

M365 Supplemental Management Pack

Advanced M365 Monitoring using SCOM

Prepared for

1/13/2021

Version 1 Final

Created by

Taylour Blackwell, Brian Zoucha

M365 Supplemental Development Team

Tyson Paul, Stephen McComas, Sean Christie, Jimmy Harper

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft Corp. is strictly prohibited.

Microsoft, Microsoft Active Directory, Microsoft Hyper-V, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other products mentioned that are not trademarks include Microsoft Internet Information Services.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Overview.....	4
Services Monitored	4
M365 Subscription Health	4
Mail Flow (Exchange Online)	5
Licensing	5
SharePoint Online	5
OneDrive for Business	6
Teams.....	6
Prerequisites and Requirements.....	7
Supported Versions of SCOM.....	7
Management Pack Files	7
Support Files.....	7
Service Accounts.....	8
Azure AD Application Registration.....	9
Register a new application using the Azure portal.....	9
Add Credentials	10
Create a new application secret	11
Add Permissions to App Registration	12
Grant Admin Consent	13
Register a new application using PowerShell	15
App Permissions by Management Pack.....	17
All App Permissions – Comprehensive List	18
Watcher Node Preparation	19
Management Pack Configuration.....	21
Deploy the M365 Supplemental management packs	21
Creating a new Management Pack for customizations	21
Discover Watcher Nodes.....	22

Configure Monitoring Workflows on Watcher Nodes	23
M365 Services	23
Exchange Online	25
Licensing	27
SharePoint Online	29
OneDrive	31
Management Pack Contents.....	32
Run as Profiles	32
Library	32
Monitors	32
License	33
Monitors	33
Rules	33
Tasks	33
Mail Flow (ExO).....	34
Monitors	34
Rules	34
Tasks	35
OneDrive for Business.....	35
Monitors	35
Rules	35
Tasks	35
Services (M365 Admin Portal).....	36
Monitors	36
Rules	36
Tasks	36
SharePoint Online.....	36
Monitors	36
Rules	36
Tasks	37

Microsoft Teams.....	37
Monitors	37
Rules	37
Tasks	37
M365 Supplemental Dashboards	37
HTML 5 Dashboards	39
Troubleshooting	41
Basic Troubleshooting	41

Overview

The M365 Supplemental Management Pack includes synthetic transactions that provide an increased level of visibility into the health of the Microsoft 365 environment. Making it the perfect companion to the M365 Admin Portal. We are providing this supplemental management pack for customers who leverage System Center Operations Manager as their monitoring platform. The supplemental management pack described in this document provides a deeper view into the health of the on-premises and cloud environment. The management pack will execute these synthetic transactions from a local point-of-presence (Watcher Node) within the customer network for a comprehensive view of service availability.

Services Monitored

The following Microsoft 365 components are monitored using this supplemental management pack.

M365 Subscription Health

Subscription health state can be affected by and service bulletin or degraded services. Each alert contains additional information in its context: the list of affected services, features and their current status. An incident (and the corresponding alert) is considered as active (and shown in Active Incidents list) if any of the affected services has one of the following states:

- Information Unavailable
- Investigating
- Service Interruption
- Service Degradation
- Restoring Service
- Extended Recovery

If all affected services for the incident are in other states, then the incident (and the alert) is considered as resolved.

Note that each incident also contains “summary” status. In some cases, summary status can be updated to “Service Restored”, but internal status of the affected services is still non-operational. In such situation, the corresponding alert will be considered as active (in other words, service status has higher priority than incident status). When incident information gets updated in the Azure portal, a new alert is raised with the new information.

Mail Flow (Exchange Online)

Exchange Online is your primary cloud service for email and calendaring that helps your users collaborate in ways that do not require real-time chatting or centralized document storage. Exchange Online is how you do individual and small group short-lived communication and scheduling. This monitoring solution includes synthetic transactions that will validate mail flow by sending a test email from a sender mailbox and validating receipt in the receiver mailbox. Performance metrics collected include send duration, receive duration, and total duration of the message transit; all measured in milliseconds.

Exchange Online can be configured in a hybrid deployment, effectively extending your on-premises Exchange Server organization to Exchange Online. While the Exchange Online and Exchange Server organizations are separate, a hybrid deployment gives them a seamless look and feel, facilitating cross-organization mail flow and mailbox migrations from Exchange Server to Exchange Online.

The hybrid Exchange deployment also includes synthetic transactions to validate cross-premises mail flow by sending test email from a sender mailbox and validating delivery to the recipient mailbox.

Licensing

In Microsoft 365, licenses from licensing plans (also called SKUs or Microsoft 365 plans) give users access to the Microsoft 365 services that are defined for those plans. However, a user might not have access to all the services that are available in a license that's currently assigned to them. This solution retrieves the subscription status and monitors the available pool of licenses by percentage consumed.

SharePoint Online

The modern experience in Microsoft SharePoint is designed to be compelling, flexible, and more performant. The modern experience makes it easier for anyone to create beautiful, dynamic sites and pages that are mobile-ready. This guide is a starting point for people familiar with the classic experiences in SharePoint to help you learn about the modern experience and how you can begin to take advantage of it. This solution provides synthetic transactions that validate the ability to upload and download files to specific SharePoint Online sites. Performance metrics collected include upload duration, download duration, and total duration of the file transfers.

OneDrive for Business

OneDrive is the Microsoft cloud service that connects you to all your files. It lets you store and protect your files, share them with others, and get to them from anywhere on all your devices. When you use OneDrive with an account provided by your company or school, it's sometimes called "OneDrive for work or school." It used to be known as "OneDrive for Business," so you may still see it called that in places. This solution provides synthetic transactions that can validate the ability to Upload and download a file to the OneDrive of a test user. Performance metrics collected include upload duration, download duration, and total duration of the file transfers.

Teams

Microsoft Teams is the hub for teamwork in Microsoft 365. The Teams service enables instant messaging, audio and video calling, rich online meetings, mobile experiences, and extensive web conferencing capabilities. In addition, Teams provides file and data collaboration and extensibility features, and integrates with Microsoft 365 and other Microsoft and partner apps.

Microsoft Teams is an entirely new service, built for the cloud from the ground up by leveraging Azure and other service innovations from Microsoft. Microsoft Teams is built on Microsoft 365 groups, Microsoft Graph, and with the same enterprise-level security, compliance, and manageability as the rest of Office 365. Teams leverage identities stored in Azure Active Directory (Azure AD). These services are delivered from Microsoft data centers and are accessible to users on a wide range of devices from inside a corporate network or over the internet.

This solution includes synthetic transactions that can validate the ability to connect to a channel and send a message. Performance collection includes message send duration, message verification duration, and total duration of these activities combined.

Prerequisites and Requirements

The M365 Supplemental Management pack requires a working System Center Operations Manager Management Group as a base. The solution consists of the following elements added to the SCOM environment:

Supported Versions of SCOM

M365 Supplemental Management Pack for System Center Operations Manager is designed for the following versions of System Center Operations Manager:

- System Center Operations Manager 2012 R2
- System Center Operations Manager 2016
- System Center Operations Manager 1807
- System Center Operations Manager 2019

Management Pack Files

- **M365 Supplemental.Library.mpb** : Current version 1.0.1.0
- **M365 Supplemental.License.mpb** : Current version 1.0.1.0
- **M365 Supplemental.License.SkuNames.Addendum.xml** : Current version 1.0.1.0
- **M365 Supplemental.MailFlow.mpb** : Current version 1.0.1.0
- **M365 Supplemental.OneDrive.mpb** : Current version 1.0.1.0
- **M365 Supplemental.Services.mpb** : Current version 1.0.1.0
- **M365 Supplemental.SharePoint.mpb** : Current version 1.0.1.0
- **M365 Supplemental.Teams.mpb** : Current version 1.0.1.0

Support Files

- **Exchange Web Services:** EWS is only used to perform mail flow workflows within the management pack if configured with an Exchange Hybrid environment. For workflows that apply to Exchange (on premises), if no valid path is provided for the Exchange Web Services .DLL (Microsoft.Exchange.WebServices.dll) the management pack will use the included EWS v2.2 .dll.

Service Accounts

This solution utilizes standard user accounts in Azure AD and/or your Local Domain to execute scripted workflows. A set of service accounts is required for on-premises and M365 based monitoring workflows.

Note: This solution currently supports non-federated cloud only accounts for all M365 workloads

- **M365 Mail flow Workflows**
 - An M365 username and password for *sending* email
 - An M365 username and password for *receiving* email
- **M365 Licensing Workflows**
 - An M365 username and password for connecting to and verifying M365 subscriptions.
- **M365 SPO Workflows**
 - An M365 username and password for connecting to SharePoint Online.
- **M365 Teams Workflows**
 - An M365 username and password for connecting to SharePoint Online.
- **M365 OneDrive Workflows**
- An M365 username and password for connecting to SharePoint Online.**On-Premises Workflows**
 - An Exchange username and password for *sending* email
 - An Exchange username and password for *receiving* email



Note: User accounts can be shared across workflows to conserve M365 licenses.

Azure AD Application Registration

This solution requires you to register an application in Azure Active Directory and accounts stored in SCOM to execute scripted workflows within the Management Group. A set of service accounts is required for on-premises and M365 based monitoring workflows.

Register a new application using the Azure portal

1. Sign in to the [Azure portal](#) using either a work or school account or a personal Microsoft account.
2. If your account gives you access to more than one tenant, select your account in the top right corner, and set your portal session to the Azure AD tenant that you want.
3. In the left-hand navigation pane, select the **Azure Active Directory** service, and then select **App registrations > New registration**.
4. When the **Register an application** page appears, enter your application's registration information:
 - **Name** - Enter a meaningful application name that will be displayed to users of the app.
 - **Supported account types** - Select which accounts you would like your application to support.
 - **Redirect URI (optional)** - Select the type of app you are building, **Web** or **Public client (mobile & desktop)**, and then enter the redirect URI (or reply URL) for your application.
5. When finished, select **Register**.


 Microsoft Azure 

Home > Contoso >

Register an application

* Name

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



Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Contoso only - Single tenant)

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


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


☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

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



By proceeding, you agree to the [Microsoft Platform Policies](#) 

Add Credentials

When programmatically signing in, you need to pass the tenant ID with your authentication request and the application ID. You also need a certificate or an authentication key (described in the following section). To get those values, use the following steps:

1. Select **Azure Active Directory**
2. From **App registrations** in Azure AD, select your application.
3. Copy the **Directory (tenant) ID** and store it in your application code. The directory (tenant) ID can also be found in the default directory overview page.

M365 Management Pack



Search (Ctrl+/) << Delete Endpoints Preview features

Overview Quickstart Integration assistant Manage Branding Authentication

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

Essentials

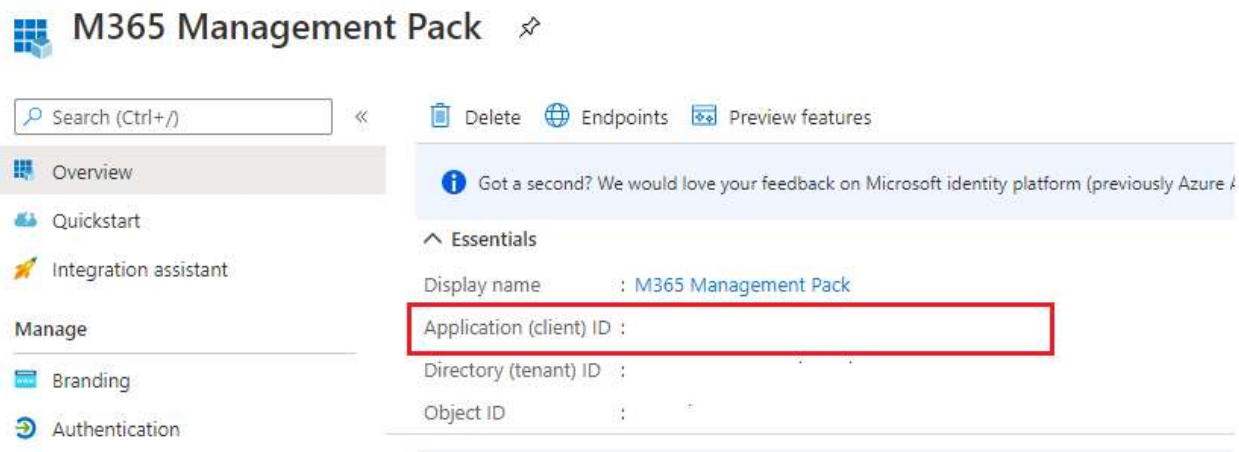
Display name : M365 Management Pack

Application (client) ID :

Directory (tenant) ID :

Object ID :

4. Copy the **Application ID** and store it in your application code.



Search (Ctrl+/) << Delete Endpoints Preview features

Overview Quickstart Integration assistant Manage Branding Authentication

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

Essentials

Display name : M365 Management Pack

Application (client) ID :

Directory (tenant) ID :

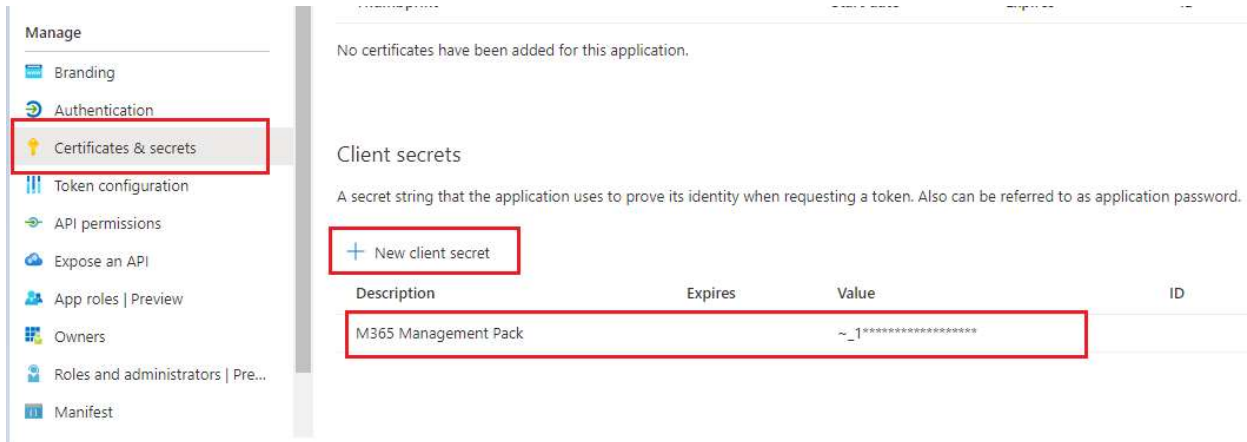
Object ID :

Create a new application secret

If you choose not to use a certificate, you can create a new application secret.

1. Select **Azure Active Directory**.
2. From **App registrations** in Azure AD, select your application.
3. Select **Certificates & secrets**.
4. Select **Client secrets -> New client secret**.
5. Provide a description of the secret, and a duration. When done, select **Add**.

After saving the client secret, the value of the client secret is displayed. Copy this value because you will not be able to retrieve the key later. You will provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it. If the key is ever lost, you can simply return to this page and create a new one.




Add Permissions to App Registration

Once you have registered both your client app, you can configure the client's permissions to the application by following these steps. These steps apply to M365 Supplemental Library, License, Mail Flow, Teams, SharePoint Online, OneDrive and Services Management Packs.

NOTE: For the **M365 Services Supplemental Management Pack** you will need to use **Application Permissions** for all APIs except for the Services MP.

Graph Delegated Permissions(For Library, License, Mail Flow, Teams, SharePoint and OneDrive MPs)


1. Sign in to the [Azure portal](#).
2. If you have access to multiple tenants, use the **Directory + subscription** filter  in the top menu to select the tenant containing your client app's registration.
3. Select **Azure Active Directory** > **App registrations**, and then select your client application.
4. Select **View API permissions** > **Add a permission** > click **Microsoft Graph**.
5. Select **Delegated Permissions**.

Delegated permissions is selected by default. Delegated permissions are appropriate for client apps that access a web API as the signed-in user, and whose access should be restricted to the permissions you select in the next step. Leave **Delegated permissions** selected for this example.

6. Under **Select permissions**, expand the resource whose scopes you defined for your web API, and select the permissions the client app should have on behalf of the signed-in user.
7. Select **Add permissions** to complete the process.

Office 365 Management API Application Permissions

1. Sign in to the [Azure portal](#).

2. If you have access to multiple tenants, use the **Directory + subscription** filter  in the top menu to select the tenant containing your client app's registration.
3. Select **Azure Active Directory** > **App registrations**, and then select your client application.
4. Select **View API permissions** > **Add a permission** > click **Office 365 Management APIs**.
5. Select **Application Permissions**.

Application permissions are for service- or daemon-type applications that need to access a web API as themselves, without user interaction for sign-in or consent. Unless you have defined application roles for your web API, this option is disabled.

6. Under **Select permissions**, expand the resource whose scopes you defined for your web API, and select the permissions the client app should have on behalf of the signed-in user.
7. Select **Add permissions** to complete the process.

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 Contoso AD (dev)					
API / Permissions name	Type	Description	Admin consent req...	Status	
▼ Contoso API 1 (1)					
Employees.Read.All	Delegated	Read-only access to Employee records	-		...
▼ Microsoft Graph (1)					
User.Read	Delegated	Sign in and read user profile	-		...

You might also notice the *User.Read* permission for the Microsoft Graph API. This permission is added automatically when you register an app in the Azure portal.

Grant Admin Consent

Assume you have a web client application that needs to request specific permissions to access a resource/API. You will learn how to do this configuration in the next section, but essentially the Azure portal is used to declare permission requests at configuration time. Like other configuration settings, they become part of the application's Azure AD registration:

M365 Management Pack | API permissions

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**

Refresh | Got feedback?

Configured permissions

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

+ Add a permission

✓ Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (10)			
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes
Directory.Read.All	Delegated	Read directory data	Yes
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes

The following steps show you how the consent experience works for both the application developer and the user.

To consent to an app's delegated permissions

1. Go to the **API permissions** page for your application
2. Click on the **Grant admin consent** button.

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**

Refresh | Got feedback?

Configured permissions

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

+ Add a permission

✓ Grant admin consent for Contoso

API / Permissions name	Type	Description	Admin consent req...
Microsoft Graph (10)			
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes
Directory.Read.All	Delegated	Read directory data	Yes
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes

Important:

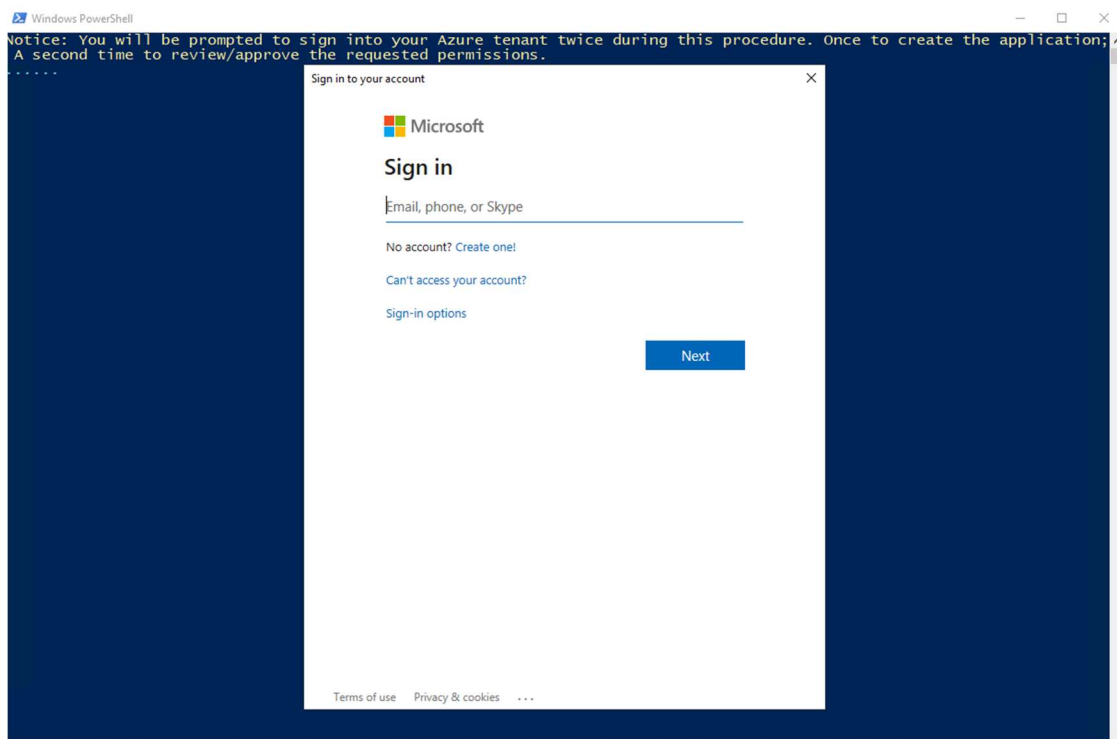
Granting explicit consent using the **Grant permissions** button is currently required for single-page applications (SPA) that use ADAL.js. Otherwise, the application fails when the access token is requested.

Register a new application using PowerShell

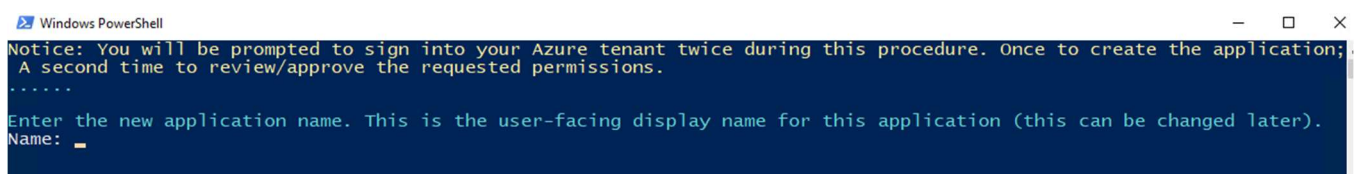
Instead of manually creating the app registration and granting permissions you can run a single script to accomplish all steps. From any computer with the Azure AD PowerShell module installed, you can run the **M365 SCOM MP App Registration.ps1** included in the MP Files.

Running the Script will accomplish the following:

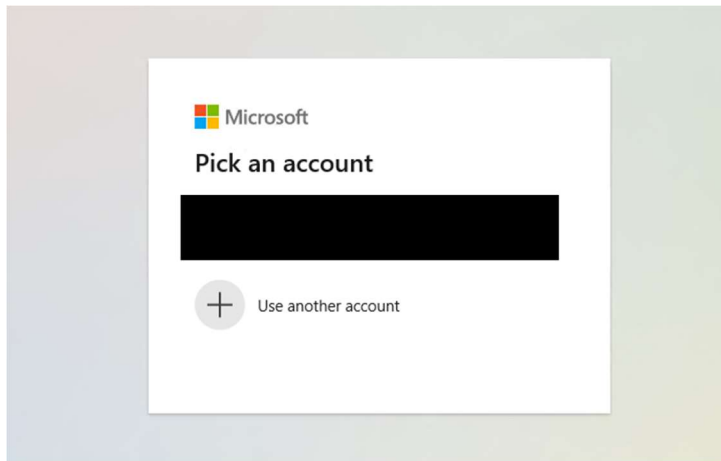
- Create the Application Registration
 - Grant **ALL** the permissions required for each management pack (OneDrive, Exchange, Services, etc).
 - Grant Admin Consent
1. From a computer with the Azure AD PowerShell module installed run the **M365 SCOM MP App Registration.ps1**
 2. Enter your admin account with permissions to generate application registrations and grant admin consent.



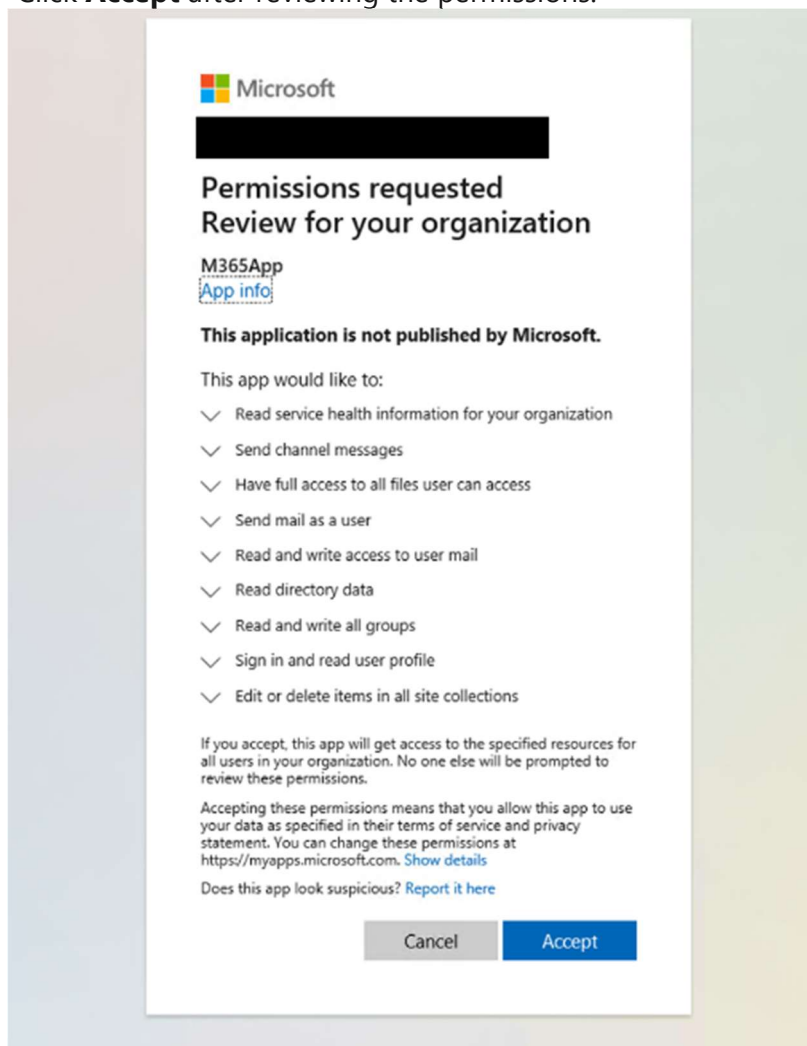
3. Enter a meaningful application name that will be displayed to users of the app and press **Enter**.



4. When prompted for your account either enter credentials again (if required) or select your account from the list.



5. Click **Accept** after reviewing the permissions.



6. **VERY IMPORTANT:** Make note of the Application ID and Client Secret before closing the PowerShell window. You will not be able to view this Secret again.

```
Success!

ApplicationID: [REDACTED] Document this ID for later use

SAVE THIS KEY!! After closing this window you will never be able to retrieve this key again.
ClientSecret: [REDACTED] Document this Secret for later use
Press Enter to continue...: [REDACTED]
```

App Permissions by Management Pack

Library

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (1)			
Directory.Read.All	Delegated	Read directory data	Yes

Mail Flow

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (2)			
Mail.ReadWrite	Delegated	Read and write access to user mail	-
Mail.Send	Delegated	Send mail as a user	-

License

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (1)			
Directory.Read.All	Delegated	Read directory data	Yes

SharePoint

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (2)			
Files.ReadWrite.All	Delegated	Have full access to all files user can access	-
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	-

Services

API / Permissions name	Type	Description	Admin consent required
Office 365 Management APIs (1)			
ServiceHealth.Read	Application	Read service health information for your organization	Yes

Teams

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (2)			
ChannelMessage.Send	Delegated	Send channel messages	-
Group.ReadWrite.All	Delegated	Read and write all groups	Yes

OneDrive

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (2)			
Files.ReadWrite.All	Delegated	Have full access to all files user can access	-
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	-

All App Permissions – Comprehensive List

A complete list of permissions for all workflows is provided below.

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (8)			
ChannelMessage.Send	Delegated	Send channel messages	-
Directory.Read.All	Delegated	Read directory data	Yes
Files.ReadWrite.All	Delegated	Have full access to all files user can access	-
Group.ReadWrite.All	Delegated	Read and write all groups	Yes
Mail.ReadWrite	Delegated	Read and write access to user mail	-
Mail.Send	Delegated	Send mail as a user	-
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	-
User.Read	Delegated	Sign in and read user profile	-
Office 365 Management APIs (1)			
ServiceHealth.Read	Application	Read service health information for your organization	Yes

Watcher Node Preparation

This Management Pack solution requires at least one agent managed computer to execute the scripted workflows. The M365 Supplemental Management Pack supports the following Operating Systems for watcher nodes:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 10

The M365 Supplemental Management Pack requires one or more watcher nodes with the SCOM agent installed to perform synthetic transactions. Once you have identified one or more computers to function as a watcher node you will need to make sure all the components below are installed on every watcher node.

- **SCOM Agent:** This SCOM agent needs to be a member of the SCOM management group that the M365 Supplemental MP is imported on.
- **Exchange Web Services:** Install EWS 2.2 from the following link on the watcher nodes that will run the scripted workflows for Hybrid mail flow environments (only required for hybrid environments):
<https://www.microsoft.com/en-us/download/details.aspx?id=42951>
- For workflows that apply to Exchange (on premises), if no valid path is provided for the

Exchange Web Services .DLL (Microsoft.Exchange.WebServices.dll) the management pack will use the included EWS v2.2 .dll.

Management Pack Configuration

The steps below walk through the process to import and configure the M365 Supplemental Management pack into Operations Manager.

Deploy the M365 Supplemental management packs

Import the M365 Supplemental management pack using the steps below.

1. Log on to the computer with an account that is a member of the **Operations Manager Administrators** role for the Operations Manager management group.
2. In the Operations console, click **Administration**.
3. Right-click the **Management Packs** node, and then click **Import Management Packs**.
4. The **Import Management Packs** wizard opens. Click **Add**, and then click **Add from disk**.
5. The **Select Management Packs** to import dialog box appears. If necessary, change to the directory that holds your management pack file. Select the appropriate M365 Supplemental management packs to import from that directory, and then click **Open**.
6. On the **Select Management Packs** page, the management packs that you selected for import are listed. An icon next to each management pack in the list indicates the status of the selection, click **Import**.
7. The **Import Management Packs** page appears and shows the progress for each management pack. If there is a problem at any stage of the import process, select the management pack in the list to view the status details and take the necessary action to correct the issue. When done select **Close**.

Creating a new Management Pack for customizations

The M365 Supplemental management pack is sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a separate unsealed management pack. As a best practice, you should instead create a separate management pack for each sealed management pack that you want to customize.

1. Open the **Operations Manager** console, and then click **Administration** button.
2. Right-click **Management Packs**, and then click **Create New Management Pack**.
3. Enter a name (for example, **M365 Supplemental Overrides**), and then click **Next**.
4. Click **Create**.

Discover Watcher Nodes

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **Windows Computer** view, click the **Tasks** pane.
3. Select '**M365 Supplemental – Configure Watcher Node Default Settings**'
4. In the **Task Parameters** window the **Default Properties** are displayed.
5. Click **Override**, then in the **Override Task Parameter** window click on the parameters that you want to override.
6. The parameters required to configure the **Watcher Node** are:
 - a. M365_AccountName
 - b. M365_ClientID
 - c. M365_ClientSecret
 - d. M365_Password
 - e. TenantName
7. Click **Override**, select '**Use the predefined Run As Account**' and then click **Run**.
8. The task results should indicate the status of the configuration procedure.

Note: If the default action account on the Watcher Node is not LocalSystem (as is common on a SCOM management server) and there exists no user profile for the action account, you may encounter an error. To correct this error simply log into the Watcher Node with whichever default action account is configured to execute the task. Then run the configuration task again once the user profile exists.
9. Once the **Watcher Node** is discovered you can then begin configuration of the additional monitoring components.

M365 Supplemental – Configure Watcher Node parameters.

Parameter	Default Value	Details
ApiURL	https://graph.microsoft.com	Reference
ApiTokenURL	https://login.microsoftonline.com	Reference
ApiTokenScopeURL	https://graph.microsoft.com/.default	Reference
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the Watcher Node.
TLSVersion	1.2	Default TLS version for all workflows

M365 Supplemental – Configure Watcher Node parameters.

IntervalSeconds	900	This will become the default interval for Watcher Node monitoring workflows as well as the default IntervalSeconds value for subsequent M365 service component configuration tasks.
M365_AccountName	None	Account name used to connect to Microsoft 365
M365_AccountPassword	None	Password used to connect to Microsoft 365
M365_ClientID	None	This value uniquely identifies your application in the Microsoft identity platform.
M365_ClientSecret	None	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.
PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.
TenantName	None	Microsoft 365 Tenant name

Configure Monitoring Workflows on Watcher Nodes

The M365 Supplemental Management pack provides the ability to monitor only targeted or selected services.

M365 Services

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **M365 Supplemental** view, click the **M365 Watcher Nodes** state view.
3. Select '**M365 Supplemental – Configure Services**'

4. In the **Task Parameters** window the review the default parameter values.
5. If needed, you may customize any of these values but it is not necessary.
6. The following parameters are inherited from the **Watcher Node** class and do not need to be modified:
 - a. M365_ClientID
 - b. M365_ClientSecret
 - c. IntervalSeconds
7. If you wish to exclude specific services from being discovered, you can provide a comma-separated list of service IDs in the **ExcludeServiceID** parameters.
Example: DynamicsCRM,Sway,OrgLiveID
8. Click **Override**, select '**Use the predefined Run as Account**' and then click **Run**.
9. Upon successful configuration of the **M365 Services** you will be see the results in the Tasks Status window.
10. Once the discovery is complete, check the **M365 Supplemental - Services** state view.

M365 Supplemental – Configure Services parameters.

Parameter	Default Value	Details
MgmtApiURL	https://manage.office.com	Reference
MgmtApiTokenURL	https://login.windows.net	Reference
MgmtApiTokenScopeURL	https://manage.office.com	Reference
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the Watcher Node
ExcludeServiceID	None	You can choose any number of services to exclude from being discovered, provide the IDs of the services in a comma separated list.
IntervalSeconds*	900	Default interval for monitoring workflows. .
M365_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform.
M365_ClientSecret	Inherited	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.
PoshLibraryPath	5 Sec	For support engineer use only.

M365 Supplemental – Configure Services parameters.

WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.

Exchange Online

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **M365 Supplemental** view, click the **M365 Watcher Nodes** state view.
3. Select '**M365 Supplemental – Configure Mailflow**'
4. In the **Task Parameters** window the default parameter values are displayed.
5. The following parameters are inherited from the **Watcher Node** class. If needed, you may customize any of these values but it is not necessary:
 - a. M365_AccountName
 - b. M365_ClientID
 - c. M365_ClientSecret
 - d. M365_Password
 - e. IntervalSeconds
6. These additional parameters are required to configure mail flow for Hybrid and/or Exchange Online (M365):
 - a. M365_SenderEmailAddress
 - b. M365_SenderPassword
 - c. M365_ReceiverEmailAddress
 - d. M365_ReceiverPassword
 - e. Exchange_SenderEmailAddress
 - f. Exchange_SenderPassword
 - g. Exchange_ReceiverEmailAddress
 - h. Exchange_ReceiverPassword
 - i. ExchangeURL
7. Click **Override**, select '**Use the predefined Run As Account**' and then click **Run**.
8. Upon successful configuration of the **M365 Mailflow** you will be seeing the results in the Tasks Status window.

- Once the discovery is complete, check the **M365 Supplemental - Mailflow** state view.

M365 Supplemental – Configure Mail Flow parameters.

Parameter	Default Value	Details
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the Watcher Node
IntervalSeconds	900	Default interval for monitoring workflows.
M365_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform
M365_ClientSecret	Inherited	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.
PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.
ExchangeURL	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment. If you have no Exchange (on premises) leave blank.
M365_SenderEmailAddress	None	M365 Sender Address
M365_SenderPassword	None	M365 Sender Password
M365_ReceiverEmailAddress	None	M365 Receiver Address
M365_ReceiverPassword	None	M365 Receiver Password
M365_TotalDurationCriticalSeconds	120	Threshold at which the 'TotalDuration' measurement will cause a Critical state.
M365_TotalDurationWarningSeconds	60	Threshold at which the 'TotalDuration' measurement will cause a Warning state.
Exchange_SenderEmailAddress	None	On-Prem Exchange Sender Address
Exchange_SenderPassword	None	On-Prem Exchange Password
Exchange_ReceiverEmailAddress	None	On-Prem Exchange Receiver Address

M365 Supplemental – Configure Mail Flow parameters.

Exchange_ReceiverPassword	None	On-Prem Exchange Password
Exch_TotalDurationCriticalSeconds	180	Threshold at which the 'TotalDuration' measurement will cause a Critical state.
Exch_TotalDurationWarningSecond	120	Threshold at which the 'TotalDuration' measurement will cause a Critical state.

Licensing

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **M365 Supplemental** view, click the **M365 Watcher Nodes** state view.
3. Select '**M365 Supplemental – Configure Licensing**
4. In the **Task Parameters** window the **Default Properties** are displayed.
5. The following parameters are inherited from the **Watcher Node** class. If needed, you may customize any of these values but it is not necessary:
 - a. M365_AccountName
 - b. M365_ClientID
 - c. M365_ClientSecret
 - d. M365_Password
 - e. IntervalSeconds
6. Click **Override**, select '**Use the predefined Run as Account**' and then click **Run**.
7. Upon successful configuration of the **M365 Licensing** you will be seeing the results in the Tasks Status window.
8. Once the discovery is complete, check the **M365 Supplemental – License** state view.

M365 Supplemental – Configure License parameters.

Parameter	Default Value	Details
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the Watcher Node
IntervalSeconds	900	Default interval for monitoring workflows.
M365_AccountName	Inherited	Account name used to connect to Microsoft 365
M365_AccountPassword	Inherited	Password used to connect to Microsoft 365

M365 Supplemental – Configure License parameters.

M365_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform
M365_ClientSecret	Inherited	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.
PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.

Teams

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **M365 Supplemental** view, click the **M365 Watcher Nodes** state view.
3. Select '**M365 Supplemental – Configure Teams**
4. In the **Task Parameters** window the **Default Properties** are displayed.
5. The following parameters are inherited from the **Watcher Node** class. If needed, you may customize any of these values but it is not necessary:
 - a. M365_AccountName
 - b. M365_ClientID
 - c. M365_ClientSecret
 - d. M365_Password
 - e. IntervalSeconds
6. Additional parameters are required to configure Teams monitoring:
 - a. TeamName
Example: monitoringguys
 - b. ChannelName
Example: General
7. Click **Override**, select '**Use the predefined Run As Account**' and then click **Run**.
8. Upon successful configuration of **M365 Teams** you will be see the results in the Tasks Status window.
9. Once the discovery is complete, check the **M365 Supplemental – Teams** state view.

M365 Supplemental – Configure Teams parameters.

Parameter	Default Value	Details
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the WatcherNode
IntervalSeconds	900	Default interval for monitoring workflows.
M365_AccountName	Inherited	Account name used to connect to Microsoft 365 Teams
M365_AccountPassword	Inherited	Password used to connect to Microsoft 365 Teams
M365_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform
M365_ClientSecret	Inherited	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.
PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.
ChannelName	None	M365 Services Teams Channel Name
TeamName	None	M365 Services Team Name

SharePoint Online

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **M365 Supplemental** view, click the **M365 Watcher Nodes** state view.
3. Select '**M365 Supplemental – Configure SharePoint**
4. In the **Task Parameters** window the **Default Properties** are displayed.
5. The following parameters are inherited from the **Watcher Node** class. If needed, you may customize any of these values but it is not necessary:
 - a. M365_AccountName
 - b. M365_ClientID

- c. M365_ClientSecret
- d. M365_Password
- e. IntervalSeconds
- 6. Additional parameters are needed to configure SharePoint Online monitoring
 - a. SiteName

Note: This is the display name of the site as it appears in the online portal.
- 7. Click **Override**, select '**Use the predefined Run As Account**' and then click **Run**.
- 8. Upon successful configuration of **M365** SharePoint you will be see the results in the Tasks Status window.
- 9. Once the discovery is complete, check the **M365 Supplemental – SharePoint** state view.

M365 Supplemental – Configure SharePoint parameters.

Parameter	Default Value	Details
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the WatcherNode
IntervalSeconds	900	Default interval for monitoring workflows.
M365_AccountName	Inherited	Account name used to connect to Microsoft 365 SharePoint
M365_AccountPassword	Inherited	Password used to connect to Microsoft 365 SharePoint
M365_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform
M365_ClientSecret	Inherited	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.
PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.
SiteName	None	SharePoint Online Site Name

OneDrive

1. Open the **Operations Manager** console, and then click **Monitoring**.
2. Open the **M365 Supplemental** view, click the **M365 Watcher Nodes** state view.
3. Select '**M365 Supplemental – Configure OneDrive**
4. In the **Task Parameters** window the **Default Properties** are displayed.
5. The following parameters are inherited from the **Watcher Node** class. If needed, you may customize any of these values but it is not necessary:
 - a. M365_AccountName
 - b. M365_ClientID
 - c. M365_ClientSecret
 - d. M365_Password
 - e. IntervalSeconds
6. Click **Override**, select '**Use the predefined Run as Account**' and then click **Run**.
7. Upon successful configuration of **M365** OneDrive you will be see the results in the Tasks Status window.
8. Once the discovery is complete, check the **M365 Supplemental – OneDrive** state view.

M365 Supplemental – Configure OneDrive parameters.

Parameter	Default Value	Details
DeleteConfiguration	False	Setting this parameter to True will remove the configuration from the Watcher Node
IntervalSeconds	900	Default interval for monitoring workflows.
M365_AccountName	Inherited	Account name used to connect to Microsoft 365 OneDrive
M365_AccountPassword	Inherited	Password used to connect to Microsoft 365 OneDrive
M365_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform
M365_ClientSecret	Inherited	The client secret, known also as an application password, is a string value your app can use in place of a certificate to identity itself.

M365 Supplemental – Configure OneDrive parameters.

PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	300	Timeout value in seconds for Write Action to complete
WritetoEventLog	True	Enable/Disable logging to the Application event log.

Management Pack Contents

Run as Profiles

- Included in the M365 Supplemental Library management pack is a single Run As security profile. It is not necessary to configure this profile with any account. All necessary credentials become stored in the Watcher Node registry as encrypted values upon running the service component configuration task. **M365 Supplemental Library Default RunAs Profile**
 - All monitoring workflows reference this security profile however it is not required to provide a RunAs account.

Library

Monitors

- **M365 – Directory Percent Usage Quota Monitor**
 - Monitors the percent of directory quota used.
- **M365 - Application Secret Expiration Monitor**
 - Monitors the application status. Will alert if app expiration date is near.

Rules

- **M365 Supplemental - Application Nearest Expiration (Days)**

Will identify the application with the earliest expiration date and collect the days remaining, even if the expiration date has already passed; the value collected will be negative.

- **M365 Supplemental - Directory Percent Usage**
Will collect the percentage of tenant directory space consumed.

Tasks

- **M365 Supplemental – Configure Watcher Node Default Settings**
 - This task will store the default tenant settings in the registry of the Watcher Node. Many of these values will become the default parameter values for subsequent component configuration tasks.

License

Monitors

- **M365 License - Status Monitor**
 - Monitor the M365 subscription status for active/valid status.
- **M365 License - Active Units (Percent) Monitor**
 - Monitor license SKU usage by percentage (%)

Rules

- **M365 License - Licenses Available (Units) Performance Collection Rule**
 - Licenses available units
- **M365 License - Licenses Consumed (%) Performance Collection Rule**
 - Licenses consumed by %
- **M365 License - Download Sku DisplayNames to CSV Timed Rule**
 - At the time of this writing, License objects do not contain friendly display name information. This workflow will attempt to download display names from the Microsoft documents website to be stored locally in a CSV file. The license discovery workflow will use these display names only if the file exists.

Tasks

- **M365 Supplemental – Configure License**
 - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.
- **M365 Supplemental – Write LicenseSku DisplayNames to CSV**
 - This task is included in the SkuNames Addendum management pack. It allows you to customize the M365 SKUs display names if the automatic download rule cannot run successfully.

Mail Flow (ExO)

Monitors

- **M365 MailFlow - ExchangeOnline (M365 to M365) Monitor**
 - This monitor sends a test message between M365 and M365 then logs into the account specified and verifies receipt of the email from the Sender.
- **M365 MailFlow - ExchangeHybrid (Exchange to M365) Monitor**
 - This monitor sends a test message between Exchange and M365 then logs into the account specified and verifies receipt of the email from the Sender.
- **M365 MailFlow - ExchangeHybrid (M365 to Exchange) Monitor**
 - This monitor sends a test message between M365 and Exchange then logs into the account specified and verifies receipt of the email from the Sender.

Rules

- **M365 MailFlow - ExchangeOnline (M365 to M365) Message Send/Receive TotalDuration (ms) Performance Collection Rule**
 - Message send/receive total duration in MS
- **M365 MailFlow - ExchangeHybrid (Exchange to M365) Message Send Duration (ms) Performance Collection Rule**
 - Message send duration in MS
- **M365 MailFlow - ExchangeOnline (M365 to M365) Message Send Duration (ms) Performance Collection Rule**
 - Message send duration in MS
- **M365 MailFlow - ExchangeOnline (M365 to M365) Message Receive Duration (ms) Performance Collection Rule**
 - Message receive duration in MS
- **M365 MailFlow - ExchangeHybrid (Exchange to M365) Message Send/Receive Duration (ms) Performance Collection Rule**
 - Message send/receive duration in MS
- **M365 MailFlow - ExchangeHybrid (Exchange to M365) Message Receive Duration (ms) Performance Collection Rule**
 - Message receive duration in MS
- **M365 MailFlow - ExchangeHybrid (M365 to Exchange) Message Send/Receive Duration (ms) Performance Collection Rule**
 - Message send/receive duration in MS
- **M365 MailFlow - ExchangeHybrid (M365 to Exchange) Message Send Duration (ms) Performance Collection Rule**

- Message send duration in MS
- **M365 MailFlow - ExchangeHybrid (M365 to Exchange) Message Receive Duration (ms) Performance Collection Rule**
 - Message receive duration in MS

Tasks

- **M365 Supplemental – Configure MailFlow**
 - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.

OneDrive for Business

Monitors

- **M365 OneDrive - Folder Read/Write Synthetic Test Monitor**
 - Synthetic transaction monitor that uploads and downloads a file to a OneDrive folder.

Rules

- **M365 OneDrive - Synthetic Test File Upload Duration Performance Collection Rule**
 - Upload duration in MS
- **M365 OneDrive - Synthetic Test File Upload/Download Total Duration Performance Collection Rule**
 - Collects file Upload/Download Total Duration in MS
- **M365 OneDrive - Synthetic Test File Download Duration Performance Collection Rule**
 - Download duration in MS

Tasks

- **M365 Supplemental – Configure OneDrive**
 - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.

Services (M365 Admin Portal)

Monitors

- **M365 Services - Status Monitor**
 - Monitors M365 Service Status

Rules

- **M365 Services - Incident Message Alert Rule**
 - Will raise a critical alert for M365 Services incidents.

Tasks

- **M365 Supplemental – Configure Services**
 - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.

SharePoint Online

Monitors

- **M365 SharePoint - Site Read/Write Synthetic Test Monitor**
 - This monitor logs into SPO using the SPO Profile and creates a test file. It then logs into the account specified in the SPO Profile and verifies the file is in the specified folder.

Rules

- **M365 SharePoint - Synthetic Test File Download Duration Performance Collection Rule**
 - Download duration in MS
- **M365 SharePoint - Synthetic Test File Upload/Download Total Duration Performance Collection Rule**
 - Upload/Download Total duration in MS
- **M365 SharePoint - Synthetic Test File Upload Duration Performance Collection Rule**
 - Upload duration in MS

Tasks

- **M365 Supplemental – Configure SharePoint**
 - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.

Microsoft Teams

Monitors

- **M365 Teams - Send Message Synthetic Test Monitor**
 - Synthetic transaction to validate ability to post a message, then verify that message by posting a reply.

Rules

- **M365 Teams - Synthetic Test Channel MessageReply Duration Performance Collection Rule**
 - Duration of reply activity.
- **M365 Teams - Synthetic Test Channel SendMessage Total Duration Performance Collection Rule**
 - Total duration of send and reply activities.
- **M365 Teams - Synthetic Test Channel MessageSend Duration Performance Collection Rule**
 - Duration of send activity.




Tasks

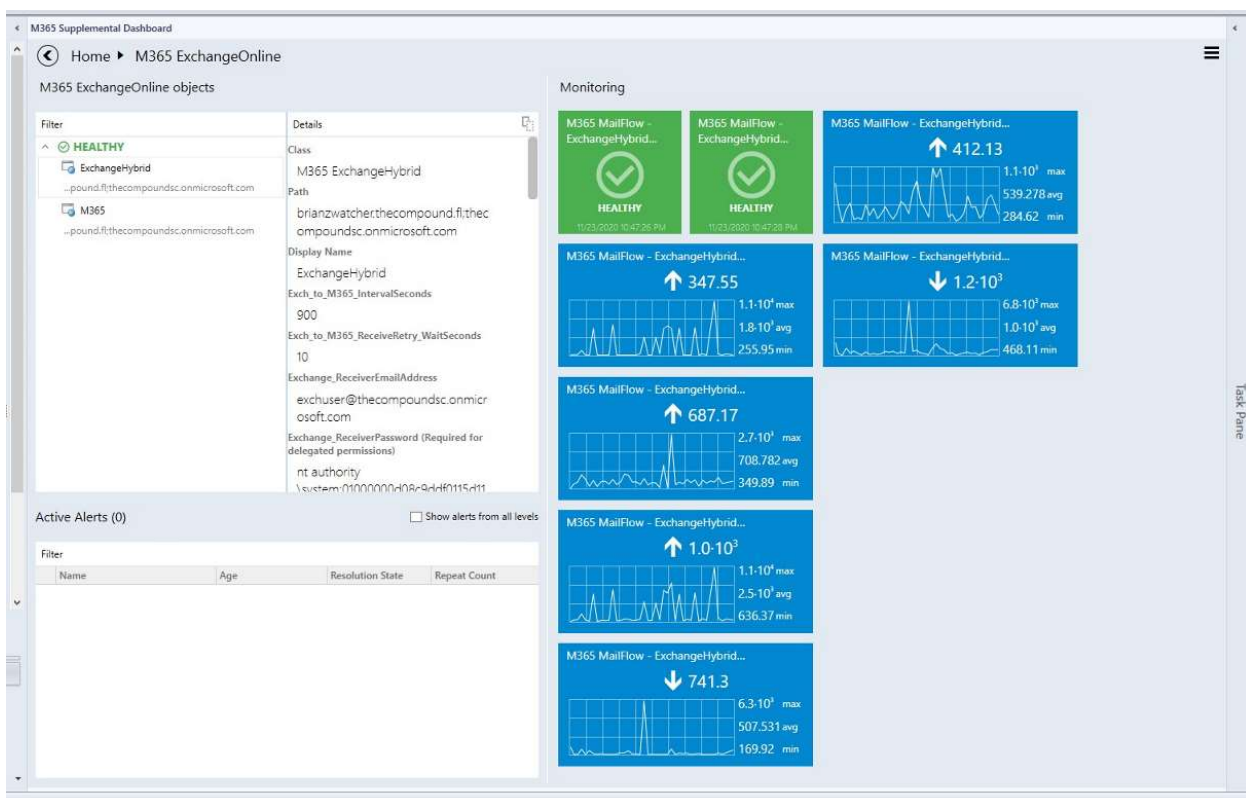
- **M365 Supplemental – Configure Teams**
 - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.

M365 Supplemental Dashboards

This dashboard allows you to create an overarching look at the Office 365 workflows from a single pane. This dashboard is not shipped with the Management Pack but can be easily created leveraging the SQL Server Dashboards template.

1. Create a new **unsealed MP** for the **Dashboard**, you can use the same MP that you stored your overrides in when enabling the Performance Counters, Monitors and Rules.

2. Click the **Monitoring Pane**, right click the folder for your new unsealed MP and choose **New Dashboard View**.
3. In the **New Dashboard and Widget Wizard** click **SQL Server Dashboards**, then choose **Datacenter Dashboard template**.
4. Provide a **Name** for your new Dashboard on the **General Properties** page, click **Next**
5. Click **Create** on the **Summary** page, then click **Close** on the **Completion** page.
6. In the dashboard pane, in the upper **right-hand** corner click the  to create a **Group**.
7. Select **Add Virtual Group**, choose a **Display Name** and then select the **M365 Exchange Online** class and click **Add**
8. Double Click the Group, then choose  from the upper right-hand corner and select **Add Performance Tile**, select and Add the related Monitor.
9. **Select 2x1** size for your Performance Tile
10. Click the  and choose **Add Monitor Tile**, you add **M365 Mail Flow** monitors.
11. You can also choose **Bulk Add tiles** and all the workflows targeted to that class will appear.
12. You can then select the ones you wish to have displayed for the **Virtual Group**.



HTML 5 Dashboards

Many of the prebuilt dashboards are available and functioning natively in the HTML5 console. These instructions assist in creating an executive dashboard with an overarching look at the Office 365 workflows from a single pane. This dashboard is not shipped with the Management Pack but can be easily created leveraging the HTML5 console.

1. Create a new **unsealed MP** for the **Dashboard**, you can use the same MP that you stored your overrides in when enabling the Performance Counters, Monitors and Rules.
2. Open the HTML5 console.
3. Click the **New Dashboard** on the HTML5 console.
4. In the **New Dashboard Wizard** provide a **Name** for your new Dashboard and **Select** the MP to store the dashboard, click **Save**.
5. Click **Add widget** on the **Dashboard** page.
6. From the drop-down menu **Select** State Widget.
7. Under Scope enter **M365 Services Class (abstract)** for the class.
8. **Expand** Criteria and leave the defaults.
9. **Expand** Display, From the select columns to display drop down choose the following.
 1. Health
 2. Display Name
 3. Tenant Name
10. **Expand** Completion, Enter a name for your widget.
11. **Click** Save.
12. Click **Add widget** on the **Dashboard** page.
13. From the drop-down menu **Select** Alert Widget.
14. Under Scope **enter** *M365SL WatcherNode Computers Instances Group* for the group.
15. **Expand** Criteria and leave the defaults.
16. **Expand** Display, From the select columns to display drop down choose the following.
 1. Age
 2. Created
 3. Name
 4. Repeat Count
 5. Severity
 6. Source
17. **Expand** Completion, Enter a name for your widget.
18. **Click** Save.
19. Click **Add widget** on the **Dashboard** page.
20. From the drop-down menu **Select** Topology Widget.
21. Under Scope **enter** *M365 Supplemental Service Monitoring Watcher Node* for the class.
22. **Expand** Display, Select or upload your desired image.
23. **Expand** Completion, Enter a name for your widget.
24. **Click** Save.

M365 Executive


Add widget
Edit dashboard
Delete dashboard
View in fullscreen

Service Health (44)

Filter by keyword

Health	Display name	TenantName
OneDrive for Business		monitoringguysonmicrosoft.com
Mobile Device Management for Office 365		gov961526.onmicrosoft.com
Power BI		gov961526.onmicrosoft.com
Exchange Online		monitoringguysonmicrosoft.com
Dynamics 365		monitoringguysonmicrosoft.com
Azure Information Protection		monitoringguysonmicrosoft.com
Sway		monitoringguysonmicrosoft.com
Microsoft Power Automate		monitoringguysonmicrosoft.com
SharePoint Online		gov961526.onmicrosoft.com
Microsoft 365 suite		monitoringguysonmicrosoft.com
Planner		gov961526.onmicrosoft.com
Power BI		monitoringguysonmicrosoft.com
Microsoft Forms		monitoringguysonmicrosoft.com
Office for the web		gov961526.onmicrosoft.com
Microsoft Teams		monitoringguysonmicrosoft.com
SharePoint Online		monitoringguysonmicrosoft.com
Microsoft Power Automate in Microsoft 365		gov961526.onmicrosoft.com
Exchange Online		gov961526.onmicrosoft.com
Yammer Enterprise		monitoringguysonmicrosoft.com
Office for the web		monitoringguysonmicrosoft.com
Skype for Business		monitoringguysonmicrosoft.com
Azure Information Protection		gov961526.onmicrosoft.com
Mobile Device Management for Office 365		monitoringguysonmicrosoft.com
Planner		monitoringguysonmicrosoft.com
Microsoft Stream		gov961526.onmicrosoft.com

Watcher Node Status



M365 Alerts (17)

Filter by keyword

Sever	Source	Name	Age	Repeat count	Last modified	Created
Exchange Online		M365 Services - Incident Message Alert Rule	1 days, 0 hours	0	1/12/2021, 10:11:37 AM	1/12/2021, 10:11:37 AM
Microsoft 365 suite		M365 Services - Incident Message Alert Rule	6 days, 4 hours	0	1/7/2021, 6:10:53 AM	1/7/2021, 6:10:53 AM
Microsoft 365 suite		M365 Services - Incident Message Alert Rule	1 days, 0 hours	0	1/12/2021, 10:11:37 AM	1/12/2021, 10:11:37 AM
VS-M365-Watch-1.L4y3R8JINT		Power Shell Script failed to run	5 days, 10 hours	2	1/8/2021, 12:51:56 AM	1/8/2021, 12:06:56 AM
OneDrive for Business		M365 Services - Incident Message Alert Rule	3 minutes, 27 seconds	0	1/13/2021, 10:45:39 AM	1/13/2021, 10:45:39 AM
Planner		M365 Services - Incident Message Alert Rule	14 hours, 52 minutes	0	1/12/2021, 7:56:40 PM	1/12/2021, 7:56:40 PM
SharePoint Online		M365 Services - Incident Message Alert Rule	48 minutes, 27 seconds	0	1/13/2021, 10:00:39 AM	1/13/2021, 10:00:39 AM
Microsoft Teams		M365 Services - Incident Message Alert Rule	2 hours, 33 minutes	0	1/13/2021, 8:15:38 AM	1/13/2021, 8:15:38 AM

Troubleshooting

This solution is powered by a custom management pack consisting of multiple workflows and Run as Profiles used to execute scripts programmatically to monitor mail flow and licensing. This provides additional insight regarding the health of an organizations email infrastructure.

Basic Troubleshooting

In order to diagnose connectivity or the ability to execute the scripted workflows from the Watcher Nodes we first need to verify that all modules have been installed and we can programmatically connect outside of System Center Operations Manager, this will help us rule out any basic configuration issues.

1. Check the **Operations Manager Event Log** on the **Watcher Node**, filter events ranging from 9990-9995. This is the default logging for all M365 Supplemental workflows.
2. **M365 Connectivity** from the **Watcher Node** can be verified using the following PowerShell code and the steps below.
 - a. Open **Windows PowerShell ISE** on the **Watcher Node**.
 - b. Press **Ctrl+N** for a new session. **Copy and Paste** the code sample below into the new session
 - c. **Change** the **<username>** and **<password>** credentials that you want to test connectivity with so that they match your subscription, Administrator credentials are not needed. A standard user account will work. You must also provide the **Client ID** and **Client Secret** from the **Service Principal** (App Registration) that you created previously.
 - d. **Press F5** to execute the code snippet, when connected successfully you will be returned to the PowerShell ISE prompt.
 - e. Once complete you should have received a token response.

```
# Begin Tshooting Sample
#####
# These will need to be changed based on Tenant (Commercial, GCC HIGH, DOD)
# https://docs.microsoft.com/en-us/graph/deployments#microsoft-graph-and-graph-
explorer-service-root-endpoints
#####

$Graph = "https://graph.microsoft.com"
$GraphScope = "https://graph.microsoft.com/.default"
$LoginURL = "https://login.microsoftonline.com"

#####

$Username = "<username>@<tenant>.onmicrosoft.com"
$Password = "<password>"
$TenantName = "<tenantname>.onmicrosoft.com"
$ClientID = "<ClientID>"
$ClientSecret = "<ClientSecret>"

$ReqTokenBody = @{
Grant_Type = "password"
```

```
Scope          = $GraphScope
client_Id      = $clientID
Client_Secret  = $clientSecret
Password= $password
Username= $username
}

$TokenResponse = Invoke-RestMethod -Uri "$LoginURL/$TenantName/oauth2/v2.0/token" -
Method POST -Body $ReqTokenBody
return $TokenResponse

#####
# End Tshooting Sample
```

3. If you wish to retire or decommission a watcher node, you can remove the watcher node by using the **M365 Supplemental – Configure Watcher Node Default Settings** task.
 - a. Locate the **Watcher Node** in the **Windows Computer** View in the Operations Manager Console
 - b. Select the **M365 Supplemental – Configure Watcher Node Default Settings** task from the Task Pane
 - c. Click **Override**, then select **DeleteConfiguration** and set the Value to **True**
 - d. You will also need to provide your **TenantName**.
 - e. Once complete click **Override**, then click **Run**.
4. In most cases the default logging is more than sufficient to diagnose issues with connectivity and even basic workflow diagnostics. In order to provide additional diagnostic information, we have included additional workflow logging that can be enabled for the scripted workflows via override.
 - a. Locate the workflow (Monitor or Rule) that you wish to diagnose, right-click and choose **Properties**.
 - b. Select the **Overrides Tab**, click **Override**.
 - c. Choose **For the object**, the **Override Properties** window will open
 - d. Under **Override-Controlled** parameters, select **WriteToEventLog**
 - e. Change the **Override** value to **True**
 - f. Select a destination **Management Pack** for the override
 - g. Click **Apply**, then click **Ok**.
 - h. Check the **Application Event Log** on the **Watcher Node**, filter events ranging from 9990-9999.