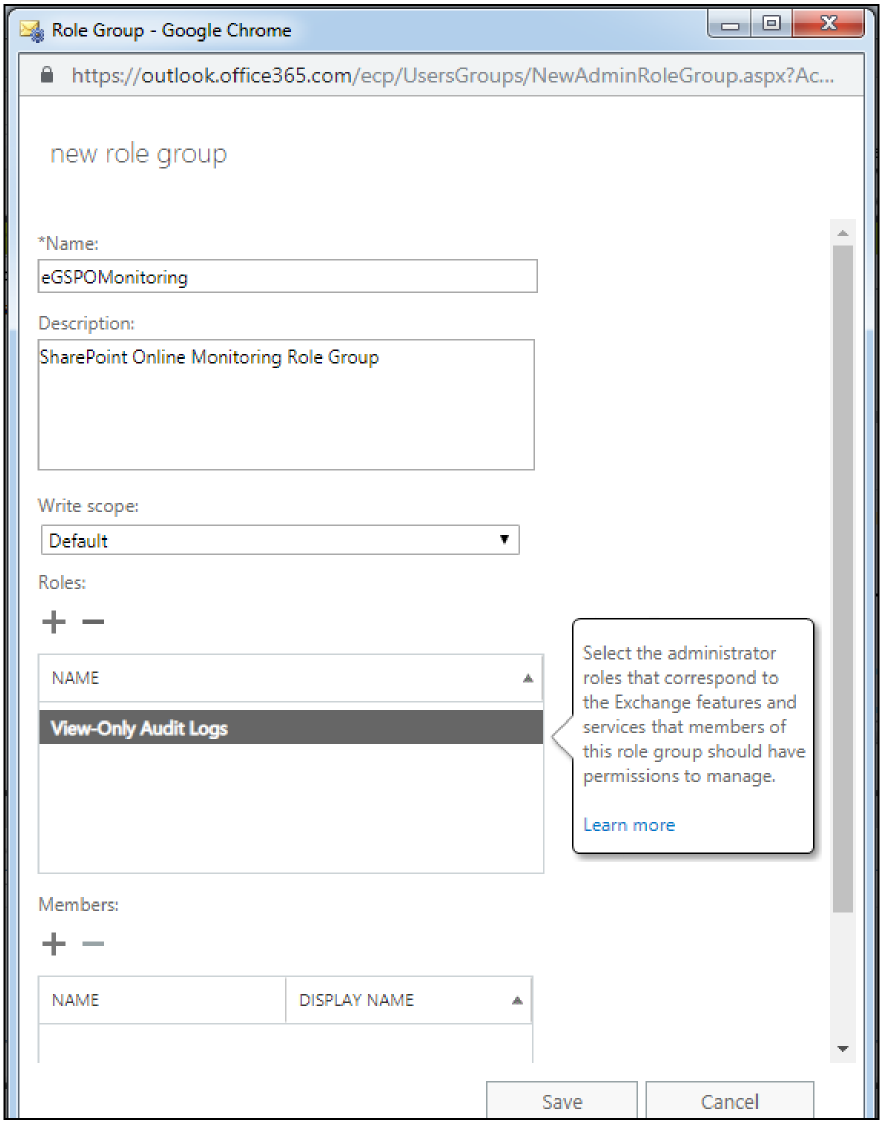
View-Only Audit Logs

This role enables administrators and end users, such as legal and compliance officers, to search the administrator audit log and view the results that are returned. The audit log can be searched using the Shell or reports can be run from the Exchange Control Panel. Users and groups assigned this role can view anything contained within the audit log, including the cmdlets that were run and who ran them, the objects they were run against, and the parameters and values that were provided. Because the results returned might include sensitive information, this

View-Only Audit Logs [remove];

Figure 2.13: Adding the View-Only Audit Logs permission to the new role

18. Figure 2.14 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 2.14.


Role Group - Google Chrome
https://outlook.office365.com/ecp/UsersGroups/NewAdminRoleGroup.aspx?Ac...
new role group
Roles:
NAME
Members:
NAME
DISPLAY NAME
Learn more
Save
Cancel

*Name: eGSPOMonitoring

Description: SharePoint Online Monitoring Role Group

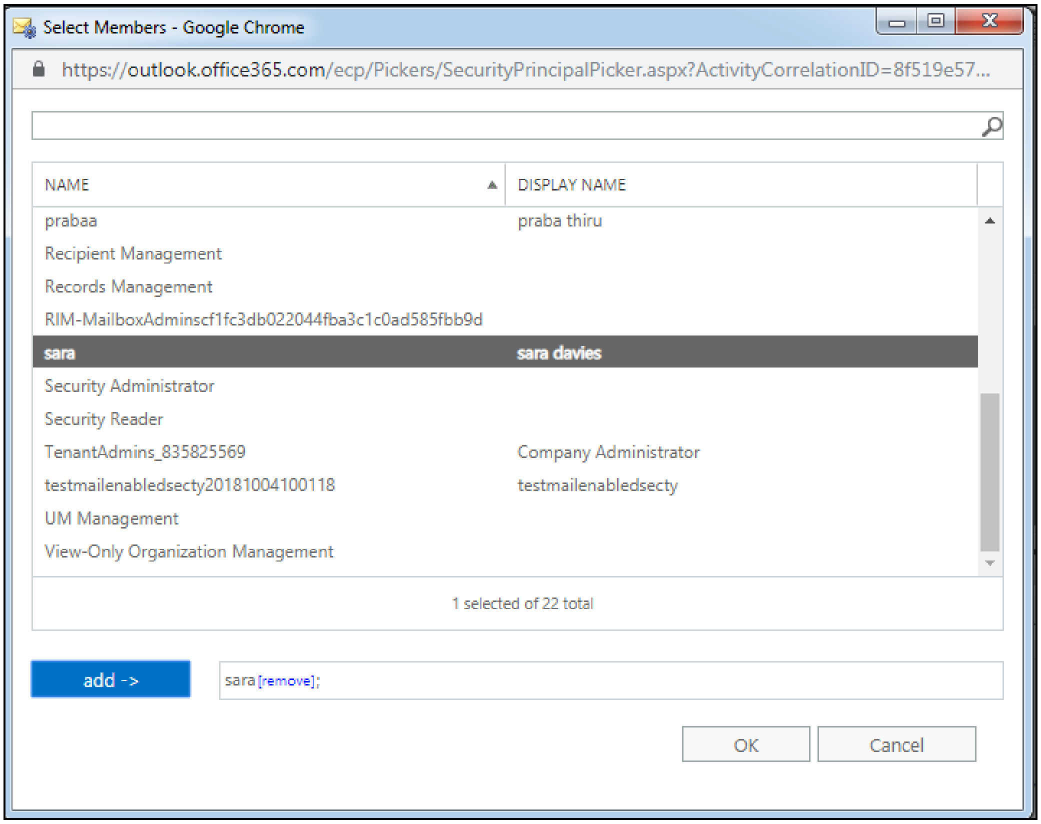
Write scope: Default

View-Only Audit Logs

Select the administrator roles that correspond to the Exchange features and services that members of this role group should have permissions to manage.

Figure 2.14: Clicking on the '+' icon in the Members section

19. Figure 2.15 will then appear. From the list of user names displayed in Figure 2.15, select the name of the user you created for monitoring purposes and click the **add ->** button. Then, click **OK**.



https://outlook.office365.com/ecp/Pickers/SecurityPrincipalPicker.aspx?ActivityCorrelationID=8f519e57...

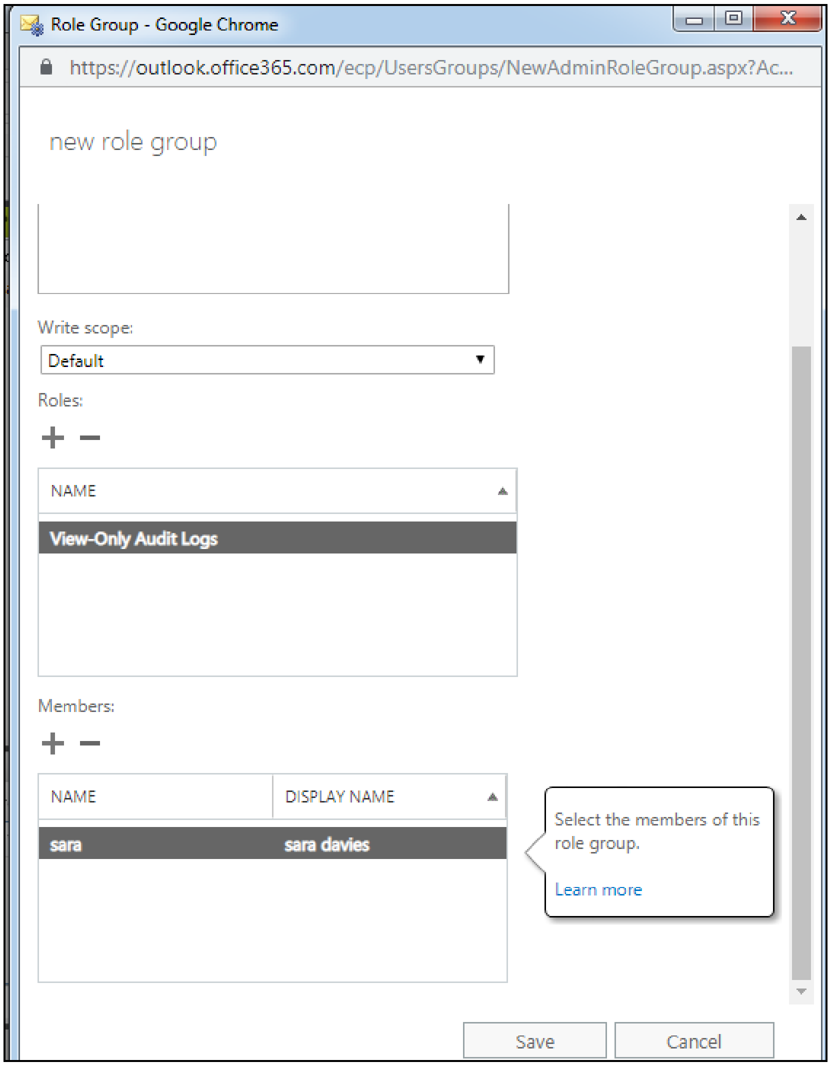
NAME	DISPLAY NAME
prabaa	praba thiru
Recipient Management	
Records Management	
RIM-MailboxAdminscf1fc3db022044fba3c1c0ad585fbb9d	
sara	sara davies
Security Administrator	
Security Reader	
TenantAdmins_835825569	Company Administrator
testmailenabledsecty20181004100118	testmailenabledsecty
UM Management	
View-Only Organization Management	

1 selected of 22 total

sara [remove];

Figure 2.15: Assigning the role group to a user

20. When Figure 2.16 appears, click the **Save** button to save the new role group definition.



Role Group - Google Chrome

https://outlook.office365.com/ecp/UsersGroups/NewAdminRoleGroup.aspx?Ac...

new role group

Write scope: Default

Roles:

NAME
View-Only Audit Logs

Members:

NAME	DISPLAY NAME
sara	sara davies

Select the members of this role group.

Learn more

Figure 2.16: 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 2.17).

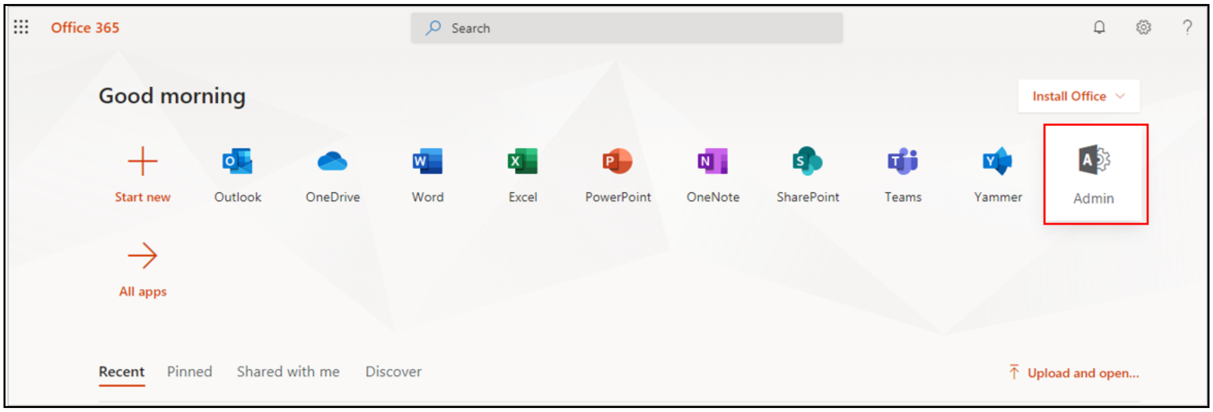


Figure 2.17: Clicking on Admin option in Office 365 portal

2. When Figure 2.18 appears, browse the left panel of Figure 2.18 for the **Admin Centers** node. Expand the node and select the **Azure Active Directory** sub-node within.

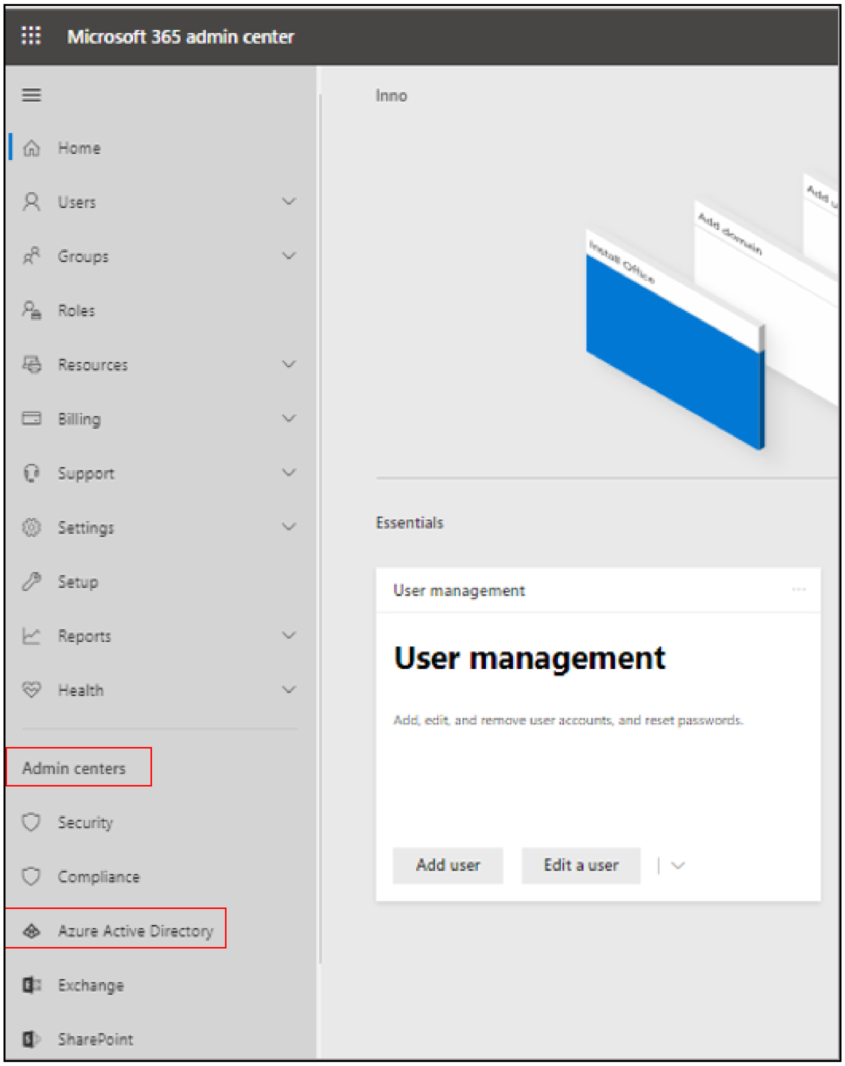
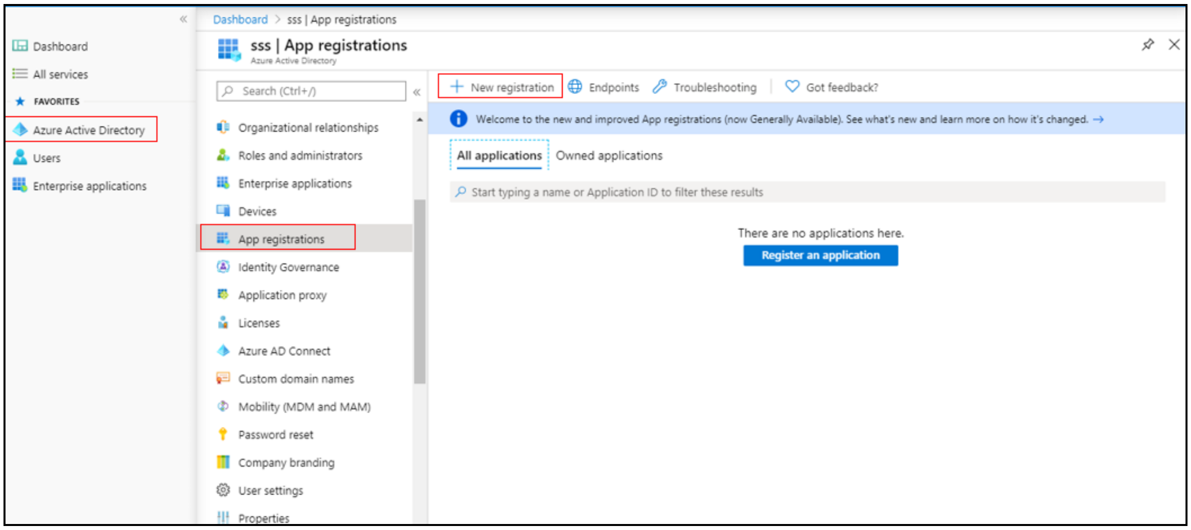


Figure 2.18: Clicking on Azure Active Directory under Admin Centers

3. Figure 2.19 then appears. Select **Azure Active Directory** from the list of **FAVORITES** in the left-most panel of Figure 2.19. Then, from the **App Registrations** list for Azure Active Directory, select **App registrations** to register the Microsoft Graph app.

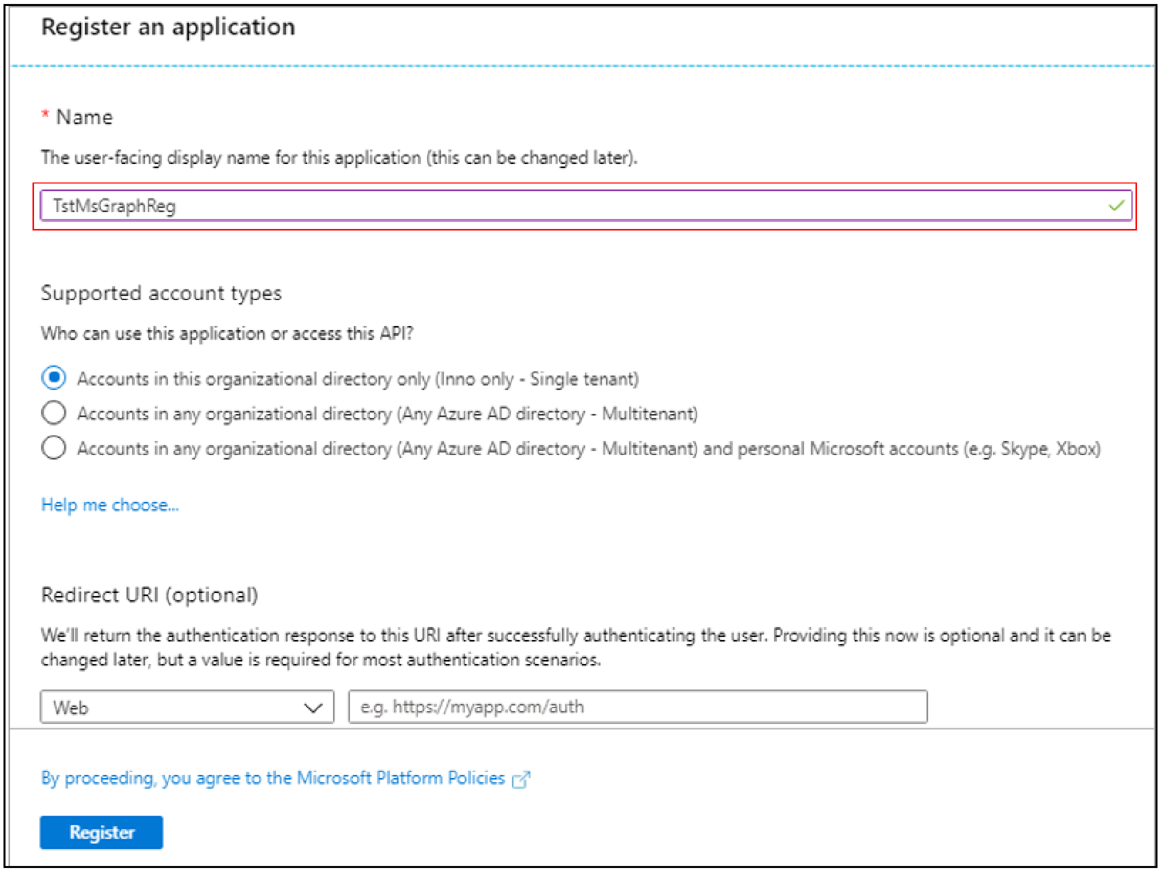


Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

There are no applications here.

Figure 2.19: Selecting the App registrations option to register a new app on Azure AD

4. Figure 2.20 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 2.20 to register Microsoft Graph on Azure AD.



Register an application

* Name

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

TstMsGraphReg ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Inno only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

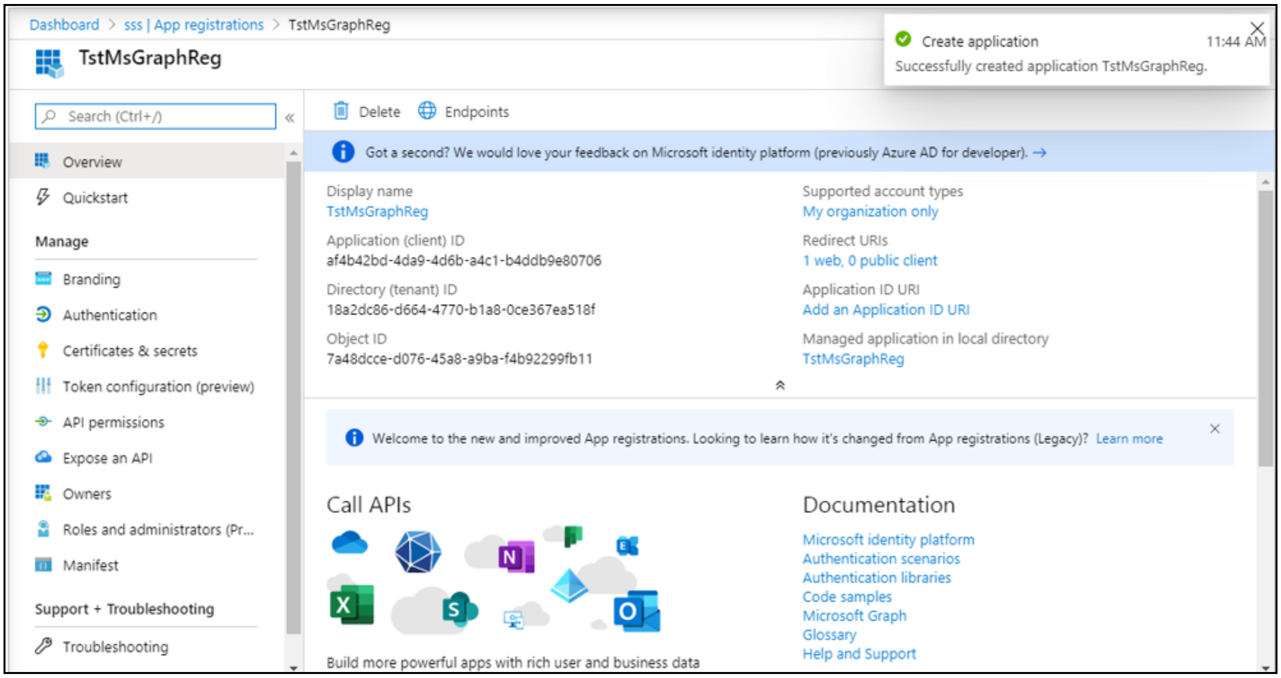
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Figure 2.20: Registering the Microsoft Graph app on Azure AD

5. Upon successful app registration, Figure 2.21 will appear displaying a message to that effect. Additionally, Figure 2.21 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**.



Create application 11:44 AM
Successfully created application TstMsGraphReg.

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name: TstMsGraphReg

Application (client) ID: af4b42bd-4da9-4d6b-a4c1-b4ddb9e80706

Directory (tenant) ID: 18a2dc86-d664-4770-b1a8-0ce367ea518f

Object ID: 7a48dcce-d076-45a8-a9ba-f4b92299fb11

Supported account types: My organization only

Redirect URIs: 1 web, 0 public client

Application ID URI: Add an Application ID URI

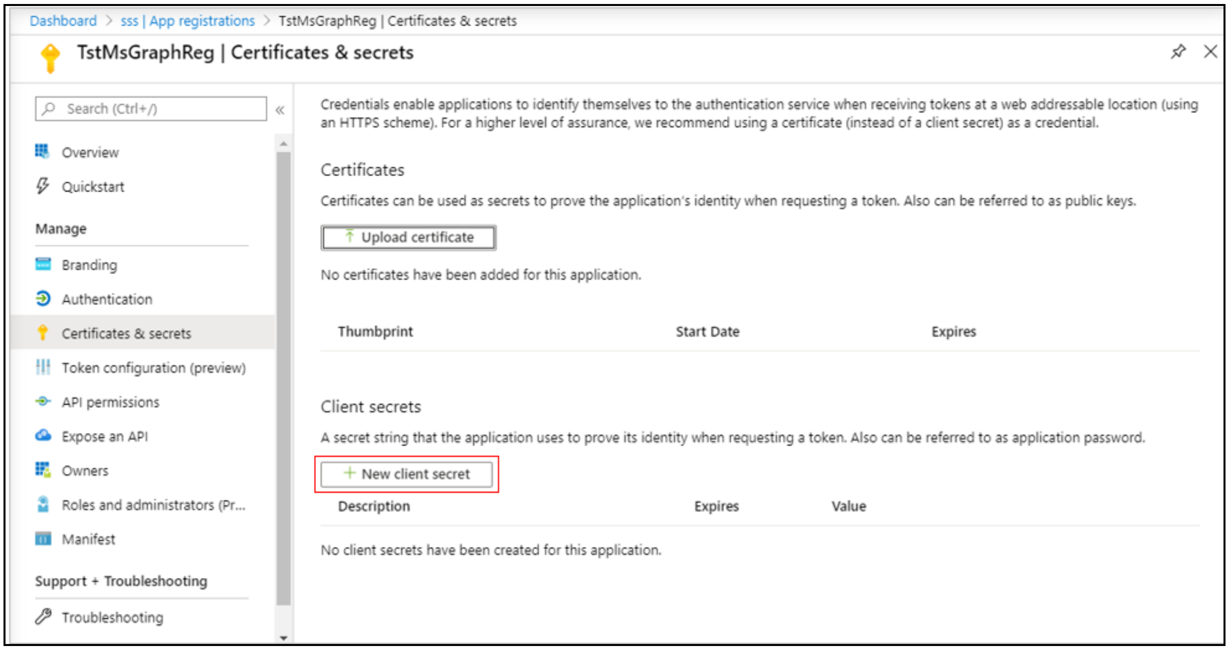
Managed application in local directory: TstMsGraphReg

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Build more powerful apps with rich user and business data

Figure 2.21: 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 2.21. Figure 2.22 will then appear. Now, click on the **New client secret** button in the **Client Secrets** section in the right panel of Figure 2.22.


Dashboard > sss | App registrations > TstMsGraphReg | Certificates & secrets
TstMsGraphReg | Certificates & secrets
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Pr...
Manifest
Support + Troubleshooting
Troubleshooting

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

No certificates have been added for this application.

Thumbprint	Start Date	Expires

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

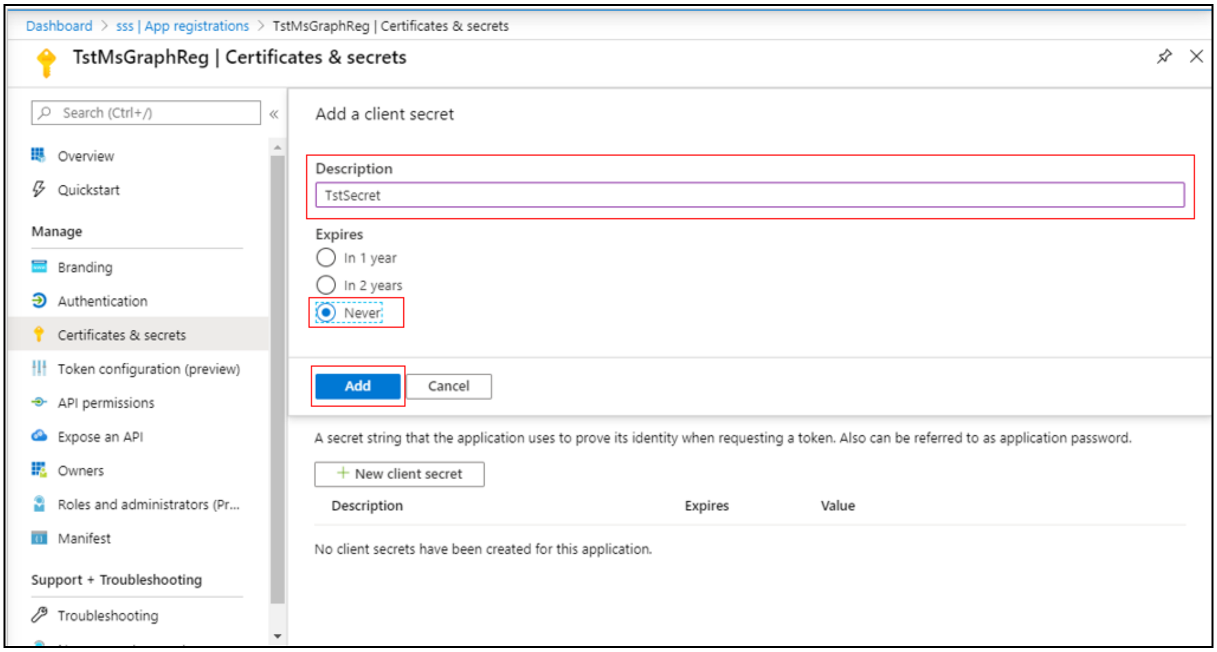
+ New client secret

Description	Expires	Value

No client secrets have been created for this application.

Figure 2.22: Clicking on the New client secret button

7. When Figure 2.23 appears, provide a **Description** for the new secret, set it to **Never** expire, and click the **Add** button to add the new secret.


Dashboard > sss | App registrations > TstMsGraphReg | Certificates & secrets
TstMsGraphReg | Certificates & secrets
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Pr...
Manifest
Support + Troubleshooting
Troubleshooting

Add a client secret

Description: TstSecret

Expires
○ In 1 year
○ In 2 years
● Never

Add Cancel

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

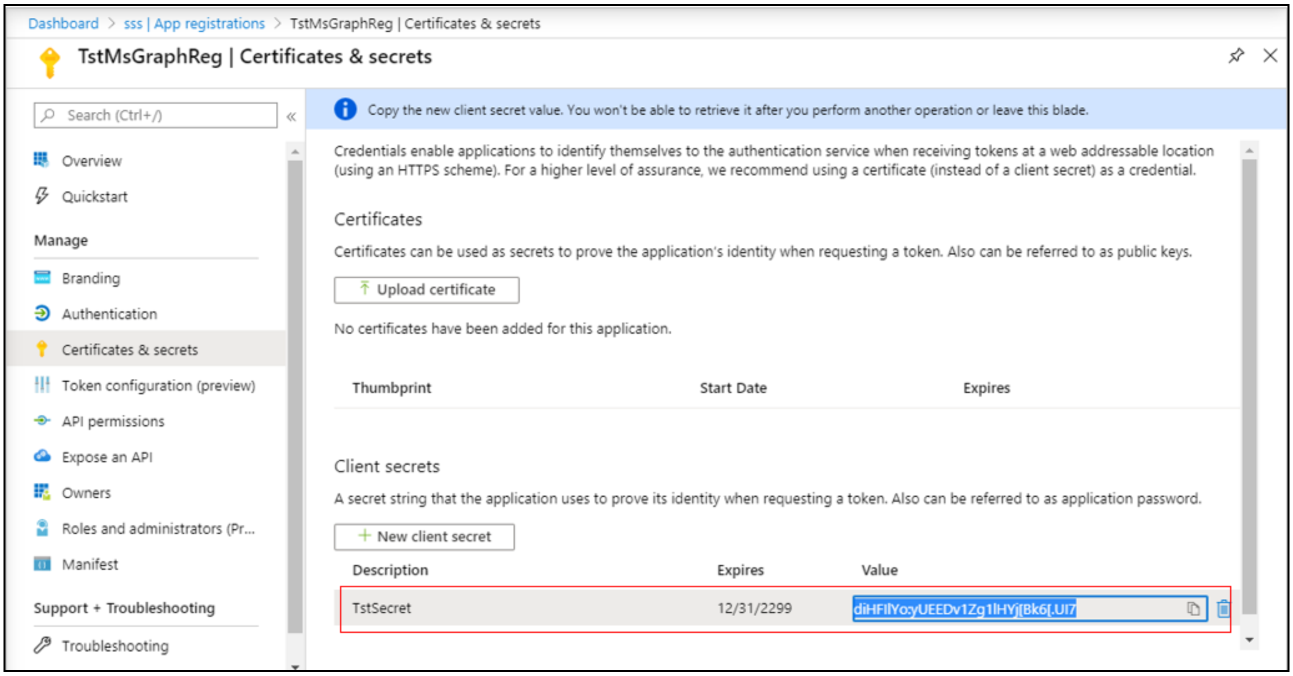
Description	Expires	Value

No client secrets have been created for this application.

Figure 2.23: 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

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



TstMsGraphReg | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

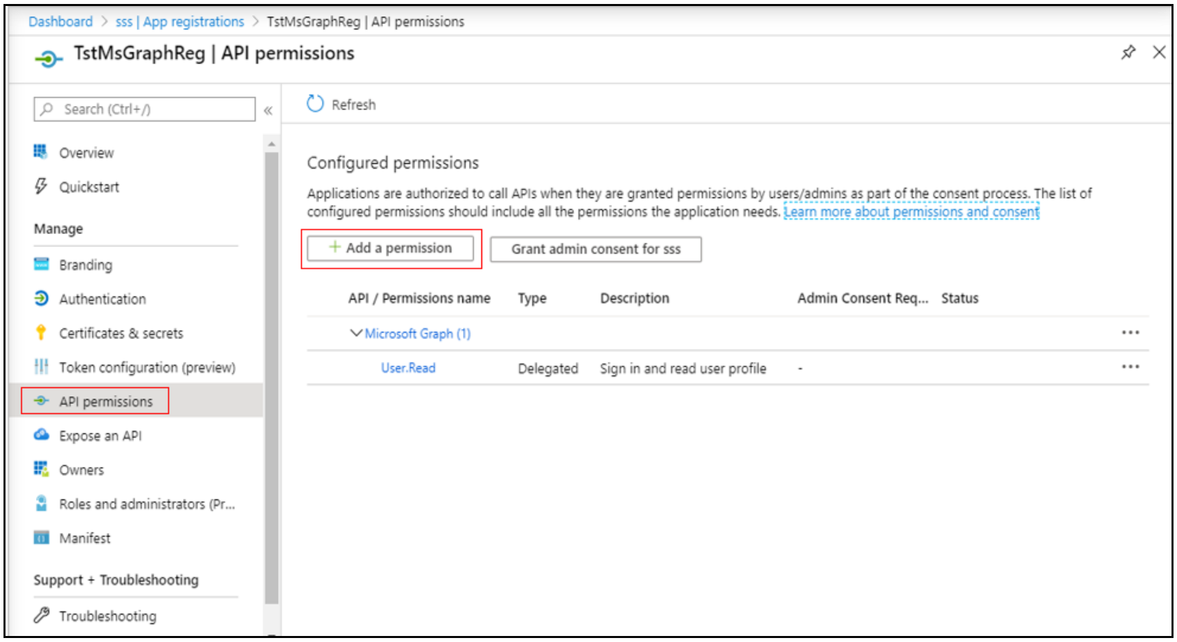
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
TstSecret	12/31/2299	diHFIlYo:yUEEDv1Zg1lHYj[Bk6[.UI7

Figure 2.24: 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 2.24. This will invoke Figure 2.25. In the right panel of Figure 2.25, click on the **Add a permission** button.

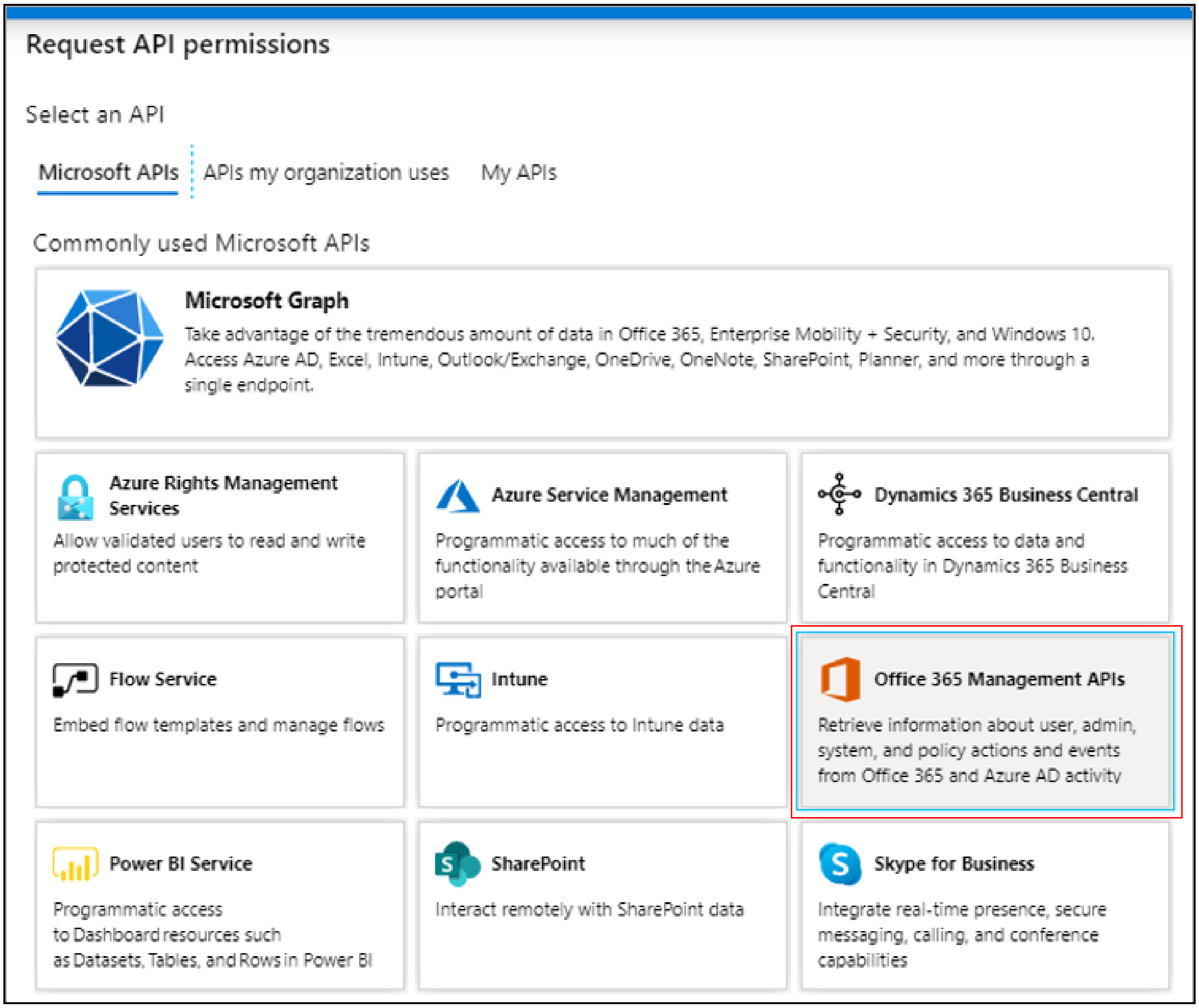

Dashboard > sss | App registrations > TstMsGraphReg | API permissions
TstMsGraphReg | API permissions
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Pr...
Manifest
Support + Troubleshooting
Troubleshooting
Refresh
Configured permissions
+ Add a permission
Grant admin consent for sss

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin Consent Req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

Figure 2.25: 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 2.26).



Request API permissions

Select an API

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

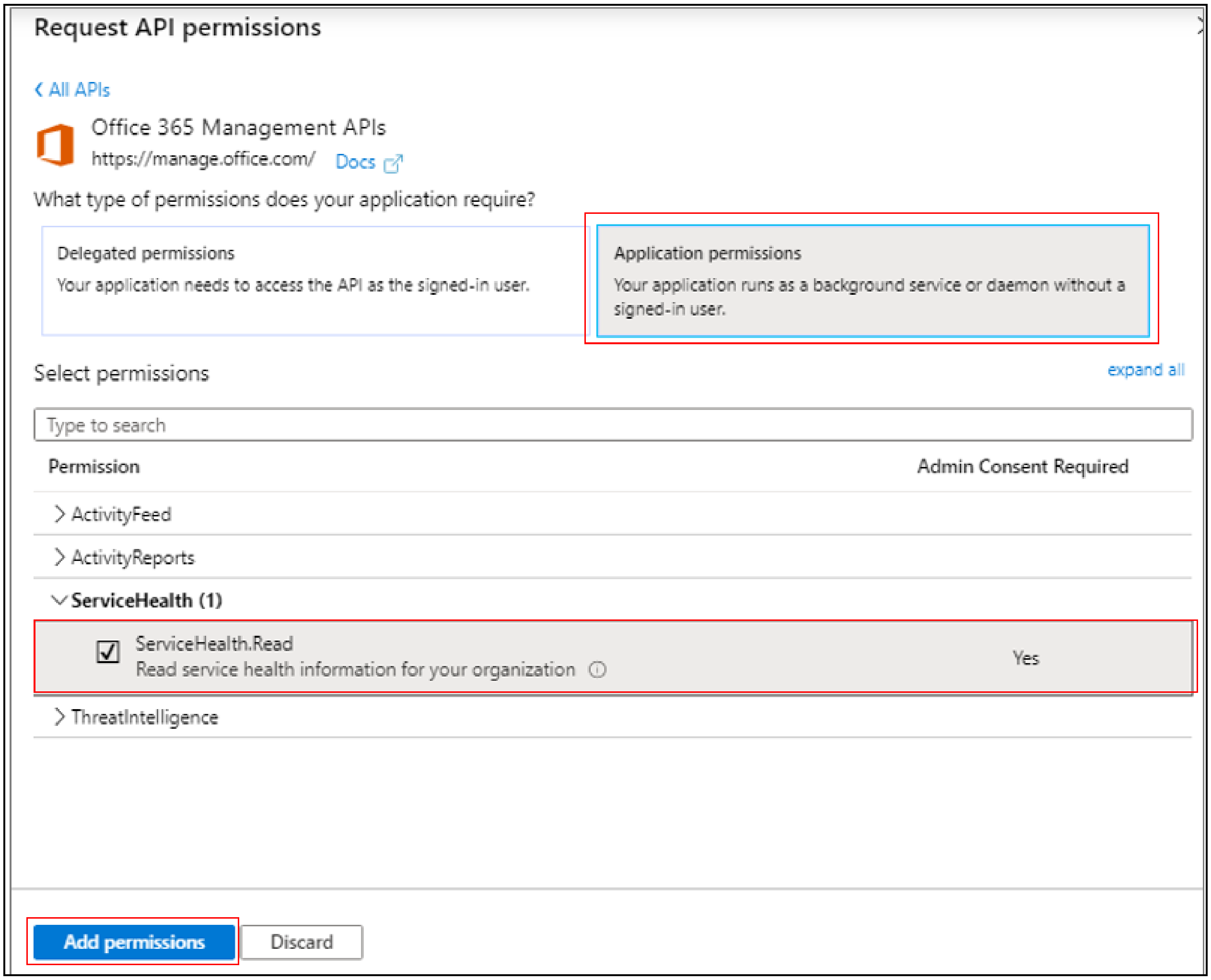
Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

Figure 2.26: Selecting the Office 365 Management APIs option

11. When Figure 2.27 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.



Request API permissions

‹ All APIs

Office 365 Management APIs
https://manage.office.com/ Docs

What type of permissions does your application require?

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

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

Select permissions

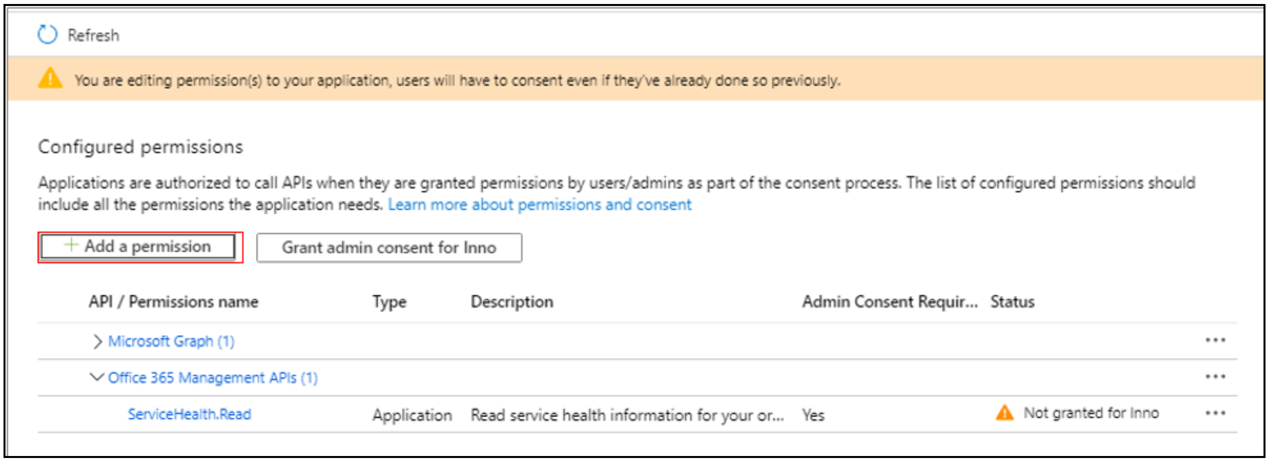
expand all

Type to search

Permission	Admin Consent Required
› ActivityFeed	
› ActivityReports	
⌄ **ServiceHealth (1)**	
☑ ServiceHealth.Read Read service health information for your organization ⓘ	Yes
› ThreatIntelligence	

Figure 2.27: Granting permission to the Microsoft Graph app to read service health

12. When Figure 2.28 appears, click on the **Add a permission** button again.



Refresh

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

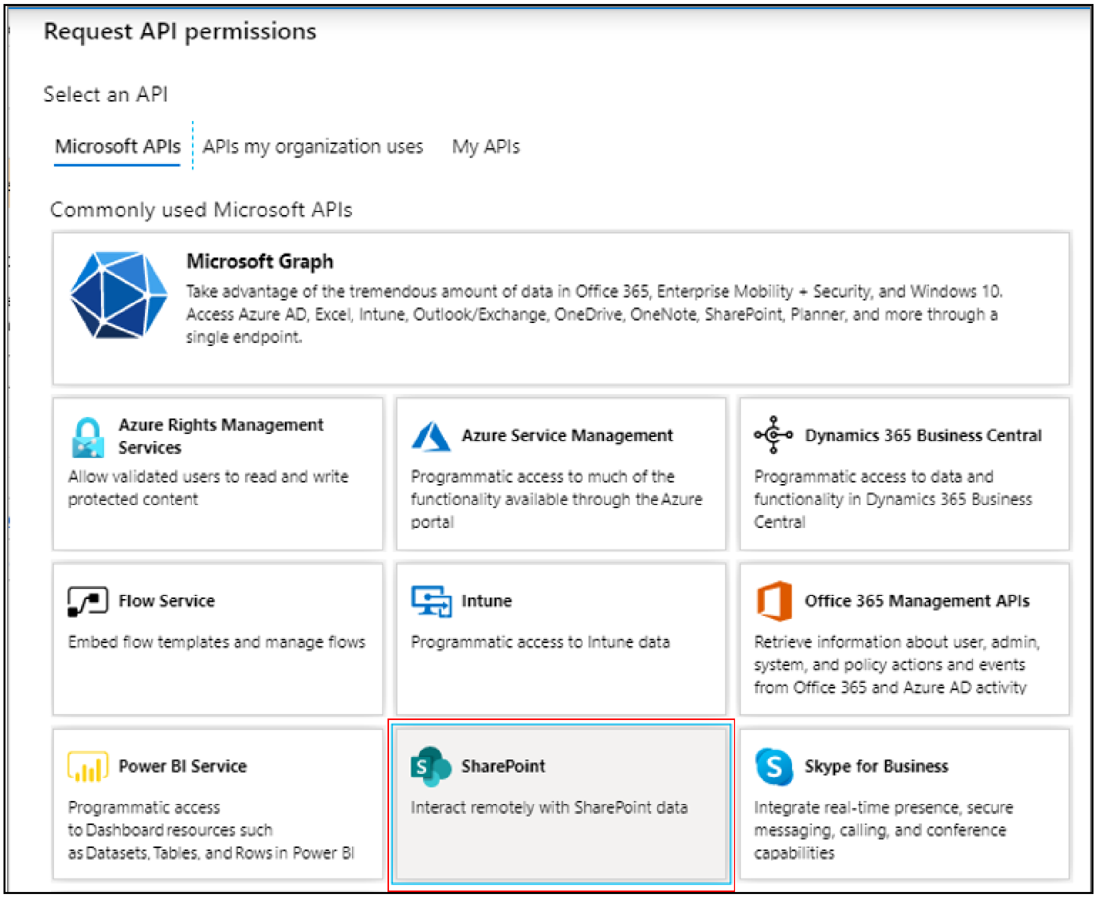
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission | Grant admin consent for Inno

API / Permissions name	Type	Description	Admin Consent Requir...	Status	
> Microsoft Graph (1)					•••
∨ Office 365 Management APIs (1)					•••
ServiceHealth.Read	Application	Read service health information for your or...	Yes	⚠ Not granted for Inno	•••

Figure 2.28: Clicking on the Add a permission button again to add permission to read from and write to user files

13. From Figure 2.29 that then appears, select the **SharePoint** option.



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

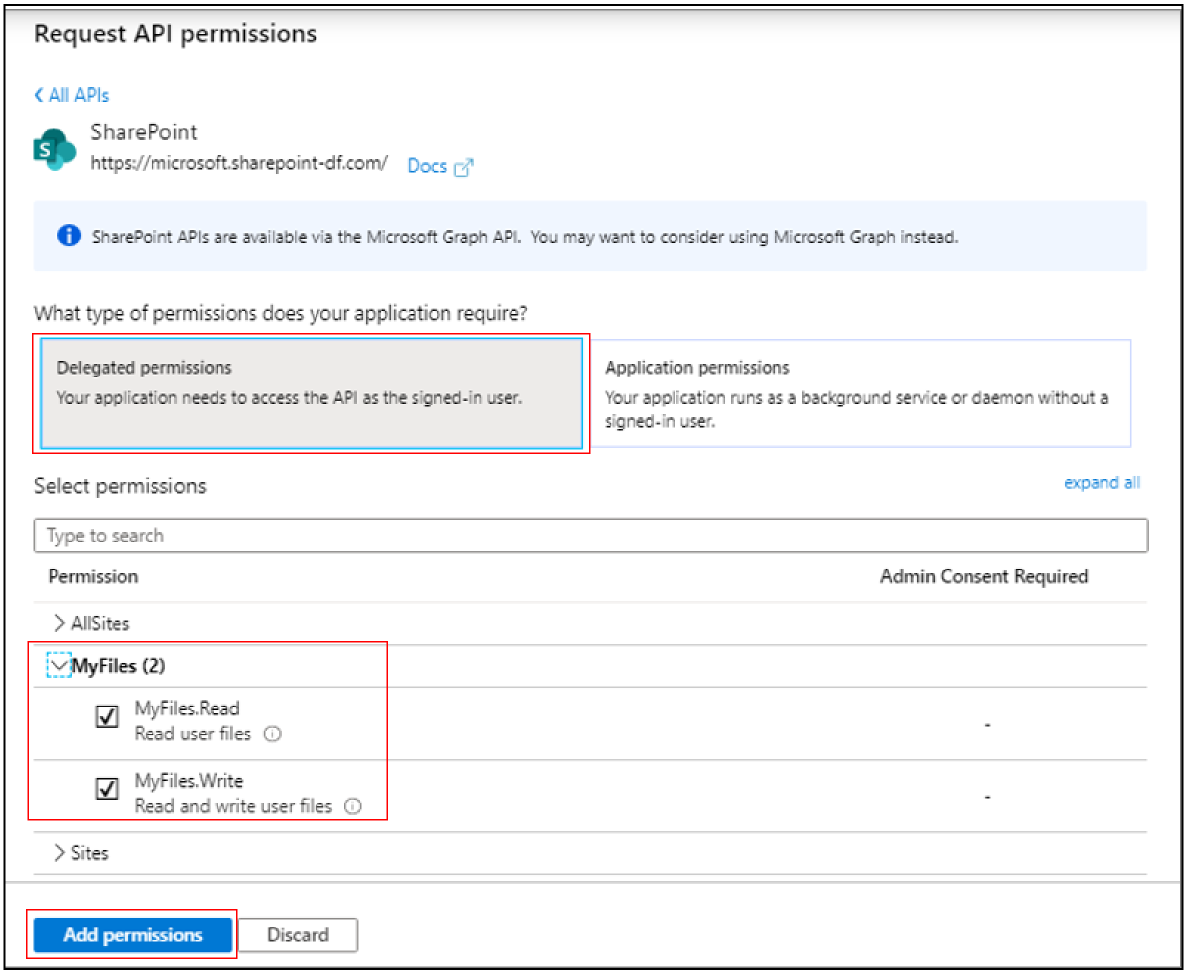
Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

Figure 2.29: Selecting the SharePoint option

14. Then, select the **Delegated permissions** option from Figure 2.30, 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.



Request API permissions

‹ All APIs

SharePoint
https://microsoft.sharepoint-df.com/ Docs

SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

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

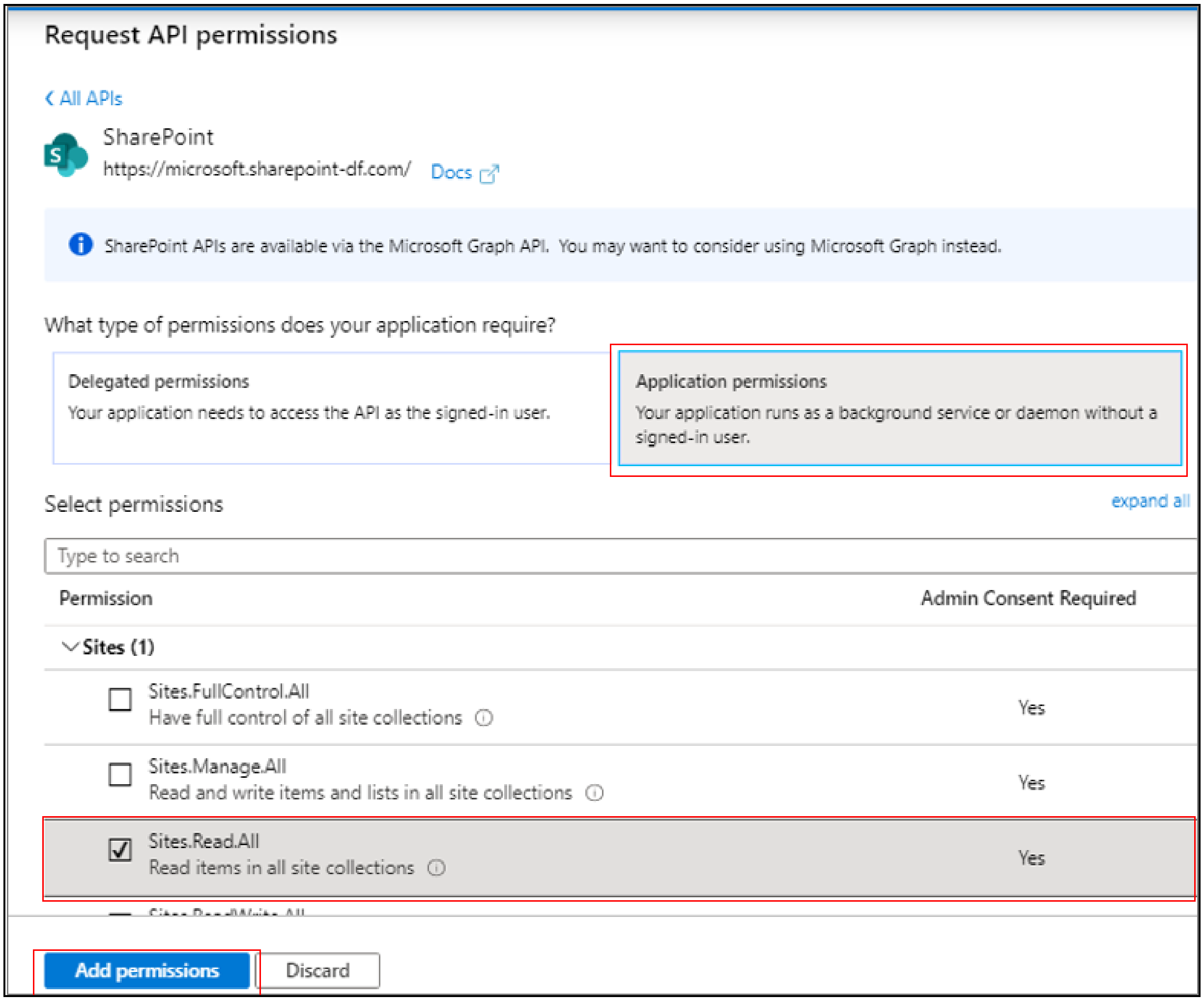
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Permission	Admin Consent Required
> AllSites	
∨ MyFiles (2)	
☑ MyFiles.Read Read user files	-
☑ MyFiles.Write Read and write user files	-
> Sites	

Figure 2.30: Granting permission to Microsoft Graph app to read from and write to user files

15. You will now return to Figure 2.28. Once again, click on the **Add a permission** button therein to grant another permission to Microsoft Graph. When Figure 2.29 appears, select the **SharePoint** option yet again. Next, as depicted by Figure 2.31, 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 2.31 to add the chosen permission to Microsoft Graph app.



Request API permissions

< All APIs

SharePoint
https://microsoft.sharepoint-df.com/ Docs

SharePoint APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

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

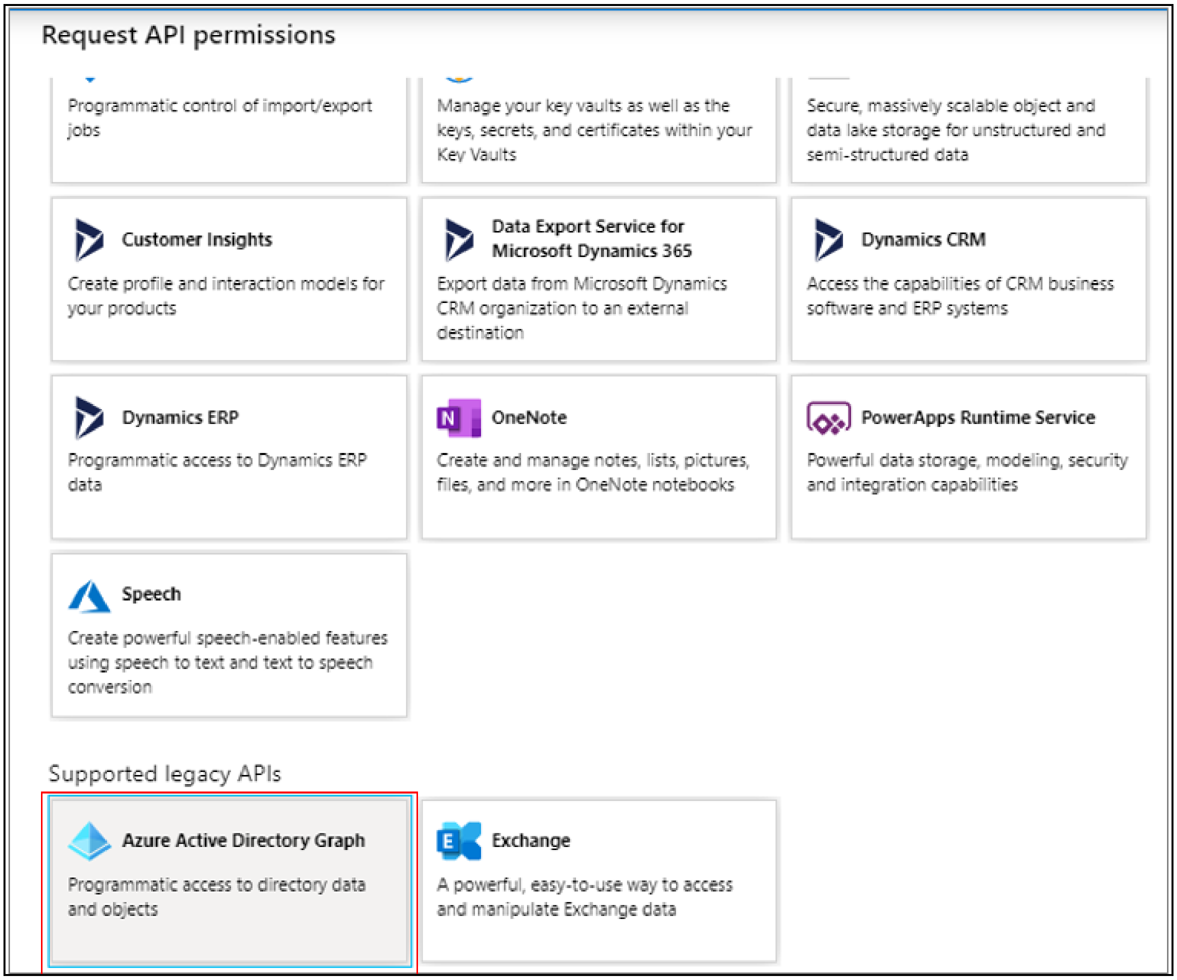
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Permission	Admin Consent Required
Sites (1)	
□ Sites.FullControl.All Have full control of all site collections	Yes
□ Sites.Manage.All Read and write items and lists in all site collections	Yes
☑ Sites.Read.All Read items in all site collections	Yes

Figure 2.31: Granting permission to Microsoft Graph app to read items in all site collections

16. You will once again return to Figure 2.28. Click on the **Add a permission** button therein. When Figure 2.32 appears, select the **Azure Active Directory Graph** option.



Request API permissions

Programmatic control of import/export jobs

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Dynamics ERP
Programmatic access to Dynamics ERP data

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

PowerApps Runtime Service
Powerful data storage, modeling, security and integration capabilities

Speech
Create powerful speech-enabled features using speech to text and text to speech conversion

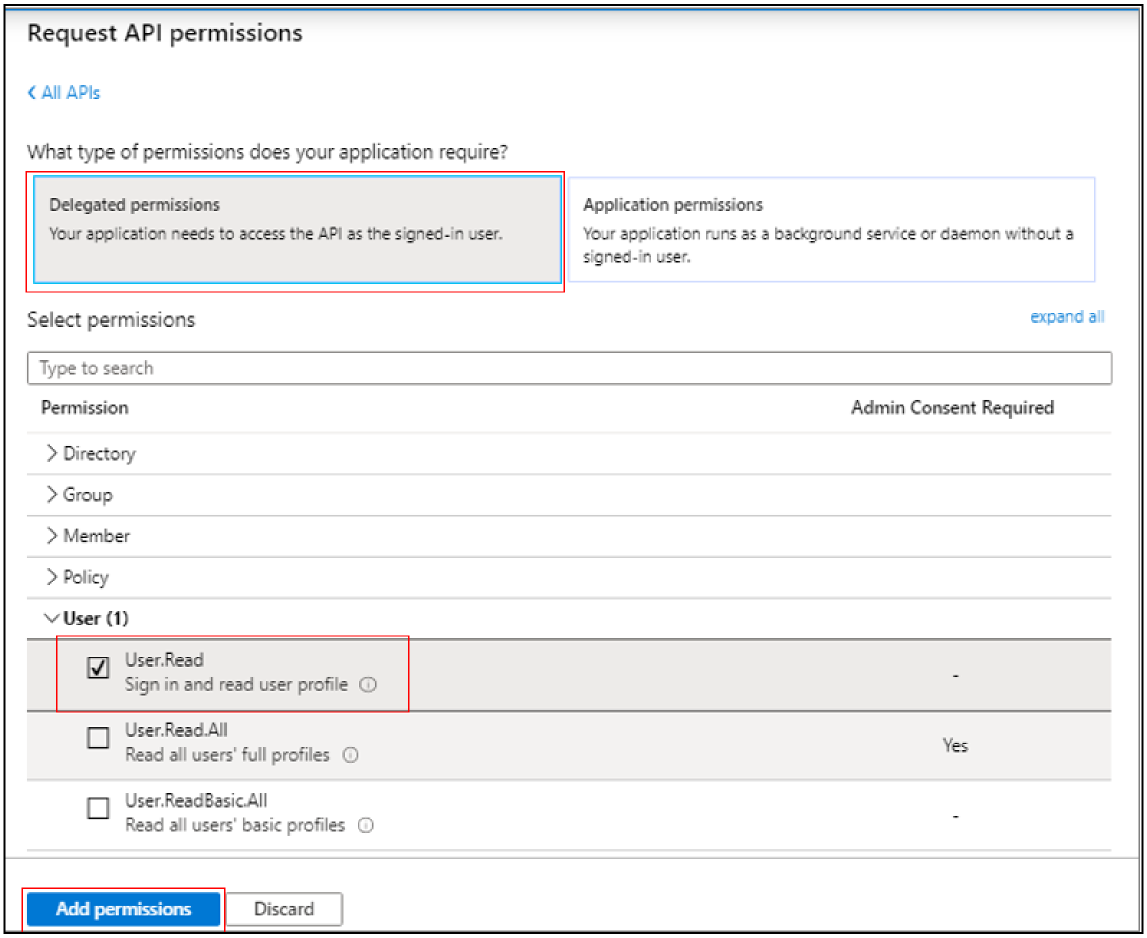
Supported legacy APIs

Azure Active Directory Graph
Programmatic access to directory data and objects

Exchange
A powerful, easy-to-use way to access and manipulate Exchange data

Figure 2.32: Selecting the Azure Active Directory Graph option

17. From Figure 2.33, 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.



Request API permissions

‹ All APIs

What type of permissions does your application require?

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

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

Select permissions

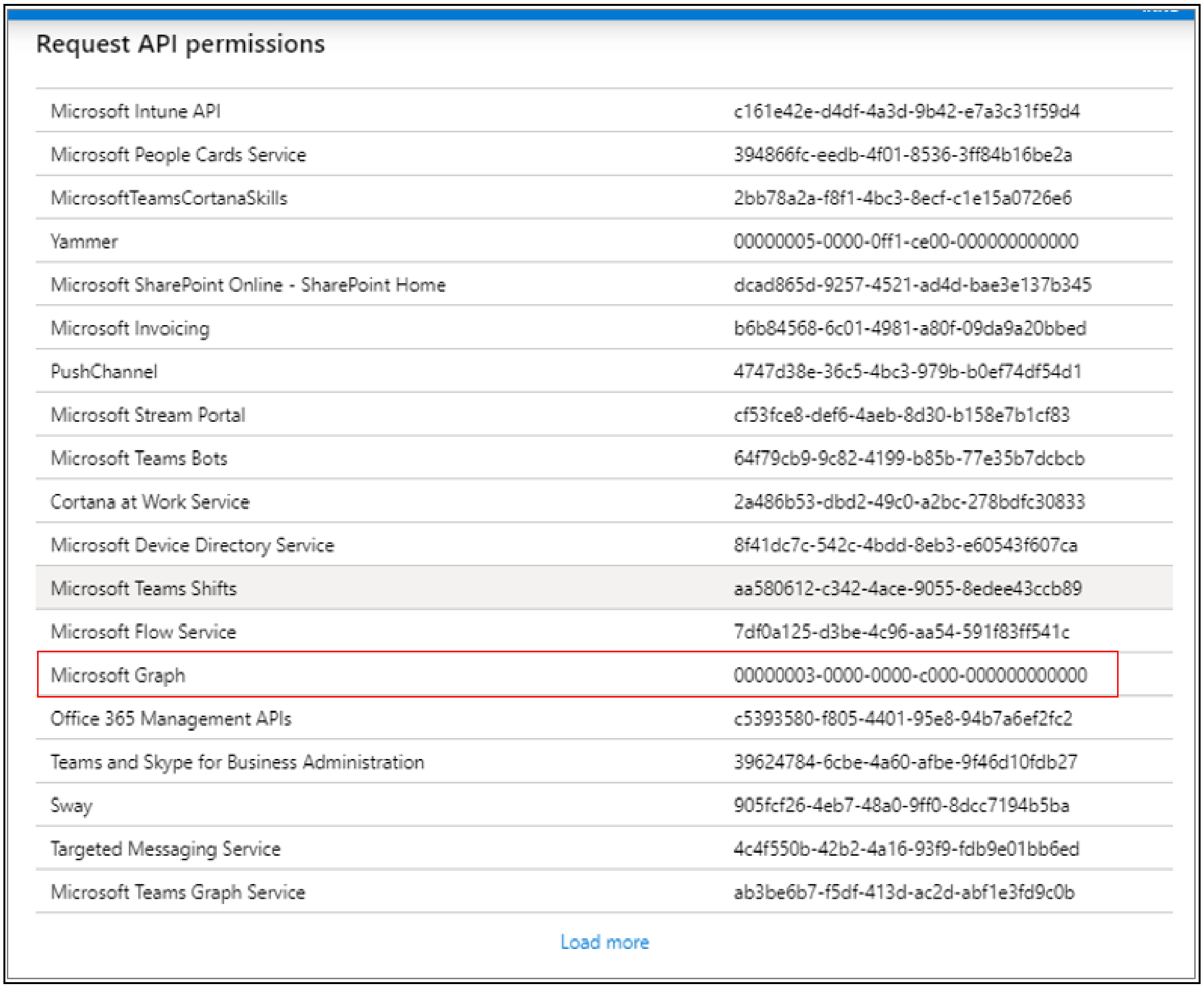
expand all

Type to search

Permission	Admin Consent Required
› Directory	
› Group	
› Member	
› Policy	
∨ User (1)	
☑ User.Read Sign in and read user profile ⓘ	-
□ User.Read.All Read all users' full profiles ⓘ	Yes
□ User.ReadBasic.All Read all users' basic profiles ⓘ	-

Figure 2.33: Granting the Microsoft Graph app permission to sign in and read user profile

18. As soon as you return to Figure 2.28, 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 2.29. Scroll down the list of APIs that appears until the **Microsoft Graph** API comes into view. Choose this API.

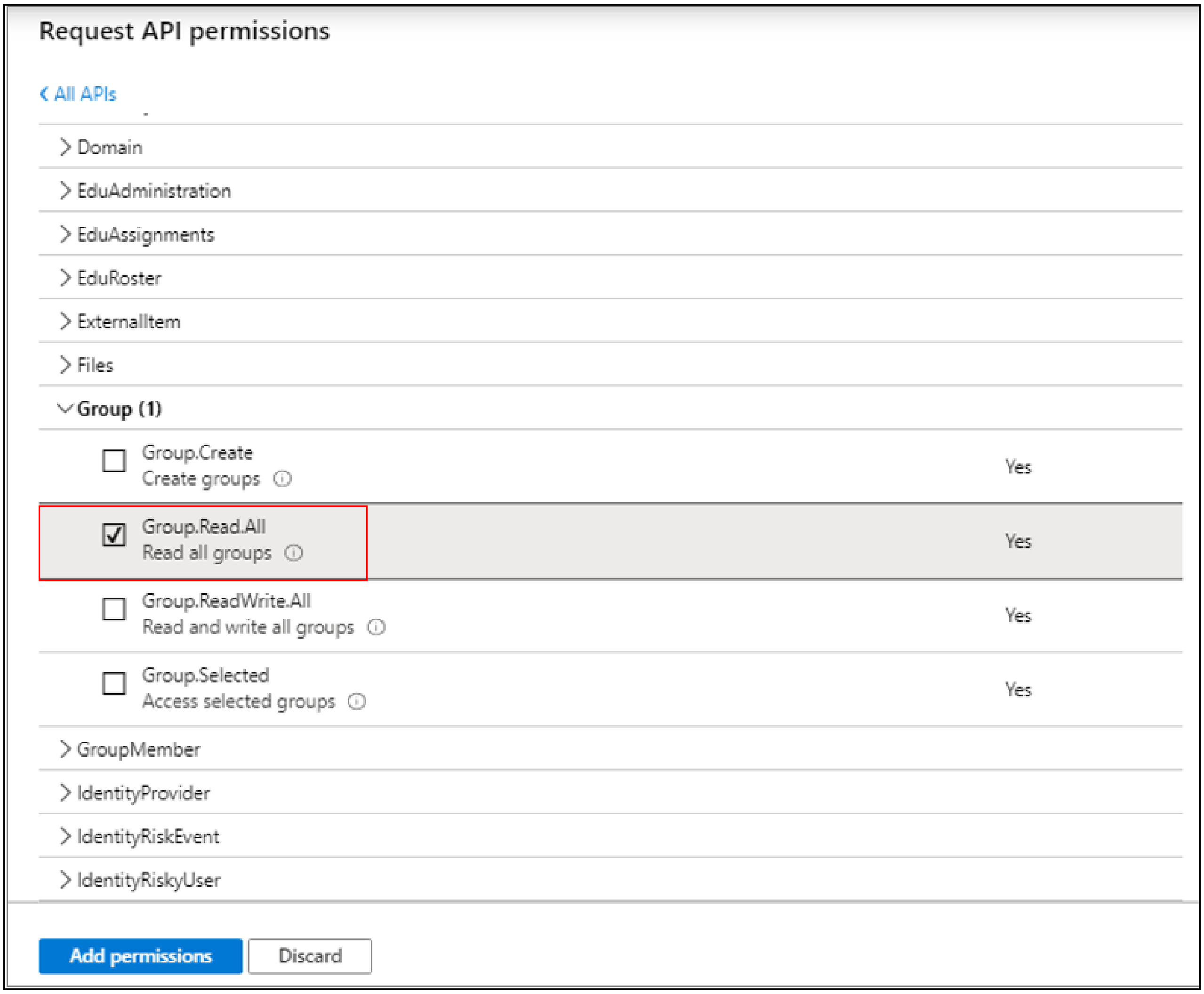


Request API permissions

Microsoft Intune API	c161e42e-d4df-4a3d-9b42-e7a3c31f59d4
Microsoft People Cards Service	394866fc-eedb-4f01-8536-3ff84b16be2a
MicrosoftTeamsCortanaSkills	2bb78a2a-f8f1-4bc3-8ecf-c1e15a0726e6
Yammer	00000005-0000-0ff1-ce00-000000000000
Microsoft SharePoint Online - SharePoint Home	dcad865d-9257-4521-ad4d-bae3e137b345
Microsoft Invoicing	b6b84568-6c01-4981-a80f-09da9a20bbed
PushChannel	4747d38e-36c5-4bc3-979b-b0ef74df54d1
Microsoft Stream Portal	cf53fce8-def6-4aeb-8d30-b158e7b1cf83
Microsoft Teams Bots	64f79cb9-9c82-4199-b85b-77e35b7dcbcb
Cortana at Work Service	2a486b53-dbd2-49c0-a2bc-278bdfc30833
Microsoft Device Directory Service	8f41dc7c-542c-4bdd-8eb3-e60543f607ca
Microsoft Teams Shifts	aa580612-c342-4ace-9055-8edee43ccb89
Microsoft Flow Service	7df0a125-d3be-4c96-aa54-591f83ff541c
Microsoft Graph	00000003-0000-0000-c000-000000000000
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Teams and Skype for Business Administration	39624784-6cbe-4a60-afbe-9f46d10fdb27
Sway	905fcf26-4eb7-48a0-9ff0-8dcc7194b5ba
Targeted Messaging Service	4c4f550b-42b2-4a16-93f9-fdb9e01bb6ed
Microsoft Teams Graph Service	ab3be6b7-f5df-413d-ac2d-abf1e3fd9c0b

Figure 2.34: 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.



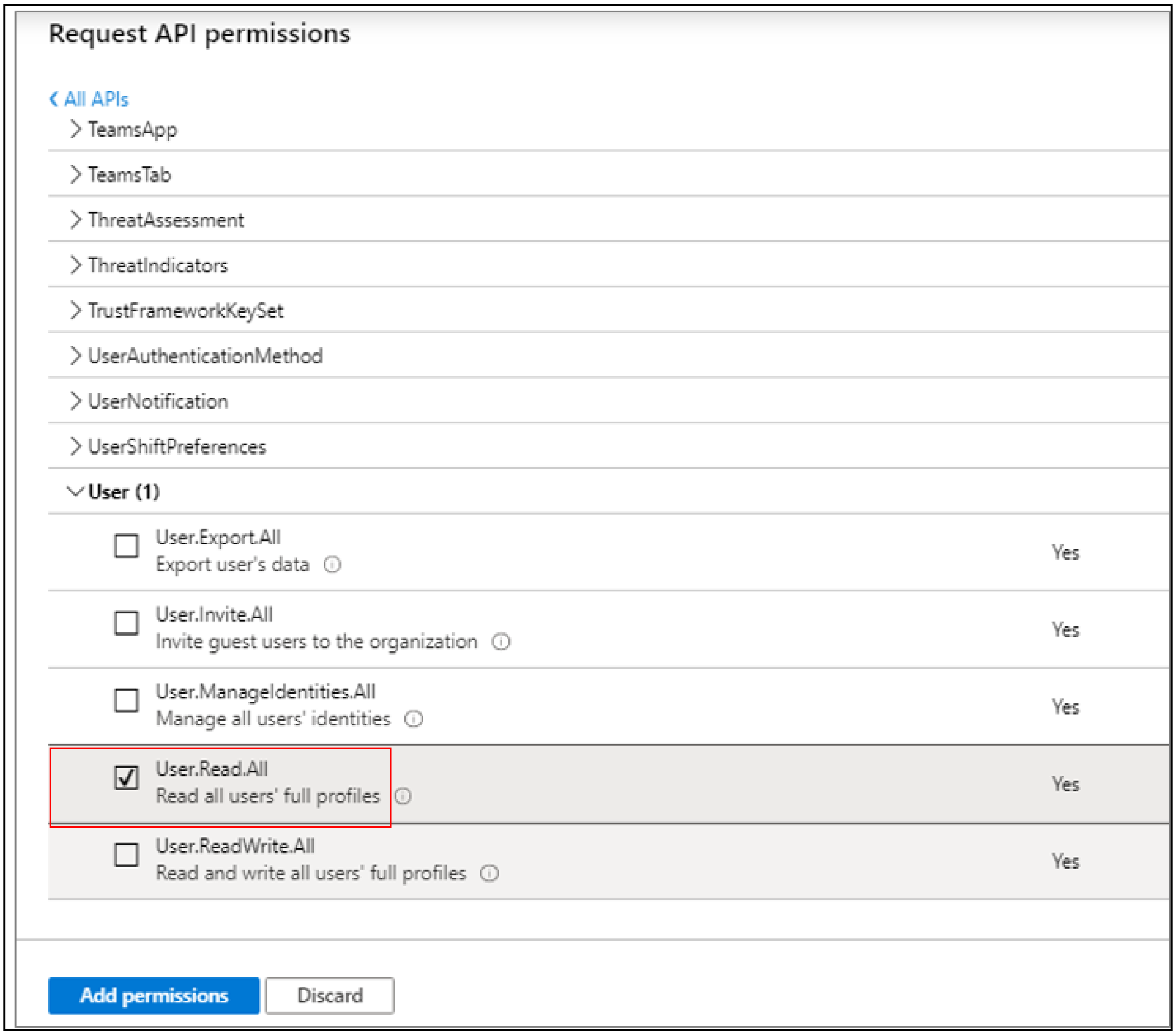
Request API permissions

‹ All APIs

- › Domain
- › EduAdministration
- › EduAssignments
- › EduRoster
- › ExternalItem
- › Files
- ⌄ Group (1)
  - □ Group.Create — Create groups — Yes
  - ☑ Group.Read.All — Read all groups — Yes
  - □ Group.ReadWrite.All — Read and write all groups — Yes
  - □ Group.Selected — Access selected groups — Yes
- › GroupMember
- › IdentityProvider
- › IdentityRiskEvent
- › IdentityRiskyUser

Figure 2.35: 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.



Request API permissions

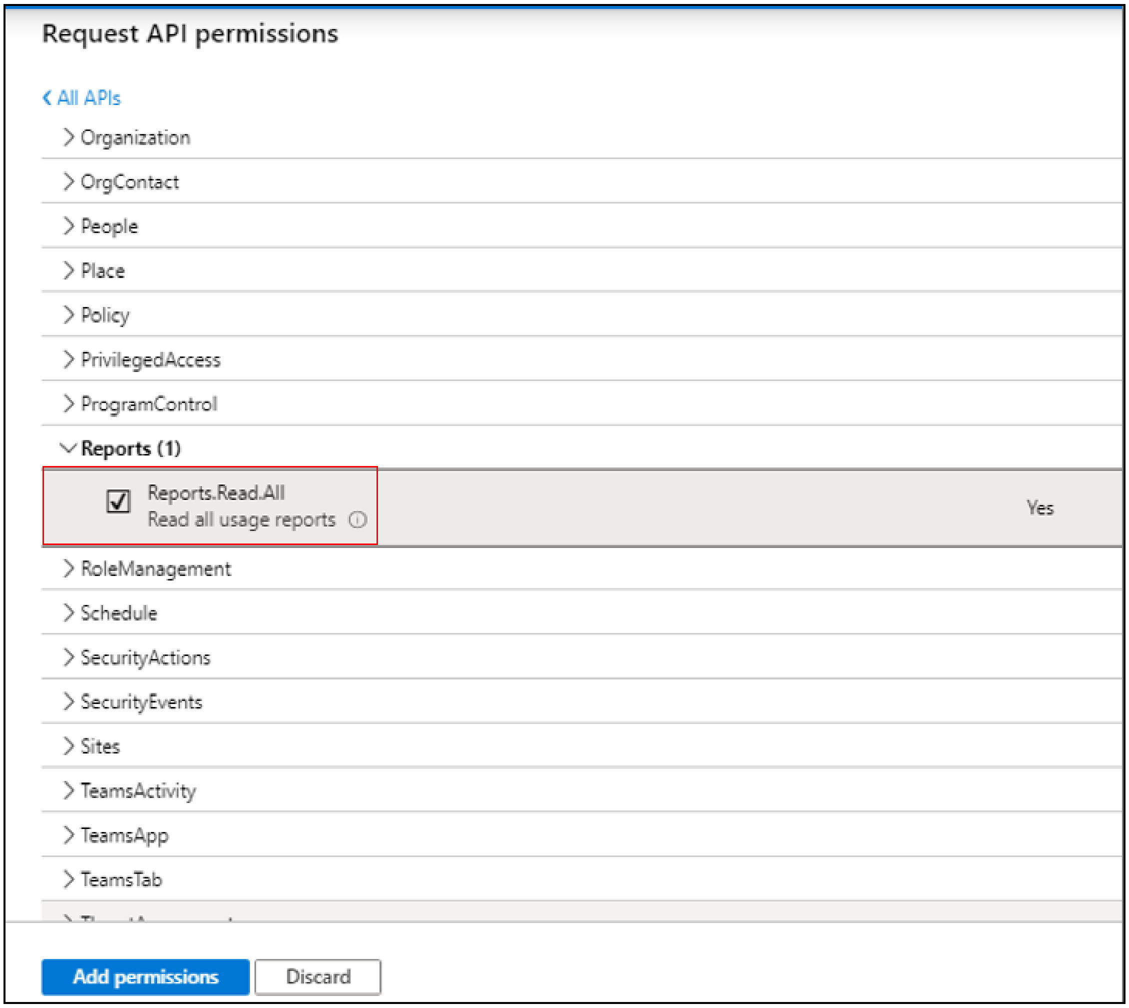
< All APIs

- > TeamsApp
- > TeamsTab
- > ThreatAssessment
- > ThreatIndicators
- > TrustFrameworkKeySet
- > UserAuthenticationMethod
- > UserNotification
- > UserShiftPreferences
- ∨ User (1)

□	User.Export.All Export user's data	Yes
□	User.Invite.All Invite guest users to the organization	Yes
□	User.ManageIdentities.All Manage all users' identities	Yes
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadWrite.All Read and write all users' full profiles	Yes

Figure 2.36: 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.



Request API permissions

< All APIs

> Organization

> OrgContact

> People

> Place

> Policy

> PrivilegedAccess

> ProgramControl

∨ Reports (1)

☑	Reports.Read.All Read all usage reports ⓘ	Yes

> RoleManagement

> Schedule

> SecurityActions

> SecurityEvents

> Sites

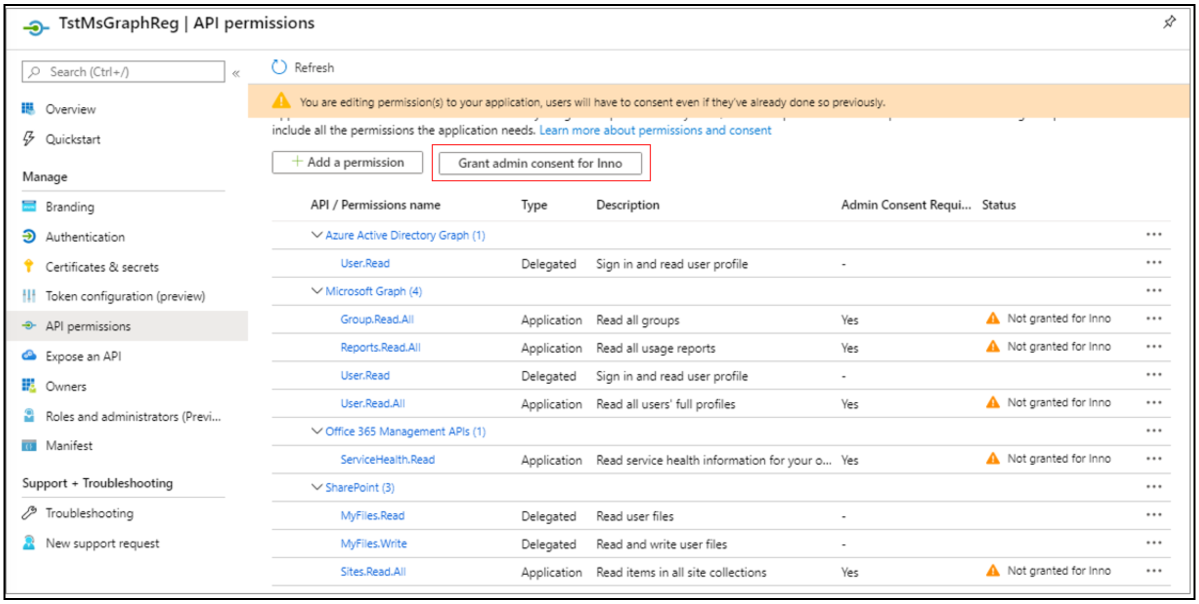
> TeamsActivity

> TeamsApp

> TeamsTab

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

22. Finally, click the **Add permissions** button in Figure 2.37 to add all the chosen permissions to the Microsoft Graph app. When Figure 2.38 appears, click the **Grant admin consent for <user>** button therein to grant admin consent for the user.



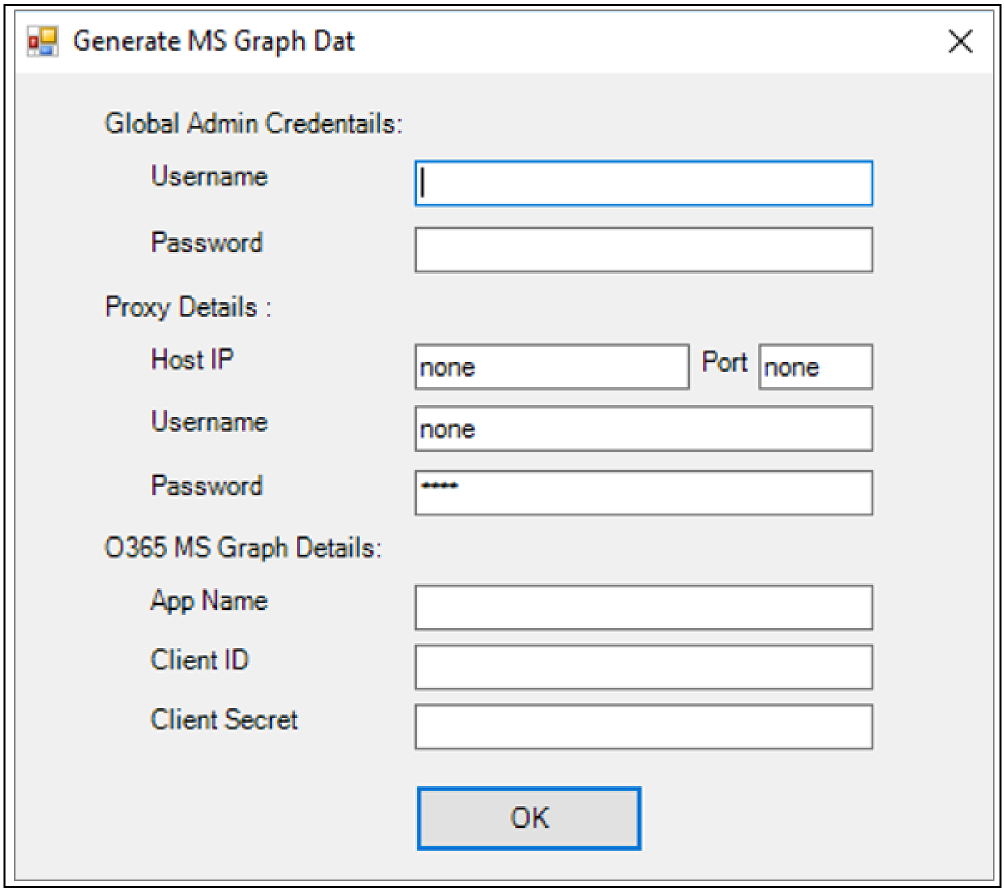
You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin Consent Requi...	Status
Azure Active Directory Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	
Microsoft Graph (4)				
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Inno
Reports.Read.All	Application	Read all usage reports	Yes	⚠ Not granted for Inno
User.Read	Delegated	Sign in and read user profile	-	
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Inno
Office 365 Management APIs (1)				
ServiceHealth.Read	Application	Read service health information for your o...	Yes	⚠ Not granted for Inno
SharePoint (3)				
MyFiles.Read	Delegated	Read user files	-	
MyFiles.Write	Delegated	Read and write user files	-	
Sites.Read.All	Application	Read items in all site collections	Yes	⚠ Not granted for Inno

Figure 2.38: 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 2.39 will appear.



Generate MS Graph Dat

Global Admin Credentails:

Username

Password

Proxy Details :

Host IP none Port none

Username none

Password ****

O365 MS Graph Details:

App Name

Client ID

Client Secret

Figure 2.39: Generating MS Graph Dat

24. In Figure 2.39, 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 2.21). The **Client secret** should be the key that is generated and assigned to the client secret in step 8 above (see Figure 2.24). Finally, click the **OK** button.

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

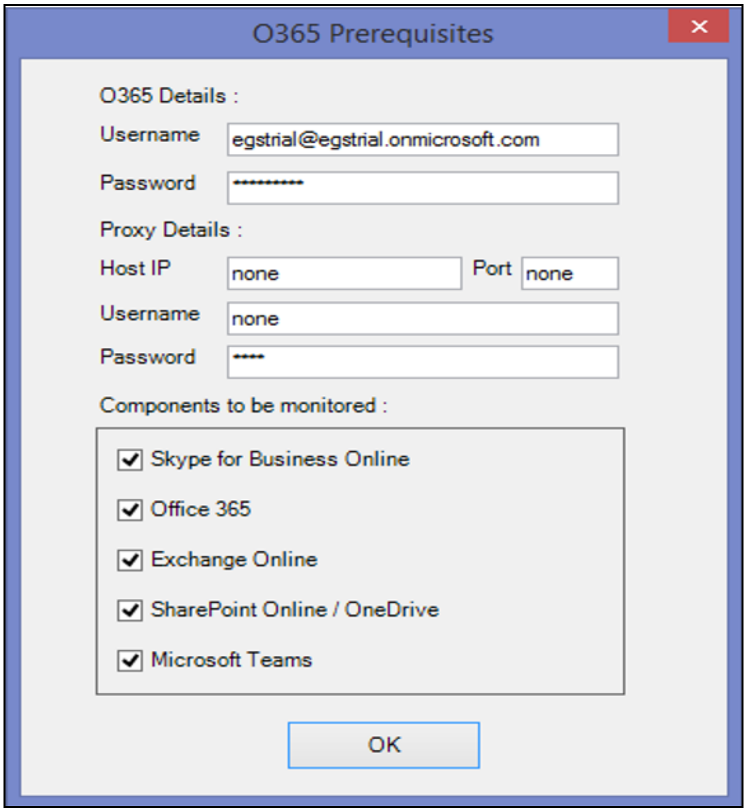
2.1.3 Using Powershell Scripts to Fulfill Requirements for Monitoring SharePoint Online

To ensure that pre-requisites 5, 6, 7, and 8 discussed in Section **2.1** are fulfilled without a glitch, eG Enterprise provides customized PowerShell scripts. By running these scripts, you can have these requirements automatically fulfilled. This way, you can eliminate the effort, time, and the likelihood of errors in getting SharePoint Online 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 SharePoint 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 it

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 2.40 will appear.



O365 Prerequisites

O365 Details :

Username: egstrial@egstrial.onmicrosoft.com

Password: **********

Proxy Details :

Host IP: none Port: none

Username: none

Password: ****

Components to be monitored :

- ☑ Skype for Business Online
- ☑ Office 365
- ☑ Exchange Online
- ☑ SharePoint Online / OneDrive
- ☑ Microsoft Teams

Figure 2.40: Selecting the components for which modules/packages should be automatically downloaded and installed

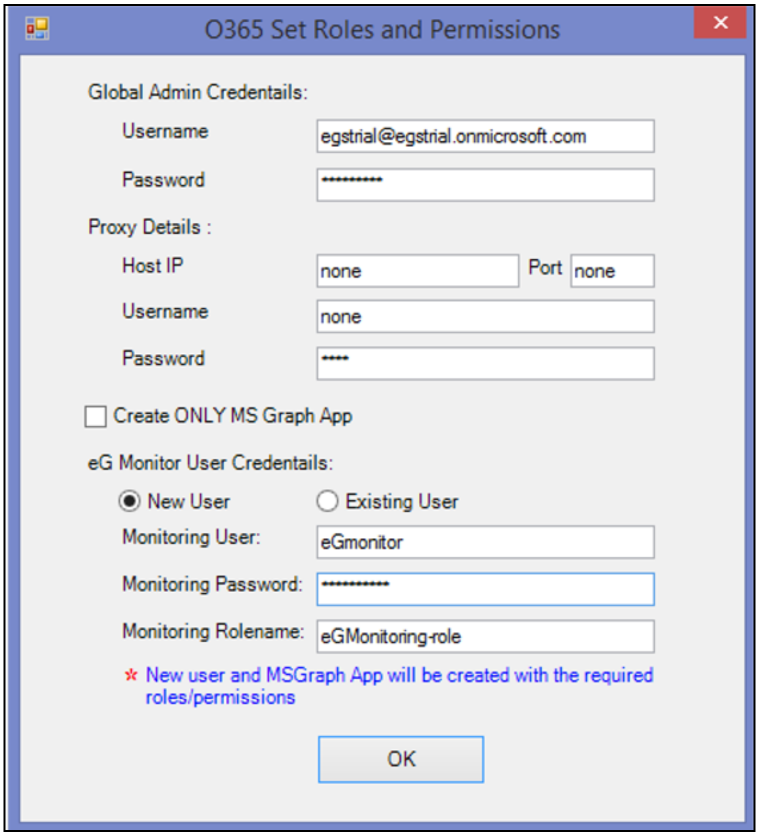
Specify the following in Figure 2.40:

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 2.40). 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 SharePoint Online, select the **SharePoint Online** check box.
5. Then, click the **OK** button. If the **SharePoint 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**;
- The SharePoint Online Management Shell

If you run the **O365SetRolesAndpermissions.ps1** script from the <EG_AGENT_INSTALL_ DIR>\lib directory, then the dialog box shown by Figure 2.41 will appear:



O365 Set Roles and Permissions

Global Admin Credentails:

Username: egstrial@egstrial.onmicrosoft.com

Password: **********

Proxy Details :

Host IP: none Port: none

Username: none

Password: ****

□ Create ONLY MS Graph App

eG Monitor User Credentails:

● New User ○ Existing User

Monitoring User: eGmonitor

Monitoring Password: ***********

Monitoring Rolename: eGMonitoring-role

* New user and MSGraph App will be created with the required roles/permissions

Figure 2.41: Automatically creating a new user with the required permissions

Specify the following in Figure 2.41:

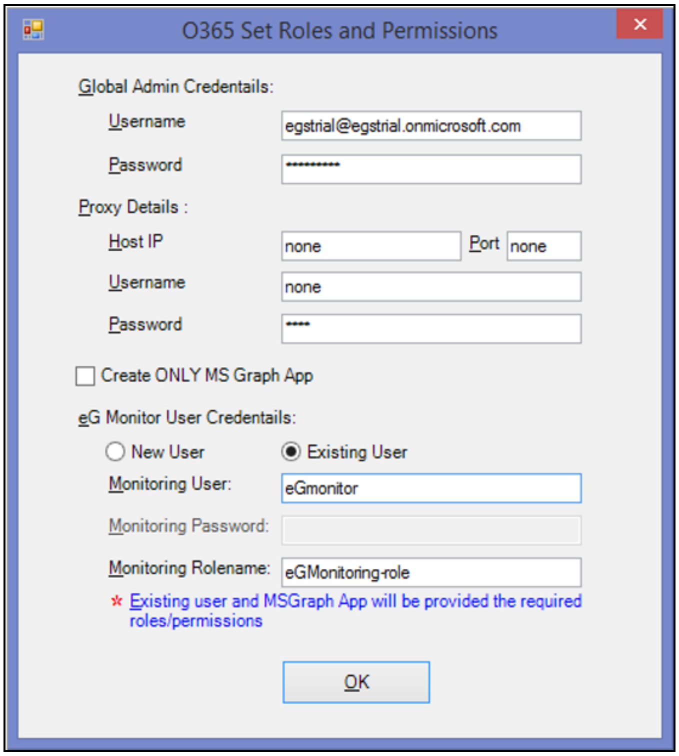
1. First, enter the **Username** and **Password** of the global administrator. This is because, only a global administrator is authorized to create new users/apps and set their permissions.

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 2.41. 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 2.42). 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.



O365 Set Roles and Permissions

Global Admin Credentails:

Username: egstrial@egstrial.onmicrosoft.com

Password: ••••••••••

Proxy Details :

Host IP: none Port: none

Username: none

Password: ••••

□ Create ONLY MS Graph App

eG Monitor User Credentails:

○ New User ● Existing User

Monitoring User: eGmonitor

Monitoring Password:

Monitoring Rolename: eGMonitoring-role

* Existing user and MSGraph App will be provided the required roles/permissions

Figure 2.42: Using an existing user for monitoring purposes

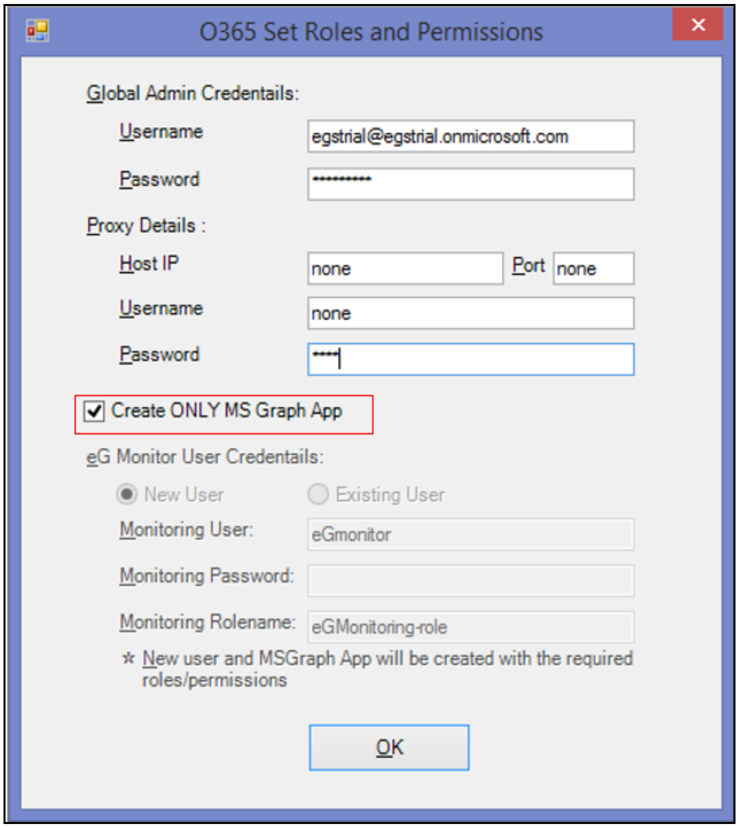
6. Finally, click the **OK** button in Figure 2.42. Doing so, will result in the following:

   - 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**Service support admin**, **SharePoint admin**, and **View-Only Audit Logs** permissions required for monitoring SharePoint 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 **Service support admin**, **SharePoint admin**, and **View-Only Audit Logs**permissions required for monitoring SharePoint 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 **Service support admin**, **SharePoint admin**, and **View-Only Audit Logs**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 2.43. Then, click the **OK** button.



O365 Set Roles and Permissions

Global Admin Credentails:

Username	egstrial@egstrial.onmicrosoft.com
Password	••••••••••

Proxy Details :

Host IP	none	Port	none
Username	none		
Password	••••		

☑ Create ONLY MS Graph App

eG Monitor User Credentails:

● New User ○ Existing User

Monitoring User:	eGmonitor
Monitoring Password:	
Monitoring Rolename:	eGMonitoring-role

* New user and MSGraph App will be created with the required roles/permissions

Figure 2.43: Choosing to only install the Microsoft Graph App

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

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

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

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

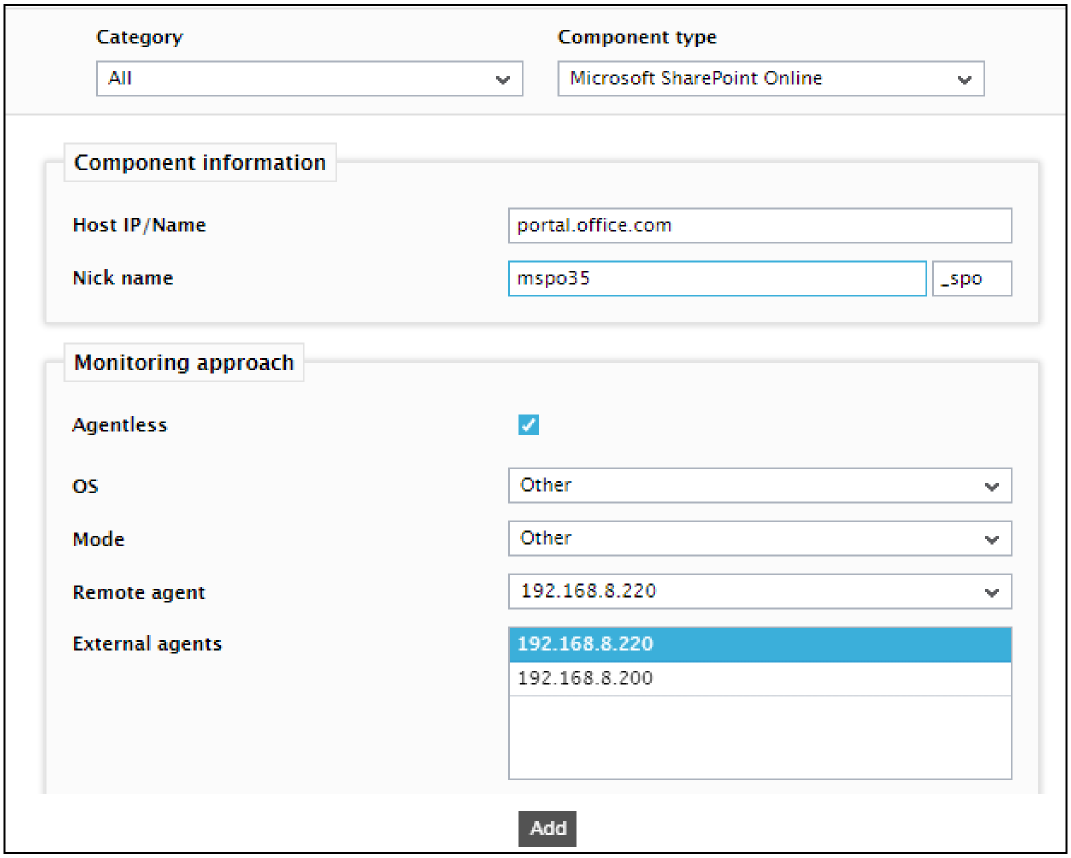
Section **3.1**

Section **3.2**

3.1 Adding a Microsoft SharePoint Online Component

eG Enterprise cannot auto-discover a Microsoft SharePoint 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 SharePoint 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 SharePoint Online* as the **Component type** and click the **Add New Component** button.
4. Figure 3.1 will then appear.



Category: All

Component type: Microsoft SharePoint Online

Component information

Host IP/Name: portal.office.com

Nick name: mspo35 _spo

Monitoring approach

Agentless: ☑

OS: Other

Mode: Other

Remote agent: 192.168.8.220

External agents: 192.168.8.220
192.168.8.200

Figure 3.1: Adding a Microsoft SharePoint Online component

5. In Figure 3.1, by default, portal.office.com will be displayed as the **Host IP/Name** of the target Microsoft SharePoint Online component. If the host name of the SharePoint Online component you want to monitor is different in your environment, then modify this specification.

6. Provide a unique **Nick Name** for the SharePoint Online component being added. Note that any nick name you specify here will be automatically suffixed with the string, *_spo*.

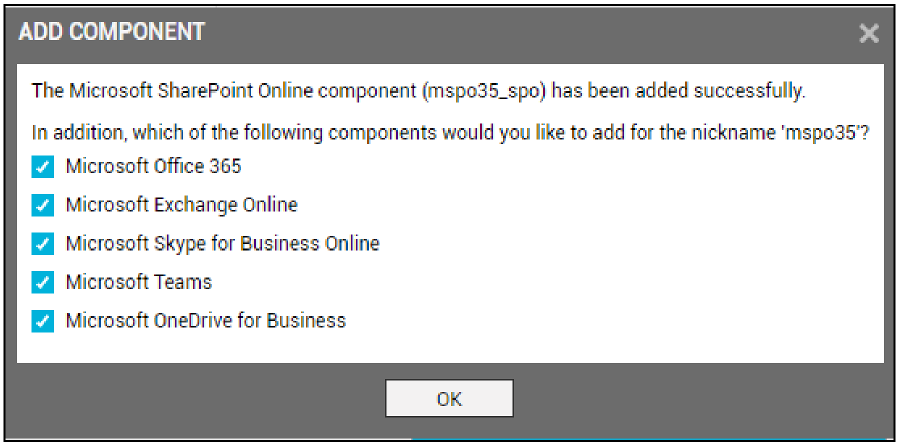
7. Since SharePoint Online is by default monitored in an agentless manner, the **Agentless** flag will be enabled. Let the default settings remain in the **OS** and **Mode** selection boxes.

8. Next, select the **Remote agent** and **External agent** that will monitor the target SharePoint 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 an Exchange Online, Office 365, Skype for Business Online, Microsoft Teams, and/or a Microsoft OneDrive for Business component, when adding a SharePoint Online component. This is why, when clicking the **Add** button in Figure 3.1, you will be immediately prompted to manage the above-mentioned components using the same nick name as the SharePoint 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 SharePoint Online, then click **OK** without selecting any of the check boxes.



The Microsoft SharePoint Online component (mspo35_spo) has been added successfully.

In addition, which of the following components would you like to add for the nickname 'mspo35'?

☑ Microsoft Office 365
☑ Microsoft Exchange Online
☑ Microsoft Skype for Business Online
☑ Microsoft Teams
☑ Microsoft OneDrive for Business

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:

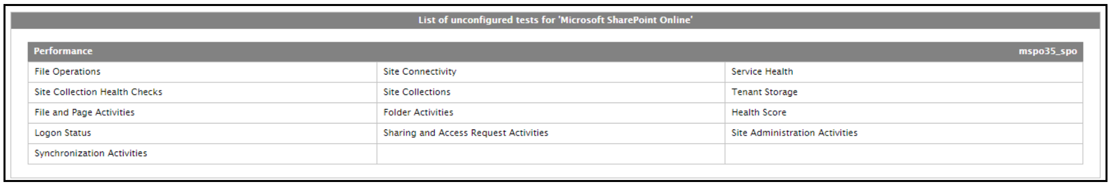
Component Type	Nick name
Microsoft Office 365	eGOffice_365
Microsoft Exchange Online	eGOffice_exo

- 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 SharePoint Online Component

After adding a Microsoft SharePoint 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 SharePoint Online component.

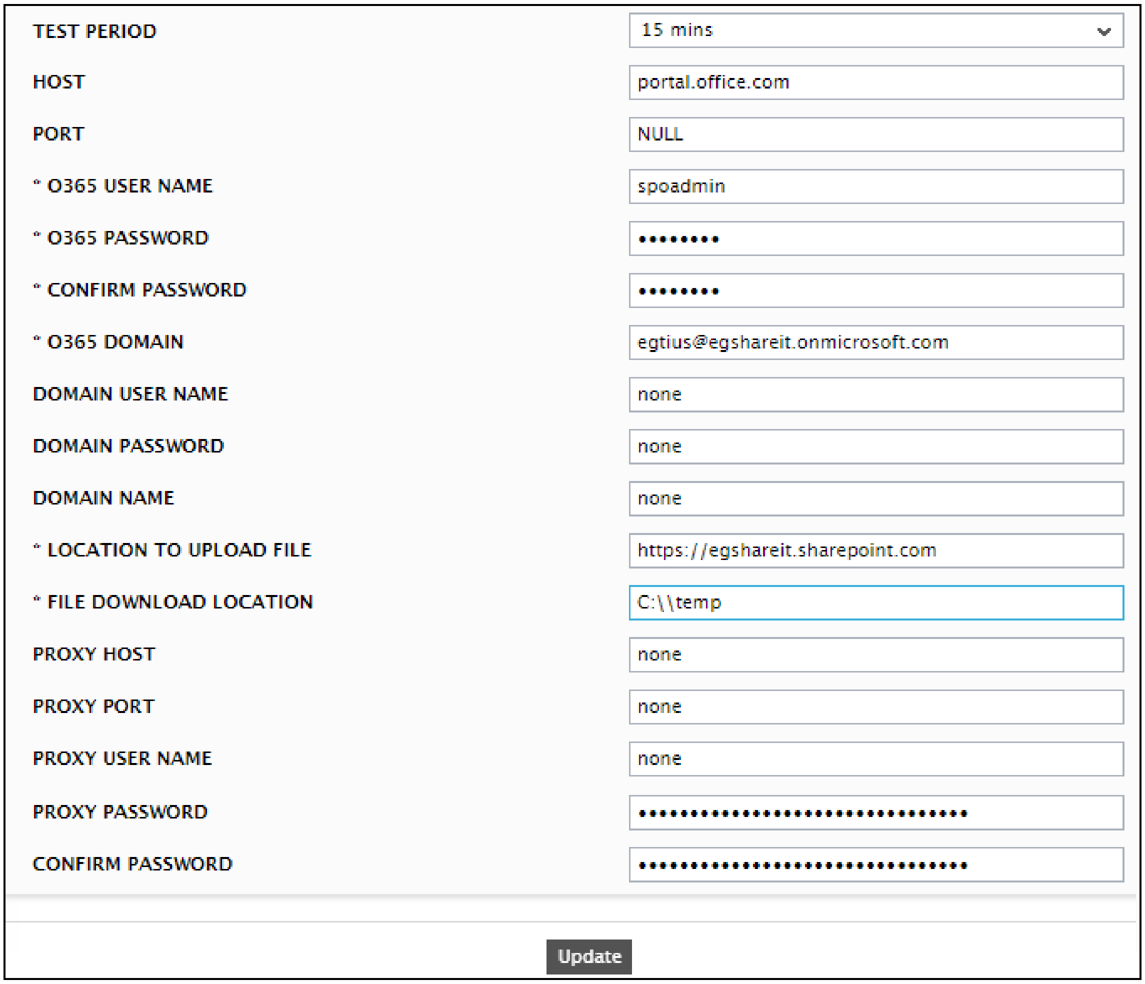


List of unconfigured tests for 'Microsoft SharePoint Online'

Performance		mspo35_spo
File Operations	Site Connectivity	Service Health
Site Collection Health Checks	Site Collections	Tenant Storage
File and Page Activities	Folder Activities	Health Score
Logon Status	Sharing and Access Request Activities	Site Administration Activities
Synchronization Activities		

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

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

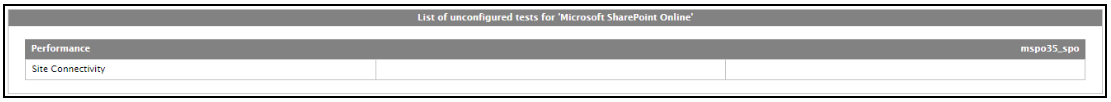


TEST PERIOD	15 mins
HOST	portal.office.com
PORT	NULL
* O365 USER NAME	spoadmin
* O365 PASSWORD	••••••••
* CONFIRM PASSWORD	••••••••
* O365 DOMAIN	egtius@egshareit.onmicrosoft.com
DOMAIN USER NAME	none
DOMAIN PASSWORD	none
DOMAIN NAME	none
* LOCATION TO UPLOAD FILE	https://egshareit.sharepoint.com
* FILE DOWNLOAD LOCATION	C:\\temp
PROXY HOST	none
PROXY PORT	none
PROXY USER NAME	none
PROXY PASSWORD	••••••••••••••••••••••••••••••••
CONFIRM PASSWORD	••••••••••••••••••••••••••••••••

Figure 3.4: Configuring the File Operations test

This test emulates a file upload, download, checkin, checkout, and delete operation, and reports the status and time taken by each operation. In the process, the test proactively alerts administrators to the failure/slowness in a file operation, thereby enabling them to investigate and resolve the bottleneck before users complain. To know what parameters this test takes and how to configure it, refer to the File Operations Test 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 Site Connectivity test (see Figure 3.5).



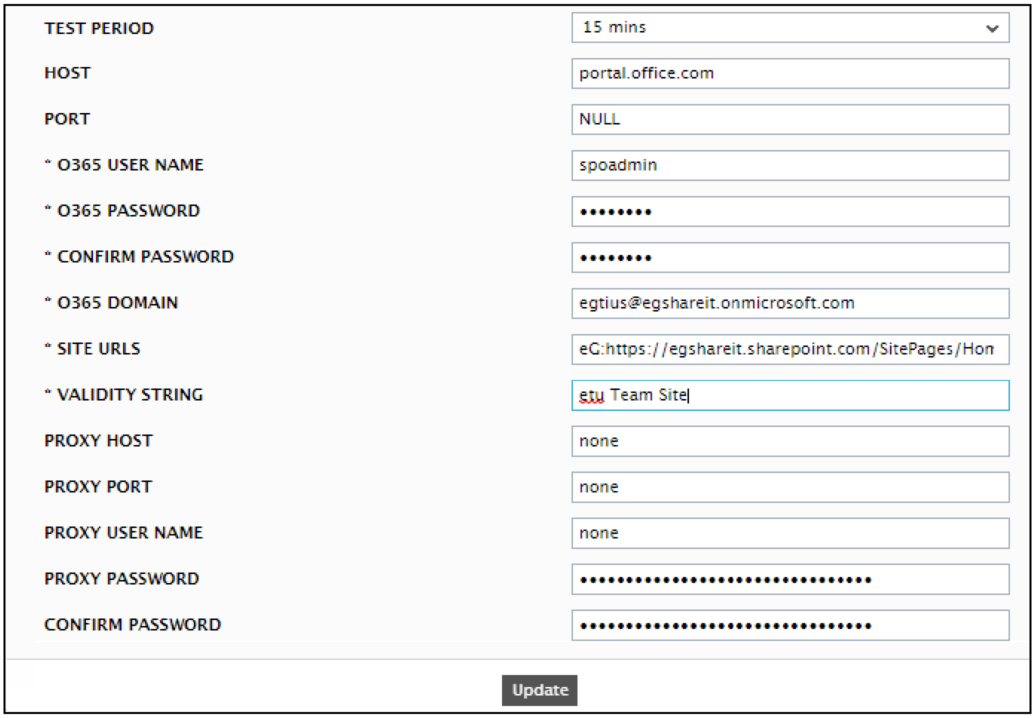
List of unconfigured tests for 'Microsoft SharePoint Online'

Performance		mspo35_spo
Site Connectivity		

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

For each site that is configured for monitoring, this test, at frequent intervals, emulates an HTTP/S connection to that site and reports on the availability and responsiveness of that site.

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



TEST PERIOD	15 mins
HOST	portal.office.com
PORT	NULL
* O365 USER NAME	spoadmin
* O365 PASSWORD	••••••••
* CONFIRM PASSWORD	••••••••
* O365 DOMAIN	egtius@egshareit.onmicrosoft.com
* SITE URLS	eG:https://egshareit.sharepoint.com/SitePages/Hon
* VALIDITY STRING	etu Team Site
PROXY HOST	none
PROXY PORT	none
PROXY USER NAME	none
PROXY PASSWORD	••••••••••••••••••••••••••••••••
CONFIRM PASSWORD	••••••••••••••••••••••••••••••••

Figure 3.6: Configuring the Site Connectivity test

Refer to the Section **4.6.2** 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 SharePoint Online

To monitor the managed Microsoft SharePoint Online component, login to the eG management console as a user with monitoring privileges. To learn more refer to, Top-8-sharepoint-metrics-performance-monitoring.

Browse the **Components At-A-Glance** section of the Monitor Home page that appears, and locate the *Microsoft SharePoint 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 SharePoint Online (see Figure 4.1).

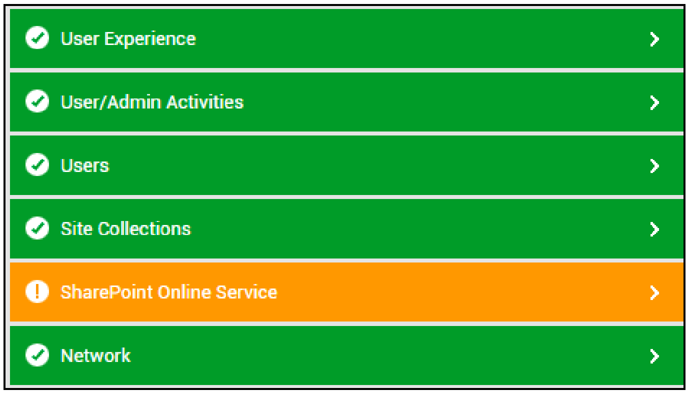


Figure 4.1: Layer model for the Microsoft SharePoint Online component

Each layer of Figure 4.1 is mapped to tests that report metrics, which help audit a wide variety of operations performed on SharePoint Online (eg., file operations, folder operations, site administration operations, etc.), and also help manage the health of sites and site collections. Using these metrics, administrators can find quick and accurate answers to the following performance queries:

- Is SharePoint Online accessible over the network?
- Has any latency been noticed in network connections to SharePoint Online?
- Is any SharePoint site unavailable? If so, which site is it?
- Is any SharePoint site taking too long to respond to requests?
- Were any sites deleted recently? Which ones are they?
- Are there any inactive site collections? If so, which ones?
- Which site collection is locked?

- Is any site collection accessed by external users?
- Is any site collection running out of server and/or storage resources? If so, why? - is it because the resource usage quotas for the site collection has been poorly set? Or is it because the tenant's resource usage quota has not been properly set?
- What type of operations are performed on SharePoint Online - file and page operations? folder operations? sharing and access operations? site administration operations? synchronization operations? or all of the above?
- Are file and page operations imposing too much load on SharePoint Online? If so, what type of operations are contributing to this load? Who initiated such operations, from where? Is anything suspicious about these operations?
- Are folder operations imposing too much load on SharePoint Online? If so, what type of folder operations are contributing to this load? Who initiated such operations, from where? Is anything suspicious about these operations?
- Are too many sharing and access activities been performed on SharePoint Online? If so, what type of operations are contributing to this load? Who initiated such operations, from where? Is anything suspicious about these operations?
- Are any synchronization operations in progress currently? If so, who initiated such operations and from where?
- Were any sync relationships not allowed?
- Are an abnormally large number of synchronization operations been performed? If so, what type of synchronization operations are contributing to this unusual workload, and who is initiating such operations? Are all such operations performed only by authorized users?
- Did any file operation - checkin, checkout, download, upload, or deletion - fail?
- Did any file operation - checkin, checkout, download, upload, or deletion - take too long a time?
- Is the health score of SharePoint abnormal?
- Did any health check fail? If so, which health check failed on which site collection?

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**

The User/Admin Activities Layer

Section **4.6**

4.1 The Network Layer

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

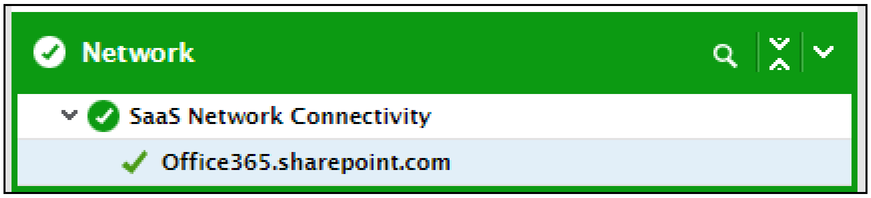


Figure 4.2: The test mapped to the Network layer

4.1.1 SaaS Network Connectivity Test

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

This is an external test that emulates a network-level ping to the cloud-based SharePoint 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 SharePoint Online service.

Target of the test : Microsoft SharePoint Online

Agent deploying the test : An external agent

Outputs of the test : One set of results for the SharePoint 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 Office365.sharepoint.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 server.	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 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.

4.2 The SharePoint Online Service Layer

With the help of the tests mapped to the SharePoint Online Service layer, you can:

- Glean problem information from response headers sent out by SharePoint Online;
- Understand server and storage resource quotas definitions at the tenant-level, and server and storage resource allocations to site collections;
- Capture service incidents as and when they occur

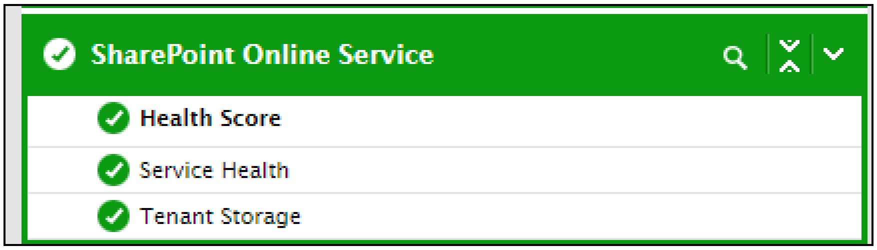


Figure 4.3: The tests mapped to the SharePoint Online Service layer

4.2.1 Health Score Test

Information that a browser sends back in the response headers for each file can serve as an effective tool for diagnosing performance issues with SharePoint Online. The three most useful values contained in response headers are:

- **X-SharePointHealthScore:** This is the value, from zero to ten, that indicates how heavily loaded the SharePoint Server is at the time when the page was served.
- **SPRequestDuration:** This is the amount of time (again, in milliseconds) that it took to process the request on the server. Basically, this is the end-to-end processing time for the page.
- **SPIislatency:** This is a measure of the amount of time (in milliseconds) that the request spent queued and waiting to be processed by IIS (Internet Information Services – the web server).

Using the Health Score test, administrators can easily track these values, proactively capture potential performance issues with SharePoint Online, and rapidly initiate measures to fix them before any irreparable damage is done.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Health score	Indicates the current health score of the SharePoint server.	Number	This number ranges from 0 to 10 where 0 indicates the server is idle and 10 indicates the server is very busy. A HealthScore that is consistently 9 or 10 might indicate an ongoing performance issue with the server. Any other number indicates that server is operating within the expected range.
Request duration	Indicates the amount of time (again, in milliseconds) that it took to process the request on the server.	Seconds	Healthy pages range from a couple hundred milliseconds to around a second depending on the content of the page.
IIS latency	Indicates time (in milliseconds) that the request spent queued and waiting to be processed by IIS server.	Seconds	Ideally, the value of this measure should be zero or very close to zero.

4.2.2 Service Health Test

To ensure the high uptime and peak performance of SharePoint Online, administrators should be able to detect issues in the SharePoint Online service much before users complain. The **Service Health** test helps administrators with this! This test reports the status of the SharePoint 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 SharePoint 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 SharePoint Online.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with

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

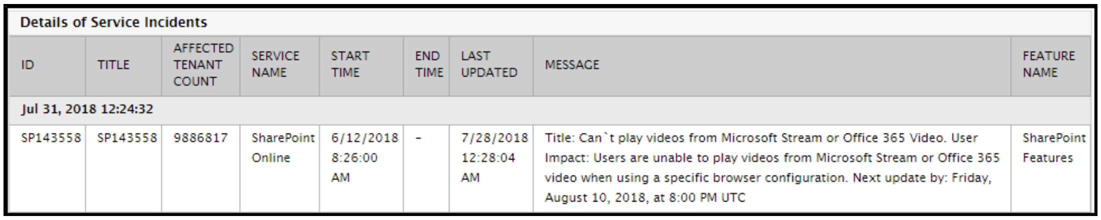
Parameters	Description
	• The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Service status</td><td>Indicates the current health status of this service.</td><td></td><td>If the service is not experiencing any service incidents currently. , then this measure will report the value <i>Healthy</i>. On the other hand, if even one service incident is occurring on the service, then this measure will report the value <i>Service Degraded</i>.
The numeric values that correspond to these measure values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Healthy</td><td>1</td></tr><tr><td>Service degraded</td><td>0</td></tr></table><b>Note:</b>
By default, this measure reports the <b>Measure Valu</b>es listed in the table above to indicate current health status of a service. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Service incidents</td><td>Indicates the number of service incidents that are currently occurring on this service.</td><td>Number</td><td>Unplanned service incidents occur when SharePoint Online is unavailable or unresponsive.
Use the detailed diagnosis of this measure to know the complete details</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			of the service incidents.
Maintenance events	Indicates the number of maintenance events currently occurring on this service.	Number	Planned maintenance is regular Microsoft-initiated service updates to the infrastructure and software applications. Microsoft typically plans maintenance for times when service usage is historically at its lowest based on regional time zones.

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



Details of Service Incidents

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

Figure 4.4: The detailed diagnosis of the Service incidents measure

4.2.3 Tenant Storage Test

Tenant is a term used for an Office 365 Organization. It is a sandboxed environment for your and your assets. It is within the overall O365 Data Center and is the container for items of your Organization such as users, domains, subscriptions etc.

Typically, server resources such as CPU and RAM are allocated to an Office 365 tenant as a whole based on the number of user licenses; these resources are then shared by all site collections in the tenant. This means that there is the danger of a single site collection exhausting the resources across the tenancy. To avoid this, organizations that have customized site collections or sandboxed solutions use resource quotas. By applying resource quotas to specific collections, administrators can ensure that custom code running in specific site collections does not deplete all server resources assigned to the tenancy.

Like CPU and RAM, storage resources are also allocated to a tenant based on the number of user licenses associated with that tenancy. This storage can then be allocated to the site collections in one of the following ways:

- Automatically, using pooled storage
- Manually, by explicitly configuring storage allocations on a per-site collection basis

Regardless of what the resource is (CPU, memory, or storage) and how it is allocated to site collections, it is important that administrators know the total server resource pool/quota and storage quota set for a monitored tenant, and also track how much of the tenant's resources have been assigned/allocated to site collections. This insight will enable administrators proactively detect a potential server/storage resource shortage on the tenant and promptly prevent it by tweaking the quota setting. The **Tenant Storage** test provides administrators with this useful insight!

This test reports the server and storage resource quotas that have been set for the monitored tenant, and also tracks how much of these resources have been assigned/allocated to site collections. This way, the test reveals whether/not the quotas set for the tenant are adequate, thus urging administrators to fine-tune the quota settings (if required) to avert any resource contention. Additionally, by reporting the count and details of sites deleted, the test also sheds light on how much storage and server resources the deleted sites have released. This information provides useful pointers to administrators for fine-tuning the quota setting.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said

Parameters	Description
	privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to none.
Proxy Host, Proxy Port, Proxy User Name, Proxy 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, provide the IP/host name and port number of the Proxy server that the eG agent should use in the **PROXY HOST** and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that

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

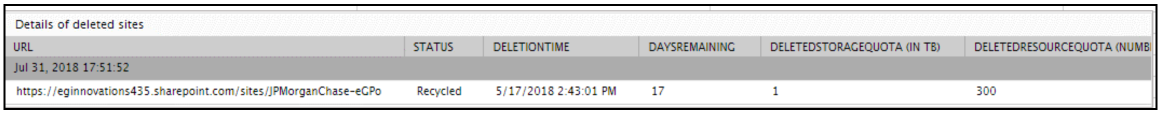
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
OneDrive storage quota	Indicates the OneDrive storage quota.	GB	
Total server resource quota	Indicates the total server resource quota.	Number	The server resource quota is a site collection metric calculated by SharePoint Online. The main purpose of server resource quotas is to limit the risk that sand-boxed custom code can have on available resources on a site collection - bad code causing unhandled

Measurement	Description	Measurement Unit	Interpretation
			exceptions or excessive CPU usage are good examples. Your organization is assigned a total Server Resource Pool that is based on the total number of users. By default when you create a site collection it is assigned a Server Resource Quota of 300. Generally this an acceptable quota. If you do not want to allow any sandbox solutions to be used within your site collection you can set this value to zero (0).
Assigned server resource quota	Indicates the server resource quota that has been assigned to site collections in the monitored tenant.	Number	If the value of this measure is equal to or close to the value of the Total server resource quota measure, it indicates that a huge chunk of the tenant's resources have been assigned to site collections via site collection-specific resource quotas. To ensure that the tenant does not run out of CPU and memory resources, you may want to increase the tenant's server resource pool or the reduce the allocations to the site collections.
Tenant storage quota	Indicates the storage quota of the monitored tenant.	TB	
Tenant storage quota assigned	Indicates the storage quota of the tenant that has been assigned to all site collections in the tenant.	TB	If the value of this measure is equal to or close to the value of the Tenant storage quota measure, it indicates that a huge chunk of the tenant's storage resources have been assigned to site collections. To ensure that the tenant does not run out of storage resources, you may want to increase the tenant's storage quota or the reduce the allocations to the site collections.

Measurement	Description	Measurement Unit	Interpretation
Deleted sites	Indicates the number of sites in the tenant that have been deleted.	Number	Use the detailed diagnosis of this measure to know which sites have been deleted.
Applications	Indicates the number of applications the tenant hosts.	Number	Use the detailed diagnosis of this measure to know which applications are hosted by the tenant.
Web templates	Indicates the number of web templates in the monitored tenant.	Number	To know which are the web templates, use the detailed diagnosis of this measure.

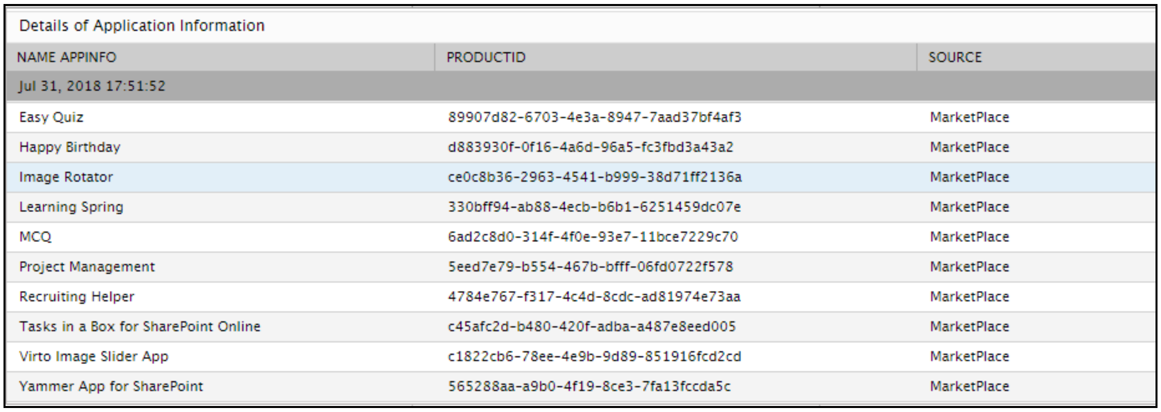
The detailed diagnosis of the *Deleted sites* measure lists the deleted sites in the tenant, the current status of each site, when they were deleted, and how much resource and storage quota was released upon their deletion. In the event of a resource contention, if administrators decide to increase the storage and/or server resource quota, then knowing how much resources were freed up by deleted sites will help them figure out how much more resources the tenant will need. The quota can be reset based on this analysis.


Details of deleted sites

URL	STATUS	DELETIONTIME	DAYSREMAINING	DELETEDSTORAGEQUOTA (IN TB)	DELETEDRESOURCEQUOTA (NUMB
Jul 31, 2018 17:51:52					
https://eginnovations435.sharepoint.com/sites/JPMorganChase-eGPo	Recycled	5/17/2018 2:43:01 PM	17	1	300

Figure 4.5: The detailed diagnosis of the Deleted sites measure

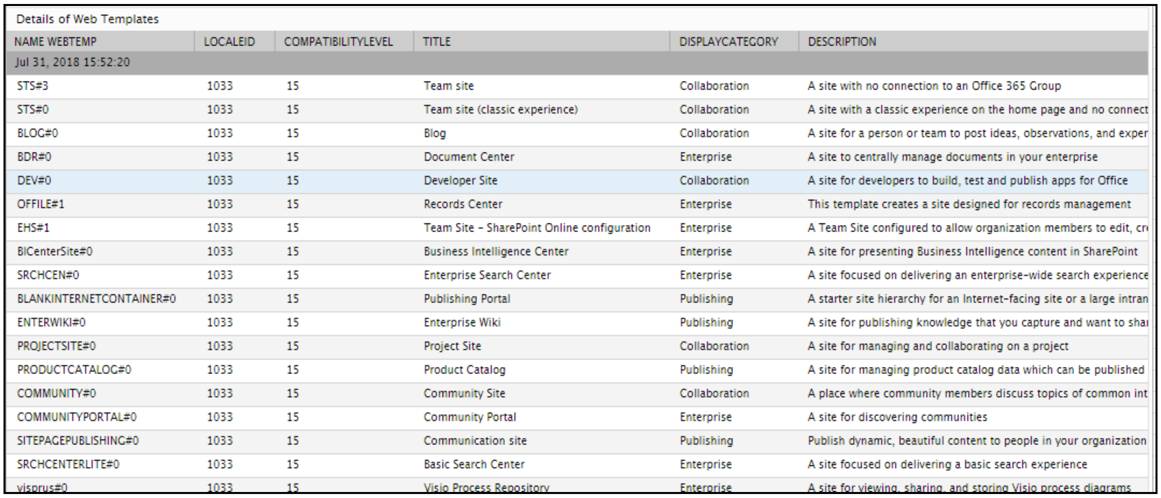
The detailed diagnosis of the *Applications* measure lists applications that are hosted on the monitored tenant.


Details of Application Information

NAME APPINFO	PRODUCTID	SOURCE
Jul 31, 2018 17:51:52		
Easy Quiz	89907d82-6703-4e3a-8947-7aad37bf4af3	MarketPlace
Happy Birthday	d883930f-0f16-4a6d-96a5-fc3fbd3a43a2	MarketPlace
Image Rotator	ce0c8b36-2963-4541-b999-38d71ff2136a	MarketPlace
Learning Spring	330bff94-ab88-4ecb-b6b1-6251459dc07e	MarketPlace
MCQ	6ad2c8d0-314f-4f0e-93e7-11bce7229c70	MarketPlace
Project Management	5eed7e79-b554-467b-bfff-06fd0722f578	MarketPlace
Recruiting Helper	4784e767-f317-4c4d-8cdc-ad81974e73aa	MarketPlace
Tasks in a Box for SharePoint Online	c45afc2d-b480-420f-adba-a487e8eed005	MarketPlace
Virto Image Slider App	c1822cb6-78ee-4e9b-9d89-851916fcd2cd	MarketPlace
Yammer App for SharePoint	565288aa-a9b0-4f19-8ce3-7fa13fccda5c	MarketPlace

Figure 4.6: The detailed diagnosis of the Applications measure

The detailed diagnosis of the *Web templates* measure provides complete details of the web templates in the monitored tenant. This includes the locale to which each template belongs, the compatibility level of the template, and also a brief description of the template.



Details of Web Templates

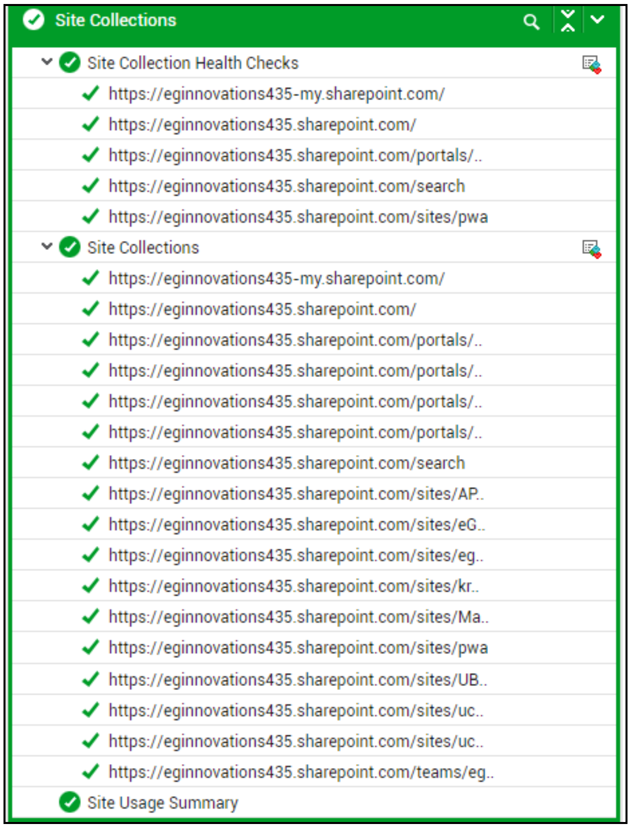
NAME WEBTEMP	LOCALEID	COMPATIBILITYLEVEL	TITLE	DISPLAYCATEGORY	DESCRIPTION
Jul 31, 2018 15:52:20					
STS#3	1033	15	Team site	Collaboration	A site with no connection to an Office 365 Group
STS#0	1033	15	Team site (classic experience)	Collaboration	A site with a classic experience on the home page and no connect
BLOG#0	1033	15	Blog	Collaboration	A site for a person or team to post ideas, observations, and exper
BDR#0	1033	15	Document Center	Enterprise	A site to centrally manage documents in your enterprise
DEV#0	1033	15	Developer Site	Collaboration	A site for developers to build, test and publish apps for Office
OFFILE#1	1033	15	Records Center	Enterprise	This template creates a site designed for records management
EHS#1	1033	15	Team Site - SharePoint Online configuration	Enterprise	A Team Site configured to allow organization members to edit, cr
BICenterSite#0	1033	15	Business Intelligence Center	Enterprise	A site for presenting Business Intelligence content in SharePoint
SRCHCEN#0	1033	15	Enterprise Search Center	Enterprise	A site focused on delivering an enterprise-wide search experience
BLANKINTERNETCONTAINER#0	1033	15	Publishing Portal	Publishing	A starter site hierarchy for an Internet-facing site or a large intran
ENTERWIKI#0	1033	15	Enterprise Wiki	Publishing	A site for publishing knowledge that you capture and want to sha
PROJECTSITE#0	1033	15	Project Site	Collaboration	A site for managing and collaborating on a project
PRODUCTCATALOG#0	1033	15	Product Catalog	Publishing	A site for managing product catalog data which can be published
COMMUNITY#0	1033	15	Community Site	Collaboration	A place where community members discuss topics of common int
COMMUNITYPORTAL#0	1033	15	Community Portal	Enterprise	A site for discovering communities
SITEPAGEPUBLISHING#0	1033	15	Communication site	Publishing	Publish dynamic, beautiful content to people in your organization
SRCHCENTERLITE#0	1033	15	Basic Search Center	Enterprise	A site focused on delivering a basic search experience
visprus#0	1033	15	Visio Process Repository	Enterprise	A site for viewing, sharing, and storing Visio process diagrams

Figure 4.7: The detailed diagnosis of the Web templates measure

4.3 The Site Collections Layer

The tests mapped to this layer monitor site collections and sites. With the help of the metrics these tests report, you can:

- Understand the composition of site collections;
- Identify site collections that are running out of server and/or storage resources;
- Pinpoint inactive collections;
- Isolate site collections on which health checks failed;
- Know which sites are unavailable and/or unresponsive;



Site Collections

- Site Collection Health Checks
  - https://eginnovations435-my.sharepoint.com/
  - https://eginnovations435.sharepoint.com/
  - https://eginnovations435.sharepoint.com/portals/..
  - https://eginnovations435.sharepoint.com/search
  - https://eginnovations435.sharepoint.com/sites/pwa
- Site Collections
  - https://eginnovations435-my.sharepoint.com/
  - https://eginnovations435.sharepoint.com/
  - https://eginnovations435.sharepoint.com/portals/..
  - https://eginnovations435.sharepoint.com/portals/..
  - https://eginnovations435.sharepoint.com/portals/..
  - https://eginnovations435.sharepoint.com/portals/..
  - https://eginnovations435.sharepoint.com/search
  - https://eginnovations435.sharepoint.com/sites/AP..
  - https://eginnovations435.sharepoint.com/sites/eG..
  - https://eginnovations435.sharepoint.com/sites/eg..
  - https://eginnovations435.sharepoint.com/sites/kr..
  - https://eginnovations435.sharepoint.com/sites/Ma..
  - https://eginnovations435.sharepoint.com/sites/pwa
  - https://eginnovations435.sharepoint.com/sites/UB..
  - https://eginnovations435.sharepoint.com/sites/uc..
  - https://eginnovations435.sharepoint.com/sites/uc..
  - https://eginnovations435.sharepoint.com/teams/eg..
- Site Usage Summary

Figure 4.8: The tests mapped to the Site Collections layer

4.3.1 Site Collections Test

SharePoint Site Collection, just as the name implies, is a collection of SharePoint Sites. Each site collection contains a single top-level site and subsites below it. Each site collection has its unique site columns (metadata), navigation, permissions (security groups), site templates, branding, etc.

Typically, server resources such as CPU and RAM are allocated to an Office 365 tenant as a whole based on the number of user licenses; these resources are then shared by all site collections in the tenant. This means that there is the danger of a single site collection exhausting the resources across the tenancy. To avoid this, organizations that have customized site collections or sandboxed solutions use resource quotas. By applying resource quotas to specific collections, administrators can ensure that custom code running in specific site collections does not deplete all server resources assigned to the tenancy.

Like CPU and RAM, storage resources are also allocated to a tenant based on the number of user licenses associated with that tenancy. This storage can then be allocated to the site collections in one of the following ways:

- Automatically, using pooled storage
- Manually, by explicitly configuring storage allocations on a per-site collection basis

The pooled storage model allows SharePoint Online to manage storage automatically rather than storage management being a task performed manually by an administrator. Site collections automatically draw the storage resources from the pool as and when they need it, upto a maximum of 25 TB per collection.

On the other hand, if you prefer to fine tune the storage space allocated to each site collection, you can set your storage management option to "manual" and specify individual site collection storage limits.

Regardless of what resource (whether CPU, memory, or storage) is managed and how it is managed (whether automatically or manually), the goal is to ensure that all site collections have the resources they need at their disposal at all times! A resource contention will not only impact the performance of sites in the collection, but also that of the web applications they support. This is why, it is imperative that administrators track the resource usage of each site collection closely, proactively detect resource contentions, accurately isolate the contentious resource and the site collection that is impacted, and promptly fine-tune the resource allocation, before performance suffers. This is exactly what the **Site Collections Test** does!

This test monitors the status, composition (count of subsites), resource allocations, and resource usage of each site collection, and promptly alerts administrators to inactive collections and those that are consuming resources excessively. This way, the test accurately pinpoints the site collections that may exhaust their resource quota/allocation soon, thereby prompting administrators to rapidly right-size the collections. Additionally, the test also reports whether/not a site collection is locked, with detailed diagnostics revealing the type of lock applied (read-only, no access, etc.). When users complain that they are unable to access their site collection or add content to it, this information will enable administrators to figure out why. The count of external users accessing each site collection and the details of these users are also provided, so that administrators can easily perform security audits on accesses to a site collection.

Target of the test : Microsoft SharePoint Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each site collection

First-level descriptor: Site collection URL

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 support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box.

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

Measurements made by the test

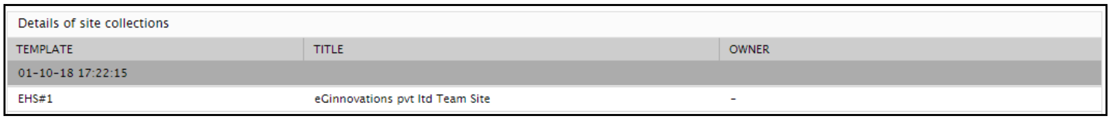
<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this site collection.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Active</td><td>1</td></tr><tr><td>Inactive</td><td>0</td></tr></table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s in the table above to indicate the status of a site collection. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Webs count</td><td>Indicates the number of sites in this site collection.</td><td>Number</td><td></td></tr>
<tr><td>Storage quota limit</td><td>Indicates the maximum storage space allocated to this site collection.</td><td>GB</td><td></td></tr>
<tr><td>Storage used</td><td>Indicates the percent usage of the storage resources allocated to this collection.</td><td>Percent</td><td>If the value of this measure is close to 100%, it implies that the site collection is about to exhaust the allocated storage resources. You may want to allocate more resources to such a collection, in this case, so that the performance of sites in that collection do not deteriorate.</td></tr>
<tr><td>Current resource usage</td><td>Indicates the number of server resources currently utilized by this site collection.</td><td>Number</td><td>If the value of this measure is close to the value of the <i>Resource quota limit</i> measure for a site collection, it implies that the site collection is consistently over-utilizing its resources and may run out of server resources very shortly. In such a case, you may want to consider fine-tuning</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>the Resource quota of that site collect</td></tr>
<tr><td>Average resource usage</td><td>Indicates the average number of server resources utilized by this site collection.</td><td>Number</td><td>If the value of this measure is close to the value of the *Resource quota limit* measure for a site collection, it could imply a sudden spike in resource usage of that collection.</td></tr>
<tr><td>Resource quota limit</td><td>Indicates the server resource quota set for this site collection.</td><td>Number</td><td>If the value of the *Current resource usage* measure is close to the value of this measure for a site collection, it could imply a sudden spike in resource usage.
On the other hand, if the value of the *Average resource usage* measure is close to the value of this measure, it implies that the site collection is consistently over-utilizing its resources and may run out of server resources very shortly. In such a case, you may want to consider fine-tuning the Resource quota of that site collection.</td></tr>
<tr><td>Resource quota warning level</td><td>Indicates at what usage level administrators should be warned of a resource contention on this site collection.</td><td></td><td>You can configure an email to be sent to the primary site collection administrator when the resource utilization reaches a specific percentage of the assigned quota.
If such a warning level is set, this measure will report a percentage value. This means that the primary site collection administrator can expect an email alert if the site collection consumes the configured percentage of its *Resource quota limit*.</td></tr>
<tr><td>Locked?</td><td>Indicates whether/not this site collection is locked.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:
<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></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s in the table above to indicate the lock status of a site collection. In the graph of this measure however, the same is indicated using the numeric equivalents only.
If the value of this measure is Yes, then you can use the detailed diagnosis of this measure to know the type of lock that has been applied on the site collection. The possible options are as follows:
<table>
<tr><th>Locking option</th><th>Description</th></tr>
<tr><td>Adding content prevented</td><td>Prevents users from adding new content to the site collection. Updates and deletions are still allowed.</td></tr>
<tr><td>Read-only</td><td>Prevents users from adding, updating, or deleting content. When a user attempts to add, update, or delete content, the user receives an error message that informs the user that access is denied and that the user does not have permission to</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><th>Locking option</th><th>Description</th></tr>
<tr><td></td><td>perform the action or access the resource. A read-only lock can be either site collection administrator controlled if the site collection is archived or farm administrator controlled.</td></tr>
<tr><td>No access</td><td>Prevents users from accessing the site collection and its content. Users who attempt to access the site receive an error page that informs the user that the website declined to show the webpage.</td></tr>
</table></td></tr>
<tr><td>Days since content was modified</td><td>Indicates the number of days that has elapsed since the content in this site collection was last modified.</td><td>Days</td><td></td></tr>
<tr><td>External users</td><td>Indicates the number of external users to this site collection.</td><td>Number</td><td>Use the detailed diagnosis of this measure to know who are the external users accessing the site collection.</td></tr>
</table>

The detailed diagnosis of the *Status* measure reveals the template, title, and owner of the site collection.

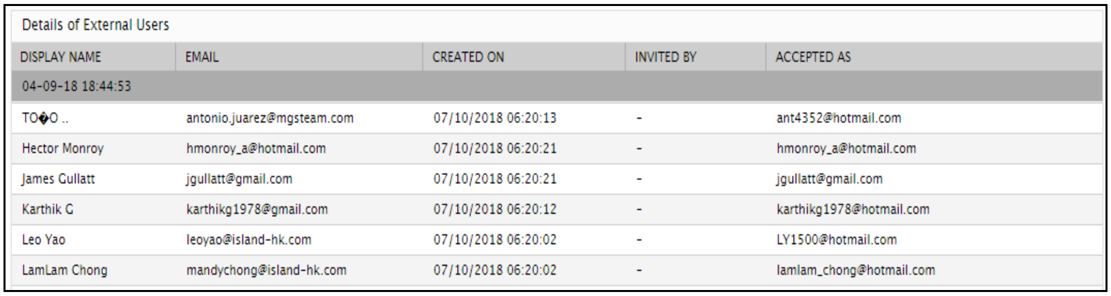


Details of site collections

TEMPLATE	TITLE	OWNER
01-10-18 17:22:15		
EHS#1	eCinnovations pvt ltd Team Site	-

Figure 4.9: The detailed diagnosis of the Status measure reported by the Site Collections test

The detailed diagnosis of the *External users* measure lists the name and email ID of every external user who accesses the site collection. The date on which each user was created, who invited that user to access the site collection, and the email ID using which the invitation was accepted by the external user are also provided as part of detailed diagnostics.



Details of External Users

DISPLAY NAME	EMAIL	CREATED ON	INVITED BY	ACCEPTED AS
04-09-18 18:44:53				
TO�O ..	antonio.juarez@mgsteam.com	07/10/2018 06:20:13	-	ant4352@hotmail.com
Hector Monroy	hmonroy_a@hotmail.com	07/10/2018 06:20:21	-	hmonroy_a@hotmail.com
James Gullatt	jgullatt@gmail.com	07/10/2018 06:20:21	-	jgullatt@gmail.com
Karthik G	karthikg1978@gmail.com	07/10/2018 06:20:12	-	karthikg1978@hotmail.com
Leo Yao	leoyao@island-hk.com	07/10/2018 06:20:02	-	LY1500@hotmail.com
LamLam Chong	mandychong@island-hk.com	07/10/2018 06:20:02	-	lamlam_chong@hotmail.com

Figure 4.10: The detailed diagnosis of the External users measure

4.3.2 Site Collection Health Checks Test

SharePoint Online includes a set of rules that you can run against a site collection to verify that it is working as expected. These rules are part of the site collection health checks.

You run the health checks manually to prepare for an upgrade. In addition, the health checks are run automatically in repair mode when you start to upgrade a site collection.

The site collection health checker includes the following rules:

Rule Name	Description
Conflicting Content Types	This rule checks for conflicts between existing content types and content types that are created when you upgrade the site. A conflict occurs when both content types have the same name.
Customized Files	This rule checks for any files that were customized (or unghosted) in the site collection or subsites. When run in repair mode, it can reset the page to the default (reghost the file).
Missing Galleries	This rule checks for all default galleries and reports if any are missing from the site collection or subsites.

Rule Name	Description
Missing Parent Content Types	This rule checks for missing parent content types. If a missing parent content type is found, you can either delete the orphaned content type or associate the orphaned content type with a different parent content type.
Missing Site Templates	This rule checks to make sure that the template the site is based on is available and reports if any elements are missing.
Unsupported Language Pack References	This rule checks to make sure that the language packs that are used by the site collection exist and are referenced correctly by the site collection.
Unsupported MUI References	This rule checks to make sure that the multi-user interface elements that are used by the site collection exist and are referenced correctly.

Whenever one/more of the aforesaid health checks are run - whether manually or automatically - an administrator needs to know which health checks were run, on which site collection they were run, which of these checks passed, and which ones failed. This way, administrators can identify the unhealthy site collections or collections that are not upgrade-ready. Additionally, the knowledge of rules that failed will enable administrators initiate measures to investigate the reasons for the failure and fix them, so that they can then confidently proceed to upgrade the site collections. This is what the **Site Collection Health Checks** test helps administrators achieve!

This test automatically discovers the site collections on which health checks are run, and reports the count of rules that passed, rules that failed with warnings, and rules that failed with errors. This will point administrators to unhealthy site collections or site collections that are not upgrade-ready. Using the detailed diagnostics provided by the test, administrators can accurately identify the precise rules that passed and failed, and can thus easily troubleshoot the failures.

Target of the test : Microsoft SharePoint Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each site collection

First-level descriptor: Site collection URL

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed

Parameters	Description
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 support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.

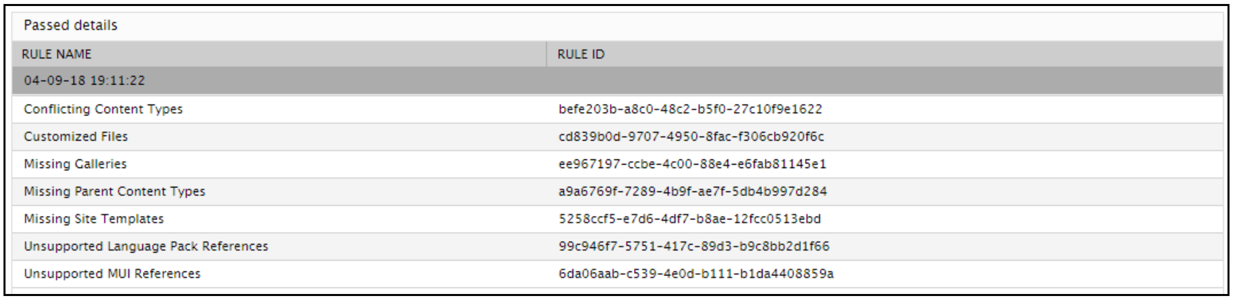
Parameters	Description
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent 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*.
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
Passed	Indicates the number of health checks run on this site collection that passed.	Number	Use the detailed diagnosis of this measure to know which rules passed.

Measurement	Description	Measurement Unit	Interpretation
Failed warnings	Indicates the number of health checks run on this site collection that failed with warnings.	Number	Use the detailed diagnosis of this measure to know which rules failed with warnings.
Failed errors	Indicates the number of health checks run on this site collection that failed due to errors.	Number	Use the detailed diagnosis of this measure to know which rules failed owing to errors.

The detailed diagnosis of the *Passed* measure reveals the names and IDs of the rules that passed

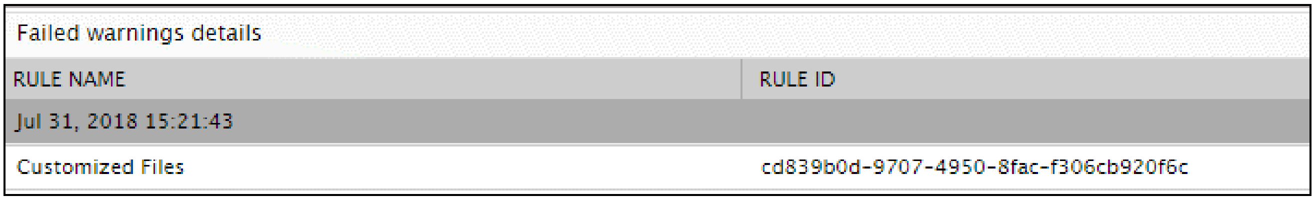


Passed details

RULE NAME	RULE ID
04-09-18 19:11:22	
Conflicting Content Types	befe203b-a8c0-48c2-b5f0-27c10f9e1622
Customized Files	cd839b0d-9707-4950-8fac-f306cb920f6c
Missing Galleries	ee967197-ccbe-4c00-88e4-e6fab81145e1
Missing Parent Content Types	a9a6769f-7289-4b9f-ae7f-5db4b997d284
Missing Site Templates	5258ccf5-e7d6-4df7-b8ae-12fcc0513ebd
Unsupported Language Pack References	99c946f7-5751-417c-89d3-b9c8bb2d1f66
Unsupported MUI References	6da06aab-c539-4e0d-b111-b1da4408859a

Figure 4.11: The detailed diagnosis of the Passed measure

The detailed diagnosis of the *Failed warnings* measure lists the names and IDs of rules that failed with warnings. The reason for the failure will have to be investigated.



Failed warnings details

RULE NAME	RULE ID
Jul 31, 2018 15:21:43	
Customized Files	cd839b0d-9707-4950-8fac-f306cb920f6c

Figure 4.12: The detailed diagnosis of the Failed warnings measure

4.3.3 Site Usage Summary Test

By default, each SharePoint Online site is allocated 1 TB of storage space for its use. Some sites however may be more actively used or may contain more files than the rest; such sites may hence utilize more storage. To identify such sites, use the Site Usage Summary test.

This test monitors the workload of sites in terms of page views, visits, and file activity, and reports how this demand impacts storage usage across sites. Detailed diagnostics reveals those sites with a high level of activity. Additionally, the test also looks for sites that are using more than a configured percentage of storage space allocated to them, and reports the count of such sites (if any). Detailed metrics will point you to the exact sites that are using up storage resources excessively. With the help of the detailed metrics, you can correlate the load on the individual sites with their storage allocation and usage. In the process, you can figure out if any site requires additional storage space to handle its current demand.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
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*.

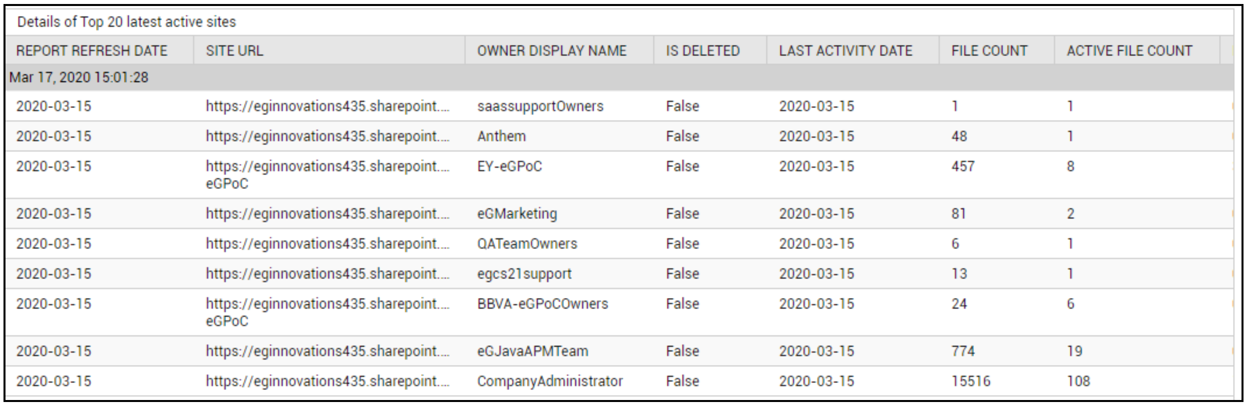
Parameters	Description
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent 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*.
Storage Percentage Limit	This test reports the count of sites consuming more storage than the rest. If the percentage of storage space utilized by a site is higher than the percentage specified here, then such a site will be counted as a site consuming more storage.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *2:1*. This indicates that, by default, detailed measures will be generated at the end of every second test execution cycle during normal operations, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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 sites	Indicates the total number of sites for this tenant on SharePoint Online.	Number	
Active sites	Indicates the number of active sites.	Number	An active site is a SharePoint Online site that has seen some activity in terms of page views, page visits, or any file activity (eg., creation, modification, deletion). To view the sites that were active recently, use the detailed diagnosis of this measure.
Total files	Indicates the total number of files across site collections.	Number	Use the detailed diagnosis of this measure to know which sites have the maximum number of files.
Active files	Indicates the number of active files.	Number	Use the detailed diagnosis of this measure to know which sites have the maximum number of active files - i.e., files that have been accessed recently.
Active files	Indicates what percentage of total files is active.	Percent	A high value of this measure indicates that the tenant is accessing or working with SharePoint files very frequently.
Page views	Indicates the number of times pages on sites were viewed.	Number	To know which sites have the maximum number of page views, use the detailed diagnosis of this measure.
Visited pages	Indicates the number of web pages visited across SharePoint Online sites.	Number	To know which sites have the maximum number of page visits, use the detailed diagnosis of this measure.
Sites consuming more storage	Indicates the number of sites that are consuming the allocated storage resources excessively.	Number	The value of this measure will be incremented by 1 if the percent storage usage of any site is more than the percentage configured against the **STORAGE PERCENTAGE LIMIT** parameter.

Measurement	Description	Measurement Unit	Interpretation
			Ideally, the value of this measure should be 0. A non-zero value indicates that one/more web sites are over-utilizing the storage space allocated to them. To know which sites they are, use the detailed diagnosis of this measure.
Storage used across sites	Indicates the amount of storage currently used across sites.	GB	
Storage allocated across sites	Indicates the total amount of storage space allocated across sites.	GB	
Storage used	Indicates the percentage of allocated storage that is currently in use across sites.	Percent	A value close to 100% indicates a probable storage space crunch, owing to excessive space usage by one/more sites. In such a situation, use the detailed diagnosis of the *Sites consuming more storage* measure to know which sites are hogging storage resources.

The detailed diagnosis of the *Active sites* measure reports the top-20 sites that have seen activity recently. The URL of the sites, who owns each site, the date of last activity, and the level of activity on each site - i.e., the count of active files and the count of page views and page visits to every site - are reported as part of thedetailed metrics.

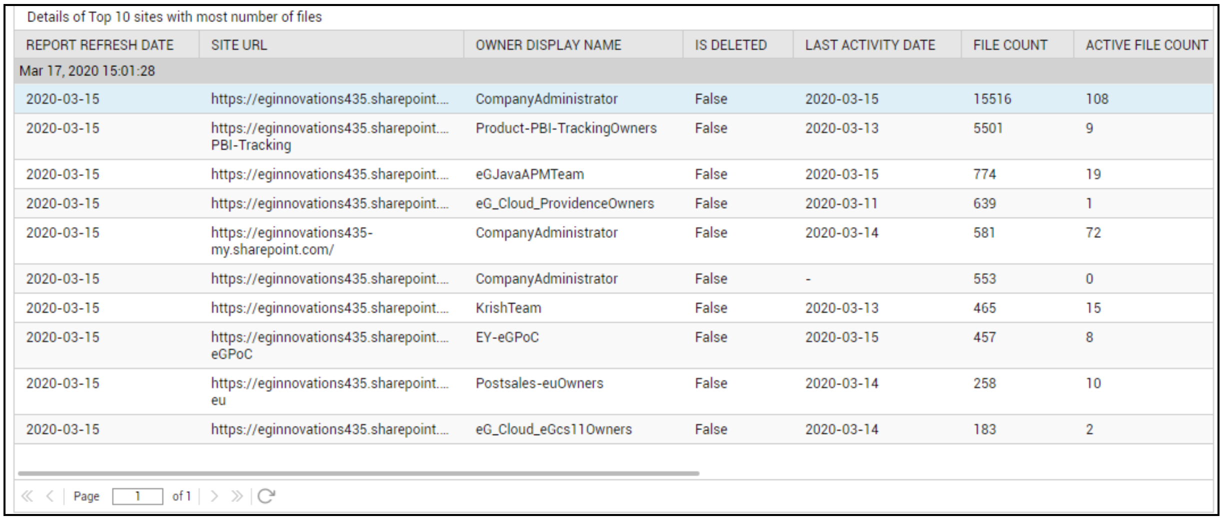


Details of Top 20 latest active sites

REPORT REFRESH DATE	SITE URL	OWNER DISPLAY NAME	IS DELETED	LAST ACTIVITY DATE	FILE COUNT	ACTIVE FILE COUNT
Mar 17, 2020 15:01:28						
2020-03-15	https://eginnovations435.sharepoint....	saassupportOwners	False	2020-03-15	1	1
2020-03-15	https://eginnovations435.sharepoint....	Anthem	False	2020-03-15	48	1
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	EY-eGPoC	False	2020-03-15	457	8
2020-03-15	https://eginnovations435.sharepoint....	eGMarketing	False	2020-03-15	81	2
2020-03-15	https://eginnovations435.sharepoint....	QATeamOwners	False	2020-03-15	6	1
2020-03-15	https://eginnovations435.sharepoint....	egcs21support	False	2020-03-15	13	1
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	BBVA-eGPoCOwners	False	2020-03-15	24	6
2020-03-15	https://eginnovations435.sharepoint....	eGJavaAPMTeam	False	2020-03-15	774	19
2020-03-15	https://eginnovations435.sharepoint....	CompanyAdministrator	False	2020-03-15	15516	108

Figure 4.13: The detailed diagnosis of the Active sites measure

Use the detailed diagnosis of the *Total files* measure to know which sites have the maximum number of files. In the event of a storage space crunch on SharePoint Online, knowing which sites have a large number of files will point you to the sites that are probably consuming a large amount of storage space.

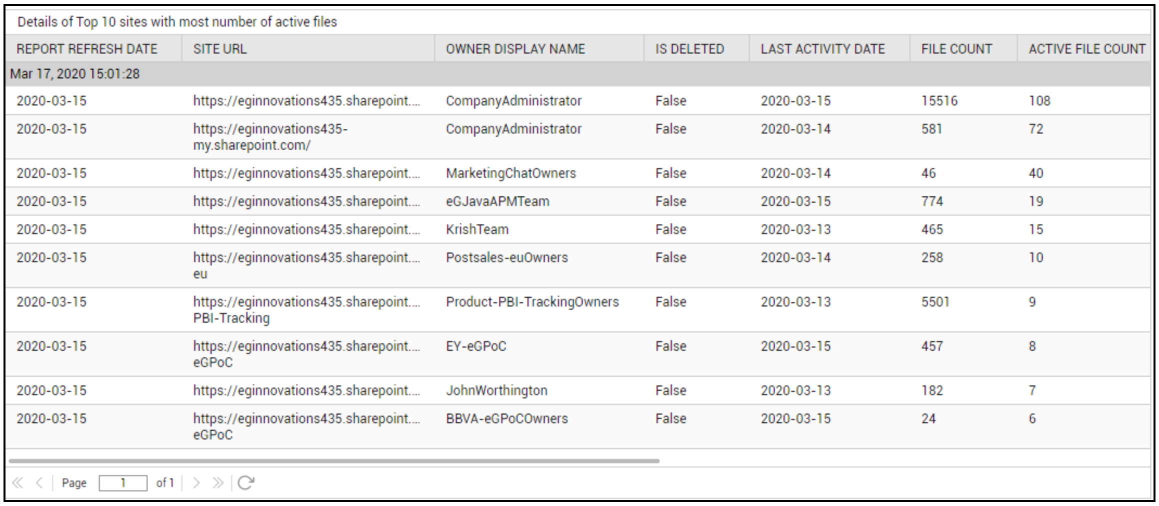


Details of Top 10 sites with most number of files

REPORT REFRESH DATE	SITE URL	OWNER DISPLAY NAME	IS DELETED	LAST ACTIVITY DATE	FILE COUNT	ACTIVE FILE COUNT
Mar 17, 2020 15:01:28						
2020-03-15	https://eginnovations435.sharepoint....	CompanyAdministrator	False	2020-03-15	15516	108
2020-03-15	https://eginnovations435.sharepoint.... PBI-Tracking	Product-PBI-TrackingOwners	False	2020-03-13	5501	9
2020-03-15	https://eginnovations435.sharepoint....	eGJavaAPMTeam	False	2020-03-15	774	19
2020-03-15	https://eginnovations435.sharepoint....	eG_Cloud_ProvidenceOwners	False	2020-03-11	639	1
2020-03-15	https://eginnovations435- my.sharepoint.com/	CompanyAdministrator	False	2020-03-14	581	72
2020-03-15	https://eginnovations435.sharepoint....	CompanyAdministrator	False	-	553	0
2020-03-15	https://eginnovations435.sharepoint....	KrishTeam	False	2020-03-13	465	15
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	EY-eGPoC	False	2020-03-15	457	8
2020-03-15	https://eginnovations435.sharepoint.... eu	Postsales-euOwners	False	2020-03-14	258	10
2020-03-15	https://eginnovations435.sharepoint....	eG_Cloud_eGcs11Owners	False	2020-03-14	183	2

Figure 4.14: The detailed diagnosis of the Total files measure

Use the detailed diagnosis of the *Active files* measure to view the top-10 sites with the most number of active files - i.e., files that have been accessed recently.

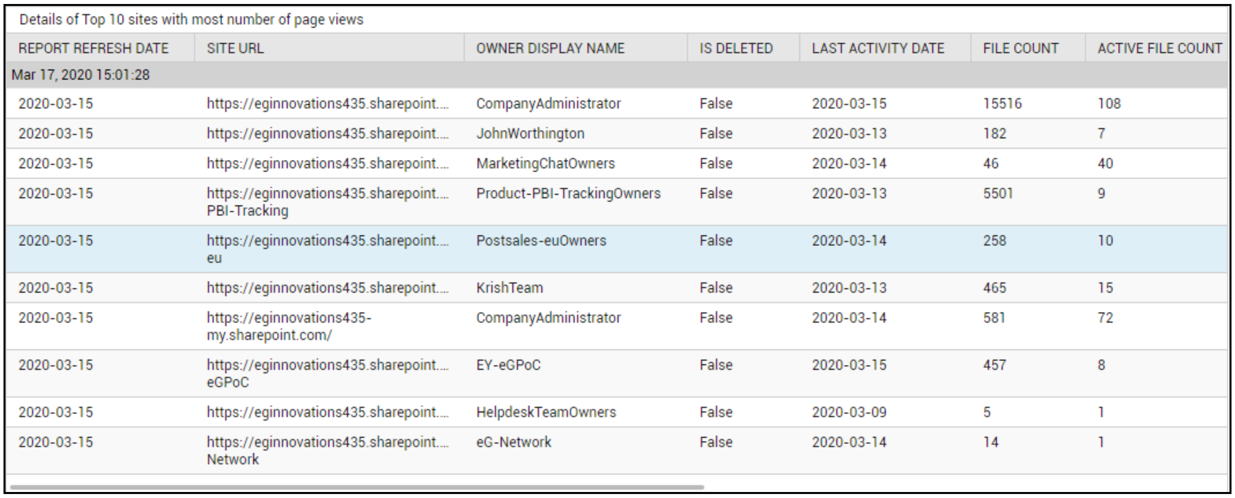


Details of Top 10 sites with most number of active files

REPORT REFRESH DATE	SITE URL	OWNER DISPLAY NAME	IS DELETED	LAST ACTIVITY DATE	FILE COUNT	ACTIVE FILE COUNT
Mar 17, 2020 15:01:28						
2020-03-15	https://eginnovations435.sharepoint....	CompanyAdministrator	False	2020-03-15	15516	108
2020-03-15	https://eginnovations435- my.sharepoint.com/	CompanyAdministrator	False	2020-03-14	581	72
2020-03-15	https://eginnovations435.sharepoint....	MarketingChatOwners	False	2020-03-14	46	40
2020-03-15	https://eginnovations435.sharepoint....	eGJavaAPMTeam	False	2020-03-15	774	19
2020-03-15	https://eginnovations435.sharepoint....	KrishTeam	False	2020-03-13	465	15
2020-03-15	https://eginnovations435.sharepoint.... eu	Postsales-euOwners	False	2020-03-14	258	10
2020-03-15	https://eginnovations435.sharepoint.... PBI-Tracking	Product-PBI-TrackingOwners	False	2020-03-13	5501	9
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	EY-eGPoC	False	2020-03-15	457	8
2020-03-15	https://eginnovations435.sharepoint....	JohnWorthington	False	2020-03-13	182	7
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	BBVA-eGPoCOwners	False	2020-03-15	24	6

Figure 4.15: The detailed diagnosis of the Active files measure

To know which sites have the maximum number of page views, use the detailed diagnosis of the *Page views* measure.

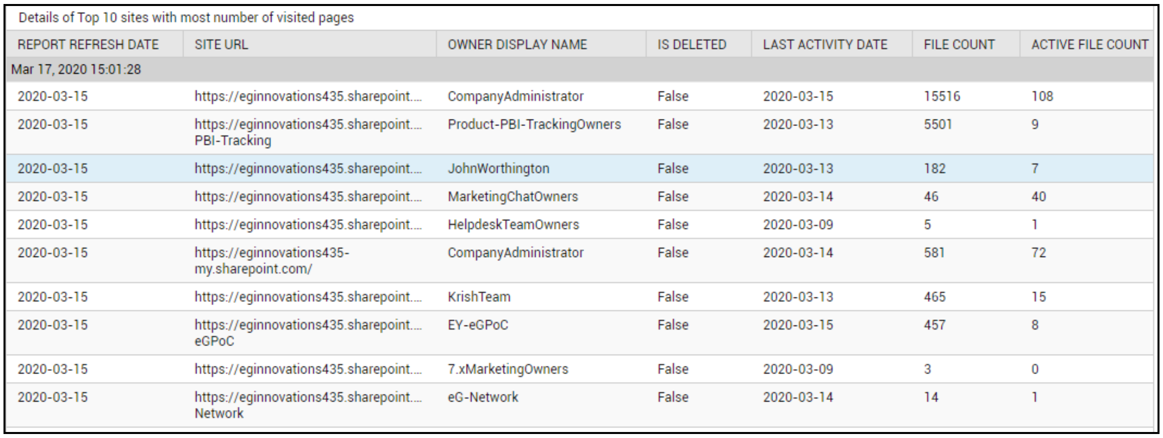


Details of Top 10 sites with most number of page views

REPORT REFRESH DATE	SITE URL	OWNER DISPLAY NAME	IS DELETED	LAST ACTIVITY DATE	FILE COUNT	ACTIVE FILE COUNT
Mar 17, 2020 15:01:28						
2020-03-15	https://eginnovations435.sharepoint....	CompanyAdministrator	False	2020-03-15	15516	108
2020-03-15	https://eginnovations435.sharepoint....	JohnWorthington	False	2020-03-13	182	7
2020-03-15	https://eginnovations435.sharepoint....	MarketingChatOwners	False	2020-03-14	46	40
2020-03-15	https://eginnovations435.sharepoint.... PBI-Tracking	Product-PBI-TrackingOwners	False	2020-03-13	5501	9
2020-03-15	https://eginnovations435.sharepoint.... eu	Postsales-euOwners	False	2020-03-14	258	10
2020-03-15	https://eginnovations435.sharepoint....	KrishTeam	False	2020-03-13	465	15
2020-03-15	https://eginnovations435-my.sharepoint.com/	CompanyAdministrator	False	2020-03-14	581	72
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	EY-eGPoC	False	2020-03-15	457	8
2020-03-15	https://eginnovations435.sharepoint....	HelpdeskTeamOwners	False	2020-03-09	5	1
2020-03-15	https://eginnovations435.sharepoint.... Network	eG-Network	False	2020-03-14	14	1

Figure 4.16: The detailed diagnosis of the Page views measure

To know which sites have the maximum number of page visits, use the detailed diagnosis of the *Visited pages* measure.

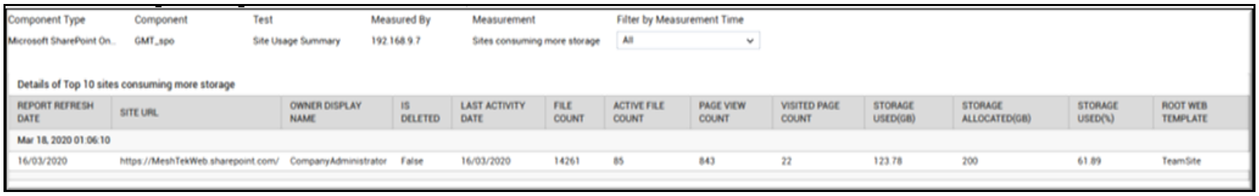


Details of Top 10 sites with most number of visited pages

REPORT REFRESH DATE	SITE URL	OWNER DISPLAY NAME	IS DELETED	LAST ACTIVITY DATE	FILE COUNT	ACTIVE FILE COUNT
Mar 17, 2020 15:01:28						
2020-03-15	https://eginnovations435.sharepoint....	CompanyAdministrator	False	2020-03-15	15516	108
2020-03-15	https://eginnovations435.sharepoint.... PBI-Tracking	Product-PBI-TrackingOwners	False	2020-03-13	5501	9
2020-03-15	https://eginnovations435.sharepoint....	JohnWorthington	False	2020-03-13	182	7
2020-03-15	https://eginnovations435.sharepoint....	MarketingChatOwners	False	2020-03-14	46	40
2020-03-15	https://eginnovations435.sharepoint....	HelpdeskTeamOwners	False	2020-03-09	5	1
2020-03-15	https://eginnovations435-my.sharepoint.com/	CompanyAdministrator	False	2020-03-14	581	72
2020-03-15	https://eginnovations435.sharepoint....	KrishTeam	False	2020-03-13	465	15
2020-03-15	https://eginnovations435.sharepoint.... eGPoC	EY-eGPoC	False	2020-03-15	457	8
2020-03-15	https://eginnovations435.sharepoint....	7.xMarketingOwners	False	2020-03-09	3	0
2020-03-15	https://eginnovations435.sharepoint.... Network	eG-Network	False	2020-03-14	14	1

Figure 4.17: The detailed diagnosis of the Visited pages measure

To know which sites are consuming more storage, use the detailed diagnosis of the S*ites consuming more storage* measure. In the event of a storage crunch, these detailed metrics will point you to the exact sites that are responsible for the contention.



Component Type	Component	Test	Measured By	Measurement	Filter by Measurement Time
Microsoft SharePoint On...	GMT_spo	Site Usage Summary	192.168.9.7	Sites consuming more storage	All

Details of Top 10 sites consuming more storage

REPORT REFRESH DATE	SITE URL	OWNER DISPLAY NAME	IS DELETED	LAST ACTIVITY DATE	FILE COUNT	ACTIVE FILE COUNT	PAGE VIEW COUNT	VISITED PAGE COUNT	STORAGE USED(GB)	STORAGE ALLOCATED(GB)	STORAGE USED(%)	ROOT WEB TEMPLATE
Mar 18, 2020 01:06:10												
16/03/2020	https://MeshTekWeb.sharepoint.com/	CompanyAdministrator	False	16/03/2020	14261	85	843	22	123.78	200	61.89	TeamSite

Figure 4.18: The detailed diagnosis of the Sites consuming more storage measure

4.4 The Users Layer

Use the test mapped to this layer to know the count of active and inactive users.

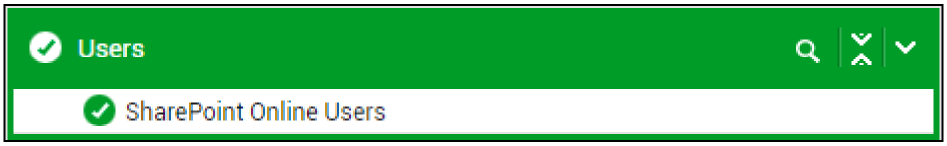


Figure 4.19: The test mapped to the Users layer

4.4.1 SharePoint Online Users Test

It is important to audit the usage of SharePoint Online periodically. Such audits reveal if there are any inactive users on SharePoint Online. Inactive users are those who have not interacted with any file on SharePoint Online by way of creating, modifying, deleting, viewing, sharing, or synchronizing it (to clients) for a considerably long period of time. Administrators can then identify the inactive users, understand the reason for inactivity, and decide whether/not their corresponding user accounts on SharePoint Online need to be removed.

To run these useful usage audits at configured intervals, administrators can use the SharePoint Online Users test. This test reports the count of active and inactive SharePoint Online users, and alerts administrators if there is even one inactive user.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against

Parameters	Description
	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*.

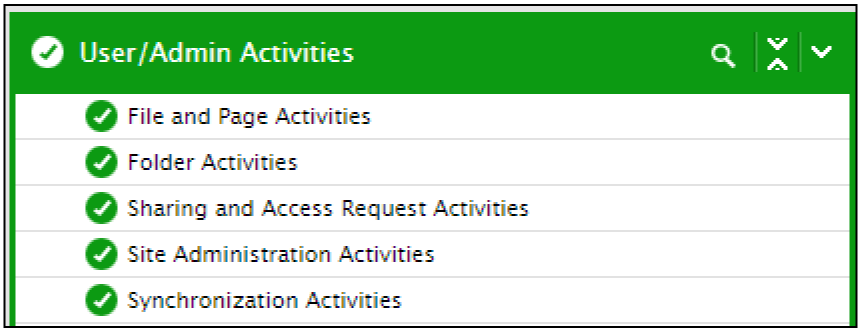
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active users	Indicates the number of active SharePoint Online	Number	

Measurement	Description	Measurement Unit	Interpretation
	users.		
Inactive users	Indicates the number of inactive SharePoint Online users.	Number	

4.5 The User/Admin Activities Layer

The tests mapped to this layer help audit file and page activities, folder activities, sharing and access request activities, site administration activities, synchronization activities, and user activities on SharePoint Online.



User/Admin Activities

- ✓ File and Page Activities
- ✓ Folder Activities
- ✓ Sharing and Access Request Activities
- ✓ Site Administration Activities
- ✓ Synchronization Activities

Figure 4.20: The tests mapped to the User/Admin Activities layer

4.5.1 File and Page Activities Test

Users perform many operations on the files stored in document libraries. Users can access files, view their contents, modify them, rename them, and even delete them. Likewise, users can view SharePoint pages in a site. To be able to efficiently audit the operations that are performed on files and pages, administrators should track each operation closely, determine whether it is a file operation or page operation, accurately identify what operation it is (file access, page view, file modifications, etc.), and also pinpoint which user performed that operation. This is exactly what the File and Page Activities test helps administrators do!

This test tracks the file and page operations that users perform on SharePoint Online and reports the total count of operations of each type. The type of operations that is most commonly performed on SharePoint Online is thus revealed to administrators. Additionally, the count of unique users who performed the various file/page operations is reported, with detailed diagnostics pointing administrators to the precise users and the operations they performed. This helps administrators identify users who may have performed an unauthorized operation. The unique clients from which the users initiated the file/page operations, the unique sites where the files are stored, and the unique pages viewed are provided as part of detailed diagnostics, so as to enable administrators audit the operations efficiently.

Target of the test : Microsoft SharePoint 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**Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
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.

Parameters	Description
	If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify none against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.
Report System Account Log Entries	By default, this flag is set to **No**. This means that, by default, the test ignores all operations performed by Windows System Accounts. A System Account in Windows is used by the operating system and by services that run under Windows. There are many services and processes within Windows that need the capability to log on internally (for example during a Windows installation). The system account was designed for that purpose; it is an internal account, does not show up in User Manager, cannot be added to any groups, and cannot have user rights assigned to it. On the other hand, the system account does show up on an NTFS volume in File Manager in the Permissions portion of the Security menu. By default, the system account is granted full control to all files on an NTFS volume. Here the system account has the same functional privileges as the administrator account.. If you want the test to monitor and report on operations performed by Windows System Accounts as well, set this flag to **Yes**. **Note:** By default, this test does not monitor the operations of the *NT AUTHORITY\SYSTEM and SHAREPOINT\system* accounts. This is governed by the **System_Account_Names** parameter in the **[SPO_Audited_Activities]** section of the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). If required, you can exclude more Windows system accounts from monitoring. For that, do the following: 1. Edit the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). 2. Look for the **System_ Account_ Names** parameter in the **[SPO_ Audited_Activities]** section of the file. You will find that this parameter is by default set as follows: *System_ Account_ Names=NT AUTHORITY\SYSTEM,SHAREPOINT\system* 3. To exclude more Windows system accounts from monitoring, you need to modify

Parameters	Description
	the **System_Account_Names** parameter by appending more system accounts to the comma-separated list. 4. Finally, save the file.
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 • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

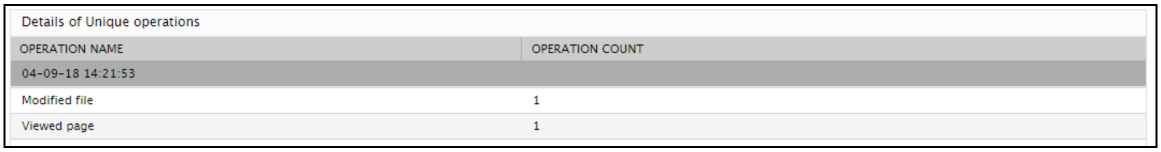
Measurement	Description	Measurement Unit	Interpretation
Total operations	Indicates the total number of file and page operations that were performed by users of SharePoint Online.	Number	The value of this measure is the sum of the values of all measures reported under the section *File/Page Operations*, in the Layers tab page of the eG monitoring console
Unique operations	Indicates the count of unique file/page operations performed on SharePoint Online.	Number	To know which operations were performed, use the detailed diagnosis of this measure.
Unique users	Indicates the count of unique users who	Number	To know which are the users who performed a file/page operation, use

Measurement	Description	Measurement Unit	Interpretation
	performed file/page operations on SharePoint Online.		the detailed diagnosis of this measure.
Unique client IPs	Indicates the number of unique clients from which the users initiated the file/page operations.	Number	Use the detailed diagnosis of this measure to determine the IP addresses of the clients from which users performed a file/page operation.
Unique sites	Indicates the number of unique sites where the files/pages accessed, reside.	Number	Use the detailed diagnosis of the SharePoint Online sites that were accessed for performing a file/page operation.
Affected item types	Indicates the number of types (file and/or page) of items that were affected by user operations.	Number	To know what type of items were affected by the user operations, use the detailed diagnosis of this measure.
Unique destinations	Indicates the destination URLs of the file/page operations .	Number	To know the unique destination URLs, use the detailed diagnosis of this measure.
Unique user agents	Indicates the unique user agents of browsers used for performing file/page operations.	Number	To know the unique user-agent strings of the browsers used in file/page operations, use the detailed diagnosis of thi measure.
File accesses	Indicates the number of file access operations that were performed.	Number	If you want to make changes to a file on a site and you want to make sure no one else can edit it, check out the file. When you have the file checked out, you can edit it online or offline, and save it—multiple times, if necessary. When you finish editing a file, you need to check the file back into the library, so that other people can see your changes and edit the file, if they have permission. If you decide not to make or keep any changes in the file, you can simply discard your checkout so you do not

Measurement	Description	Measurement Unit	Interpretation
			affect version history.
File check-ins	Indicates the number of times files were checked in.	Number	
File checkouts	Indicates the number of file checkout operations performed.	Number	
File checkout discards	Indicates the number of file checkout discards performed.	Number	
File copies	Indicates the number of times files were copied.	Number	
File deletes	Indicates the number of times file delete operations were performed.	Number	
File deletes from I stage recycle bin	Indicates the number of file deletes performed from the first-stage recycle bin.	Number	The Recycle Bin in SharePoint Online in Office 365 for business provides a safety net when an site content and site collections are deleted. When you delete content from a SharePoint site, it's sent to the site's Recycle Bin or first-stage Recycle Bin, where you can restore the deleted content if needed. If the file is deleted from the site Recycle Bin (i.e., from the first-stage Recycle Bin), it is sent to the Site Collection or Second-Stage Recycle Bin, where a site collection administrator can restore it or delete it permanently.
File deletes from II stage recycle bin	Indicates the number of files deleted from the second-stage recycle bin.	Number	
File downloads	Indicates the number of times users have downloaded files from SharePoint Online.	Number	
File modifications	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
	times files on SharePoint Online have been modified.		
File moves	Indicates the number of times files have been moved.	Number	Files on SharePoint Online can be moved to a different destination in the current library, to OneDrive, or to another SharePoint site.
File renames	Indicates the number of times files have been renamed.	Number	
File restores	Indicates the number of times files have been restored from the Recycle Bin to their original location.	Number	
File uploads	Indicates the number of file uploads to SharePoint Online.	Number	
Page views	Indicates the number of times SharePoint pages have been accessed.	Number	

The detailed diagnosis of the *Unique operations* measure lists the unique file/page operations that were performed, and the number of times each operation was performed. This way, administrators can quickly identify which operation was most common.

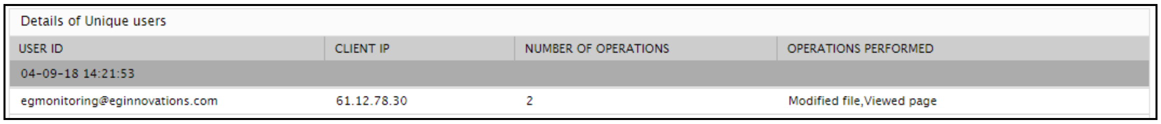


Details of Unique operations

OPERATION NAME	OPERATION COUNT
04-09-18 14:21:53	
Modified file	1
Viewed page	1

Figure 4.21: The detailed diagnosis of the Unique operations measure

The detailed diagnosis of the *Unique users* measure lists the users who performed file/page operations on SharePoint Online. For each user, the operations performed by that user, the number of times the operations were performed, and the client from which that user initiated the operations are revealed. This way, administrators can quickly figure out if any user has performed any unauthorized operation.

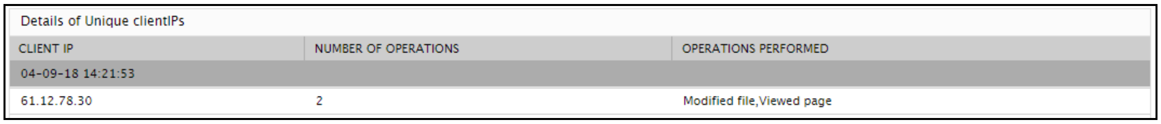


Details of Unique users

USER ID	CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:21:53			
egmonitoring@eginnovations.com	61.12.78.30	2	Modified file,Viewed page

Figure 4.22: The detailed diagnosis of the Unique users measure

The detailed diagnosis of the *Unique client IPs* measure reveals which user operations were performed from which clients. The number of times the operations were performed from each client is also reported.

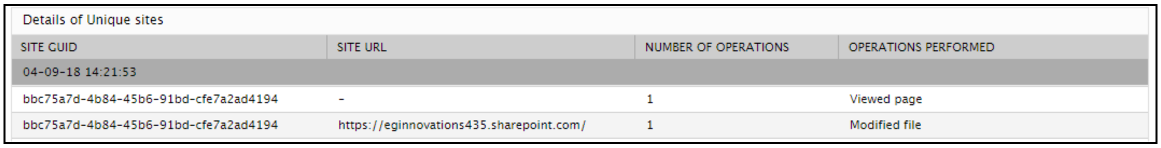


Details of Unique clientIPs

CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:21:53		
61.12.78.30	2	Modified file,Viewed page

Figure 4.23: The detailed diagnosis of the Unique client IPs measure

The detailed diagnosis of the *Unique sites* measure reveals the GUID and URL of each of the SharePoint sites on which file/page operations were performed. The type of operation that was performed and the number of times these operations were performed is also reported, so that administrators can accurately identify the site that experienced a high level of activity.

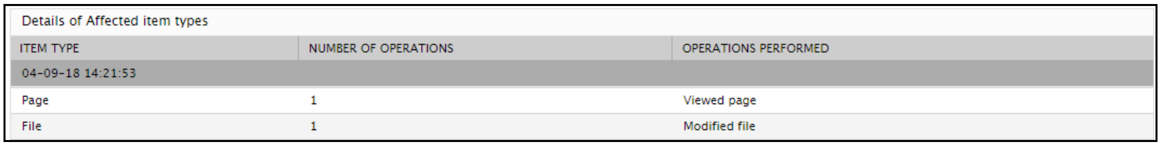


Details of Unique sites

SITE GUID	SITE URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:21:53			
bbc75a7d-4b84-45b6-91bd-cfe7a2ad4194	-	1	Viewed page
bbc75a7d-4b84-45b6-91bd-cfe7a2ad4194	https://eginnovations435.sharepoint.com/	1	Modified file

Figure 4.24: The detailed diagnosis of the Unique sites measure

To know which type of items - i.e., whether files or pages - was the target of the maximum number of operations, use the detailed diagnosis of the *Affected item types* measure. For each item type, the detailed metrics reveal the type of operations performed on that type and the number of times the operations were performed.

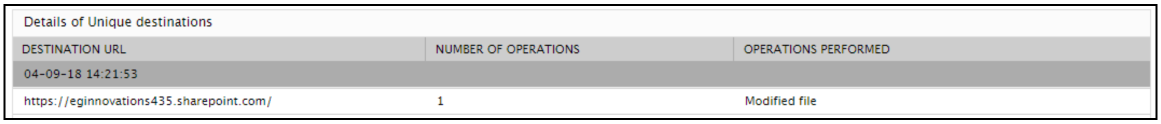


Details of Affected item types

ITEM TYPE	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:21:53		
Page	1	Viewed page
File	1	Modified file

Figure 4.25: The detailed diagnosis of the Affected item types measure

The detailed diagnosis of the *Unique destinations* measure lists the destination URLs of the file/page operations. For each URL, the operations that resulted in the URL and the number of times the operations were performed are reported.

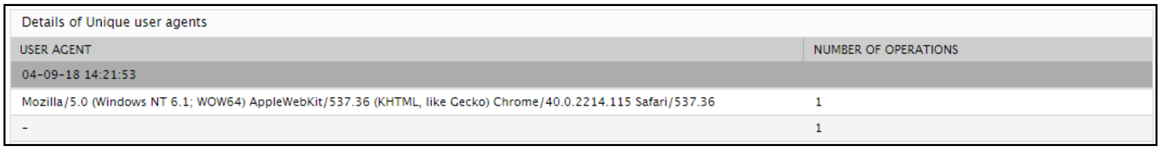


Details of Unique destinations

DESTINATION URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:21:53		
https://eginnovations435.sharepoint.com/	1	Modified file

Figure 4.26: The detailed diagnosis of the Unique destinations measure

The detailed diagnosis of the *Unique user agents* measure lists the user-agent strings of browsers used by users for performing the different file/page operations. For each user-agent string, the detailed metrics further reveals the number of operations performed using that browser. This will help administrators to identify the browser that was used most often to perform file/page operations.



Details of Unique user agents

USER AGENT	NUMBER OF OPERATIONS
04-09-18 14:21:53	
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36	1
-	1

Figure 4.27: The detailed diagnosis of the Unique user agents measure

4.5.2 Folder Activities Test

Folders provide administrators with an efficient way to group and manage content in a SharePoint Online document library - for eg., using folders you can group reports by fiscal year or department.

By auditing operations performed on folders, administrators can quickly capture folder operations that are unauthorized/suspect, and even identify the users who may have performed them. Monitoring folder operations is also essential for assessing the workload of SharePoint Online and the type of operations that are contributing to the load. Using the **Folder Activities** test, administrators can efficiently audit and analyze the workload generated by folder operations.

This test tracks the folder operations that users perform on SharePoint Online and reports the total count of operations of each type. The load imposed by folder operations and the type of operations contributing to this load can thus be determined. Additionally, the count of unique users who performed the various folder operations is reported, with detailed diagnostics pointing administrators to the precise users and the operations they performed. This helps administrators identify users who may have performed an unauthorized operation. The unique clients from which the users initiated the folder operations and the unique sites where the folders are stored are provided as part of detailed diagnostics, so as to enable administrators audit the operations efficiently.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
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*.
Report System Account Log Entries	By default, this flag is set to **No**. This means that, by default, the test ignores all operations performed by Windows System Accounts. A System Account in Windows is used by the operating system and by services that run under Windows. There are many services and processes within Windows that need the capability to log on internally (for example during a Windows installation). The system account was designed for that purpose; it is an internal account, does not show up in User Manager, cannot be added to any groups, and cannot have user rights assigned to it. On the other hand, the system account does show up on an NTFS volume in File Manager in the Permissions portion of the Security menu. By default, the system account is granted full control to all files on an NTFS volume. Here the system account has the same functional privileges as the administrator account.. If you want the test to monitor and report on operations performed by Windows System Accounts as well, set this flag to **Yes**. **Note:** By default, this test does not monitor the operations of the *NT AUTHORITY\SYSTEM and SHAREPOINT\system* accounts. This is governed by the **System_Account_Names** parameter in the **[SPO_Audited_Activities]** section of the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). If required, you can exclude more Windows system accounts from monitoring. For that, do the following: 1. Edit the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). 2. Look for the **System_ Account_ Names** parameter in the **[SPO_ Audited_Activities]** section of the file. You will find that this parameter is by default set as follows: *System_ Account_ Names=NT AUTHORITY\SYSTEM,SHAREPOINT\system* 3. To exclude more Windows system accounts from monitoring, you need to modify the **System_Account_Names** parameter by appending more system accounts to the comma-separated list. 4. Finally, save the file.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for

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

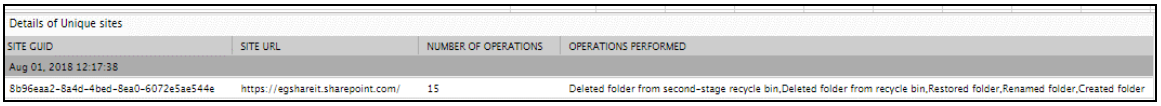
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total operations	Indicates the total number of folder operations that were performed by users of SharePoint Online.	Number	The value of this measure is the sum of the values of all measures reported under the section *Folder Operations*, in the Layers tab page of the eG monitoring console The value of this measure is a good indicator of the workload imposed by folder operations on SharePoint Online.
Unique operations	Indicates the count of unique folder operations performed on SharePoint Online.	Number	To know which operations were performed, use the detailed diagnosis of this measure.
Unique users	Indicates the count of unique users who performed folder operations on SharePoint	Number	To know which are the users who performed folder operations, use the detailed diagnosis of this measure.

Measurement	Description	Measurement Unit	Interpretation
	Online.		
Unique client IPs	Indicates the number of unique clients from which the users initiated the folder operations.	Number	Use the detailed diagnosis of this measure to determine the IP addresses of the clients from which users performed a folder operation.
Unique sites	Indicates the number of unique sites where the folders accessed, reside.	Number	Use the detailed diagnosis of the SharePoint Online sites that were accessed for performing a folder operation.
Affected item types	Indicates the number of types of items that were affected by the folder operations.	Number	To know what type of items were affected by the folder operations, use the detailed diagnosis of this measure.
Unique destinations	Indicates the destination URLs of the folder operations that were performed.	Number	To know the unique destination URLs, use the detailed diagnosis of this measure.
Unique user agents	Indicates the unique user agents of browsers used for performing folder operations.	Number	To know the unique user-agent strings of the browsers used in folder operations, use the detailed diagnosis of thi measure.
Folder copies	Indicates the number of times folders were copied.	Number	
Folder creations	Indicates the number of folders created.	Number	
Folder deletions	Indicates the number of times folder delete operations were performed.	Number	
Folder deletions from I stage recycle bin	Indicates the number of folder deletions performed from the first-stage recycle bin.	Number	The Recycle Bin in SharePoint Online in Office 365 for business provides a safety net when an site content and site collections are deleted. When you delete content from a SharePoint site, it's sent to the site's

Measurement	Description	Measurement Unit	Interpretation
			Recycle Bin or first-stage Recycle Bin, where you can restore the deleted content if needed. If the file/folder is deleted from the site Recycle Bin (i.e., from the first-stage Recycle Bin), it is sent to the Site Collection or Second-Stage Recycle Bin, where a site collection administrator can restore it or delete it permanently.
Folder deletions from II stage recycle bin	Indicates the number of folders deleted from the second-stage recycle bin.	Number	
Folder modifications	Indicates the number of times folders on SharePoint Online have been modified.	Number	
Folder moves	Indicates the number of times folders have been moved.	Number	Files/folders on SharePoint Online can be moved to a different destination in the current library, to OneDrive, or to another SharePoint site.
Folder renames	Indicates the number of times folders have been renamed.	Number	
Folder restores	Indicates the number of times folders have been restored from the Recycle Bin to their original location.	Number	

The detailed diagnosis of the *Unique operations* measure lists the unique folder operations that were performed, and the number of times each operation was performed. This way, administrators can quickly identify which operation was most common and imposed the maximum load on SharePoint Online.

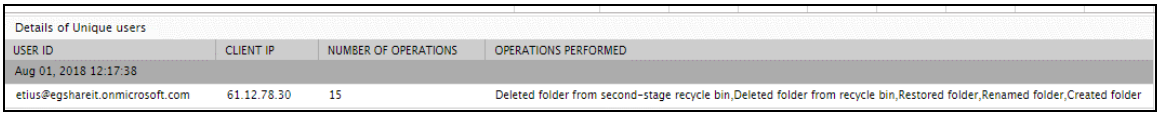


Details of Unique sites

SITE GUID	SITE URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:17:38			
8b96eaa2-8a4d-4bed-8ea0-6072e5ae544e	https://egshareit.sharepoint.com/	15	Deleted folder from second-stage recycle bin,Deleted folder from recycle bin,Restored folder,Renamed folder,Created folder

Figure 4.28: The detailed diagnosis of the Unique operations measure reported by the Folder Activities test

The detailed diagnosis of the *Unique users* measure lists the users who performed file/page operations on SharePoint Online. For each user, the operations performed by that user, the number of times the operations were performed, and the client from which that user initiated the operations are revealed. This way, administrators can quickly figure out if any user has performed any unauthorized operation.

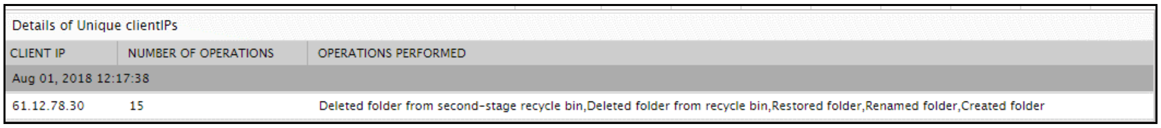


Details of Unique users

USER ID	CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:17:38			
etius@egshareit.onmicrosoft.com	61.12.78.30	15	Deleted folder from second-stage recycle bin,Deleted folder from recycle bin,Restored folder,Renamed folder,Created folder

Figure 4.29: The detailed diagnosis of the Unique users measure reported by the Folder Activities test

The detailed diagnosis of the *Unique client IPs* measure reveals which user operations were performed from which clients. The number of times the operations were performed from each client is also reported.

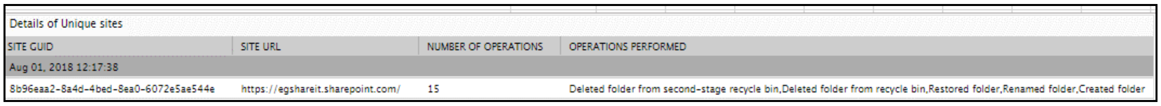


Details of Unique clientIPs

CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:17:38		
61.12.78.30	15	Deleted folder from second-stage recycle bin,Deleted folder from recycle bin,Restored folder,Renamed folder,Created folder

Figure 4.30: The detailed diagnosis of the Unique client IPs measure reported by the Folder Activities test

The detailed diagnosis of the *Unique sites* measure reveals the GUID and URL of each of the SharePoint sites on which folder operations were performed. The type of operation that was performed and the number of times these operations were performed is also reported, so that administrators can accurately identify the site that experienced a high level of activity.

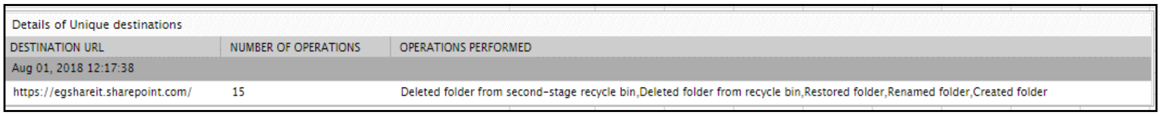


Details of Unique sites

SITE GUID	SITE URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:17:38			
8b96eaa2-8a4d-4bed-8ea0-6072e5ae544e	https://egshareit.sharepoint.com/	15	Deleted folder from second-stage recycle bin,Deleted folder from recycle bin,Restored folder,Renamed folder,Created folder

Figure 4.31: The detailed diagnosis of the Unique sites measure reported by the Folder Activities test

The detailed diagnosis of the *Unique destinations* measure lists the destination URLs of the folder operations. For each URL, the operations that resulted in the URL and the number of times the operations were performed are reported.

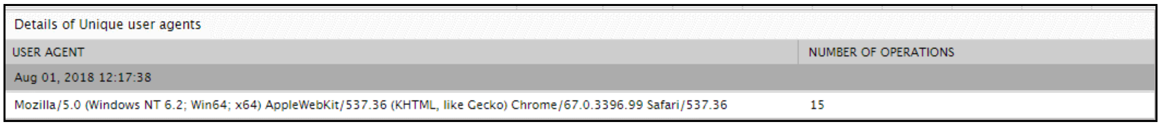


Details of Unique destinations

DESTINATION URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:17:38		
https://egshareit.sharepoint.com/	15	Deleted folder from second-stage recycle bin,Deleted folder from recycle bin,Restored folder,Renamed folder,Created folder

Figure 4.32: The detailed diagnosis of the Unique destinations measure reported by the Folder Activities test

The detailed diagnosis of the *Unique user agents* measure lists the user-agent strings of browsers used by users for performing the different folder operations. For each user-agent string, the detailed metrics further reveals the number of operations performed using that browser. This will help administrators to identify the browser that was used most often to perform folder operations.



Details of Unique user agents

USER AGENT	NUMBER OF OPERATIONS
Aug 01, 2018 12:17:38	
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36	15

Figure 4.33: The detailed diagnosis of the Unique user agents measure reported by the Folder Activities test

4.5.3 Sharing and Access Activities Test

The access request feature allows people to request access to content that they do not currently have permission to see. As a site owner, you can configure the feature to send you mail when someone requests access to a site. You can then choose whether to approve or decline their request. If you approve the request, you can also specify the specific level of permission you'd like to assign to a user.

The access request feature also works together with the Share command for sites. If someone who is not a site owner for a site (that is, someone who does not have full control for a site) uses the Share command to invite other people to view a site, then that action will generate an access request for the site owner. The site owner can then approve or decline the request, or specify the permission level to be assigned to the new user.

At some other times, instead of sending out Share invitations to other users to view the contents of a site, users may choose to share a link to the site with other users. These users can be members of your organization or guest users who are external to your organization.

However, regardless of how a site's contents are accessed (whether it is by requesting access, or via sharing invitations, or via sharing links), maintaining the security and integrity of the data stored in the sites at all times is of utmost importance to administrators! This is why, it is super-imperative that administrators monitor access requests, sharing invitations, and sharing links, promptly capture all activities related to these operations (eg., request creation, request acceptance, invite creation, link creation, invite withdrawal, etc.) as and when they occur, and closely scrutinize them to understand who initiated the operation, on which site, and from where. This is exactly what the **Sharing and Access Activities test** helps administrators do!

This test tracks access and sharing operations from the time of their creation to their acceptance/withdrawal, and captures and reports the number of times every activity related to each of these operations is performed. Detailed diagnostics shed more light on these activities by revealing the users who initiated them, the clients from which the activities were initiated, and even the sites that were impacted. This will enable administrators to efficiently audit these sensitive activities and ensure that they are performed only by authorized individuals on sites that such individuals have control over. Additionally, the test also provides administrators with a measure of the workload that such operations and their related activities impose on SharePoint Online.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
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	**These parameters are applicable only if the eG agent needs to communicate**

Parameters	Description
Port, Proxy User Name, and Proxy Password	**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*.
Report System Account Log Entries	By default, this flag is set to **No**. This means that, by default, the test ignores all operations performed by Windows System Accounts. A System Account in Windows is used by the operating system and by services that run under Windows. There are many services and processes within Windows that need the capability to log on internally (for example during a Windows installation). The system account was designed for that purpose; it is an internal account, does not show up in User Manager, cannot be added to any groups, and cannot have user rights assigned to it. On the other hand, the system account does show up on an NTFS volume in File Manager in the Permissions portion of the Security menu. By default, the system account is granted full control to all files on an NTFS volume. Here the system account has the same functional privileges as the administrator account. If you want the test to monitor and report on operations performed by Windows System Accounts as well, set this flag to **Yes**. **Note:** By default, this test does not monitor the operations of the *NT AUTHORITY\SYSTEM and SHAREPOINT\system* accounts. This is governed by the **System_Account_Names** parameter in the **[SPO_Audited_Activities]** section of the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). If required, you can exclude more Windows system accounts from monitoring. For that, do the following: 1. Edit the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). 2. Look for the **System_Account_Names** parameter in the **[SPO_Audited_ Activities]** section of the file. You will find that this parameter is by default

Parameters	Description
	set as follows: *System_ Account_ Names=NT AUTHORITY\SYSTEM,SHAREPOINT\system* 3. To exclude more Windows system accounts from monitoring, you need to modify the **System_ Account_ Names** parameter by appending more system accounts to the comma-separated list. 4. Finally, save the file.
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 • 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 access request and sharing-related operations that were performed by users of SharePoint Online.	Number	The value of this measure is the sum of the values of all measures reported under the section *Sharing and access request Operations*, in the Layers tab page of the eG monitoring console

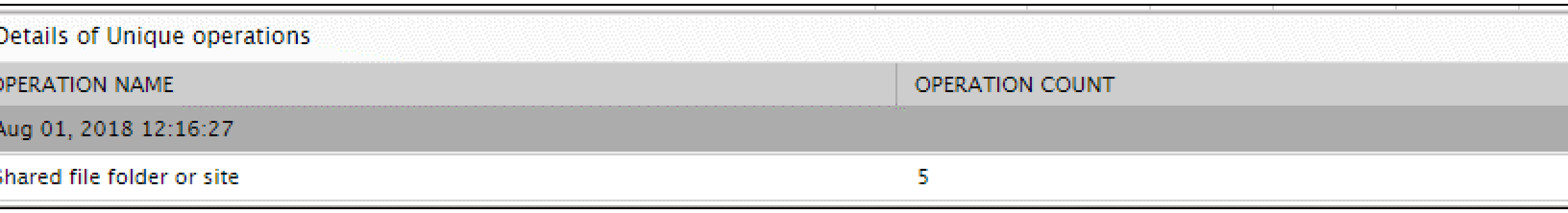
Measurement	Description	Measurement Unit	Interpretation
Unique operations	Indicates the count of unique access request and sharing-related operations that were performed on SharePoint Online.	Number	To know which operations were performed, use the detailed diagnosis of this measure.
Unique users	Indicates the count of unique users who performed operations related to access requests and sharing.	Number	To know which are the users who performed access request and sharing-related operations, use the detailed diagnosis of this measure.
Unique client IPs	Indicates the number of unique clients from which the users initiated the access requests and operations.	Number	Use the detailed diagnosis of this measure to determine the IP addresses of the clients from which users performed an access request or sharing-related operation.
Unique sites	Indicates the number of unique sites on which the access request and sharing-related operations were performed.	Number	Use the detailed diagnosis of the SharePoint Online sites on which access request and sharing-related operations were performed.
Affected item types	Indicates the number of types (file/folder/site) of items that were affected by access request and sharing-related operations.	Number	To know what type of items were affected by the access request and sharing-related operations, use the detailed diagnosis of this measure.
Unique destinations	Indicates the destination URLs of the access request and sharing-related operations that were performed.	Number	To know the unique destination URLs, use the detailed diagnosis of this measure.
Unique user agents	Indicates the unique user agents of browsers used for performing access request and sharing-related operations.	Number	To know the unique user-agent strings of the browsers used in access request and sharing-related operations, use the detailed diagnosis of this measure.

Measurement	Description	Measurement Unit	Interpretation
Access requests acceptances	Indicates the number of access requests that were accepted.	Number	A non-zero value for this measure implies that an access request to a site, folder, or document was accepted and the requesting user has been granted access.
Sharing invitations acceptances	Indicates the number of sharing invitations that were accepted.	Number	If this measure reports a non-zero value, it means that one/more users have accepted sharing invitations, thus obtaining access to that resources that are shared.
Sharing invitations blocked	Indicates the number of sharing invitations that were blocked.	Number	A sharing invitation sent by a user in your organization is blocked because of an external sharing policy that either allows or denies external sharing based on the domain of the target user. In this case, the sharing invitation was blocked because: • The target user's domain isn't included in the list of allowed domains; (Or) • The target user's domain is included in the list of blocked domains.
Company link creations	Indicates the number of company links created.	Number	Company-wide links can only be used by members in your organization. They cannot be used by guests.
Access request creations	Indicates the number of access requests created.	Number	A non-zero value for this measure implies that one/more users have access to one/more sites, documents, or folders they do not have permissions to access.
Anonymous link creations	Indicates the number of anonymous links that have been created.	Number	Documents and folders (but not sites) can be shared via an anonymous link where anyone with the link can view or edit the document, or upload to the

Measurement	Description	Measurement Unit	Interpretation
			folder. Though this is the least restrictive of sharing options, administrators must exercise caution when granting an external user an anonymous link to edit a resource
Sharing invitations creations	Indicates the number of sharing invitations created.	Number	A non-zero value for this measure indicates that one/more users invited other users who are not in your organization's directory to share a resource in SharePoint Online or OneDrive for Business.
Access request denials	Indicates the count of access requests that were declined.	Number	A non-zero value denotes that access requests to one/more sites, folders, or documents were denied.
Company link removals	Indicates the count of company-wide links that were removed.	Number	Once a company-wide link or anonymous link is removed, that link can no longer be used to access the resource.
Anonymous link removals	Indicates the count of anonymous links that were removed.	Number	
File/folder/site shares	Indicates the number of files/folders/sites that were shared with other users.	Number	
Anonymous link updates	Indicates the number of anonymous link updates that occurred.	Number	
Anonymous link usage	Indicates the number of times resources were accessed by anonymous users using one/more anonymous links.	Number	If this measure reports a non-zero value, then use the detailed diagnosis of the *Unique users* measure to identify the IP address of the clients from which the anonymous accesses happened.
Sharing revokes	Indicates the number of shares that were revoked.	Number	A non-zero value for this measure indicates that users have unshared one/more files, folders, or sites that

Measurement	Description	Measurement Unit	Interpretation
			were previously shared with other users.
Company link usage	Indicates the number of times company-wide links were used by users to access resources.	Number	If this measure reports a non-zero value, then use the detailed diagnosis of the *Unique users* measure to identify the users who revoked sharing invitations.
Sharing invitation withdrawals	Indicates the count of sharing invitations withdrawn.	Number	A non-zero value for this measure is indicative of one/more sharing invitations that were withdrawn. To withdraw a sharing invitation that has already been sent to an external user, you need to revoke the invitation before it is accepted.

The detailed diagnosis of the *Unique operations* measure lists the unique access request and sharing-related operations that were performed on SharePoint Online, and the number of times each operation was performed. This way, administrators can quickly identify which operation was most common and imposed maximum load on SharePoint Online.

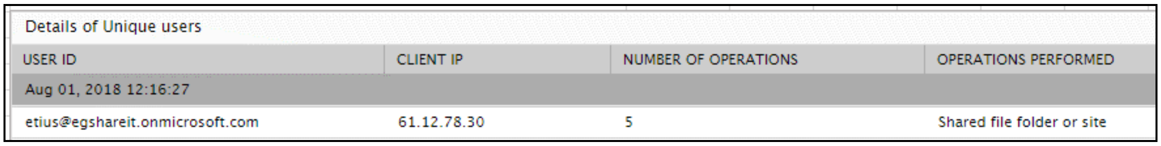


Details of Unique operations

OPERATION NAME	OPERATION COUNT
Aug 01, 2018 12:16:27	
Shared file folder or site	5

Figure 4.34: The detailed diagnosis of the Unique operations measure reported by the Sharing and Access Activities test

The detailed diagnosis of the *Unique users* measure lists the users who performed access request and/or sharing-related operations on SharePoint Online. For each user, the operations performed by that user, the number of times the operations were performed, and the client from which that user initiated the operations are revealed. This way, administrators can quickly figure out if any user has performed any unauthorized operation.

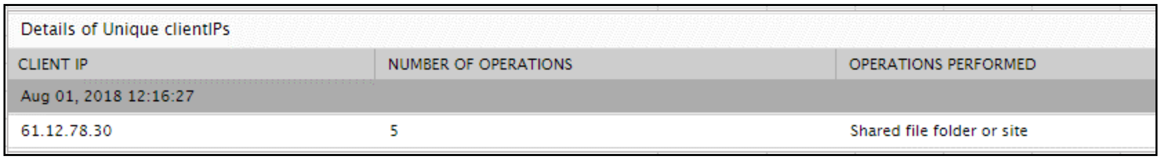


Details of Unique users

USER ID	CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:16:27			
etius@egshareit.onmicrosoft.com	61.12.78.30	5	Shared file folder or site

Figure 4.35: The detailed diagnosis of the Unique users measure reported by the Sharing and Access Activities test

The detailed diagnosis of the *Unique client IPs* measure reveals which access request and/or sharing-related operations were performed from which clients. The number of times the operations were performed from each client is also reported.

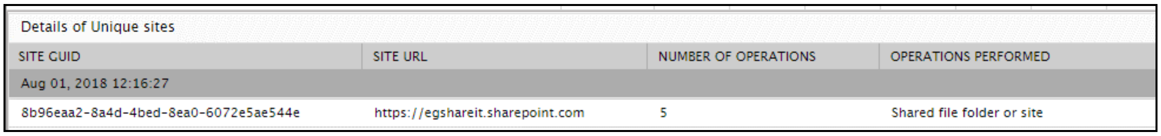


Details of Unique clientIPs

CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:16:27		
61.12.78.30	5	Shared file folder or site

Figure 4.36: The detailed diagnosis of the Unique client IPs measure reported by the Sharing and Access Activities test

The detailed diagnosis of the *Unique sites* measure reveals the GUID and URL of each of the SharePoint sites on which access request and/or sharing-related operations were performed. The type of operation that was performed and the number of times these operations were performed is also reported, so that administrators can accurately identify the site that experienced a high level of activity of this type.

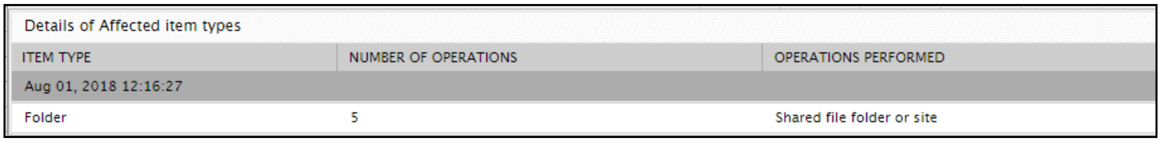


Details of Unique sites

SITE GUID	SITE URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:16:27			
8b96eaa2-8a4d-4bed-8ea0-6072e5ae544e	https://egshareit.sharepoint.com	5	Shared file folder or site

Figure 4.37: The detailed diagnosis of the Unique sites measure reported by the Sharing and Access Activities test

To know which type of items - i.e., whether a file/folder/site - was the target of the maximum number of access request and/or sharing-related operations, use the detailed diagnosis of the *Affected item types* measure. For each item type, the detailed metrics reveal the specific operations performed on that type and the number of times the operations were performed.

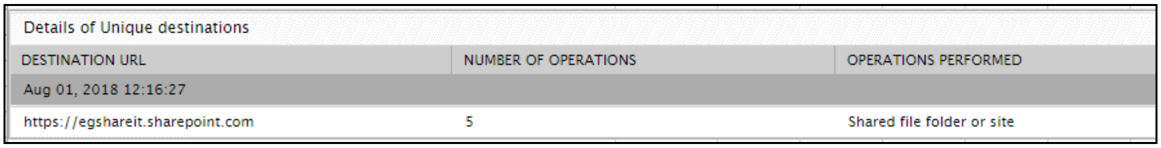


Details of Affected item types

ITEM TYPE	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:16:27		
Folder	5	Shared file folder or site

Figure 4.38: The detailed diagnosis of the Affected item types measure reported by the Sharing and Access Activities test

The detailed diagnosis of the *Unique destinations* measure lists the destination URLs of the access request and sharing-related operations. For each URL, the specific operations that resulted in that URL and the number of times the operations were performed are reported.

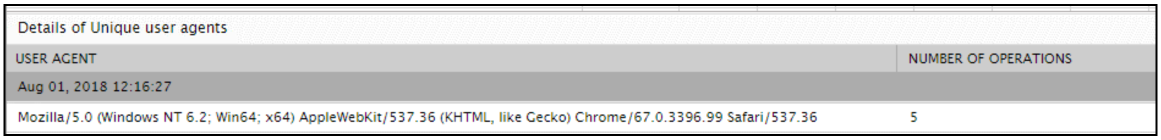


Details of Unique destinations

DESTINATION URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 12:16:27		
https://egshareit.sharepoint.com	5	Shared file folder or site

Figure 4.39: The detailed diagnosis of the Unique destinations measure reported by the Sharing and Access Activities test

The detailed diagnosis of the *Unique user agents* measure lists the user-agent strings of browsers used by users for performing the access request and/or sharing-related operations. For each user-agent string, the detailed metrics further reveals the number of operations performed using that browser. This will help administrators to identify the browser that was used most often to perform such operations.



Details of Unique user agents

USER AGENT	NUMBER OF OPERATIONS
Aug 01, 2018 12:16:27	
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36	5

Figure 4.40: The detailed diagnosis of the Unique user agents measure reported by the Sharing and Access Activities test

4.5.4 Site Administration Activities Test

In SharePoint Online for Office 365, administration can be separated into four primary roles: Office 365 Global Administrator, SharePoint Online Administrator, Site Collection Administrator, and Site Owner/Administrator

- Global Administrators: Global Administrators, also known as the “Company Admin” or the “Tenant Admin”, can configure any Office 365 settings and gain access to any level of the SharePoint site. Compared to the SharePoint Admin and the Site Collection admin, the Global Admin is the only role able to manage user groups and reset user passwords. Furthermore, global admins are the only admins who can assign other admin roles, outside of Site Collection admins. You can have more than one Global Admin.
- SharePoint Administrators: SharePoint Online Administrators can create and manage site collections, delegate site collection administrators and allocate space between the different Site Collections. Compared to the Global Admin, SharePoint Admins will be able to view user

information but, will not be able to modify existing information. In SharePoint Online, Global Administrators are also SharePoint Online Administrators.

- Site Collection Administrators: Site Collection Administrators are responsible for creating and maintaining sites and content within a site collection. Primary functions for the Site Collection Admin include managing permissions and restricting access where necessary, and managing content types, site columns and templates for re-use in the sites and update site structure based on content requirements. Site Collection Administrators can also assign other users to be a Site Collection Administrator to their Site Collection. Compared to Global and SharePoint admins, Site Collection Admins do not have access to the Office 365 Admin portal, thus they will not be able to see any user information.
- Site Owner/Administrator: A Site Owner/Administrator is vested with “Full control” to specific site(s) within a site collection. He/she is allowed to create and delete lists and libraries, grant other users permissions, activate site features, create new subsites, etc.

Because administrators are vested with many privileges and few restrictions, and since only a thin line separates the privileges of one administrator from another's, there is always the probability that changes made by one administrator get inadvertently overridden by another! This presents a strong case for monitoring administrative operations, capturing changes made across the SharePoint Online organization, and most importantly, identifying which administrator effected what change. This is exactly what the Site Administration Activities test does!

This test helps in auditing administrative operations by closely monitoring administrative activities on SharePoint Online and reporting the count of such activities. Detailed diagnostics provided by the test shed light on what administrative operations were performed on SharePoint Online, who are the administrators who performed them, from which clients were such operations initiated, and which sites were impacted by them.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
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*.
Report System Account Log Entries	By default, this flag is set to **No**. This means that, by default, the test ignores all operations performed by Windows System Accounts. A System Account in Windows is used by the operating system and by services that run under Windows. There are many services and processes within Windows that need the capability to log on

Parameters	Description
	internally (for example during a Windows installation). The system account was designed for that purpose; it is an internal account, does not show up in User Manager, cannot be added to any groups, and cannot have user rights assigned to it. On the other hand, the system account does show up on an NTFS volume in File Manager in the Permissions portion of the Security menu. By default, the system account is granted full control to all files on an NTFS volume. Here the system account has the same functional privileges as the administrator account.. If you want the test to monitor and report on operations performed by Windows System Accounts as well, set this flag to **Yes**. **Note:** By default, this test does not monitor the operations of the *NT AUTHORITY\SYSTEM and SHAREPOINT\system* accounts. This is governed by the **System_Account_Names** parameter in the **[SPO_Audited_Activities]** section of the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). If required, you can exclude more Windows system accounts from monitoring. For that, do the following: 1. Edit the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). 2. Look for the **System_Account_Names** parameter in the **[SPO_Audited_Activities]** section of the file. You will find that this parameter is by default set as follows: *System_Account_Names=NT AUTHORITY\SYSTEM,SHAREPOINT\system* 3. To exclude more Windows system accounts from monitoring, you need to modify the **System_Account_Names** parameter by appending more system accounts to the comma-separated list. 4. Finally, save the file.
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

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
Total operations	Indicates the total number of operations performed by administrators.	Number	The value of this measure is the sum of the values of all measures reported under the section *Site Administration Operations*, in the Layers tab page of the eG monitoring console
Unique operations	Indicates the count of unique administrative operations that were performed on SharePoint Online.	Number	To know which operations were performed, use the detailed diagnosis of this measure.
Unique users	Indicates the count of unique administrative users who performed the operations.	Number	To know which are the administrators who performed the administrative operations, use the detailed diagnosis of this measure.
Unique client IPs	Indicates the number of unique clients from which the administrators initiated their administrative operations.	Number	Use the detailed diagnosis of this measure to determine the IP addresses of the clients from which the administrators performed administrative operations.
Unique sites	Indicates the number of unique sites on which the administrative operations	Number	Use the detailed diagnosis of the SharePoint Online sites on which the administrative operations were

Measurement	Description	Measurement Unit	Interpretation
	were performed.		performed.
Affected item types	Indicates the number of types of items that were affected by the administrative operations.	Number	To know what type of items were affected by the administrative operations, use the detailed diagnosis of this measure.
Unique destinations	Indicates the destination URLs of the administrative operations that were performed.	Number	To know the unique destination URLs, use the detailed diagnosis of this measure.
Unique user agents	Indicates the unique user agents of browsers used for performing administrative operations.	Number	To know the unique user-agent strings of the browsers used in administrative tasks, use the detailed diagnosis of this measure.
User agent exempt additions	Indicates the number of times additions were made to the list of exempt user agents in the SharePoint admin center.	Number	InfoPath Forms Services in SharePoint Online lets you deploy your organization's forms to your sites, enabling users fill out these forms in a web browser. To make indexing InfoPath forms faster and easier, you can specify which user agents to exempt from receiving an entire webpage to index. This means that when a user agent you have specified as exempt encounters an InfoPath form, the form will be returned as an XML file (which looks like a hierarchical text file) instead of an entire webpage. This measure reports a non-zero value if a SharePoint administrator or Global administrator adds one/more user agents to the list of exempt user agents, so that InfoPath forms are indexed quickly.

Measurement	Description	Measurement Unit	Interpretation
User agent exempt modifications	Indicates the number of times administrators have modified the list of exempt user agents in the SharePoint admin center.	Number	This measure reports a non-zero value if a SharePoint administrator or Global administrator customized the list of exempt user agents.
Site collection admin additions	Indicates the number of site collection administrators added.	Number	Site collection administrators have full control permissions for the site collection and all subsites. A Site Collection administrator can also add a person as a site collection administrator for a site. If this happens, then the value of this measure will get incremented.
User/group additions	Indicates the number of times new members or guests were added to SharePoint groups.	Number	Sometimes, intentionally or as a result of another activity (eg., sharing), a user may add a member or guest to a SharePoint group. When this happens, the value of this measure will increase.
Add user/group permits	Indicates the number of times administrators allowed other users to create groups.	Number	A Site administrator can add a permission level to a site hat allows a user assigned that permission to create a group for that site. When this happens, the value of this measure will increase.
Sharing policy modifications	Indicates the number of times sharing policies were modified by administrators.	Number	A SharePoint administrator or Global administrator changed a SharePoint sharing policy by using the Office 365 admin portal, SharePoint admin portal, or SharePoint Online Management Shell. Whenever a SharePoint sharing policy is so changed, the value of this measure gets incremented.
Group additions	Indicates the number of times administrators added groups to sites.	Number	Site administrator or owner creates a group for a site, or performs a task that results in a group being created. For

Measurement	Description	Measurement Unit	Interpretation
			example, the first time a user creates a link to share a file, a system group is added to the user's OneDrive for Business site. This event can also be a result of a user creating a link with edit permissions to a shared file. Whenever a group is so created for a site, the value of this measure gets incremented.
Sent to connection creations	Indicates the number of Send To connections that were created by administrators.	Number	A SharePoint or Global administrator can create a new Send To connection on the Records management page in the SharePoint admin center. A Send To connection specifies settings for a document repository or a records center. When you create a Send To connection, a Content Organizer can submit documents to the specified location. When a Send To connection is so created, the value of this measure increased.
Site collection creations	Indicates the number of times administrators created site collections in the SharePoint Online organization.	Number	A SharePoint or global administratorcan create a new site collection in your SharePoint Online organization or a user can provision their OneDrive for Business site. Whenever one of these events occur, the value of this measure gets incremented.
Group deletes	Indicates the number of groups deleted by users/administrators.	Number	Whenever a user/administrator deletes a group from site, the value of this measure gets incremented.
Send to connection deletes	Indicates the number of Send To connections deleted by administrators.	Number	A SharePoint or global administrator deletes a Send To connection on the Records management page in the

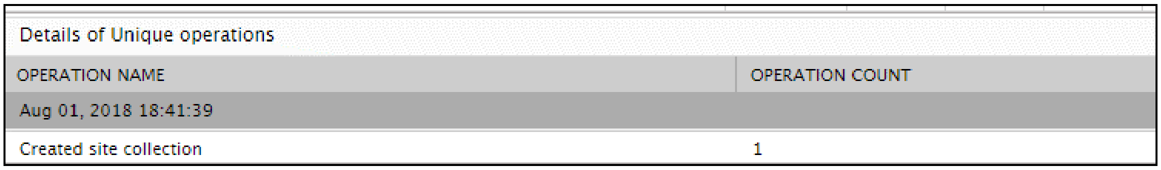
Measurement	Description	Measurement Unit	Interpretation
			SharePoint admin center. A Send To connection specifies settings for a document repository or a records center. When you create a Send To connection, a Content Organizer can submit documents to the specified location. When a Send To connection is deleted, the value of this measure is incremented.
Site deletes	Indicates the number of sites deleted by administrators.	Number	Whenever a site administrator deletes a site, the value of this measure is incremented.
Document preview permits	Indicates the number of times site administrators enabled document preview.	Number	Document Preview, when enabled, extends and leverages SharePoint document management capabilities by embedding pure HTML viewers for dozens of file formats into SharePoint document libraries and SharePoint Search centers. These viewers facilitate graphical preview of document content. The value of this measure increases whenever a Site administrator enables document preview for a site.
Workflow task content type additions	Indicates the number of SharePoint 2013 Workflow task content types added by site administrators to their sites.	Number	SharePoint workflows are pre-programmed mini-applications that streamline and automate a wide variety of business processes. Workflows can range from collecting signatures, feedback, or approvals for a plan or document, to tracking the current status of a routine procedure. For example, take a document approval process. Running this

Measurement	Description	Measurement Unit	Interpretation
			process manually can mean a lot of checking up and keeping track, forwarding documents and sending reminders — and each of those tasks has to be performed by you or by one or more of your colleagues. That means a lot of extra work and (maybe even worse) a constant stream of interruptions. But when you use the SharePoint Document Approval workflow to run the process, all of that checking and tracking and reminding and forwarding is done by the workflow, automatically. If someone is late in completing a task, or if some other hitch arises, most of the included workflows generate a notification to let you know about it. Nobody in the group has to proactively monitor the process because with a SharePoint workflow, the process is always proactively monitoring itself. When a task is added to a Workflow, the value of this measure increases.
Office on demand permits	Indicates the number of times the Office on Demand feature was enabled.	Number	Office on Demand is a feature that provides online access to full rich Office desktop applications, including Word, Excel, and PowerPoint, when you are using a PC that doesn't have the latest version of Office installed locally. Whenever a Site administrator/owner enables Office on Demand, the value of this measure gets incremented.
News feed permits	Indicates the number of times RSS feeds were allowed.	Number	Really Simple Syndication (RSS) is a way for you to make news, blogs, and other content on a site available to

Measurement	Description	Measurement Unit	Interpretation
			subscribers. When RSS is turned on, it can be managed for site collections, sites, lists, and libraries. Your permissions on the site determine at what level you can manage RSS. Whenever a Site administrator/Site owner enables RSS feeds for a site, or a Global administrator enables RSS feeds for an entire organization, the value of this measure increases.
Site permissions modifications	Indicates the number of times administrators modified site permissions.	Number	Site administrator or owner (or system account) can change the permission level that are assigned to a group on a site. Whenever this happens, the value of this measure increases.
Removals from group	Indicates the number of times members/guests were removed from SharePoint groups.	Number	Whenever a user removes a member/guest from a SharePoint group, the value of this measure increases.
Site renames	Indicates the number of times sites were renamed.	Number	Whenever a Site administrator/owner renames a site, the value of this measure increases.
Site admin requests	Indicates the number of times users requested to be added as site collection administrators to a site collection.	Number	Whenever a Site collection administrator receives a request from a user to add him/her as a site collection administrators, the value of this measure gets incremented.
Host site changes	Indicates the number of times the sites hosted by the desginated site were changed.	Number	A SharePoint or global administrator can change the designated site to host personal or OneDrive for Business sites. When this happens, the value of this measure changes.
Group settings changes	Indicates the number of times the settings of groups	Number	A Site administrator or owner can change the settings of a group for a

Measurement	Description	Measurement Unit	Interpretation
	were changed.		site. This can include changing the group's name, who can view or edit the group membership, and how membership requests are handled. Whenever such a change is made, the value of this measure increases.

The detailed diagnosis of the *Unique operations* measure lists the unique administrative operations that were performed on SharePoint Online, and the number of times each operation was performed. This will point to those administrative activities that were most common.

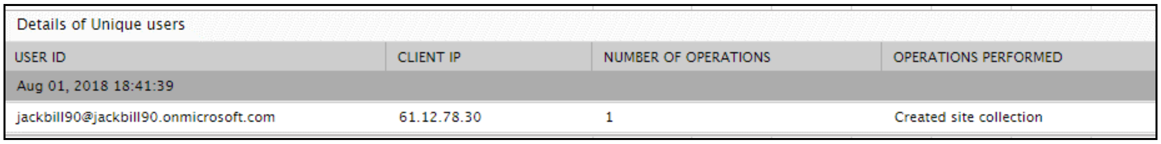


Details of Unique operations

OPERATION NAME	OPERATION COUNT
Aug 01, 2018 18:41:39	
Created site collection	1

Figure 4.41: The detailed diagnosis of the Unique operations measure reported by the Site Administration Activities test

The detailed diagnosis of the *Unique users* measure lists the administrators who performed different administrative operations on SharePoint Online. For each administrator, the operations performed by that admin, the number of times the operations were performed, and the client from which that operation was initialized are revealed. This may reveal if two/more administrators made conflicting changes. This will also reveal performance- or UX-impacting changes that were made and the administrator who made them. Changes made with malicious intent may also surface in the process.

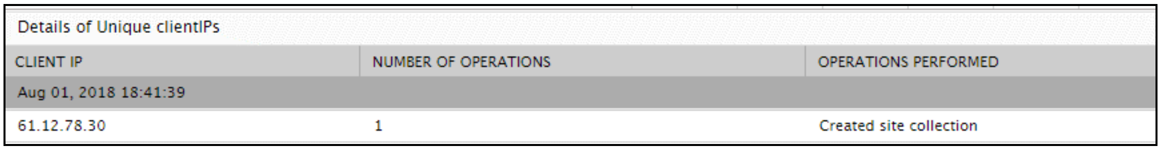


Details of Unique users

USER ID	CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 18:41:39			
jackbill90@jackbill90.onmicrosoft.com	61.12.78.30	1	Created site collection

Figure 4.42: The detailed diagnosis of the Unique users measure reported by the Site Administration Activities test

The detailed diagnosis of the *Unique client IPs* measure reveals which administrative operations were performed from which clients. The number of times the operations were performed from each client is also reported.

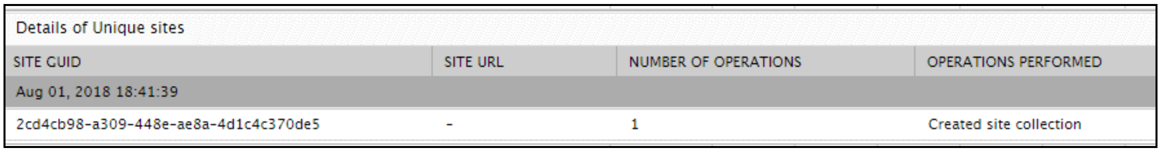


Details of Unique clientIPs

CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 18:41:39		
61.12.78.30	1	Created site collection

Figure 4.43: The detailed diagnosis of the Unique client IPs measure reported by the Site Administration Activities test

The detailed diagnosis of the *Unique sites* measure reveals the GUID and URL of each of the SharePoint sites on which administrative operations were performed. The type of operation that was performed and the number of times these operations were performed is also reported, so as to highlight those sites where the maximum number of administrative operations were performed.

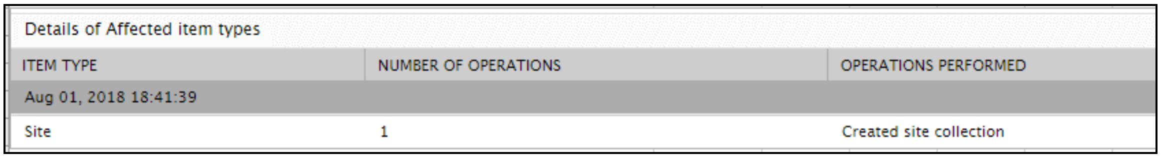


Details of Unique sites

SITE GUID	SITE URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 18:41:39			
2cd4cb98-a309-448e-ae8a-4d1c4c370de5	-	1	Created site collection

Figure 4.44: The detailed diagnosis of the Unique sites measure reported by the Site Administration Activities test

To know which type of items - i.e., whether a file/folder/web/site/tenant/document library- was the target of the maximum number of administrative operations, use the detailed diagnosis of the *Affected item types* measure. For each item type, the detailed metrics reveal the specific operations performed on that type and the number of times the operations were performed.

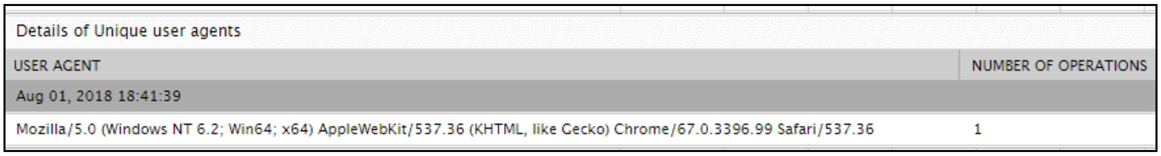


Details of Affected item types

ITEM TYPE	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
Aug 01, 2018 18:41:39		
Site	1	Created site collection

Figure 4.45: The detailed diagnosis of the Affected item types measure reported by the Site Administration Activities test

The detailed diagnosis of the *Unique user agents* measure lists the user-agent strings of browsers used by users for performing the administrative operations. For each user-agent string, the detailed metrics further reveals the number of operations performed using that browser. This will help administrators to identify the browser that was used most often to perform such operations.



Details of Unique user agents

USER AGENT	NUMBER OF OPERATIONS
Aug 01, 2018 18:41:39	
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36	1

Figure 4.46: The detailed diagnosis of the Unique user agents measure reported by the Site Administration Activities test

4.5.5 Synchronization Activities Test

If your organization has an Office 365 business subscription or uses SharePoint Server 2019 Public Preview, you can sync your SharePoint files to a folder on your computer where you can work directly in File Explorer and access the files even when you are offline. Whenever you are online, any changes that you or others make will sync automatically.

Issues in file synchronization may result in loss of critical changes made to data. This is why, it is imperative that administrators keep track of each operation related to file synchronization. Auditing synchronization activities enables administrators to promptly capture each synchronization-related operation as and when it occurs, ensure that only authorized personnel perform synchronization, and also determine whether/not the documents in the document library and in your local computer are in sync. This is exactly what the Synchronization Activities test helps administrators achieve!

This test monitors synchronized-related operations and reports the count of each operation. This enables administrators to understand if any synchronization-task is in progress currently or not. Detailed diagnostics reported by the test reveal which user performed each operation, thus helping administrators promptly identify unauthorized/suspect synchronization operations. The client IPs from which each operation was initiated and the sites that were impacted are also revealed as part of the detailed diagnostics. Additionally, the test also reports the count of changes successfully uploaded to the SharePoint document library and/or successfully downloaded by the local computer. If administrators know of uploads/downloads that have been initiated, then these metrics will help them figure out whether/not all such operations were successful. Failed synchronizations thus come to light, so that they can be investigated.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
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*.
Report System Account Log Entries	By default, this flag is set to **No**. This means that, by default, the test ignores all operations performed by Windows System Accounts. A System Account in Windows is used by the operating system and by services that run under Windows. There are many services and processes within Windows that need the capability to log on

Parameters	Description
	internally (for example during a Windows installation). The system account was designed for that purpose; it is an internal account, does not show up in User Manager, cannot be added to any groups, and cannot have user rights assigned to it. On the other hand, the system account does show up on an NTFS volume in File Manager in the Permissions portion of the Security menu. By default, the system account is granted full control to all files on an NTFS volume. Here the system account has the same functional privileges as the administrator account.. If you want the test to monitor and report on operations performed by Windows System Accounts as well, set this flag to **Yes**. **Note:** By default, this test does not monitor the operations of the *NT AUTHORITY\SYSTEM and SHAREPOINT\system* accounts. This is governed by the **System_Account_Names** parameter in the **[SPO_Audited_Activities]** section of the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). If required, you can exclude more Windows system accounts from monitoring. For that, do the following: 1. Edit the eg_tests.ini file (in the <EG_INSTALL_DIR>\manager\config directory). 2. Look for the **System_Account_Names** parameter in the **[SPO_Audited_ Activities]** section of the file. You will find that this parameter is by default set as follows: *System_Account_Names=NT AUTHORITY\SYSTEM,SHAREPOINT\system* 3. To exclude more Windows system accounts from monitoring, you need to modify the **System_Account_Names** parameter by appending more system accounts to the comma-separated list. 4. Finally, save the file.
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

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.

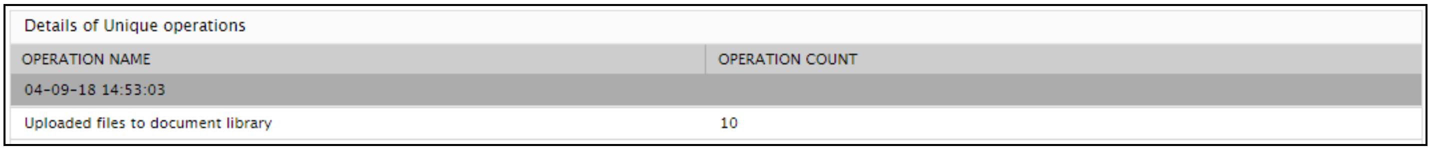
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total operations	Indicates the total number of synchronization-related operations that were performed .	Number	The value of this measure is the sum of the values of all measures reported under the section *Synchronization Operations*, in the Layers tab page of the eG monitoring console
Unique operations	Indicates the count of unique synchronization-related operations that were performed.	Number	To know which operations were performed, use the detailed diagnosis of this measure.
Unique users	Indicates the count of unique users who performed operations related to synchronization.	Number	To know which are the users who performed synchronization-related operations, use the detailed diagnosis of this measure.
Unique client IPs	Indicates the number of unique clients from which the users initiated the synchronization operations.	Number	Use the detailed diagnosis of this measure to determine the IP addresses of the clients from which users performed synchronization operations.
Unique sites	Indicates the number of unique sites on which the synchronization-related operations were performed.	Number	Use the detailed diagnosis of the SharePoint Online sites on which synchronization-related operations were performed.

Measurement	Description	Measurement Unit	Interpretation
Affected item types	Indicates the number of types (eg., file, folder) of items that were affected by synchronization-related operations.	Number	To know what type of items were affected by the synchronization-related operations, use the detailed diagnosis of this measure.
Unique destinations	Indicates the destination URLs of the synchronization-related operations that were performed.	Number	To know the unique destination URLs, use the detailed diagnosis of this measure.
Unique user agents	Indicates the unique user agents of browsers used for performing synchronization-related operations.	Number	To know the unique user-agent strings of the browsers used for performing synchronization-related, use the detailed diagnosis of this measure.
File synchronization permits	Indicates the number of times users successfully established a sync relationship with the sites.	Number	For files to be synchronized between your PC and the SharePoint Online document libraries, a sync relationship has to be set between the two. Typically, a sync relationship can be successfully established only if your computer is a member of a domain that's been added to the list of domains (called the safe recipients list) that can access document libraries in your organization. If this pre-requisite is fulfilled and a sync relationship is successfully set, then the value of this measure will increase.
File synchronization blocks	Indicates the number of times a sync relationship with sites was not allowed.	Number	Typically, a sync relationship with a site will not be allowed / will fail if: • Your PC is not a member of your organization's domain; (OR) • Your PC is the member of a domain that has not been added to the list of

Measurement	Description	Measurement Unit	Interpretation
			domains (called the safe recipients list) that can access document libraries in your organization; In this case, your computer will be blocked from syncing, downloading, or uploading files on a document library. Whenever this happens, the value of this measure will increase.
File downloads	Indicates the number of times users successfully downloaded files from document library to PC.	Number	If after establishing a sync relationship, a user successfully downloads files for the very first time from the document library to his/her computer, then the value of this measure will get incremented.
File changes downloads	Indicates the number of times changes to files were successfully downloaded from document library to PC.	Number	If any changes were made to the files in the document library, and such changes were successfully downloaded by your computer, then the value of this measure will increase.
File uploads	Indicates the number of times users successfully uploaded files from their PC to the document library.	Number	If after establishing a sync relationship, a user successfully uploads files for the very first time from the his/her computer to the document library, then the value of this measure will get incremented.
File changes uploads	Indicates the number of times changes to files were successfully uploaded to document library from PC.	Number	If any changes were made to the files in the user's PC, and such changes were successfully uploaded to the document library, then the value of this measure will increase.

The detailed diagnosis of the *Unique operations* measure lists the unique synchronization-related operations that were performed on SharePoint Online, and the number of times each operation was performed.

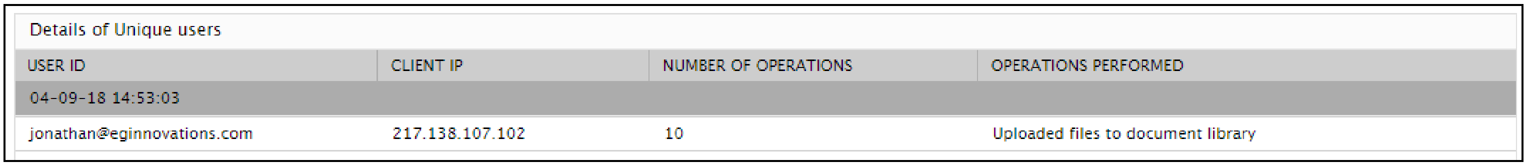


Details of Unique operations

OPERATION NAME	OPERATION COUNT
04-09-18 14:53:03	
Uploaded files to document library	10

Figure 4.47: The detailed diagnosis of the Unique operations measure reported by the Synchronization Activities test

The detailed diagnosis of the *Unique users* measure lists the users who performed synchronization-related operations on SharePoint Online. For each user, the operations performed by that user, the number of times the operations were performed, and the client from which that user initiated the operations are revealed. This way, administrators can quickly figure out if any user has performed any unauthorized operation.

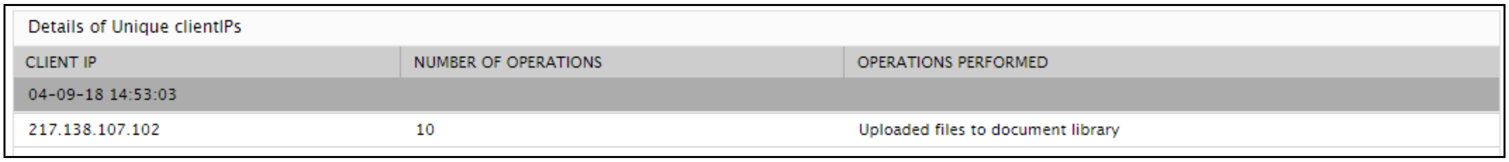


Details of Unique users

USER ID	CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:53:03			
jonathan@eginnovations.com	217.138.107.102	10	Uploaded files to document library

Figure 4.48: The detailed diagnosis of the Unique users measure reported by the Synchronization Activities test

The detailed diagnosis of the *Unique client IPs* measure reveals which synchronization-related operations were performed from which clients. The number of times the operations were performed from each client is also reported.

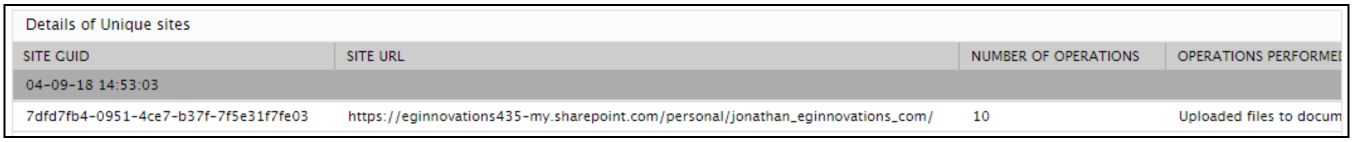


Details of Unique clientIPs

CLIENT IP	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:53:03		
217.138.107.102	10	Uploaded files to document library

Figure 4.49: The detailed diagnosis of the Unique client IPs measure reported by the Synchronization Activities test

The detailed diagnosis of the *Unique sites* measure reveals the GUID and URL of each of the SharePoint sites on which synchronization-related operations were performed. The type of operation that was performed and the number of times these operations were performed is also reported, so that administrators can accurately identify the site that experienced a high level of activity of this type.

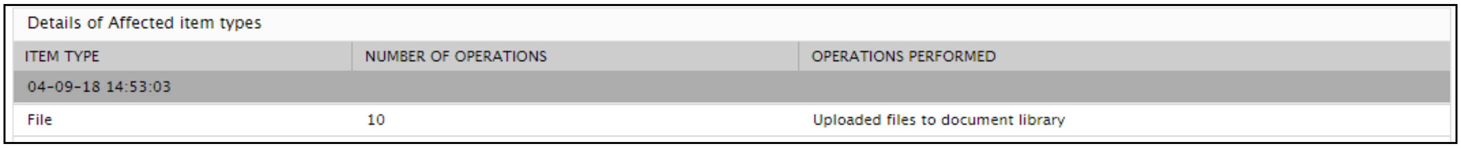


Details of Unique sites

SITE GUID	SITE URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMEI
04-09-18 14:53:03			
7dfd7fb4-0951-4ce7-b37f-7f5e31f7fe03	https://eginnovations435-my.sharepoint.com/personal/jonathan_eginnovations_com/	10	Uploaded files to docum

Figure 4.50: The detailed diagnosis of the Unique sites measure reported by the Synchronization Activities test

To know which type of items -eg., file, folder, etc. - was the target of the maximum number of synchronization-related operations, use the detailed diagnosis of the *Affected item types* measure. For each item type, the detailed metrics reveal the specific operations performed on that type and the number of times the operations were performed.

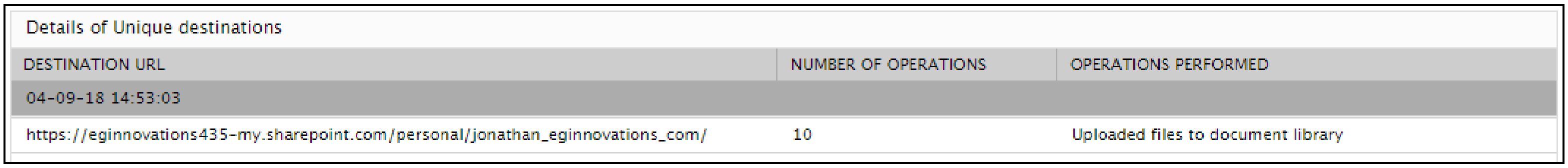


Details of Affected item types

ITEM TYPE	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:53:03		
File	10	Uploaded files to document library

Figure 4.51: The detailed diagnosis of the Affected item types measure reported by the Synchronization Activities test

The detailed diagnosis of the *Unique destinations* measure lists the destination URLs of the synchronization-related operations. For each URL, the specific operations that resulted in that URL and the number of times the operations were performed are reported.

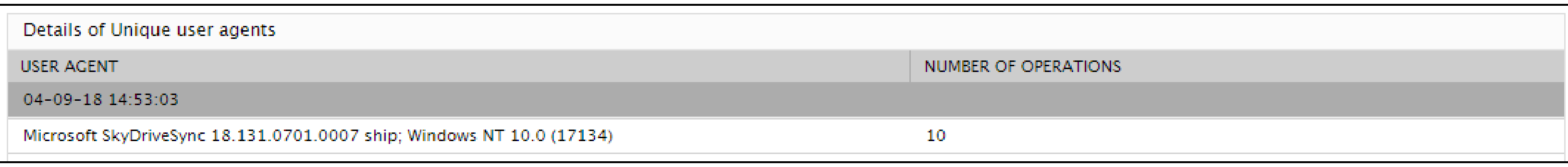


Details of Unique destinations

DESTINATION URL	NUMBER OF OPERATIONS	OPERATIONS PERFORMED
04-09-18 14:53:03		
https://eginnovations435-my.sharepoint.com/personal/jonathan_eginnovations_com/	10	Uploaded files to document library

Figure 4.52: The detailed diagnosis of the Unique destinations measure reported by the Synchronization Activities test

The detailed diagnosis of the *Unique user agents* measure lists the user-agent strings of browsers used by users for performing the synchronization operations. For each user-agent string, the detailed metrics further reveals the number of operations performed using that browser. This will help administrators to identify the browser that was used most often to perform such operations.



Details of Unique user agents

USER AGENT	NUMBER OF OPERATIONS
04-09-18 14:53:03	
Microsoft SkyDriveSync 18.131.0701.0007 ship; Windows NT 10.0 (17134)	10

Figure 4.53: The detailed diagnosis of the Unique user agents measure reported by the Synchronization Activities test

4.6 The User Experience Layer

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

- Check the availability and responsiveness of each site that is configured for monitoring;
- Optionally, emulate the logon process to SharePoint Online, track the success/failure of each step of the logon process, and measure the time taken to complete each step, so as to identify the exact step at which a failure/delay occurred

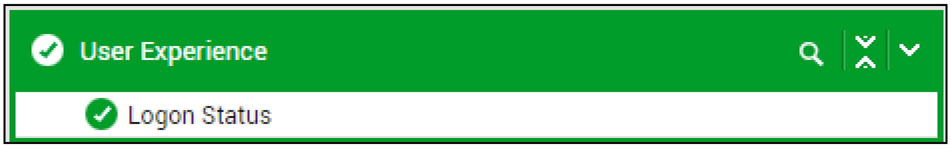


Figure 4.54: The test mapped to the User Experience layer

4.6.1 Logon Status Test

SharePoint Online is a cloud-based service that helps organizations share and collaborate with colleagues, partners, and customers. Where SharePoint Online is used, users need to be able to quickly and easily login to SharePoint Online, so that they have on-demand access to internal sites, documents, and other information. If users are unable to login to SharePoint 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 SharePoint 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 SharePoint URL of the monitored Office 365 domain to complete the login.

The test reports the success/failure of each step of the emulated logon process. Additionally, the test also measures the time taken to complete every step. This way, the test enables administrators to proactively detect problems in a typical user logon to SharePoint Online 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 SharePoint Online* as the **Component type**, select *Logon Status* test from the **DISABLED TESTS** list, and click the << button to enable it.

Target of the test : Microsoft SharePoint 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 **Service support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against O365 User Name and O365 Password text boxes. Confirm the password by retyping it in the Confirm Password text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365 portal and assign the required privileges to that user, refer to Section **2.1.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with

Parameters	Description
	.onmicrosoft.com.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify none against the Proxy User Name, Proxy Password, and Confirm Password text boxes. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of any of the Proxy-related parameters. By default, these parameters are set to *none*.

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:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><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>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>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.</td></tr>
<tr><td>Authentication time</td><td>Indicates the time taken for the login credentials to be validated.</td><td>Seconds</td><td>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 <i>Login time</i> 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?</td></tr>
<tr><td>Login status</td><td>Indicates whether/not the SharePoint URL that this test hit returned a valid response page.</td><td></td><td>If this measure reports the value <i>Success</i>, it means that the test was able to connect to the SharePoint URL of the domain, successfully. On the other hand, if this measure reports the value <i>Failed</i>, 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:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><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>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the login status. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Login time</td><td>Indicates the time taken to connect to the SharePoint URL of the monitored domain.</td><td>Seconds</td><td>An abnormally high value is a cause cor concern, as it indicates that it is taking an unusually long time to connect to the SharePoint URL.
If the <i>Total login time</i> reports an abnormally high value, then compare the value of this measure with that of the <i>Authentication time</i> 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 process. Under such circumstances, compare the value of the <i>Authentication time</i> and <i>Login time</i> measures to know what is delaying API logon - authentication? or connecting to the SharePoint URL?</td></tr>
</table>

4.6.2 Site Connectivity Test

If there is something that can mar user experience with SharePoint Online, then it is the frequent unavailability and consistently poor responsiveness of the sites hosted on SharePoint Online. This is why, administrators prioritize site accessibility-related issues above all else, and strive to capture and fix such issues before users notice and complain. This is where the **Site Connectivity** test comes in handy!

For each site that is configured for monitoring, this test, at frequent intervals, emulates an HTTP/S connection to that site and reports on the availability and responsiveness of that site. Besides sending out pre-emptive alerts to administrators regarding the unavailability/slowness of a site, the test also reports the response code returned by the site for the emulated request. In the event that the site is unavailable, the response code will point administrators to the probable reason for the non-availability. Also, a web site can be considered truly 'available', only if the page that is hit displays 'valid' content - i.e., the content that it is supposed to display during normal operations, and not junk data or error messages. The Site Connectivity test also reports the validity of the content of the target site, and thus paints a 'true' picture of availability.

Target of the test : Microsoft SharePoint Online

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each *SITE URL* monitored

First-level descriptor: Display Name of a site, in the **SITE URL** configuration

Configurable parameters for the test

Para- meters	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 support admin** and **SharePoint admin** roles and is vested with the **View-Only Audit Logs** permission. Configure the credentials of such a user against **O365 USER NAME** and **O365 PASSWORD** text boxes. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. While you can use the credentials of any existing O365 user with the afore-said privileges, it is recommended that you create a special user for monitoring purposes using the Office 365 portal and use the credentials of that user here. To know how to create a new user using the Office 365

Para-meters	Description
	portal and assign the required privileges to that user, refer to Section **2.1.1**.
O365 Domain	To have a personalized business email address, team site address, or even an account name, you set up a domain name with Office 365. A domain is a unique name that appears after the @ sign in email addresses, and after www. in web addresses. It typically takes the form of your organization's name and a standard Internet suffix, such as *yourbusiness.com* or *stateuniversity.edu*. Office 365 gives you an initial domain name to use. By default, this will be of the format: *.onmicrosoft.com - eg., abc.onmicrosoft.com. To enable this test to pull metrics, you need to configure the test with the name of this initial domain. Therefore, configure the O365 Domain parameter with the name of the initial domain. To know what is your Office 365 initial domain name, do the following: 1. Log on to the Microsoft Office 365 Online Portal using an administrative account. 2. Under **Management**, click on **Domains**. 3. The initial domain should be listed with a name ending with *.onmicrosoft.com*.
Domain, Domain User Name, Domain Password, and Confirm Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, in the Domain text box, specify the name of the Windows domain to which the eG agent host belongs. In the Domain User Name text box, mention the name of a valid domain user with login rights to the eG agent host. Provide the password of that user in the Domain Password text box and confirm that password by retyping it in the Confirm Password text box. On the other hand, if the eG agent is not behind a Proxy server, then you need not disturb the default setting of these parameters. By default, these parameters are set to *none*.
Proxy Host, Proxy Port, Proxy User Name, and Proxy Password	**These parameters are applicable only if the eG agent needs to communicate with the Office 365 portal via a Proxy server.** In this case, provide the IP/host name and port number of the Proxy server that the eG agent should use in the Proxy Host and Proxy Port parameters, respectively. If the Proxy server requires authentication, then specify the credentials of a valid Proxy user against the Proxy User Name and Proxy Password text boxes. Confirm that password by retyping it in the Confirm Password text box. If the Proxy server does not require authentication, then specify none against the Proxy User Name, Proxy 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*.

Para-meters	Description
Site URLs	Provide a comma-separated list of sites to be monitored. The format of your specification should be as follows: *<DisplayName>:<Site_URL>*. For example, your specification can be: *abc:http://www.abc.com/Homepage.aspx,zanax:https://www.zanax.com/Homepage.aspx* Note that the *<DisplayName>* specifications will be the descriptors of this test.
Validity String	For each Site URL configured, specify a validity string. This means that if a comma-separated list of Site URLs has been configured, then you will also have to configure a comma-separated list of validity strings. **Note:** • The number of validity strings configured should be the same as the number of Site URLs configured for monitoring; • The validity strings should be specified in the same order as that of the Site URLs. In other words, in a comma-separated list of validity strings, the first validity string will correspond to the first site URL, the second validity string will correspond to the second site URL, and so on. • If you do not wish to configure a validity string for any site URL, then make sure that you set the validity string for that site URL as *none*. Typically, this test checks whether the contents of a Site URL contains the validity string that corresponds to that URL. If the searched string is found in a URL's contents, then the test reports that the contents are valid.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Web availability	This measurement indicates whether this site was able to respond successfully to the query made by the test.	Percent	If this measure reports the value 100%, it implies that the site is accessible. The value 0 on the other hand indicates that the site is nopt accessible over HTTP/S. Availability failures could be caused by several factors such as the web site being down, the web site being

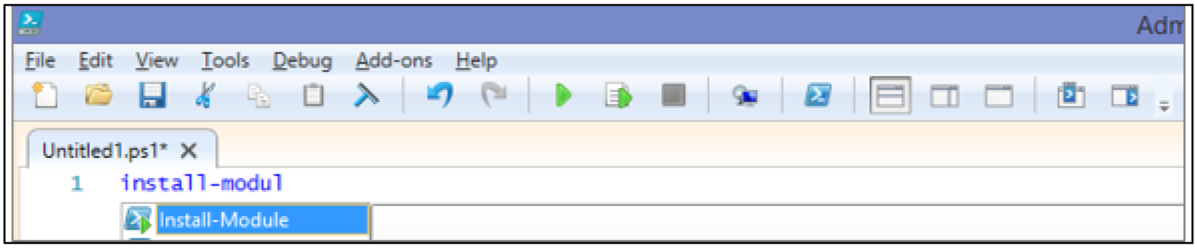
Measurement	Description	Measurement Unit	Interpretation
			misconfigured, a network failure, etc. Temporary unavailability may also occur if the web site is overloaded. Availability is determined based on the response code returned by the site. A response code between 200 to 300 indicates that the site is available.
Response code	The response code returned by this site for the simulated request	Number	A value between 200 and 300 indicates a good response. A 4xx value indicates a problem with the requested content (eg., page not found). A 5xx value indicates a server error.
Response time	This measurement indicates the time taken by this site to respond to the requests it receives.	Seconds	Response time being high denotes a problem. Poor response times may be due to the site being overloaded or misconfigured. If the URL accessed involves the generation of dynamic content, backend problems (e.g., an overload at the application server or a database failure) can also result in an increase in response time.
Content validity	This measure validates whether this site was successful in executing the request made to it.	Percent	A value of 100% indicates that the content returned by the test is valid. A value of 0% indicates that the content may not be valid. This capability for content validation is especially important for multi-tier web applications. For example, a user may not be able to login to the web site but the site may reply back with a valid HTML page where in the error message, say, "Invalid Login" is reported. In this case, the availability will be 100 % (since we got a valid HTML response). If the test is configured such that the content parameter should include the string "About Us", in the above scenario

Measurement	Description	Measurement Unit	Interpretation
			content validity would have a value 0.
Content length	The size of the content returned by this site.	KB	Typically the content length returned by a specific URL should be the same across time. Any change in this metric may indicate the need for further investigation.

Chapter 5: Troubleshooting SharePoint Online Monitoring

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



```
1   install-modul
    Install-Module
```

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 following tests do not report metrics, then check whether the SharePoint Online Management Shell has been installed and run on the eG agent:

- Tenant Storage test
- Health Score test
- Site Collections test
- Site Collection Health Checks
- Site Connectivity test
- File Operations test

To perform this check, run Windows PowerShell ISE in the elevated mode, and then type any of the following commands:

Connect-SPOService

Get-SPOSite

Get-SPOUser

If these commands auto-complete - i.e., if Windows lists these commands even before you type them fully - you can conclude that the SharePoint Online Management Shell is properly installed on the eG agent host. On the other hand, if the commands do not auto-complete, then you must proceed to install management shell on the eG agent host. To know how to install, refer to the Section **2.1**.

If the SharePoint 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.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.