



M365 Supplemental Services Monitoring Management Pack

Version 2.0 Upgrade Guide

Prepared for

12/14/2021

Version 1 Final

Created by

Tyson Paul, Brian Zoucha

Contents

Overview	3
Configure API Permissions	3
Remove Application permission granted for Office 365 Management API.....	3
Revoke admin consent for Office 365 Management APIs	4
Add GraphAPI permissions for Services and Teams Management Packs.....	5
Services	7
Teams.....	7
Verify your API Permissions	8
Remove Teams MP	9
Import New Management Packs	10
Run Configure Services task.....	12
Troubleshooting.....	14
Workflows won't initialize after the management pack rip/replace procedure	14
Import the SCOM Maintenance management pack	14
Execute DiscoveryDataPurge agent task.....	15
The Maintenance tasks won't run	19

Overview

The Office 365 Services Communications API is no longer supported as of December 17, 2021. The Services Management Pack has been updated to now leverage the new GraphAPI endpoints. Additionally, new functionality has been added to the management packs which require new permissions.

Configure API Permissions

Remove Application permission granted for Office 365 Management API.

Removing these permissions will temporarily break the Services monitoring until the following steps have been completed and the M365 Services MP has been updated and the Services configuration task run (details below).

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**
4. Select the **App Registration** currently in use with the M365 Supplemental Management Pack, click **API Permissions**.
5. Scroll to **Office 365 Management APIs**, click the ellipses next to **ServiceHealth.Read** and select **Revoke Admin Consent**
6. Once **Admin Consent** has been revoked, click on the ellipses next on **ServiceHealth.Read** and choose **Remove Permission**.

M365 Supplemental Management Pack | API permissions ✨ ...

Search (Ctrl+/) « Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest

Support + Troubleshooting
Troubleshooting
New support request

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 thecompoundsc

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (10)				...
ChannelMessage.Send	Delegated	Send channel messages	No	✓ Granted for thecompou... ...
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for thecompou... ...
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✓ Granted for thecompou... ...
Group.ReadWrite.All	Delegated	Read and write all groups	Yes	✓ Granted for thecompou... ...
Mail.ReadWrite	Delegated	Read and write access to user mail	No	✓ Granted for thecompou... ...
Mail.Send	Delegated	Send mail as a user	No	✓ Granted for thecompou... ...
ServiceHealth.Read.All	Delegated	Read service health	Yes	✓ Granted for thecompou... ...
ServiceMessage.Read.All	Delegated	Read service announcement messages	Yes	✓ Granted for thecompou... ...
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No	✓ Granted for thecompou... ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for thecompou... ...
▼ Office 365 Management APIs (1)				...
ServiceHealth.Read	Application	Read service health information for your organization	Yes	✓ Granted for thecompou... Remove permission Revoke admin consent

To view and manage permissions and user consent, try [Enterprise applications](#).

Revoke admin consent for Office 365 Management APIs

M365 Supplemental Management Pack | API permissions

Search (Ctrl+/)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Revoke admin consent

Are you sure you want to revoke admin consent for Office 365 Management APIs – ServiceHealth.Read for M365 Supplemental Management Pack?

Yes, remove

Cancel

Add a permission

Grant admin consent for thecompoundsc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (10)				
ChannelMessage.Send	Delegated	Send channel messages	No	Granted for thecompou...
Directory.Read.All	Delegated	Read directory data	Yes	Granted for thecompou...
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	Granted for thecompou...
Group.ReadWrite.All	Delegated	Read and write all groups	Yes	Granted for thecompou...
Mail.ReadWrite	Delegated	Read and write access to user mail	No	Granted for thecompou...
Mail.Send	Delegated	Send mail as a user	No	Granted for thecompou...
ServiceHealth.Read.All	Delegated	Read service health	Yes	Granted for thecompou...
ServiceMessage.Read.All	Delegated	Read service announcement messages	Yes	Granted for thecompou...
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No	Granted for thecompou...
User.Read	Delegated	Sign in and read user profile	No	Granted for thecompou...
Office 365 Management APIs (1)				
ServiceHealth.Read	Application	Read service health information for your organization	Yes	Not granted for thecom...

Note: Once Admin Consent has been removed you will notice a warning icon, it is then safe to proceed with removing the Office 365 Management APIs permissions.

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 thecompoundsc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (10)				
ChannelMessage.Send	Delegated	Send channel messages	No	Granted for thecompou...
Directory.Read.All	Delegated	Read directory data	Yes	Granted for thecompou...
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	Granted for thecompou...
Group.ReadWrite.All	Delegated	Read and write all groups	Yes	Granted for thecompou...
Mail.ReadWrite	Delegated	Read and write access to user mail	No	Granted for thecompou...
Mail.Send	Delegated	Send mail as a user	No	Granted for thecompou...
ServiceHealth.Read.All	Delegated	Read service health	Yes	Granted for thecompou...
ServiceMessage.Read.All	Delegated	Read service announcement messages	Yes	Granted for thecompou...
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No	Granted for thecompou...
User.Read	Delegated	Sign in and read user profile	No	Granted for thecompou...
Office 365 Management APIs (1)				
ServiceHealth.Read	Application	Read service health information for your organization	Yes	Not granted for thecom...

Remove permission

M365 Supplemental Management Pack | API permissions

Search (Ctrl+/) « Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration

Remove permission
Are you sure you want to remove Office 365 Management APIs – ServiceHealth.Read from the configured permissions for M365 Supplemental Management Pack?
Yes, remove Cancel

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (10) ...				
ChannelMessage.Send	Delegated	Send channel messages	No	✓ Granted for thecompou... ...
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for thecompou... ...

Add GraphAPI permissions for Services and Teams Management Packs

Microsoft Azure Search resources, services, and docs (G+)

> thecompoundsc > M365 Supplemental Management Pack

M365 Supplemental Management Pack | API permissions

Search (Ctrl+/) « Refresh Got feedback?

You are editing permission(s) to your application, users will have...

The "Admin consent required" column shows the default value for organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permission. All the permissions the application needs. [Learn more about permissions](#)

+ Add a permission ✓ Grant admin consent for thecompoundsc

API / Permissions name	Type	Description
> Microsoft Graph (10)		


To view and manage permissions and user consent, try [Enterprise app](#)


Request API permissions


Select an API


Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs

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

**Azure Communication Services**
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

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

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

Example: [ServiceHealth.Read.All](#)

The screenshot below illustrates how to add the ServiceHealth.Read.All delegated permission. You can filter by permission, place a check mark in the box and select Add Permissions.

> M365 Supplemental Management Pack

Supplemental Management Pack | API permissions

« Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if you are the app owner.

The "Admin consent required" column shows the default value for an organization. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by an administrator. Learn more about permissions and consent

+ Add a permission

Grant admin consent for the compound scope

API / Permissions name	Type	Description
▼ Microsoft Graph (9)		
ChannelMessage.Send	Delegated	Send channel messages
Directory.Read.All	Delegated	Read directory data
Files.ReadWrite.All	Delegated	Have full access to all files
Group.ReadWrite.All	Delegated	Read and write all groups
Mail.ReadWrite	Delegated	Read and write access to mail
Mail.Send	Delegated	Send mail as a user
ServiceHealth.Read.All	Delegated	Read service health
Sites.ReadWrite.All	Delegated	Edit or delete items in all sites
User.Read	Delegated	Sign in and read user profile

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

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

Application type: Your application is signed-in

Select permissions

servi

The "Admin consent required" column shows the default value for an organization, user, or app. This column may not reflect the value in your organization. Learn more

Permission
> DeviceManagementServiceConfig
> IdentityRiskyServicePrincipal
▼ ServiceHealth
<input type="checkbox"/> ServiceHealth.Read.All ⓘ Read service health

Add permissions

Discard

Once the permission has been added, you must grant admin consent for ALL permissions. Ignore the “Admin consent required” column, it’s misleading. Repeat for the remaining required permissions.

Supplemental Management Pack | API permissions

« Refresh Got feedback?

Grant admin consent confirmation.
Do you want to grant consent for the requested permissions for all accounts in thecompoundsc? This will update any existing admin consent records this application already has for the requested permissions. [Learn more about permissions and consent](#)

Yes

No

+ Add a permission

✓ Grant admin consent for thecompoundsc

API / Permissions name	Type	Description	Admin consent required	Status
▼ Microsoft Graph (11)				
ChannelMessage.Send	Delegated	Send channel messages	No	✓ Granted for thecompoundsc
Chat.ReadWrite	Delegated	Read and write user chat messages	No	✓ Granted for thecompoundsc
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for thecompoundsc
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✓ Granted for thecompoundsc
Group.ReadWrite.All	Delegated	Read and write all groups	Yes	✓ Granted for thecompoundsc
Mail.ReadWrite	Delegated	Read and write access to user mail	No	✓ Granted for thecompoundsc
Mail.Send	Delegated	Send mail as a user	No	✓ Granted for thecompoundsc
Presence.Read	Delegated	Read user's presence information	No	✓ Granted for thecompoundsc
ServiceHealth.Read.All	Delegated	Read service health	Yes	⚠ Not granted for thecompoundsc
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No	✓ Granted for thecompoundsc
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for thecompoundsc

Services

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

Teams

Note: The Teams management pack will also require two additional permissions to leverage new features.

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

Verify your API Permissions

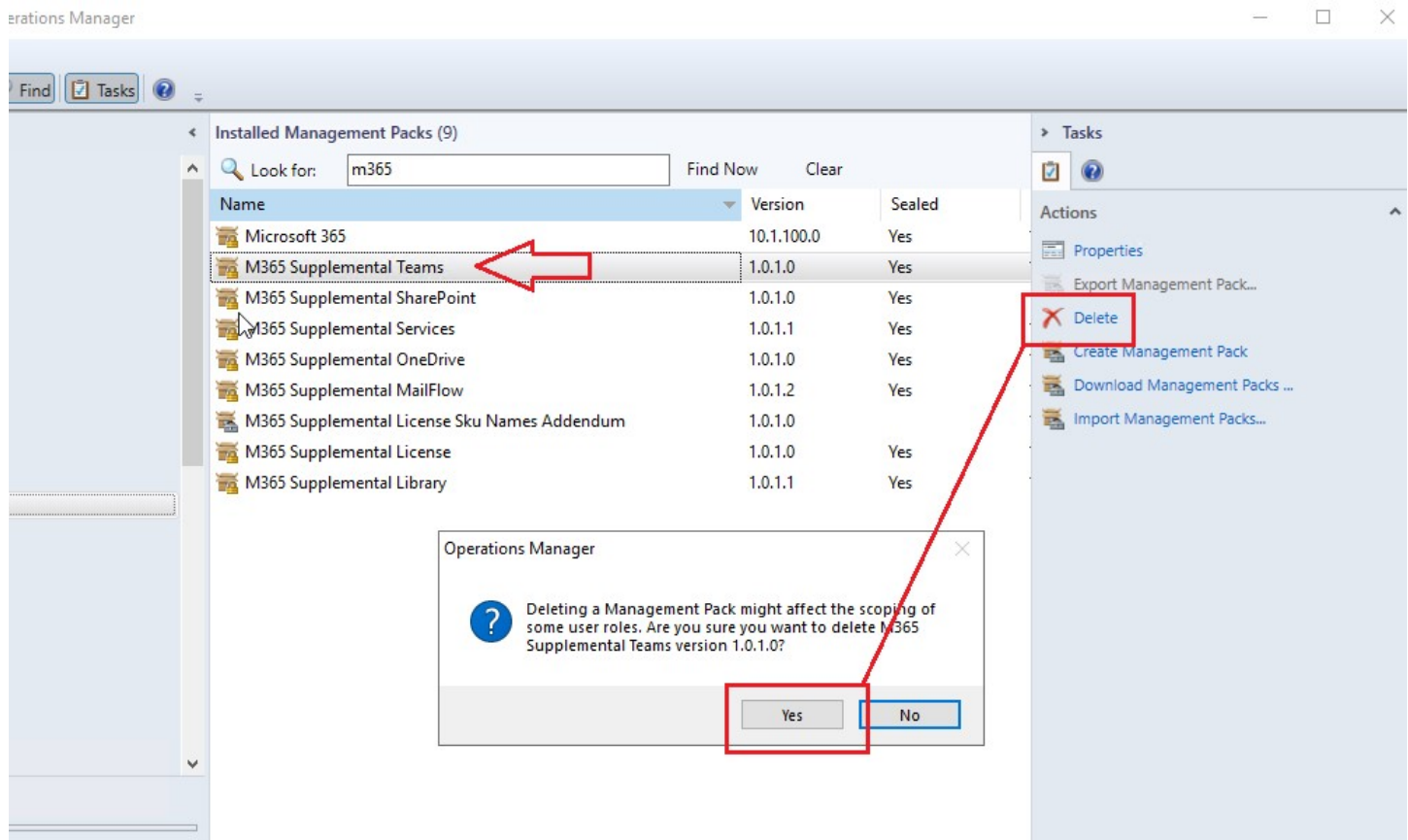
The full set of GraphAPI permissions appear as shown below, this includes permissions for each Management Pack.

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, Enterprise applications, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators | Preview, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled 'monitoringguys_scomlab1 | API permissions'. It includes a search bar, a refresh button, and a 'Got feedback?' link. A message states 'Successfully granted admin consent for the requested permissions.' Below this, a note explains the 'Admin consent required' column. The 'Configured permissions' section lists 11 permissions for Microsoft Graph, all of which are delegated and have been granted for monitoring. The permissions table is as follows:

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

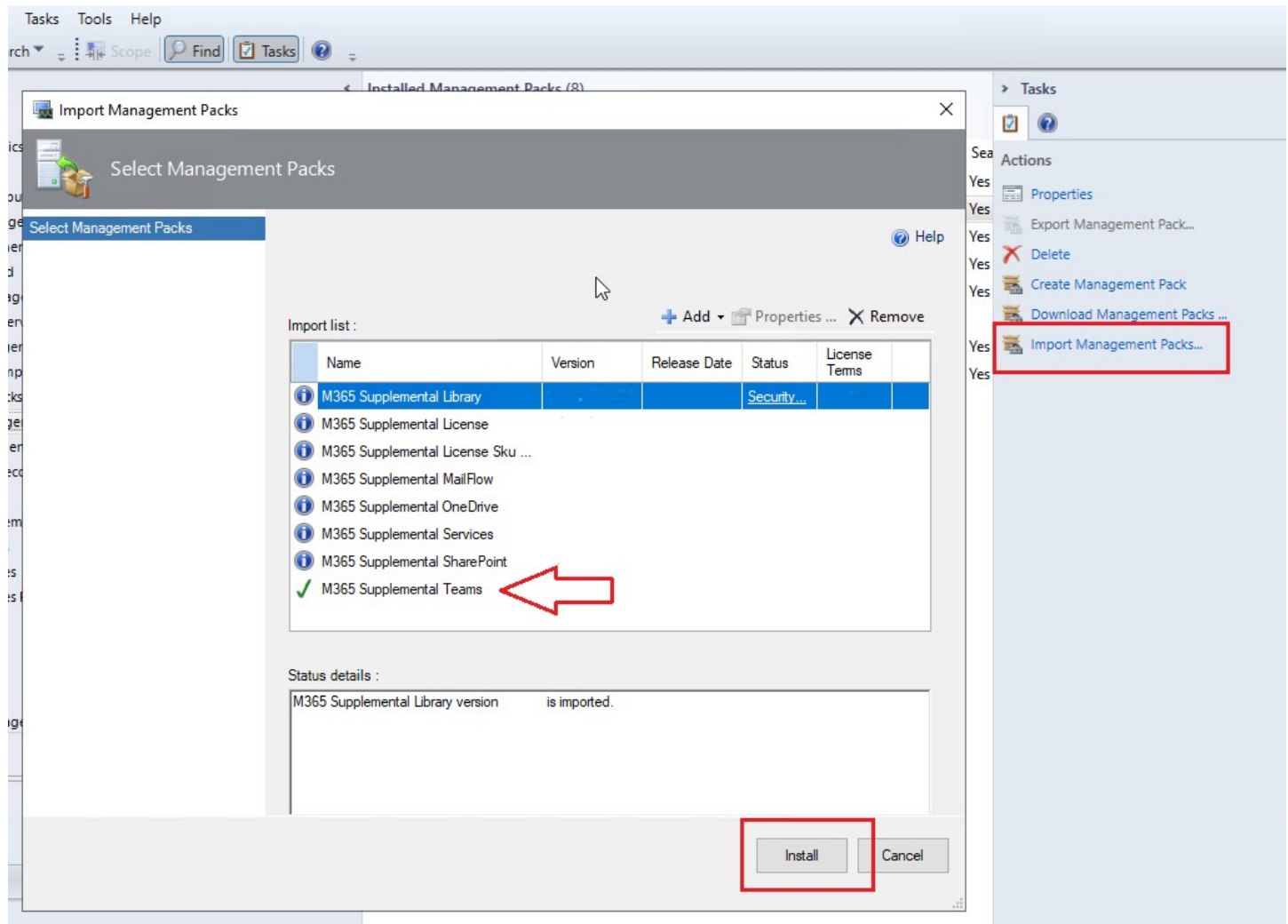
Remove Teams MP

All of the other MPs in this bundle can be upgraded, however; to leverage the new features in the Teams Monitoring Management Pack you will need to remove and import the new version. This is due to significant changes in the Teams Service Model. You may also have to delete any dependent overrides or MPs. Follow your standard procedure for removing references to the sealed MP.



Import New Management Packs

Notice: Most of the MPs already exist so they will be replaced/updated. However, Teams had been removed previously so it appears as a new MP. This is expected. The Version column of the screenshot above has been omitted intentionally.



Import Management Packs

Select Management Packs

Help

Import list :

+ Add ▾ Properties ... ✕ Remove

Name	Version	Release Date	Status	License Terms
M365 Supplemental Library			Security...	
M365 Supplemental License				
M365 Operations Manager				
M365				
M365				
M365				
M365				
M365				
M365				
M365				

One or more management packs which are ready to install present a security risk. Are you sure you want to continue?

Yes No

Status details :

M365 Supplemental Library version 1.0.0 is imported.

Install Cancel

Run Configure Services task to update GraphAPI endpoints

Services now supports GraphAPI to access the health status and message center posts about Microsoft cloud services. The endpoints used to discover/monitor Services must be updated. Run the configuration task as shown. No overrides are required.

NOTE: The new GraphAPI Endpoints

M365 Watcher Nodes (1)

State	Name	Path	M365 License Role Class	Health
Healthy	monguys.onmicrosoft.com	brianzdev.thecompound.fl	Healthy	Healthy

Run Task - M365 Supplemental - Configure Services

Run the task on these targets

Target	Run Location
<input checked="" type="checkbox"/> monguys.onmicrosoft.com	brianzdev.thecompound.fl

Task Parameters

Name	Value
PushLibraryPath	
MgmtApiURL	https://graph.microsoft.com
MgmtApiTokenURL	https://login.microsoftonline.com
MgmtApiTokenScopeURL	https://graph.microsoft.com/.default
M365_ClientSecret	LEAVE_BLANK_TO_INHERIT_DEFAULT_VALUE

Task credentials

☒ Use the predefined Run As Account

☐ Other :

User name :

Password :

Domain :

Task confirmation

☐ Don't prompt when running this task in the future

Task description

DeleteConfiguration: Set True to undiscover this component. To keep any existing configuration from being changed, use -1. Otherwise the configuration will get overwritten with the parameter defaults.

Run **Cancel**

M365 Supplemental Service Monitoring

- M365 Supplemental - Configure License
- M365 Supplemental - Configure MailFlow
- M365 Supplemental - Configure OneDrive
- M365 Supplemental - Configure Services
- M365 Supplemental - Configure SharePoint
- M365 Supplemental - Configure Teams
- M365 Supplemental - Get App Expiration Data
- M365 Supplemental - Get Org Directory Usage Data
- M365 Supplemental - Modify Watcher Node Default

Discovery is triggered on demand by the task and the new properties are updated instantly.

The screenshot shows the 'Discovered Inventory (M365 Services Role Class) (1)' section. A red arrow points to the title bar of this section. Below it is a table with columns: State, Name, Path, Display Name, IntervalSeconds, M365_AccountName, and M365_AccountID. The first row shows a 'Critical' state for 'monguys.onmicrosoft.com' with a path 'brianzdev.thec...'. Below the table is a 'Detail View' section showing the 'M365 Services Role Class properties of monguys.onmicrosoft.com'. A red box highlights the 'MgmtApiURL', 'MgmtApiTokenURL', and 'MgmtApiTokenScopeURL' properties.

State	Name	Path	Display Name	IntervalSeconds	M365_AccountName	M365_AccountID
Critical	monguys.onmicrosoft.com	brianzdev.thec...	monguys.onmi...	900	brianzadmin@...	

Detail View

M365 Services Role Class properties of monguys.onmicrosoft.com

Display Name	monguys.onmicrosoft.com
Full Path Name	brianzdev.thecompound.fl\monguys.onmicrosoft.com\monguys.onmicrosoft.com
IntervalSeconds	900
M365_AccountName	brianzadmin@monguys.onmicrosoft.com
M365_AccountID	
M365_AccountPassword	nt authority\system:01000000d08c9ddf0115d1118c7a00c04fc297eb010000001c3451c0d63ed549b8aa26220e4566b
M365_ClientID	fd924a03-e531-47fa-ba58-5e87b1605de2
M365_ClientSecret	nt authority\system:01000000d08c9ddf0115d1118c7a00c04fc297eb010000001c3451c0d63ed549b8aa26220e4566b
TenantName	monguys.onmicrosoft.com
MgmtApiURL	https://graph.microsoft.com
MgmtApiTokenURL	https://login.microsoftonline.com
MgmtApiTokenScopeURL	https://graph.microsoft.com/.default

Note: It's likely that Services may lose communication (Grey State) at first but health should re-establish connection after a while. If you have any doubts about the Services workflows running (or any of the monitoring workflows), you can always use the test tasks available for all M365 applications to get immediate status.

Example for Services; get incident details or service status instantly.

The screenshot shows a list of tasks under the heading 'M365 Service Class Tasks'. The tasks are: 'M365 Supplemental - Get Service Incident Data', 'M365 Supplemental - Get Services Data', and 'M365 Supplemental - Modify Services Configurati'.

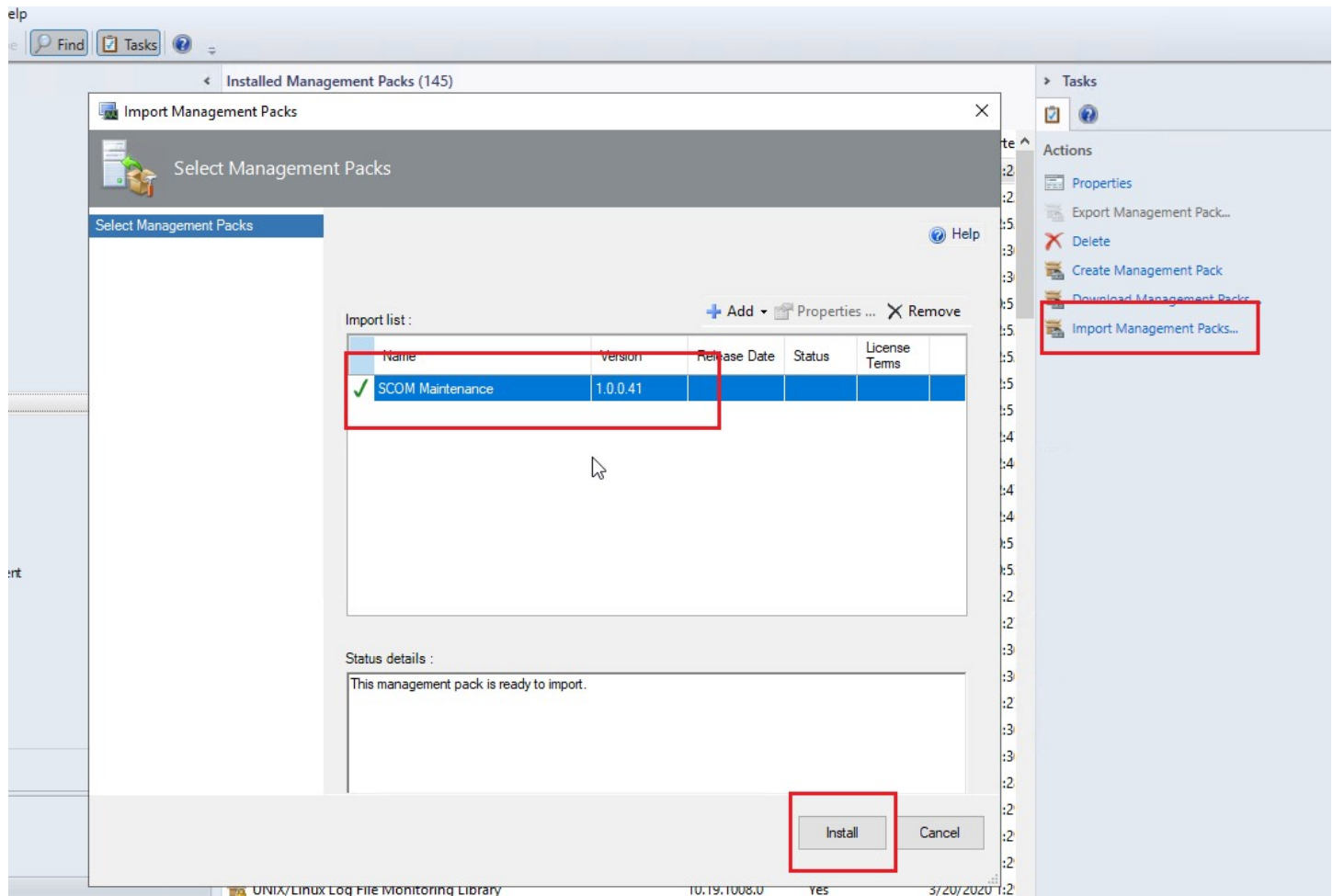
Troubleshooting

Workflows won't initialize after the management pack remove/reinstall procedure

Once the Teams MP has been removed and reinstalled the configuration stored in the registry on the Watcher Node allows for immediate restoration of monitoring. Should there be a delay, you may need to import the SCOM Maintenance Management Pack to speed up grooming to remove Discovery Data.

Import the SCOM Maintenance management pack

Download Here: <https://monitoringguys.com/download/6792/>



Teams Example: If, after configuring Teams, objects do not become discovered or they become discovered but do not become monitored:



Run the task to initiate Snapshot Synchronization. This is a process that occurs automatically every 24 hours, but the task will run it immediately. Snapshot synch will force the recalculation of all configurations. This should cause the watcher nodes to recognize the changes to the Teams service model and initialize the correct monitoring workflows.

Groom Discovery Data

In some cases after the removal and reinstall we will need to clean up stale discovery data and force snapshot synchronization.

The screenshot displays the Microsoft Operations Manager (MOM) console interface. On the left, the 'Monitoring' tree view shows the 'Maintenance' folder expanded, with 'OpsDB Watcher' selected and highlighted by a red rectangle. The main pane shows the 'OpsDB Watcher (1)' entity, which is in a 'Healthy' state. A dialog box titled 'Run Task - OpsDB - 1) Execute DiscoveryDataPurge' is open in the center. This dialog contains several sections: 'Run the task on these targets' with a table showing the target 'All Management Servers Resource Pool DB Watcher' and its location 'brianzom19.thecompound.fl'; 'Task Parameters' with a table listing parameters like 'WriteToEventLog' (true), 'SQLCMDTimeoutSeconds' (600), 'SQLCMD' (a script path), and 'ProbeActionTimeoutSeconds' (660); 'Task credentials' with 'Use the predefined Run As Account' selected; 'Task description' explaining the purpose of the task; and 'Task confirmation' with 'Don't prompt when running this task in the future' checked. The 'Run' button at the bottom right of the dialog is highlighted with a red rectangle. On the right side of the console, the 'Tasks' pane shows a list of tasks, with 'OpsDB - 1) Execute DiscoveryDataPurge' highlighted by a red rectangle. Other tasks listed include 'OpsDB - 2) Show DiscoveryDataPurgeHistory', 'OpsDB - 3) Show Snapshot Synchronization History', and 'OpsDB - 4) Execute Snapshot Synchronization'.

Monitoring

- Active Alerts
- Closed Alerts
- Discovered Inventory
- Distributed Applications
- Maintenance Schedules
- Task Status
- UNIX/Linux Computers
- Windows Computers
- Agentless Exception Monitoring
- Application Monitoring
- Azure Log Analytics
- Data Warehouse
- M365 Supplemental
- Maintenance
- OpsDB Watcher
- Microsoft 365
- Microsoft Audit Collection Services
- Microsoft SQL Server
- Microsoft SQL Server RunAs Config
- Microsoft Windows Client
- Microsoft Windows Internet Information Services
- Microsoft Windows Server
- Microsoft Windows Server DNS
- Network Monitoring

Monitoring

Authenticating

Administration

My Workspace

OpsDB Watcher (1)

Look for: Find Now Clear

State Healthy Name All Management Servers Resource Pool DB Watcher

Task Status - OpsDB - 1) Execute DiscoveryDataPurge

The task completed successfully.

Task	Status	Task Target
OpsDB - 1) Execute Discovery...	Success	all management servers resource po...

Task Output

Time: 12/11/2021 5:01:46 PM automatically every night however this is a way to manually initiate the purge.

Start Time: 12/7/2021 5:01:46 PM

Submitted By: THECOMPOUND\Administrator

Run As:

Run Location:

Target:

Target Type: Operations Manager Operational Database Watcher

Category: Maintenance

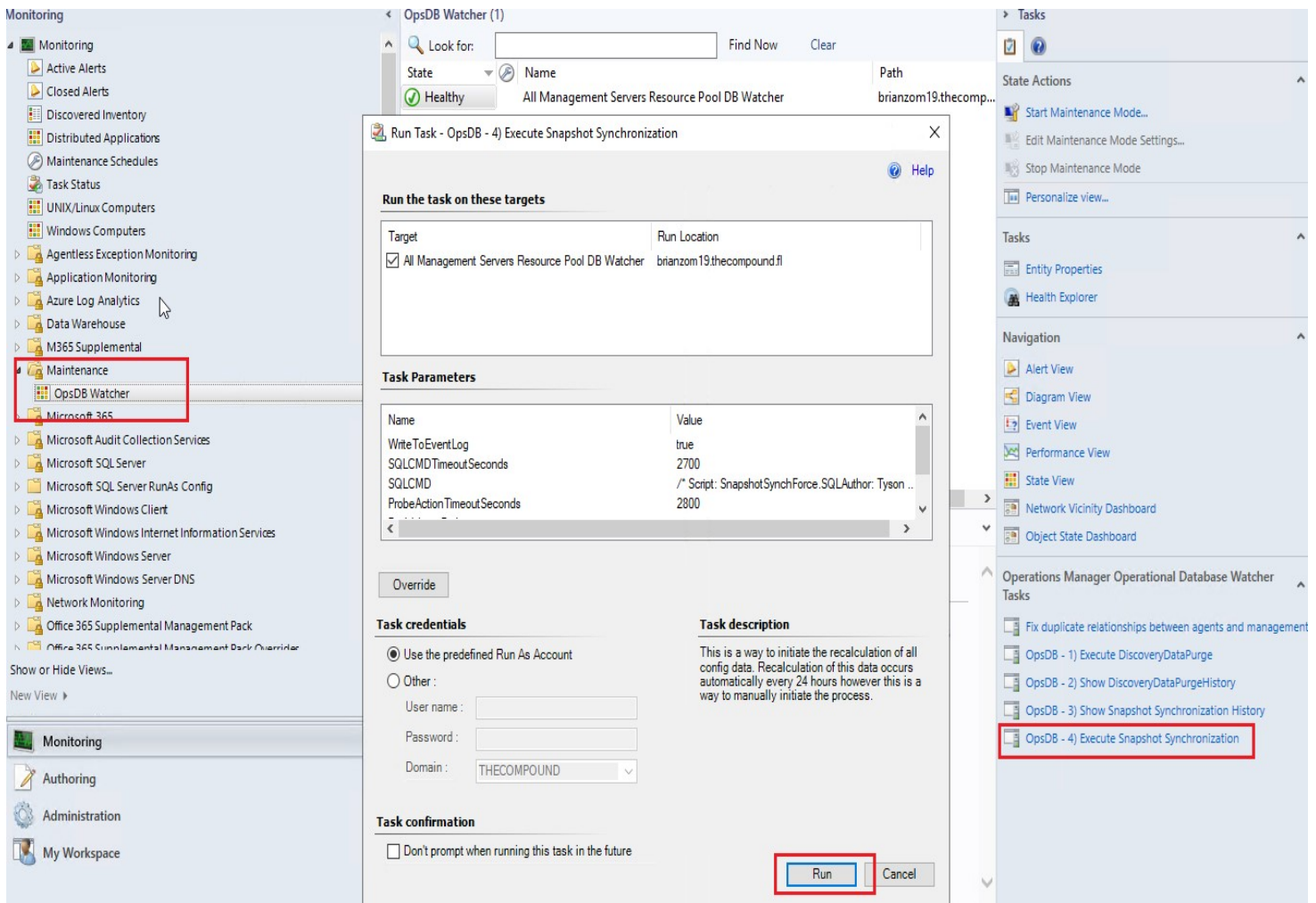
Task Output:

ItemsToPurge	ItemsDeleted	ItemsRemaining
0	0	0

You can close this dialog at any time. Doing so will not interrupt executing tasks. You can check the status of tasks in a task status view.

Close

Verify Purge results: If the ItemsRemaining count is above zero (0), run the task again. Otherwise move on to the next step.



In very large environments, this process could take as long as 30 minutes. Please be patient. You can check on the job status by running the task: **OpsDB - 3) Show Snapshot Synchronization History**.

Monitoring

- Monitoring
 - Active Alerts
 - Closed Alerts
 - Discovered Inventory
 - Distributed Applications
 - Maintenance Schedules
 - Task Status
 - UNIX/Linux Computers
 - Windows Computers
 - Agentless Reception Monitoring
 - Application Monitoring
 - Azure Log Analytics
 - Data Warehouse
 - M365 Supplemental
 - Maintenance
 - OpsDB Watcher
 - Microsoft 365
 - Microsoft Audit Collection Services
 - Microsoft SQL Server
 - Microsoft SQL Server RunAs Config
 - Microsoft Windows Client
 - Microsoft Windows Internet Information Services
 - Microsoft Windows Server
 - Microsoft Windows Server DNS
 - Network Monitoring

Show or Hide Views...

New View ▶

Monitoring

- Authoring
- Administration
- My Workspace

OpsDB Watcher (1)

Look for: Find Now Clear

State: Name: All Management Servers Resource Pool DB Watcher

Task Status - OpsDB - 4) Execute Snapshot Synchronization

The task completed successfully.

Task	Status	Task Target
OpsDB - 4) Execute Snapshot...	Success	all management servers resource po...

Task Output

Copy Text Copy HTML

```
DurationSeconds : 15
Average Runtime (seconds) : 15
ErrorMessage :

WorkItemRowId : 7895132
WorkItemName : SnapshotSynchronization
WorkItemStateId : 20
WorkItemStateName : Succeeded
ServerName : BRIANZOM19
InstanceName : Default
StartedDateTimeUtc : 12/6/2021 10:41:09 AM
CompletedDateTimeUtc : 12/6/2021 10:41:25 AM
DurationSeconds : 16
Average Runtime (seconds) : 15
ErrorMessage :
```

You can close this dialog at any time. Doing so will not interrupt executing tasks. You can check the status of tasks in a task status view.

Close

Tasks

State Actions

- Start Maintenance Mode...
- Edit Maintenance Mode Sel...
- Stop Maintenance Mode
- Personalize view...

Navigation

- Alert View
- Diagram View
- Event View
- Performance View
- State View
- Network Vicinity Dashboard
- Object State Dashboard

Generations Manager Operations

- Fix duplicate relationships t...
- OpsDB - 1) Execute Discover...
- OpsDB - 2) Show Discovery
- OpsDB - 3) Show Snapshot
- OpsDB - 4) Execute Snapsh...

After completing these tasks you will be able to return to the System Center Operations Manager console and verify that M365 Services and Teams Monitoring has resumed.

The Maintenance tasks won't run

If you cannot successfully run the maintenance tasks, then you can always run the SQL queries manually. You will first have to unseal the SCOMMaintenance.mpb file. (<https://monitoringguys.com/2020/10/14/keep-your-management-pack-files-organized/>) This will extract the SQL scripts to individual .SQL files. From there it's up to you to manually run the SQL scripts on the OpsDB SQL instance.

```
Directory: C:\Test\SCOMMaintenance\BuildArchives\20211129-150150.281_DELETE_ME

Mode                LastWriteTime         Length Name
----                -
-a-----          11/29/2021   2:58 PM           53248 SCOMMaintenance.mpb

PS C:\Test\SCOMMaintenance\BuildArchives\20211129-150150.281_DELETE_ME> Unseal-SCOMMP -indir .\ -outDir C:\temp\SCOMMaintenanceUNSEALED

GAC      Version      Location
---      -
True     v4.0.30319     C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.EnterpriseManagement.Core\v4.0.7.0.5000.0__31bf3856ad364e35\Microsoft.EnterpriseManagement.Core.dll
True     v4.0.30319     C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.EnterpriseManagement.Packaging\v4.0.7.0.5000.0__31bf3856ad364e35\Microsoft.EnterpriseManagement.Packaging.dll

PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\temp\SCOMMaintenanceUNSEALED
PSChildName  : SCOMMaintenance.mpb(1.0.0.33)
PSDrive      : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : True
Name         : SCOMMaintenance.mpb(1.0.0.33)
FullName     : C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)
Parent       : SCOMMaintenanceUNSEALED
Exists       : True
Root         : C:\
Extension    : .33)
CreationTime : 11/29/2021 7:19:28 PM
CreationTimeUtc : 11/30/2021 1:19:28 AM
LastAccessTime : 11/29/2021 7:19:28 PM
LastAccessTimeUtc : 11/30/2021 1:19:28 AM
LastWriteTime : 11/29/2021 7:19:28 PM
LastWriteTimeUtc : 11/30/2021 1:19:28 AM
Attributes   : Directory
Mode         : d-----
BaseName     : SCOMMaintenance.mpb(1.0.0.33)
Target       : {}
LinkType     :

SCOMMaintenance.mpb
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\SCOMMaintenance.xml
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\DiscoveryDataPurge.SQL
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\Maintenance.PoShSQLCmd.ps1
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\ShowDiscoveryDataPurgeHistory.SQL
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\Maintenance.Library.ps1
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\ShowSnapshotSynchHistory.SQL
C:\temp\SCOMMaintenanceUNSEALED\SCOMMaintenance.mpb(1.0.0.33)\SnapshotSynchForce.SQL

PS C:\Test\SCOMMaintenance\BuildArchives\20211129-150150.281_DELETE_ME>
```

