



# M365 Services Supplemental Monitoring Management Pack Guide

## Advanced M365 Monitoring using SCOM

*Prepared for*

12/14/2021

Version 2

*Created by*

**Taylor Blackwell, Brian Zoucha**

*M365 Supplemental Development Team*

**Tyson Paul, Stephen McComas, Jimmy Harper, Dan Reist**

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 .....	5
Teams .....	6
Prerequisites and Requirements.....	7
Supported Versions of SCOM.....	7
Management Pack Files .....	7
Support Files.....	7
PowerShell.....	8
M365 Licensing.....	8
Service Accounts.....	9
Security Considerations.....	10
Network, Firewall, Proxy .....	12
Manually edit the agent proxy configuration file .....	12
Azure AD Application Registration.....	13
Register a New Application Using the Azure Portal.....	13
Add Credentials .....	14
Create a New Application Secret.....	15
Add permissions to app registration.....	16
Grant admin consent .....	16
Register a New Application Using PowerShell .....	18
App Permissions by Management Pack.....	21
All App Permissions – Comprehensive List .....	22

Watcher Node Preparation .....	23
Management Pack Configuration .....	24
Import the M365 Supplemental Management Packs .....	24
Creating a new Management Pack for Customizations .....	24
Discover Watcher Nodes .....	24
Configure Monitoring Workflows on Watcher Nodes .....	26
M365 Services .....	26
Exchange Online .....	28
Licensing .....	30
SharePoint Online .....	32
OneDrive .....	34
Management Pack Contents.....	35
Run as Profiles .....	35
Library .....	35
Monitors .....	35
License .....	36
Monitors .....	36
Rules .....	36
Tasks .....	37
Mail Flow (ExO).....	37
Monitors .....	37
Rules .....	38
Tasks .....	39
OneDrive for Business.....	39
Monitors .....	39
Rules .....	40
Tasks .....	40
Services (M365 Admin Portal) .....	40
Monitors .....	40
Rules .....	40

Tasks	41
SharePoint Online.....	41
Monitors .....	41
Rules .....	41
Tasks .....	42
Microsoft Teams.....	42
Monitors .....	42
Rules .....	43
Tasks .....	43
M365 Supplemental Dashboards.....	44
HTML 5 Dashboards.....	45
PowerBI Dashboard.....	47
Troubleshooting.....	49
Basic Troubleshooting.....	49
Event Logs.....	49
Script Test.....	49
Watcher Node Removal.....	50
License Display Names.....	51

## Overview

The M365 Supplemental Management Pack includes synthetic transactions that provide an increased level of visibility into the health and performance of the Microsoft 365 environment making it the perfect companion to the M365 Admin Portal. The synthetic transactions will be executed from a local point-of-presence (Watcher Node) within the customer network for a comprehensive view of service availability and performance.

## Services Monitored

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

### M365 Subscription Health

Subscription health state can be affected by degraded services.

All M365 services which are available to your subscription are monitored for status. The service status in the SCOM Console will be a direct reflection of what appears in the M365 Admin Portal. Service health is determined by the category of the status as listed below.

HEALTHY	WARNING	CRITICAL
falsePositive	investigating	confirmed
mitigated	investigationSuspended	extendedRecovery
mitigatedExternal	postIncidentReviewPublished	restoringService
serviceOperational	reported	serviceDegradation
serviceRestored	verifyingService	serviceInterruption
resolved		unknownFutureValue
resolvedExternal		

Every unhealthy service will have one or more associated incidents (or advisories) which will contain detailed information about the issue. Every time this information is updated by Microsoft in the M365 Admin Portal, a corresponding alert will appear in the SCOM Console with the new information. The criteria for the alert rules are highly customizable.

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. 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. This solution provides synthetic transactions that monitor the ability to upload and download files and related performance. 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 monitor the ability to upload and download a file to OneDrive and related performance. 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 monitor the functionality and performance of channel messaging, user-to-user chat, calendar/event scheduling, and presence detection. Performance collections exist for all of the above.



## 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

Management Pack File	Version
M365.Supplemental.Library.mpb	2.0.0.0
M365.Supplemental.License.mpb	2.0.0.0
M365.Supplemental.License.SkuNames.Addendum.xml	2.0.0.0
M365.Supplemental.MailFlow.mpb	2.0.0.0
M365.Supplemental.OneDrive.mpb	2.0.0.0
M365.Supplemental.Services.mpb	2.0.0.0
M365.Supplemental.SharePoint.mpb	2.0.0.0
M365.Supplemental.Teams.mpb	2.0.0.0

### Support Files

- **Exchange Web Services:** EWS is only used to perform mail flow workflows 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) during MailFlow configuration the management pack will use the included EWS v2.2.dll.

## PowerShell

PowerShell version 5.0 or higher is required for all workflows in this management pack set.

## M365 Licensing

The following license components must be enabled for the SCOM M365 monitoring account:

- Exchange Online
- Microsoft Teams
- SharePoint

The following license component must be enabled for the SCOM M365 monitoring ChatPartner account:

- Microsoft Teams

## Service Accounts

This solution utilizes standard user accounts in Azure AD and/or your Local Domain to execute scripted 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
- **M365 SPO Workflows**
  - An M365 username and password
- **M365 Teams Workflows**
  - An M365 username and password for executing Teams workflows.
  - A 2<sup>nd</sup> M365 username (no password is needed) for executing Chat workflows. This account must be different than the account listed above and must also be licensed for Teams.
- **M365 OneDrive Workflows**
  - An M365 username and password
- **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.

Example: one M365 account can be used for all M365 workflows (except for the Teams ChatPartner).

## Security Considerations

This management pack leverages PowerShell to perform synthetic transactions to test functionality and measure performance of various M365 services: OneDrive, Teams, Licensing, etc. The synthetic transactions are conducted through Microsoft Graph API, a RESTful web API that enables programmatic access to Microsoft Cloud service resources. This programmatic access requires a registered App in Azure Active Directory and that registration must be assigned specific permissions. Microsoft Graph exposes granular permissions that control the access that apps have to resources, like users, groups, and mail. Microsoft Graph has two types of [permissions](#): "Application" and "Delegated". It's important to understand the differences.

**Delegated permissions** are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests and the app can act as the signed-in user when making calls to Microsoft Graph. Some delegated permissions can be consented by non-administrative users, but some higher-privileged permissions require administrator consent.

**Application permissions** are used by apps that run without a signed-in user present. For example, apps that run as background services or daemons. Application permissions can only be consented by an administrator.

*Effective permissions* are the permissions that your app has when making requests to Microsoft Graph. It's important to understand the difference between the delegated and application permissions that your app is granted, and its effective permissions when making calls to Microsoft Graph.

For delegated permissions, the effective permissions of your app are the intersection of the delegated permissions the app has been granted (via consent) and the privileges of the currently signed-in user. Your app can never have more privileges than the signed-in user. Within organizations, the privileges of the signed-in user are determined by policy or by membership in one or more administrator roles. For more information about administrator roles, see [Assigning administrator roles in Azure Active Directory](#).

For example, assume your app has been granted the *User.ReadWrite.All* delegated permission. This permission nominally grants your app permission to read and update the profile of every user in an organization. If the signed-in user is a global administrator, your app can update the profile of every user in the organization. However, if the signed-in user isn't in an administrator role, your app can update only the profile of the signed-in user. It won't update the profiles of other users in the organization because the signed-in user doesn't have those privileges.

For application permissions, the effective permissions of your app will be the full level of privileges implied by the permission. For example, an app that has the *Mail.Send* **application** permission can send mail as every user in the organization.

To date, the M365 Supplemental management packs use only “**Delegated**” permissions.

Use of delegated permissions requires an M365 user account so that the monitoring workflows can simulate the user. Before the monitoring workflows can interact with Microsoft Graph API, they must authenticate to Azure and retrieve an access token for the user. The authentication request must include the account password and App secret/key.

During configuration of the Watcher node, both the App secret and account password get encrypted by the security context of the configuration task (usually the default RunAs account) and both are stored locally in the Watcher node registry as encrypted strings. The account context that performed the original encryption is the only account that may decrypt the values and only on that same computer. The strings cannot be decrypted by any other account, and they cannot be decrypted on any other computer. For this reason, do not provide credentials when executing the configuration tasks.

At this time, certificate authentication is not supported by the management pack; only application secret/key. Although some in the IT community may prefer certificates for app registrations, when all things above are considered, the perceived benefits don't outweigh the administrative and configuration overhead.

If a specific RunAs account is desired, use the security profile: *M365 Supplemental Library Default RunAs Profile*. It is most common to leave this profile unused/vacant as it is usually unnecessary.

## Network, Firewall, Proxy

All of the scripted workflows leverage HTTPS(443) to authenticate to Azure and interact with Graph API. If your Watcher node requires a proxy, here are two options for configuring proxy settings:

1. [SCOM Agent Proxy Management pack](#)
2. You may edit the Monitoring Host configuration file manually.

### Manually edit the agent proxy configuration file

It is typically found in the following location:

Management Server: *C:\Program Files\Microsoft System Center <VERSION>\Operations Manager\Server\MonitoringHost.exe.config*

Agent machine: *C:\Program Files\Microsoft Monitoring Agent\Agent\MonitoringHost.exe.config*

Add the following element if it does not already exist, configure as shown:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://xxx.xx.x.xx:xxxx" bypassonlocal="false" />
    <bypasslist></bypasslist>
  </defaultProxy>
</system.net>
```

**Note:** Secure proxy connections (https) are not supported.

**Note:** proxyaddress value must be entered as follows:

<http://ProxyIPAddress:Port>

Example: <http://10.10.10.250:4040>

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://10.10.10.250:4040" bypassonlocal="false" />
    <bypasslist></bypasslist>
  </defaultProxy>
</system.net>
```

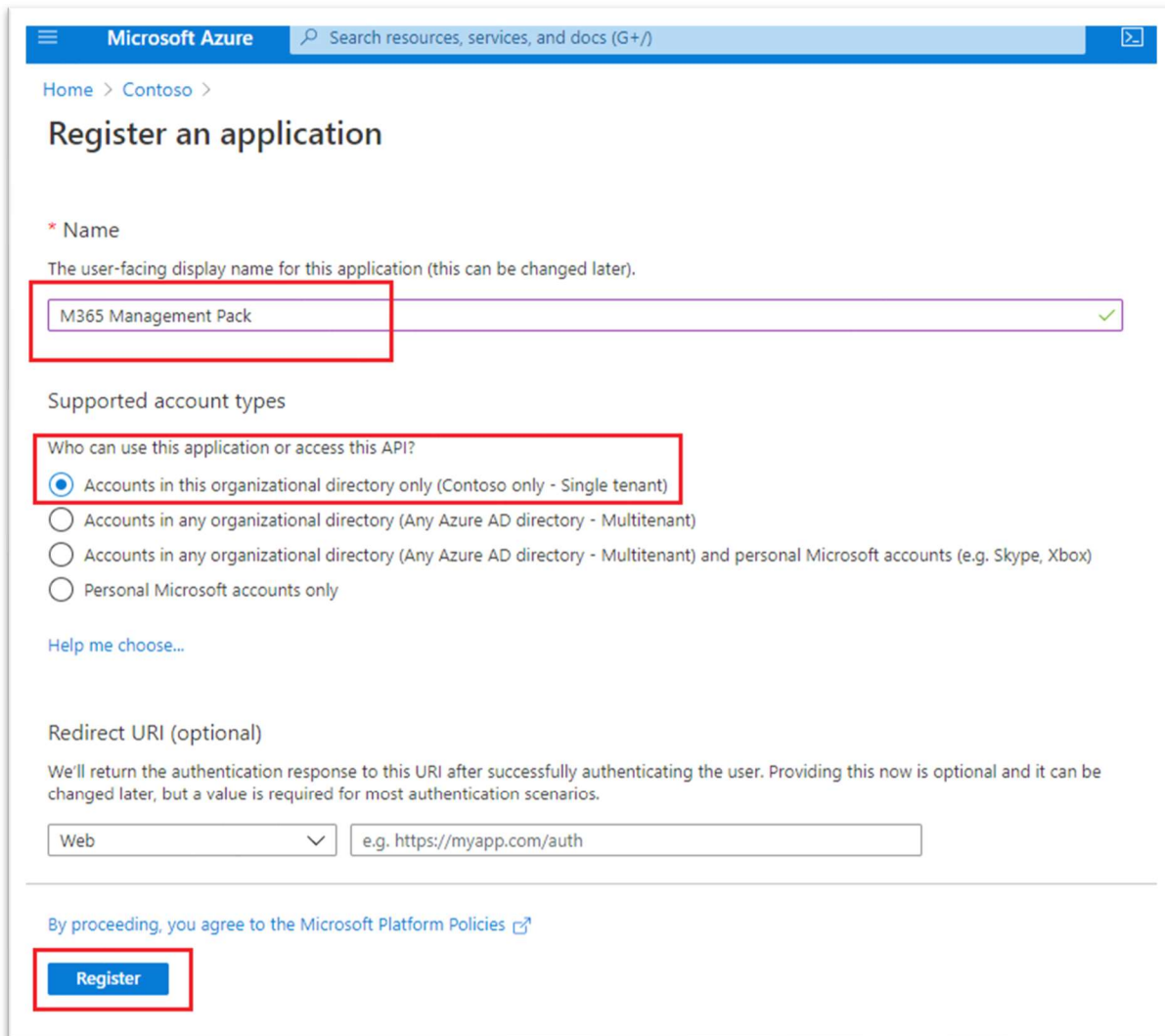
Restart the Microsoft Monitoring Agent service.

## Azure AD Application Registration

This solution leverages Microsoft Graph API with scripted workflows to perform synthetic transactions. This requires you to register an application in Azure Active Directory.

### Register a New Application Using the Azure Portal

1. Sign in to the [Azure portal](#) using either a work or school 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 appropriate Azure AD tenant.
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 Search resources, services, and docs (G+)

Home > Contoso >

## Register an application

\* Name

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

M365 Management Pack ✓

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.

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

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

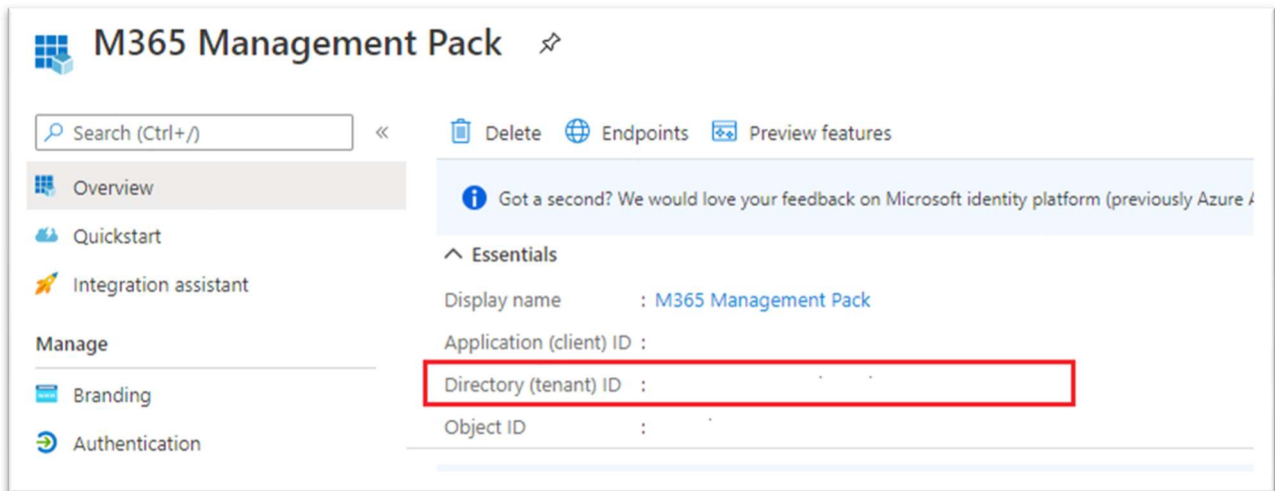
**Register**

## Add Credentials

The synthetic workflows require the tenant ID (or Name) for authentication and the application ID for the interaction with Graph API. Also required is an authentication key/secret (described in the following section). To get those values, use the following steps:

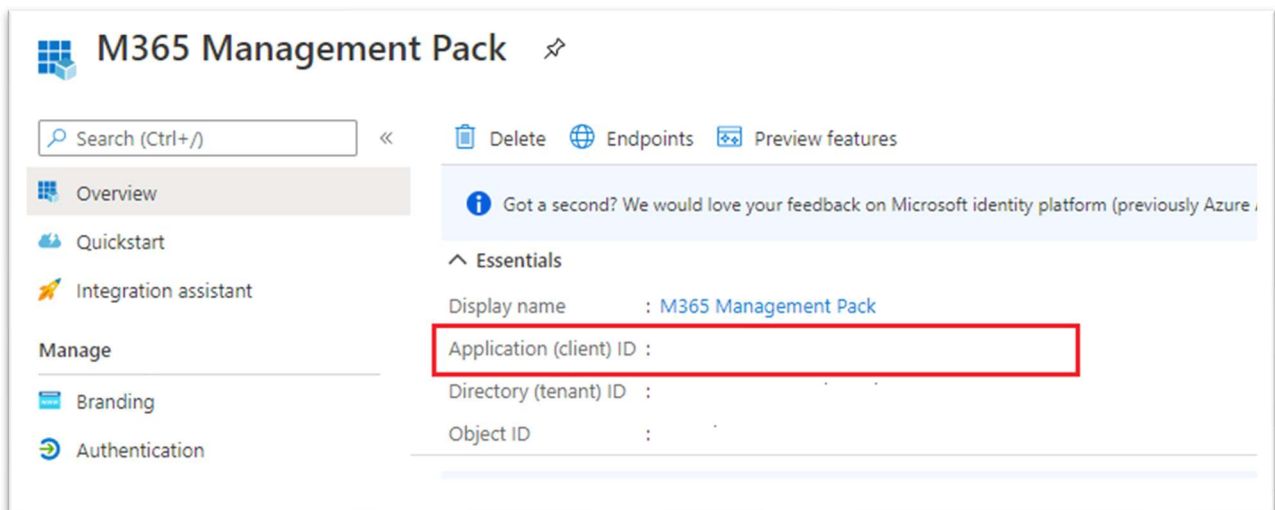
1. Select **Azure Active Directory**
2. From **App registrations** in Azure AD, select your application.
3. Make a note of the **Directory (tenant) ID** (or Name). The directory (tenant) ID can also be found in the default directory overview page.





The screenshot shows the 'M365 Management Pack' configuration page. On the left, there is a navigation menu with 'Overview', 'Quickstart', 'Integration assistant', and 'Manage' (which includes 'Branding' and 'Authentication'). The main content area shows the 'Essentials' section with the following fields: 'Display name' (M365 Management Pack), 'Application (client) ID', 'Directory (tenant) ID' (highlighted with a red box), and 'Object ID'. At the top, there is a search bar and action buttons for 'Delete', 'Endpoints', and 'Preview features'. A notification banner at the top right says 'Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD)'.

#### 4. Make a note of the **Application ID**.



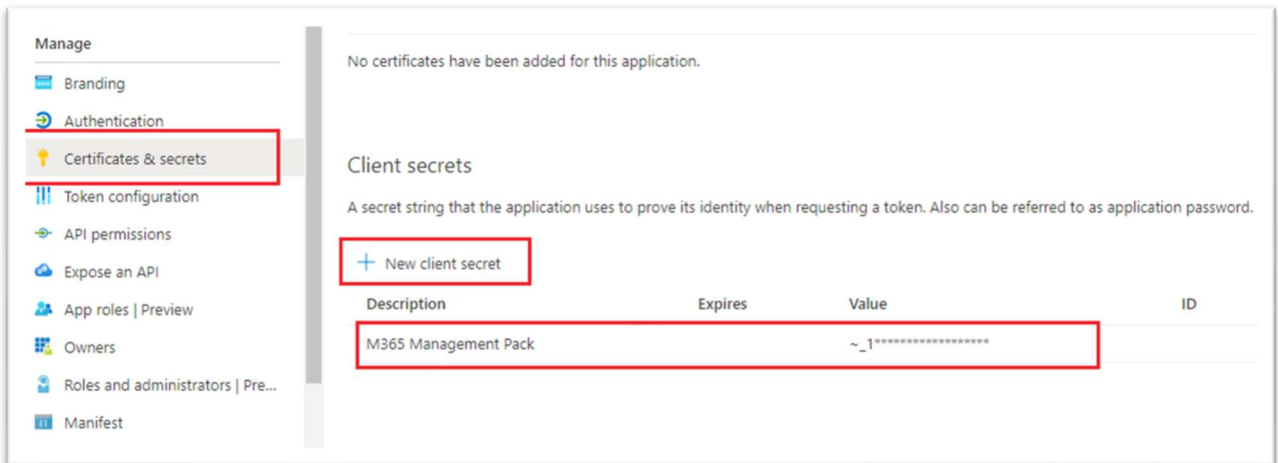
This screenshot is identical to the one above, showing the 'M365 Management Pack' configuration page. In this instance, the 'Application (client) ID' field is highlighted with a red box, indicating that this is the value to be noted.

## Create a New Application Secret

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**.

**NOTE: 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. 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.

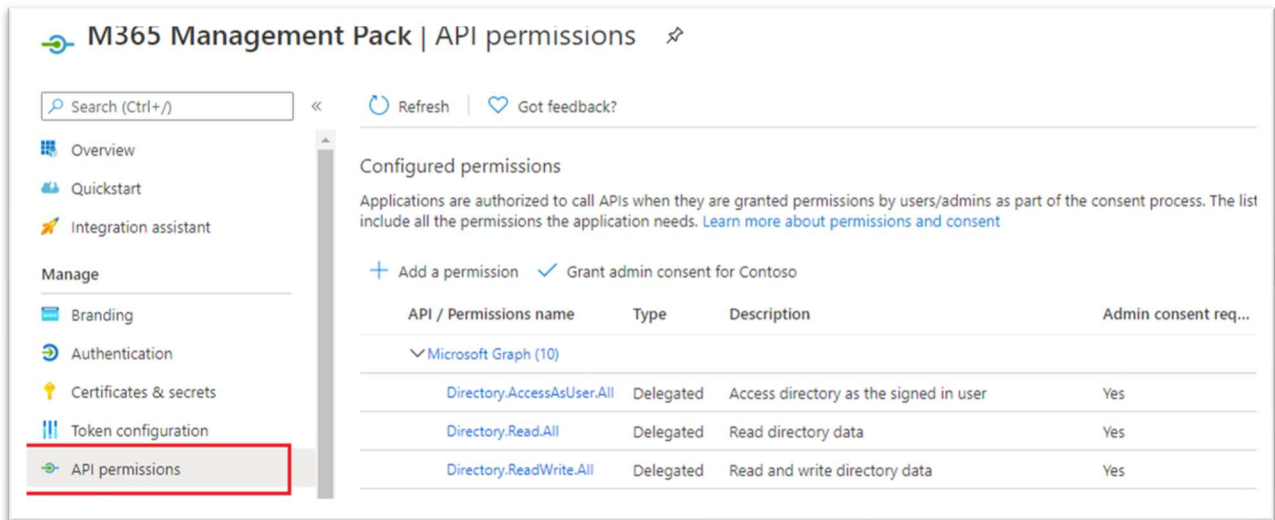
1. Sign in to the [Azure portal](#).
2. If you have access to multiple tenants, use the **Directory + subscription** filter  in the top menu to select the tenant containing your client app's registration.
3. Select **Azure Active Directory** > **App registrations**, and then select your client application.
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.

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.

## Grant admin consent

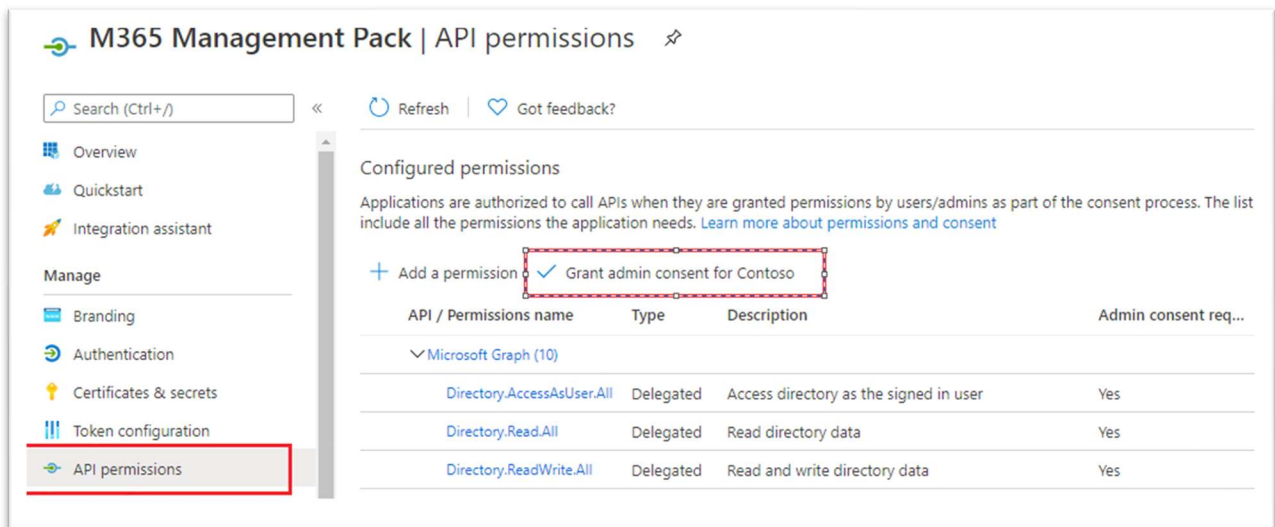
Admin consent will need to be granted for all relevant permissions regardless of the "Admin consent required" column value.



The following steps show you how the consent experience works.

### 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.



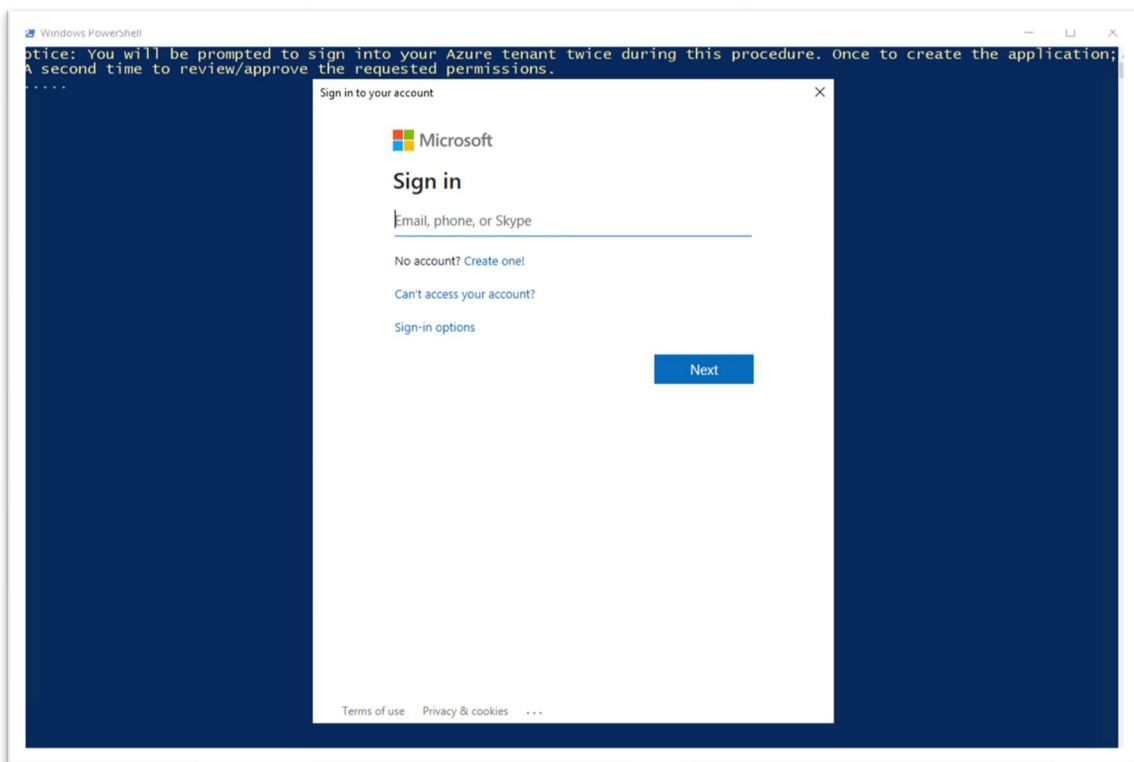
You will be prompted for confirmation. Select "Yes".

## 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 and internet access, you can run the **M365 SCOM MP App Registration.ps1** included in the MP Files.

**Note: This script will not modify existing App Registration Permissions! This is for creation of Application Registrations during new implementations.**

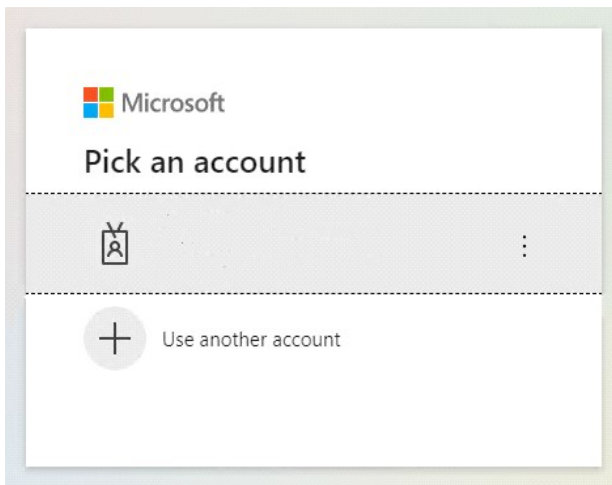
- The script will perform the following tasks: Create the new Application Registration (the application name must not already exist)
  - Grant **ALL** the permissions required for each management pack (OneDrive, Exchange, Services, etc).
  - Grant Admin Consent
1. From a computer with the Azure AD PowerShell module installed run the **M365 SCOM MP App Registration.ps1**
    - Enter your M365 admin account credentials . The M365 account must have necessary permissions to create the application registration and grant admin consent.



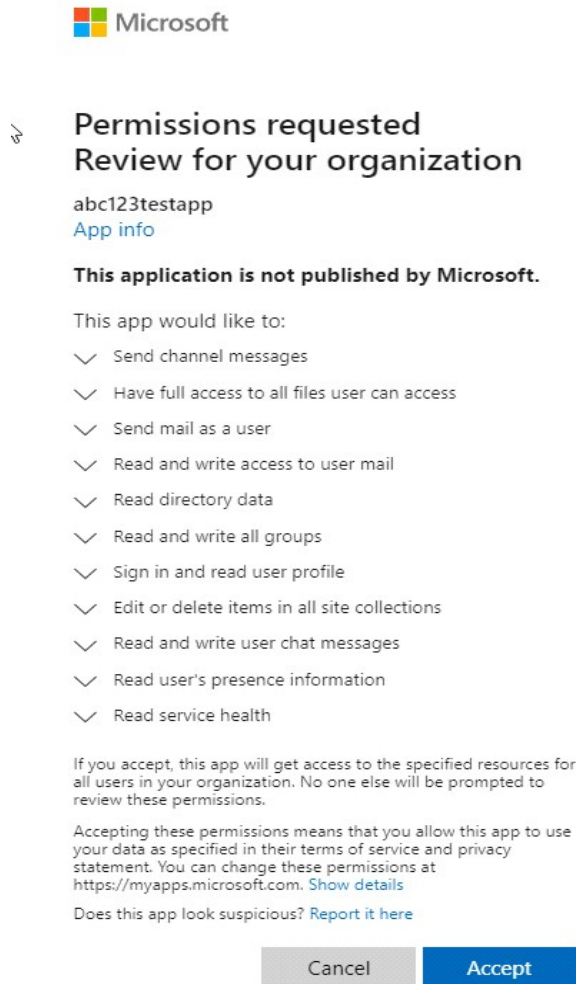
2. Enter a meaningful, descriptive application name and press **Enter**. Example:  
"SCOM\_Prod1\_M365Monitoring"

```
Windows PowerShell
Notice: You will be prompted to sign into your Azure tenant twice during this procedure. Once to create the application;
A second time to review/approve the requested permissions.
.....
Enter the new application name. This is the user-facing display name for this application (this can be changed later).
Name: _
```

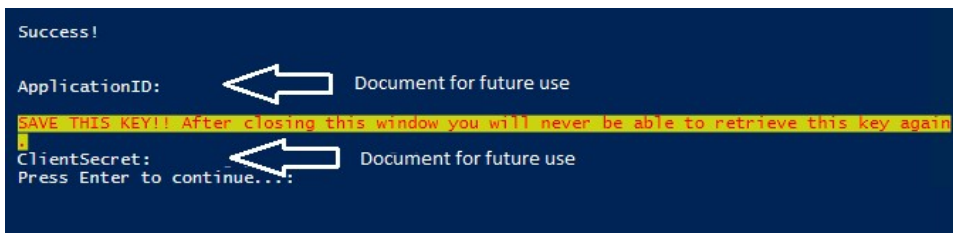
3. When prompted for your account either enter credentials again (if required) or select your account from the list.



- o Click **Accept** after reviewing the permissions.



4. **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.



**Note: If the key is ever lost, you can navigate to the application registration -> Certificates and secrets within Azure Active Directory and create a new key.**

## 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
Group.ReadWrite.All	Delegated	Read and write all groups	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 and 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	-

## Services

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (1)			
ServiceHealth.Read.All	Delegated	Read service health information for your organization	Yes

## Teams

API / Permissions name	Type	Description	Admin consent required
Microsoft Graph (3)			
ChannelMessage.Send	Delegated	Send channel messages	-
Chat.ReadWrite	Delegated	Read and write all groups	Yes
Presence.Read	Delegated	Read users presence information	-

## 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 (11)			
ChannelMessage.Send	Delegated	Send channel messages	-
Chat.ReadWrite	Delegated	Read and write user chat 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	-
Presence.Read	Delegated	Read users presence information	-
ServiceHealth.Read.All	Delegated	Read service health	Yes
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	-
User.Read	Delegated	Sign in and read user profile	-

Example:



API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (11) ...				
ChannelMessage.Send	Delegated	Send channel messages	No	✔ Granted for monguys ...
Chat.ReadWrite	Delegated	Read and write user chat messages	No	✔ Granted for monguys ...
Directory.Read.All	Delegated	Read directory data	Yes	✔ Granted for monguys ...
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✔ Granted for monguys ...
Group.ReadWrite.All	Delegated	Read and write all groups	Yes	✔ Granted for monguys ...
Mail.ReadWrite	Delegated	Read and write access to user mail	No	✔ Granted for monguys ...
Mail.Send	Delegated	Send mail as a user	No	✔ Granted for monguys ...
Presence.Read	Delegated	Read user's presence information	No	✔ Granted for monguys ...
ServiceHealth.Read.All	Delegated	Read service health	Yes	✔ Granted for monguys ...
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No	✔ Granted for monguys ...
User.Read	Delegated	Sign in and read user profile	No	✔ Granted for monguys ...

## Watcher Node Preparation

The M365 Supplemental Management Pack requires at least one agent managed computer (or management server) to be nominated as a watcher node. The watcher node will run the scripted workflows 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 present 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.
- **PowerShell version 5.0 or higher**

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

## Management Pack Configuration

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

### Import 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

You cannot modify any of the sealed management pack files. 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 unsealed management pack for each sealed management pack that you want to customize.

Example: For Teams customizations

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 Teams (Overrides)**), and then click **Next**.
4. Click **Create**.
5. Save your Teams workflow overrides to the new unsealed Teams MP.

### 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\_Password
  - c. M365\_ClientID
  - d. M365\_ClientSecret
  - e. TenantName
7. Click **Override**, select '**Use the predefined Run As Account**' and then click **Run**.  
 Note: Do not provide credentials for any of the numerous configuration tasks.
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 but instead a domain account (as is likely on a SCOM management server) and there exists no local user profile for the action account, the task may fail with an error because the script is unable to encrypt the password and secret. To correct this problem simply log into the Watcher Node (then log out) with whichever default action account is configured for the agent. This will create a local user profile for the account. Then run the configuration task again once the user profile exists.
9. The Watcher configuration task should trigger on-demand discovery which should result in rapid discovery of the Watcher instance, only a few seconds in most cases. (On-demand discovery is featured in all configuration tasks in all of the M365 Supplemental MPs.) 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	<a href="#">Reference</a>
ApiTokenURL	https://login.microsoftonline.com	<a href="#">Reference</a>
ApiTokenScopeURL	https://graph.microsoft.com/.default	<a href="#">Reference</a>
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the Watcher Node. The Watcher node will become UNdiscovered and effectively removed.
TLSVersion	1.2	Default TLS version for all workflows
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 Supplemental – Configure Watcher Node parameters.

Location		The physical location of the Watcher computer. Example: Negril, Jamaica
M365_AccountName	None	Default account name used to authenticate to Microsoft 365.
M365_AccountPassword	None	Default account password used to authenticate 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.
PoshLibraryPath	None	For support engineer use only.
WriteActionTimeoutSeconds	60	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

### 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\_AccountName
  - b. M365\_AccountPassword
  - c. M365\_ClientID
  - d. M365\_ClientSecret
  - e. 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. The configuration task should trigger on-demand discovery which should result in rapid discovery of the instance, only a few seconds in most cases. (On-demand discovery is featured in all configuration tasks in all of the M365 Supplemental MPs.)
10. Once the discovery is complete, check the **M365 Supplemental - Services** state view.

### M365 Supplemental – Configure Services parameters.

Parameter	Default Value	Details
MgmtApiURL	https://graph.microsoft.com	<a href="#">Reference</a>
MgmtApiTokenURL	https://login.microsoftonline.com	<a href="#">Reference</a>
MgmtApiTokenScopeURL	https://graph.microsoft.com/.default	<a href="#">Reference</a>
DeleteConfiguration	False	Setting this parameter to True will remove any existing configuration from the Watcher Node . The instance will become UNdiscovered and effectively removed from the Watcher.
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	Inherited	Default interval for monitoring workflows.
M365_AccountName	Inherited	Default account name used to authenticate to Microsoft 365.
M365_AccountPassword	Inherited	Default account password used to authenticate to Microsoft 365.
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		For support engineer use only.

## M365 Supplemental – Configure Services parameters.

WriteActionTimeoutSeconds	60	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\_ClientID
  - b. M365\_ClientSecret
  - c. Exch\_to\_M365\_IntervalSeconds
  - d. M365\_to\_Exch\_IntervalSeconds
  - e. M365\_to\_M365\_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. The configuration task should trigger on-demand discovery which should result in rapid discovery of the instance, only a few seconds in most cases. (On-demand discovery is featured in all configuration tasks in all of the M365 Supplemental MPs.)
9. 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. The instance will become UNdiscovered and effectively removed from the Watcher.
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	60	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_to_M365_ReceiveRetry_WaitSeconds	10	Seconds to wait between mail retrieval attempts.
M365_SenderEmailAddress	None	M365 Sender Email Address
M365_SenderPassword	None	M365 Sender Password
M365_ReceiverEmailAddress	None	M365 Receiver Email 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.
Exch_to_M365_ReceiveRetry_WaitSeconds	10	Seconds to wait between mail retrieval attempts.
Exchange_SenderEmailAddress	None	On-Prem Exchange Sender Email Address
Exchange_SenderPassword	None	On-Prem Exchange Password
Exchange_ReceiverEmailAddress	None	On-Prem Exchange Receiver Email Address
Exchange_ReceiverPassword	None	On-Prem Exchange Password
Exch_TotalDurationCriticalSeconds	180	Threshold at which the 'TotalDuration' measurement will cause a Critical state.

### M365 Supplemental – Configure Mail Flow parameters.

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\_Password
  - c. M365\_ClientID
  - d. M365\_ClientSecret
  - 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. The configuration task should trigger on-demand discovery which should result in rapid discovery of the instance, only a few seconds in most cases. (On-demand discovery is featured in all configuration tasks in all of the M365 Supplemental MPs.)
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. The instance will become UNdiscovered and effectively removed from the Watcher.
IntervalSeconds	Inherited	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_ClientID	Inherited	This value uniquely identifies your application in the Microsoft identity platform



## M365 Supplemental – Configure License parameters.

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	60	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\_Password
  - c. M365\_ClientID
  - d. M365\_ClientSecret
  - e. IntervalSeconds
6. Additional parameters are required to configure Teams monitoring:
  - a. TeamName  
*Example: monitoringguys*
  - b. ChannelName  
*Example: General*
  - c. ChatPartnerAddress  
*Example: SCOMChatTestUser@monitoringguys.com*
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	Set Setting this parameter to True will remove any existing configuration from the Watcher Node. The instance will become UNdiscovered and effectively removed from the Watcher.
IntervalSeconds	Inherited	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	60	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
ChatPartnerAddress	None	A separate M365 user account licensed for Teams. Used for testing initiation of a chat session. No password is used for Teams configuration.

## 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\_Password
  - c. M365\_ClientID

- d. M365\_ClientSecret
  - e. IntervalSeconds
6. Additional parameters are needed to configure SharePoint Online monitoring
- a. SiteName
    - Note: This is the unique name of the site as it appears in the SPO site URL.
    - Example: <https://monitoringguys.sharepoint.com/sites/SCOM1TestSite>
    - The Display Name of the site is “SCOM1 Test Site” but the SiteName is “SCOM1TestSite”
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. The configuration task should trigger on-demand discovery which should result in rapid discovery of the instance, only a few seconds in most cases. (On-demand discovery is featured in all configuration tasks in all of the M365 Supplemental MPs.)
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 Watcher Node. The instance will become UNdiscovered and effectively removed from the Watcher.
IntervalSeconds	Inherited	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	60	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\_Password
  - c. M365\_ClientID
  - d. M365\_ClientSecret
  - 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. The configuration task should trigger on-demand discovery which should result in rapid discovery of the instance, only a few seconds in most cases. (On-demand discovery is featured in all configuration tasks in all of the M365 Supplemental MPs.)
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 any existing configuration from the Watcher Node. The instance will become UNdiscovered and effectively removed from the Watcher.
IntervalSeconds	Inherited	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.
PoshLibraryPath	None	For support engineer use only.

## M365 Supplemental – Configure OneDrive parameters.

WriteActionTimeoutSeconds	60	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. The default RunAs account is typically the best option.
- **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 SCOM monitoring app registration status. Will alert if app expiration date is near.
- **M365 – Script Library Failure Repeated Event Detection Monitor**
  - Detects events in the Application event log related to the M365 Supplemental MP script library load failure(s).
- **M365 – Script Failure Repeated Event Detection Monitor**
  - Detects events in the Application even log related to the M365 Supplemental MP script activities

#### Rules

- **M365 Supplemental - Application Expiration Days Remaining**  
Will collect the days remaining until app registration secret expiration.

- **M365 Supplemental - Directory Percent Usage**  
Collects the percentage of tenant directory space consumed.
- **M365 Supplemental – Discovery Event Collection Rule**
  - Collects Discovery events
- **M365 Supplemental – OnDemand Discovery Event Collection Rule**
  - Collects OnDemand Discovery trigger events and will initiate On-Demand discovery for the applicable targets.
- **M365 Supplemental – Application Authentication Performance Collection Rule**
  - Collects time (ms) required for Azure authentication

## 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 are used as the default parameter values for subsequent component configuration tasks.
- **M365 Supplemental – Get App Expiration Data**
  - Retrieves M365 Supplemental MP App Registration (Service Principal) Expiration Data
- **M365 Supplemental – Get Org Directory Usage**
  - Retrieves Directory Quota in MB, Usage in MB and returns % Consumed and Free for AAD Tenant
- **M365 Supplemental – Modify Watcher Node Settings**
  - Modifies Watcher Node configuration properties

## License

### Monitors

- **M365 License - Status Monitor**
  - Monitor the M365 subscription status for active/valid status.
- **M365 License - Active Units (Percent) Monitor**
  - Monitor the license SKU usage by percentage (%)
- **M365 License – Script Library Failure Repeated Event Detection Monitor**
  - This will detect events in the Application event log related to the M365 Supplemental MP script library load failure(s).
- **M365 License – Script Failure Repeated Event Detection Monitor**
  - This will detect events in the Application even log related to the M365 Supplemental MP script activities

### 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:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/licensing-service-plan-reference>

to be stored locally in a CSV file ('LicenseSkuDisplayNames.csv'). The license discovery workflow will use the display names only if the CSV file exists and contains the matching names.

## 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. This task targets the “M365 License Role Class” class and should only be used if the automatic download rule (M365 License - Download Sku DisplayNames to CSV Timed Rule) does run successfully and the friendly “Display Names” are not discovered for the license instances. This task allows you to customize the M365 SKUs display names if needed by editing the Name/DisplayName pairs in the task configuration.
- **M365 Supplemental – Get License Sku Data**
  - Retrieves Licenses Available and Consumed % On Demand
- **M365 Supplemental – Modify License Configuration**
  - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component

## 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 - ExchangeOnline (M365 to M365) Message Send/Receive TotalDuration (ms) Performance Monitor**
  - Performs synthetic tests to monitor mail send/receive performance (Total Duration in seconds) from M365 to M365.
- **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 (Exchange to M365) Message Send/Receive TotalDuration (ms) Performance Monitor**
  - Performs synthetic tests to monitor mail send/receive performance (Total Duration in seconds) from Exchange to M365.
- **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.
- **M365 MailFlow - ExchangeHybrid (M365 to Exchange) Monitor Message Send/Receive TotalDuration (ms) Performance Monitor**
  - Performs synthetic tests to monitor mail send/receive performance (Total Duration in seconds) from M365 to Exchange.
- **M365 MailFlow – Script Library Failure Repeated Event Detection Monitor**
  - This will detect events in the Application event log related to the M365 Supplemental MP script library load failure(s).
- **M365 MailFlow– Script Failure Repeated Event Detection Monitor**
  - This will detect events in the Application even log related to the M365 Supplemental MP script activities

## 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
- **M365 Mailflow – ExchangeOnline Mailbox Cleanup AverageDeleteTimePerInboxMessage (ms) Performance Collection Rule**
- **M365 Mailflow – ExchangeOnline Mailbox Cleanup TotalDuration (ms) Performance Collection Rule**

## Tasks

- **M365 Supplemental – Configure MailFlow**
  - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.
- **M365 Mailbox Cleanup**
  - Executes mailbox cleanup routine.
- **M365 Supplemental - Exchange to Exchange Mailflow Test**
  - Tests Exchange to Exchange Mailflow
- **M365 Supplemental - Exchange to M365 Mailflow Test**
  - Tests Exchange to M365 Mailflow
- **M365 Supplemental - M365 to Exchange Mailflow Test**
  - Tests M365 to Exchange Mailflow
- **M365 Supplemental - M365 to M365 Mailflow Test**
  - Tests M365 to M365 Mailflow
- **M365 Supplemental – Modify Mailflow Configuration**
  - 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.
- **M365 OneDrive - Folder Read/Write Synthetic Test Performance Monitor**
  - Measures Folder Read/Write transaction time (ms)
- **M365 OneDrive – Script Library Failure Repeated Event Detection Monitor**

- Detects events in the Application event log related to the M365 Supplemental MP script library load failure(s).
- **M365 OneDrive – Script Failure Repeated Event Detection Monitor**
  - Detects events in the Application even log related to the M365 Supplemental MP script activities

## 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.
- **M365 Supplemental – Modify OneDrive Configuration**
  - 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
- **M365 Services – Script Library Failure Repeated Event Detection Monitor**
  - This will detect events in the Application event log related to the M365 Supplemental MP script library load failure(s).
- **M365 Services – Script Failure Repeated Event Detection Monitor**
  - This will detect events in the Application even log related to the M365 Supplemental MP script activities

### Rules

- **M365 Services - Incident Message Alert Rule (Critical)**

- Raises a critical alert when M365 Services incident/advisories (with matching severity) are updated with new information.
- **M365 Services - Incident Message Alert Rule (Warning)**
  - Raises a warning alert when M365 Services incident/advisories (with matching severity) are updated with new information.
- **M365 Services - Incident Message Alert Rule (Informational)**
  - Raises an informational alert when M365 Services incident/advisories (with matching severity) are updated with new information.

## Tasks

- **M365 Supplemental – Configure Services**
  - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.
- **M365 Supplemental – Get Service Incident Data**
  - Retrieves any Service Incident Data
- **M365 Supplemental – Get Services Data**
  - Retrieves Service Data including current status and statistics related to status of all services
- **M365 Supplemental – Modify Services Configuration**
  - 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**
  - Synthetic transaction monitor that uploads and downloads a file to a SharePoint site.
- **M365 SharePoint – Site Read/Write Synthetic Test Performance Monitor**
  - Upload/Download Total duration in MS
- **M365 SharePoint – Script Library Failure Repeated Event Detection Monitor**
  - Detects events in the Application event log related to the M365 Supplemental MP script library load failure(s).
- **M365 SharePoint – Script Failure Repeated Event Detection Monitor**
  - Detects events in the Application even log related to the M365 Supplemental MP script activities

### 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 SharePoint – SharePoint File Upload/Download**
  - Synthetic test that uploads and downloads a file to a SharePoint site.
- **M365 Supplemental – Modify SharePoint Configuration**
  - Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component
- **M365 Supplemental – Search for SharePoint Site**
  - Allows for search by SiteName or a single Wildcard, '\*'

## 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 to the original message.
- **M365 Teams - Chat Synthetic Test Monitor**
  - Establish chat session with chat partner
- **M365 Teams - Chat Synthetic Test Performance Monitor**
  - Duration (ms) for test chat message to be sent
- **M365 Teams - Send Channel Message Synthetic Test Monitor**
  - Sends channel message via synthetic transaction
- **M365 Teams - Send Channel Message Synthetic Test Performance Monitor**
  - Duration (ms) for test channel message to be sent
- **M365 Teams - Team Calendar Synthetic Test Monitor**
  - Create calendar event via synthetic transaction
- **M365 Teams - Team Calendar Synthetic Test Performance Monitor**
  - Duration (ms) for test calendar event creation
- **M365 Teams - Team Presence Monitor**
  - Retrieves user presence
- **M365 Teams – Script Library Failure Repeated Event Detection Monitor**
  - Detects events in the Application event log related to the M365 Supplemental MP script library load failure(s).

- **M365 Teams – Script Failure Repeated Event Detection Monitor**
  - Detects events in the Application even log related to the M365 Supplemental MP script activities

## 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.
- **M365 Teams - Chat Create Session Synthetic Test Duration Performance Collection Rule**
  - Duration (ms) of chat session creation
- **M365 Teams - Chat Message Verify Synthetic Test Duration Performance Collection Rule**
  - Duration (ms) of chat message verification
- **M365 Teams - Chat Send Synthetic Test Duration Performance Collection Rule**
  - Duration (ms) of chat message send
- **M365 Teams - Chat Send Synthetic Test TotalDuration Performance Collection Rule**
  - Total Duration (ms) of chat session creation
- **M365 Teams - Get Presence Duration Performance Collection Rule**
  - Duration (ms) to retrieve user presence
- **M365 Teams - Synthetic Test Calendar Create Event Duration Performance Collection Rule**
  - Duration (ms) of create calendar event
- **M365 Teams - Synthetic Test Calendar Delete Event Duration Performance Collection Rule**
  - Duration (ms) of delete calendar event
- **M365 Teams - Synthetic Test Calendar Event Total Duration Performance Collection Rule**
  - Total Duration (ms) of calendar event create/delete
- **M365 Teams - Synthetic Test Channel MessageReply Duration Performance Collection Rule**
  - Duration (ms) of channel message reply
- **M365 Teams - Synthetic Test Channel MessageSend Duration Performance Collection Rule**
  - Duration (ms) of channel message send
- **M365 Teams - Synthetic Test Channel SendMessage Total Duration Performance Collection Rule**
  - Total Duration (ms) of channel message send and reply




## Tasks

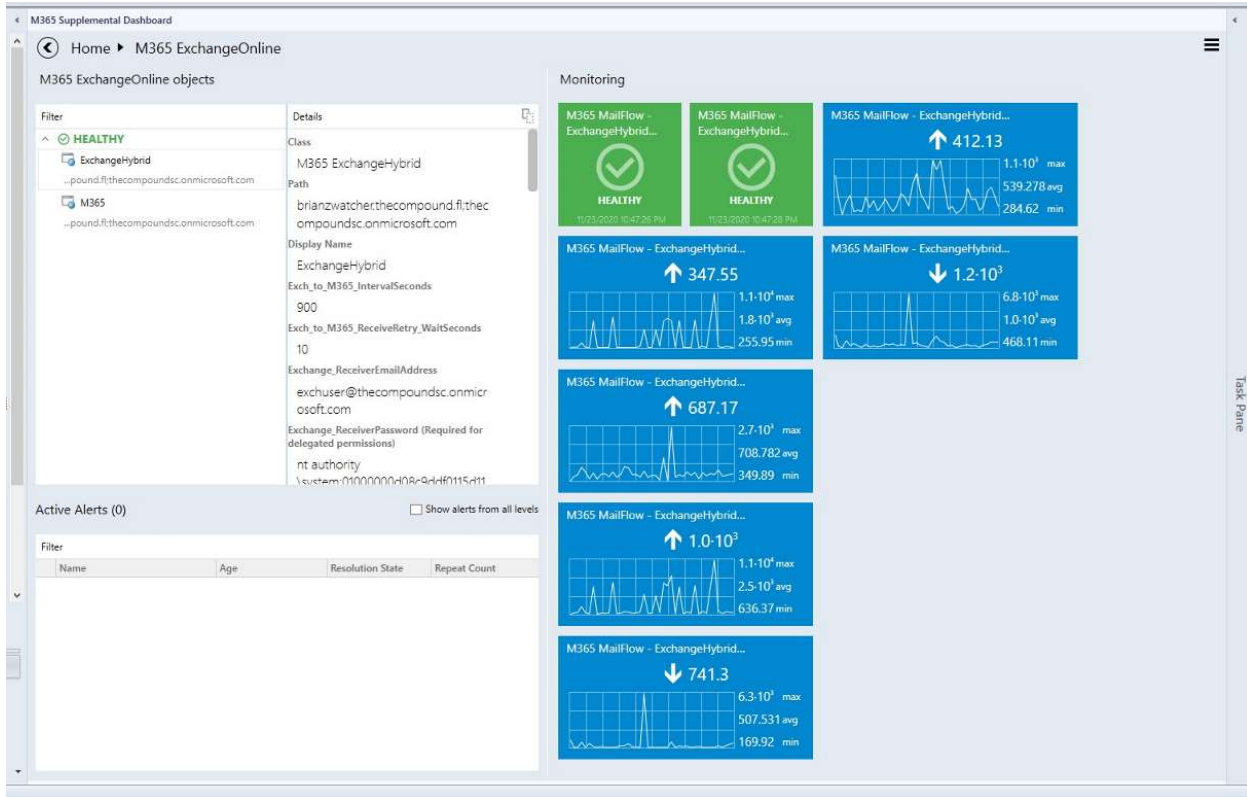
- **M365 Supplemental – Configure Teams**

- Writes the required values to the Watcher Node registry to enable discovery and monitoring of the M365 service component.
- **M365 Supplemental – Teams Presence Test**
- **M365 Supplemental – Teams Chat Message Test**
- **M365 Supplemental – Teams Calendar Event Test**
- **M365 Supplemental – Teams Channel Message Test**
- **M365 Supplemental – Modify Teams Configuration**
  - 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**.

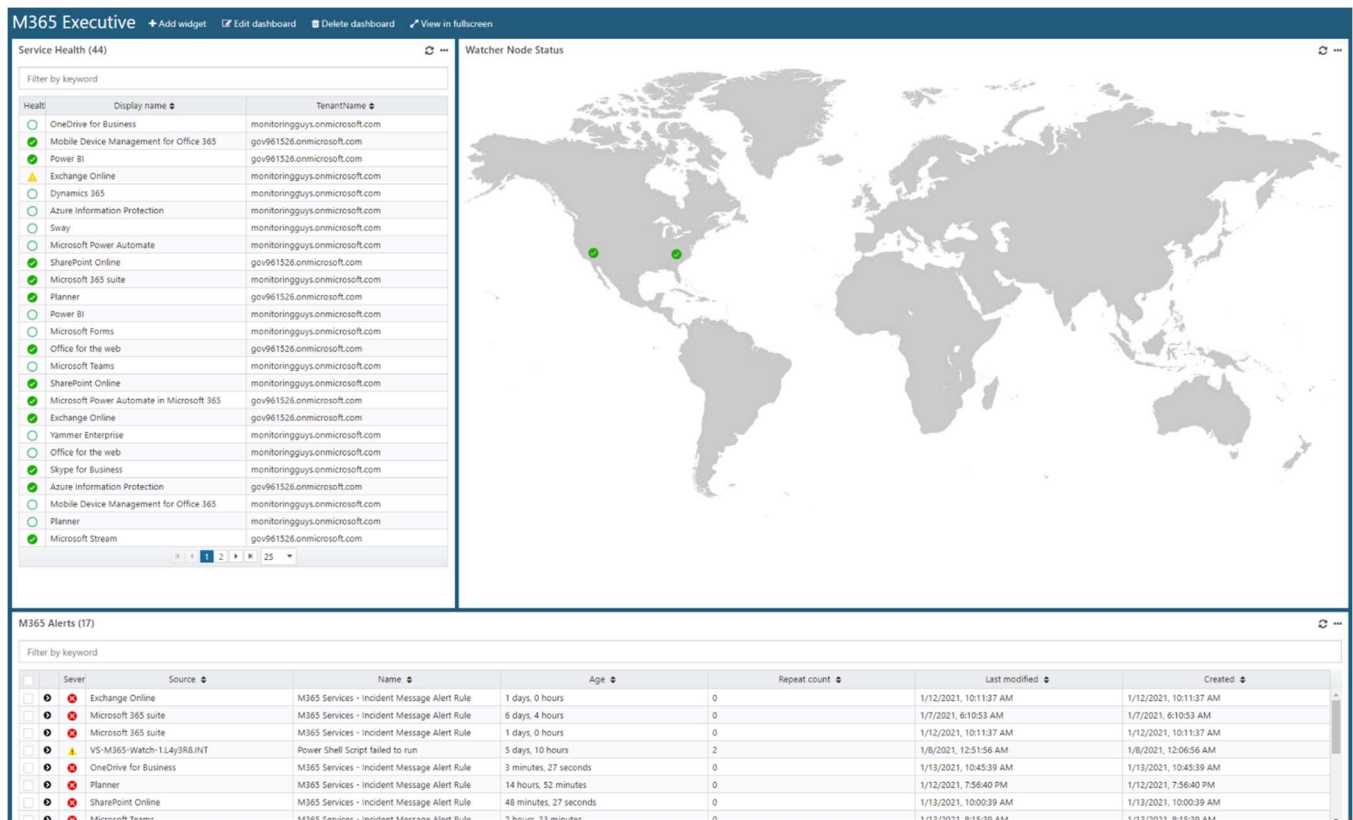


## HTML 5 Dashboards

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**.



The screenshot displays the Microsoft 365 Executive dashboard. The top navigation bar includes 'M365 Executive', 'Add widget', 'Edit dashboard', 'Delete dashboard', and 'View in fullscreen'. The main content area is divided into three sections:

- Service Health (44):** A table listing various services and their health status. The table has columns for 'Health', 'Display name', and 'TenantName'. Services listed include OneDrive for Business, Mobile Device Management for Office 365, Power BI, Exchange Online, Dynamics 365, Azure Information Protection, Sway, Microsoft Power Automate, SharePoint Online, Microsoft 365 suite, Planner, Office for the web, Microsoft Teams, and Microsoft Stream.
- Watcher Node Status:** A world map showing the status of watcher nodes across different geographical regions.
- M365 Alerts (17):** A table listing alerts with columns for 'Sever', 'Source', 'Name', 'Age', 'Repeat count', 'Last modified', and 'Created'. Alerts include incidents from Exchange Online, Microsoft 365 suite, VS-M365-Watch-1.Ly3R8.INT, OneDrive for Business, Planner, and SharePoint Online.



## PowerBI Dashboard

Included in this release is a **Microsoft 365 Health.pbix** – this is turn key solution to provide Executive Level visibility to the M365 solution deployed within your organization.

Edit the parameters to point to the Operations Manager Data Warehouse database.

1. Select the **Home** tab
2. Click **Transform data** and select **Edit parameters**
3. Enter the name of the **Operations Manager Data Warehouse** database server/SQL instance
4. Enter the name of the **Operations Manager Data Warehouse** database
5. Verify the **M365 Admin Center URL** is correct
6. Enter the **URL** to the service desk.
7. Enter the **name** for the service desk application.
8. Enter the **number of days** of data history to load. Recommended is 30 days.
9. Click **OK**
10. Click **Refresh**


Edit the locations.

1. Select the Data tab
2. Select the Location table
3. Enter a row for each watcher node. The required fields are:
  - a. Watcher Node
  - b. Location Name
  - c. Latitude
  - d. Longitude
  - e. Bubble Size (represents location on map, recommend setting to 1000)

# Microsoft 365 Health

servicenow

Refreshed on 12/9/2021 at 9:32:39 AM

<b>Healthy</b> Mail Flow (Exchange to M365) <small>(i)</small>	<b>Healthy</b> OneDrive <small>(i)</small>	<b>Healthy</b> SharePoint Online <small>(i)</small>	<b>Healthy</b> Teams <small>(i)</small>	<b>Healthy</b> M365 Directory Used <small>(i)</small>
<b>Critical</b> Mail Flow (M365 to Exchange) <small>(i)</small>	 <p>UNITED STATES</p> <p>© 2021 Microsoft Corporation. Terms</p>			<b>Healthy</b> Licenses <small>(i)</small>
<b>Healthy</b> Mail Flow (M365 to M365) <small>(i)</small>				<b>Critical</b> M365 Service Advisories <small>(i)</small>

Configuration Instructions | Cover Page | **Overview** | Mail | OneDrive | SharePoint Online | Teams | Licensing | Services | Active Alerts | Tool Tip - Monitor Health by Datacenter | Tool Tip - Monitor Health by Datacenter

## Troubleshooting

### Basic Troubleshooting

#### Event Logs

Nearly all of the workflows in the M365 Supplemental suite of MPs are scripted. The workflows include the ability to log a generous amount of activity. By default, only anomalies and errors are logged to the Windows Application event log. Verbose workflow logging can be enabled for the scripted workflows via override.

1. Locate the workflow (Monitor, Rule, Discovery) that you wish to diagnose, right-click and choose **Properties**.
2. Select the **Overrides Tab**, click **Override**.
3. Choose **For the object**, the **Override Properties** window will open
4. Under **Override-Controlled** parameters, activate **WriteToEventLog** checkbox
5. Change the **Override** value to **True**
6. Select a destination **Management Pack** for the override
7. Click **Apply**, then click **Ok**.
8. Check the **Application Event Log** on the **Watcher Node**, filter events ranging from 9990-9999.
9. Check the **Operations Manager Event Log** on the **Watcher Node**.

#### Script Test

##### Authentication Example

**Azure** authentication from the **Watcher Node** can be verified with PowerShell. Below is an example code snippet. PowerShell debugging is beyond the scope of this document, but some basic steps are provided below.

- a. Open **Windows PowerShell ISE** on the **Watcher Node**.
- b. Press **Ctrl+N** for a new document. **Copy and Paste** the code sample below into the new document.
- 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.  
**Basic Debugging:**  
Save the document. Once saved, you may set breakpoints on any line with **F9**. Once one or more breakpoints are set, you can execute the script with **F5** which will run the script normally but will pause before executing any line containing a breakpoint. You may inspect or modify any session variables while the script is paused. You may execute one line at a time with **F10** or continue normal execution with **F5**.
- 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
```

## Additional Script Testing

All of the sealed management packs may be unsealed to access the contained PowerShell script files.

(Read more about unsealing management packs [here](#).)

## Watcher Node Removal

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.

- Locate the **Watcher Node** in the **Windows Computer** View in the Operations Manager Console
- Select the **M365 Supplemental – Configure Watcher Node Default Settings** task from the Task Pane
- Click **Override**, then select **DeleteConfiguration** and set the Value to **True**
- You will also need to provide your **TenantName**.

- e. Once complete click **Override**, then click **Run**.

## License Display Names

At the time of this writing, License objects retrieved via Graph API do not contain friendly “Display Name” information. A rule exists (M365 License - Download Sku DisplayNames to CSV Timed Rule) will automatically attempt to download display name information from the [Microsoft documents website](#) to be stored locally to a CSV file (‘LicenseSkuDisplayNames.csv’) on the Watcher node to. The license discovery workflow will use the display names only if the CSV file exists and contains the matching names.

If the automatic download fails to download the current list, the rule will use a default list of Display Names. The default list is accurate as of the time of this writing but inevitably licenses get added and names are subject to change.

There is an alternative method to obtain the Display Names of the licenses. The M365.Supplemental.License.SkuNames.Addendum management pack contains an agent task which can write a default list of Display Names to the CSV file. This task targets the “M365 License Role Class” class and should only be used if the automatic download rule (M365 License - Download Sku DisplayNames to CSV Timed Rule) does not run successfully and subsequently the friendly “Display Names” are not discovered for the license instances. This task allows you to customize the M365 SKUs display names if needed by editing the Name/DisplayName pairs in the task configuration. If the task is used to create the Display Names file, then the automatic rule must be disabled otherwise any user-created file will be overwritten by the automatic rule default list.

The screenshot displays the Microsoft Operations Manager (MOM) interface. The main window is titled "Tasks - SCOMLAB - Operations Manager" and shows a search for "LicenseSku". The search results list a task named "M365 Supplemental - Write LicenseSku DisplayNames to ... (Not inherited) M365 S".

A dialog box titled "M365 Supplemental - Write LicenseSku DisplayNames to CSV Properties" is open, showing the "Configuration" tab. It contains an "Xml Configuration" section with the following text:

You are viewing the xml configuration of this object because the Management Pack does not define a specific UI to configure this object type. You can view or edit the xml and the associated schema by clicking on the button below.

Below this text is a text area containing XML configuration data:

```
<Configuration>
<DEFAULT_LIST>"skuPartNumber","DisplayName"
"ADV_COMMS","Advanced Communications"
"CDSAICAPACITY","AI Builder Capacity add-on"
"SPZA_IW","APP CONNECT IW"
"MCMEETADV","Microsoft 365 Audio Conferencing"
"AAD_BASIC","AZURE ACTIVE DIRECTORY BASIC"
"AAD_PREMIUM","AZURE ACTIVE DIRECTORY PREMIUM P1"
"AAD_PREMIUM_P2","AZURE ACTIVE DIRECTORY PREMIUM P2"
"RIGHTSMANAGEMENT","AZURE INFORMATION PROTECTION PLAN 1"
"SMB_APPS","Business Apps (free)"
"MCOCAP","COMMON AREA PHONE"
"MCOCAP_GOV","Common Area Phone for GCC"
"CDS_DB_CAPACITY","Common Data Service Database Capacity"
"CDS_LOG_CAPACITY","Common Data Service Log Capacity"
"MCOPSTNC","COMMUNICATIONS CREDITS"
"CRMSTORAGE","Dynamics 365 - Additional Database Storage (Qualified Offer)"
"CRMINSTANCE","Dynamics 365 - Additional Production Instance (Qualified Offer)"
"CRMTESTINSTANCE","Dynamics 365 - Additional Non-Production Instance (Qualified Offer)"
"DYN365_ASSETMANAGEMENT","Dynamics 365 Asset Management Addl Assets"
"DYN365_BUSCENTRAL_ADD_ENV_ADDON","Dynamics 365 Business Central Additional Environment"
"DYN365_BUSCENTRAL_DB_CAPACITY","Dynamics 365 Business Central Database Capacity"
"DYN365_BUSCENTRAL_ESSENTIAL","Dynamics 365 Business Central Essentials"
"DYN365_FINANCIALS_ACCOUNTANT_SKU","Dynamics 365 Business Central External Accountant"
"PROJECT MADEIRA_PREVIEW_IW_SKU","Dynamics 365 Business Central for IWs"
"DYN365_BUSCENTRAL_PREMIUM","Dynamics 365 Business Central Premium"
"DYN365_ENTERPRISE_PLAN1","Dynamics 365 Customer Engagement Plan"
```

An arrow points from the text "Edit the Display Names if needed." to the "Edit..." button in the dialog box. The dialog box also includes "OK" and "Cancel" buttons at the bottom.