

Guide to Microsoft 365 Management Pack for System Center Operations Manager

**Microsoft Corporation**

Published: May 2022

If you have an idea or suggestion about this management pack, the Operations Manager team encourages you to share it at the [SCOM Feedback site](mailto:m365mp@microsoft.com).

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. 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, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2022 Microsoft Corporation. All rights reserved.

Microsoft, System Center, Windows, and Microsoft 365 are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Guide to Microsoft 365 Management Pack for System Center Operations Manager 6](#_Toc104992840)

[Change history. 6](#_Toc104992841)

[Supported configurations. 7](#_Toc104992842)

[Resource pools configuration 7](#_Toc104992843)

[Watcher Node configuration 7](#_Toc104992844)

[Network, Firewalls & Proxy 7](#_Toc104992845)

[Required Permissions 8](#_Toc104992846)

[Files in this Management Pack 9](#_Toc104992847)

[Getting started 9](#_Toc104992848)

[Installing the Management Pack 9](#_Toc104992849)

[Importing the Management Pack 10](#_Toc104992850)

[Upgrading from Microsoft 365 MP Version 10.1.100.0 11](#_Toc104992851)

[Upgrading from Microsoft 365 MP Version 10.1.270.0 14](#_Toc104992852)

[Manage Microsoft 365 subscriptions. 14](#_Toc104992853)

[Monitoring configurations 15](#_Toc104992854)

[Register the application in Azure Active Directory 33](#_Toc104992855)

[Configuring the Microsoft 365 Management Pack 44](#_Toc104992856)

[Adding a Watcher Node 44](#_Toc104992857)

[Editing a Watcher Node 58](#_Toc104992858)

[Removing a Watcher Node 69](#_Toc104992859)

[Configure proxy connection. 70](#_Toc104992860)

[Run As Configuration 72](#_Toc104992861)

[Management Pack Contents 75](#_Toc104992862)

[Microsoft 365 subscriptions 75](#_Toc104992863)

[Services discovery 75](#_Toc104992864)

[Watcher Node discovery 76](#_Toc104992865)

[Connection State monitor 76](#_Toc104992866)

[Microsoft 365 Incidents and Messages 76](#_Toc104992867)

[Alert Autoclose rule 77](#_Toc104992868)

[Management Pack Elements 78](#_Toc104992869)

[Microsoft 365 Monitoring Dashboards 86](#_Toc104992870)

[Licensing Views Folder 87](#_Toc104992871)

[Mail Flow Views Folder 87](#_Toc104992872)

[Performance Views Folder 87](#_Toc104992873)

[SharePoint Views Folder 88](#_Toc104992874)

[Teams Views Folder 89](#_Toc104992875)

[M365 Dashboards Folder (Web Console) 89](#_Toc104992876)

[Subscription Health 90](#_Toc104992877)

[Service Status 91](#_Toc104992878)

[Alert widgets 92](#_Toc104992879)

[Active Incidents 93](#_Toc104992880)

[Resolved Incidents 94](#_Toc104992881)

[Admin Center 94](#_Toc104992882)

[Appendix: Troubleshooting the Watcher Node Setup 96](#_Toc104992883)

[Appendix: Troubleshooting M365 Monitoring 97](#_Toc104992884)

[Troubleshooting Mail Flow Monitoring 97](#_Toc104992885)

[Troubleshooting SharePoint Monitoring 98](#_Toc104992886)

[Troubleshooting Teams Monitoring 98](#_Toc104992887)

[Troubleshooting Licensing 99](#_Toc104992888)

[Troubleshooting Microsoft 365 Incidents and Messages 99](#_Toc104992889)

[Appendix: Application Permission Requirements 101](#_Toc104992890)

[Appendix: Certificates 103](#_Toc104992891)

[Certificate Renewal 105](#_Toc104992892)

[Appendix: Delegated Access 106](#_Toc104992893)

[SharePoint/OneDrive 106](#_Toc104992894)

[Teams 106](#_Toc104992895)

[M365 Mail 106](#_Toc104992896)

[Appendix: Known Issues 107](#_Toc104992897)

[Appendix: Event Log Entries 108](#_Toc104992898)

[Appendix: Cookdown and Interval Overrides 110](#_Toc104992899)

[Appendix: Network Assessment Tools 112](#_Toc104992900)

[Teams NAT Manual Installation and Configuration 112](#_Toc104992901)

[Skype for Business NAT Manual Installation and Configuration 112](#_Toc104992902)

[Appendix: Microsoft 365 Clouds (incl. GCC High) 113](#_Toc104992903)

[GCC High Support for Subscriptions 113](#_Toc104992904)

[GCC High Support for Watcher Nodes 114](#_Toc104992905)

[GCC High Limitations 115](#_Toc104992906)

Guide to Microsoft 365 Management Pack for System Center Operations Manager

This guide is based on version 10.2.0.0 of the Microsoft 365 Management Pack.

Change history.

|  |  |
| --- | --- |
| **Release Date** | **Changes** |
| May, 2021 | Original (CTP) release of this management pack. |
| Aug, 2021 | General Availability release of this management pack. |
| Dec, 2021 | Version 2 of this management pack. Notable changes:   * Replaced Service Comms API with Graph API for M365 Service Health alerts. * Allow choice of Certificate or Secret authentication for Graph API calls. * Updated to latest version of MSAL library. * Allow monitoring multiple license SKUs with single watcher node. * Fixed automatic application creation in the Subscription wizard (due to changes to Azure Active Directory). * Clarify internal vs. external on-premises Exchange URL’s. * Fixed accessibility issues in HTML5 dashboards. |
| May, 2022 | Version 3 of this management pack. Notable changes:   * Allow client secret, delegated or certificate authentication. * Support Teams Network Assessment tool (S4B NAT still works). * SKU license warning and critical thresholds are now defined as specific numbers rather than percentages and are defined on a per-SKU basis rather than one value applying equally to all SKUs. * Office response time performance collection rule can now test against TCP ports (for example, HTTPS or port 443). * Fixes several bugs with Service Health alerts reported by users. * Fixed remaining accessibility issues in HTML5 dashboards. * Add Teams Chat to Teams synthetic transaction (delegated authentication only). * Allow management servers and gateways to be used as watcher nodes. * Add monitor for certificates used in watcher node subscriptions. |

Supported configurations.

Microsoft 365 Management Pack for System Center Operations Manager is designed for the following versions of System Center Operations Manager:

* System Center Operations Manager 2019
* System Center Operations Manager 2022

The Operations Manager Console used to configure the management pack requires .Net Framework 4.6.2 or higher.

Management Server Pool used to run Microsoft 365 monitoring workflows requires .Net Framework 4.7.2 or higher.

For the time being, monitoring of Chinese Microsoft 365 subscriptions is not supported.

Resource pools configuration

Microsoft 365 Management Pack uses an agentless monitoring approach for monitoring the Microsoft 365 Admin Center. All other monitoring workflows are executed on watcher nodes.

It is possible to create custom Management Server pools to filter the list of Management Servers, which will run the agentless Microsoft 365 Admin Center monitoring workflows (discovery, monitor, rules). See [How to Create a Resource pool](http://go.microsoft.com/fwlink/?LinkId=692042) on Microsoft Docs for details.

Watcher Node configuration

The Microsoft 365 Management Pack uses watcher nodes to collect data from the services being monitored. This can include synthetic transactions and the times taken to execute transactions are measured and monitored. The Microsoft 365 Management Pack includes a setup wizard to simplify the setup and configuration of both the watcher node as well as the management pack itself.

The watcher node has the following requirements:

* The watcher node requires a SCOM agent, management server or gateway, and the agent must be a member of the SCOM management group where the Microsoft 365 Management Pack is installed.
* PowerShell version 5 or higher. It can be downloaded and installed as part of the Windows Management Framework 5.1:  
  <https://www.microsoft.com/en-us/download/details.aspx?id=54616>
* .NET version 4.7.2 or higher
* The Teams Network Assessment Tool is required to evaluate network performance and network connectivity to determine how well the network would perform for a Microsoft Teams call. The watcher node setup wizard will attempt to install the Teams Network Assessment Tool, however if there are problems or if it needs to be installed manually see [Appendix: Network Assessment Tools](#Appendix_Network_Assessment_Tools).

Network, Firewalls & Proxy

The watcher node requires network connectivity to the Microsoft 365 environment to execute synthetic transactions. This article provides details about the specific network requirements to connect to Microsoft 365 services:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide#bkmk_teams>

If the watcher node is behind a firewall, or requires a proxy to access the internet, most synthetic transactions will fail, unless proxying is enabled. See [the section on setting up a proxy for synthetic transactions](#Proxy_Synthetic_Transaction) for details.

Required Permissions

Many of the synthetic transactions, monitors and rules defined in Microsoft 365 Management Pack rely on Graph API for secure authentication, operations, and data collection. As a result, there are several API permissions required for registered applications in the tenant of the Microsoft 365 subscription which is being monitored.

To further restrict the Exchange Permissions, the application permissions can be scoped by creating an Application Access Policy as described in <https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access>.

To further restrict the SharePoint Permissions to specific collections, see [Controlling app access on a specific SharePoint site collections is now available in Microsoft Graph - Microsoft 365 Developer Blog](https://developer.microsoft.com/en-us/graph/blogs/controlling-app-access-on-specific-sharepoint-site-collections/).

|  |  |  |
| --- | --- | --- |
| Synthetic Transaction | Graph API methods | Minimum Application permissions required |
| Microsoft 365 Free/Busy check | Get Schedule | Calendars.Read |
| Microsoft 365 Admin Center | Get Health Overviews Get Messages Get Issues | ServiceHealth.Read.All ServiceMessage.Read.All |
| Microsoft 365 Licensing | List Subscribed Skus Get User License Details | Organization.Read.All User.Read.All1 User.Read2 |
| Mailbox Count | Get Organization Get Reports | Organization.Read.All Reports.Read.All |
| Microsoft 365 to Microsoft 365 Mail Flow | List Mail Folders List Messages  Delete Message  Send Mail | Mail.ReadWrite Mail.Send |
| Microsoft 365 to Exchange Mail Flow | Send Mail | Mail.Send |
| SharePoint / OneDrive | List Sites List Drives Upload Content Download Content Delete Drive Item | Sites.Read.All Files.ReadWrite.All |
| Teams | List Groups List Channels Get Files Folder Upload Content Download Content Delete Drive Item | GroupMember.Read.All Channel.ReadBasic.All Files.ReadWrite.All ChannelMessage.Send2 ChannelMessage.Read.All2 |

Notes:

1 Required only if using Secret or Certificate authentication (application permissions).

2 Required only if using Delegated authentication (delegated permissions).

For additional details on the required permissions please refer to [**Appendix: Application Permission Requirements**](#Appendix_Application_Permission_Requirem).

Files in this Management Pack

This release includes the following files:

|  |  |
| --- | --- |
| File | Description |
| Microsoft.SystemCenter.M365.mpb | This management pack can be used to monitor Microsoft 365 services. |
| Microsoft.SystemCenter.M365.HtmlDashboard.mp | This management pack can be used to display dashboards in the Web Console. This requires Operations Manager 2019 or later. |
| Microsoft 365 MP Operations Guide.docx | This document provides guidance to configuration and usage of Microsoft 365 Management Pack for System Center Operations Manager |

In addition, after the management pack is installed and configured, an override management pack will be automatically created to store settings used by the Microsoft 365 Management Pack.

Getting started

Microsoft 365 Management Pack can be used to:

1. Proactively monitor the service level being provided by Microsoft 365 services including email, Teams, and SharePoint (which includes OneDrive) by securely performing synthetic transactions using Graph API.
2. Monitor Microsoft 365 license use and alert when usage meets certain criteria.
3. Monitor email transactions to and from on-premises Exchange server.
4. Monitor the health of connections between various locations and the Microsoft 365 service.
5. Reflect Microsoft 365 Incidents and Admin Center messages for the subscription to the Operations Manager alerts.
6. Visualize subscription health and corresponding alerts via the dashboards and alert views including HTML5 dashboards (requires Operations Manager 2019 or later).

Installing the Management Pack

To begin with, the Microsoft 365 Management Pack needs to be installed on a system so the management pack files can be accessed. Log in as a local Administrator, locate the Microsoft 365 Management Pack which was downloaded then double-click the following file:

Microsoft System Center Management Pack for Microsoft 365.msi

* The End User License Agreement will be displayed. Review the agreement and click on **I Agree** to continue.
* Next select the location where the management pack files will be placed.
* Click OK to continue.

The installation of the Microsoft 365 Management Pack will proceed, and the management packs will be copied to the installation location selected above.

Importing the Management Pack

For general information about importing a management pack, see [How to Import a Management Pack in Operations Manager 2019](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-import-remove-delete?view=sc-om-2019" \o "http://go.microsoft.com/fwlink/?LinkId=142351)

Follow these steps to import the management packs into your Operations Manager environment:

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 Manager 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. Select the management pack files created in the **Installing the Management Pack** Step above the click **Open**.
6. On the Select Management Packs page, verify the management packs that you selected for import are correct, then click **Import**.
7. The Import Management Packs page appears and shows the import progress. If problems occur, select the management pack to view the status details. When done click **Close**.
8. ***Note****:* If the Microsoft 365 item in the Administration workspace had already been selected, then old versions of the assemblies will still be in use. Restart the Operation Manager Console.

If you are upgrading from the Office 365 Management Pack, the previous version should be removed before installing the new Microsoft 365 Management Pack. If you are upgrading from an earlier version of the Microsoft 365 Management Pack, there may be manual steps that need to be done which are detailed in the [upgrading section](#Upgrading_From_Earlier_Version) below.

The management packs are sealed; therefore, you cannot save any changes of the original settings in the management pack file itself. However, when you customize the management pack for your environment, a new override management pack will be created.

Creating a new management pack for storing overrides has the following advantages:

* It simplifies the process of exporting customizations that have already been created in your test and pre-production environments to your production environment. For example, instead of exporting the default management pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.
* It allows you to delete the original management pack without first needing to delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If all your customizations are saved to the default management pack, you must delete the default management pack before you can delete an original management pack.
* It is easier to track and update customizations to individual management packs.

For more information about sealed and unsealed management packs, management pack customizations and the default management pack, see [What is in an Operations Manager Management Pack?](https://technet.microsoft.com/library/hh212794.aspx)

Upgrading from Microsoft 365 MP Version 10.1.100.0

With the retirement of the Message Center API, Microsoft 365 MP now uses Graph API to retrieve similar information. This results in a required change to endpoints used to fetch this data and the permissions required. Note that newly created subscriptions will be correct – this only applies to subscriptions created with version 10.1.100.0 (or earlier) of the Microsoft 365 MP.

There are two ways to update subscriptions when upgrading the MP:

1. Create new subscriptions and update existing watcher nodes to use the new subscriptions, then finally delete the old no longer used subscriptions. This would be a good opportunity to use certificate or delegated authentication, if desired.
2. Update the subscriptions to use the new endpoints and manually update the application in Azure Active Directory to give it the newly required permissions.

Depending on how many watcher nodes and subscriptions have been created, you may find one of these approaches better than the other. Choice 1) should require no further instructions. Choice 2) requires the following manual updates to subscriptions.

Existing subscriptions will need edited when the updated version of the M365 MP is deployed.

1. Open the Operations Manager console.
2. Select the **Administration** workspace**.**
3. Select the **Microsoft 365** item in the **Administration** tree.
4. For each of the **Configured subscriptions**
   1. Select the subscription and click **Edit subscription**.
   2. In the **Endpoint Selection and Server Pools** page update the **Microsoft Graph Endpoint** from the old Service Comm API URL (<https://manage.office.com/api/v1.0>) to the correct Microsoft Graph API URL appropriate to the organization (possibly <https://graph.microsoft.com/v1.0>, but dependent on which cloud is being used).

Graphical user interface, text, application

Description automatically generated

* 1. Confirm that the desired management server pool is selected.
  2. Click the **Next>** button.
  3. Enter the **Client Secret** or **Certificate Thumbprint**. If the client’s secret is not known, it is possible to add a new client secret using the Azure Portal.
  4. Click **Edit Subscription**.
  5. Click **Finish** to exit the wizard.
  6. Repeat for each subscription.

After updating all subscriptions in the Operations Manager console, the corresponding applications in Azure Active Directory will need to have permissions updated.

1. Open an internet browser and navigate to <https://portal.azure.com/>
2. Sign in as a user with sufficient permission to update applications.
3. From the list of **Azure services**, select **Azure Active Directory**.

Shape

Description automatically generated with low confidence

1. Select **App registrations**.



1. Select **All applications** if the application does not show up under **Owned applications**.
2. The **Application (client) ID** column corresponds to the **Client ID** shown when editing a subscription in the Operations Manager console.
3. For each existing subscription
   1. Find the corresponding application in the Azure Portal.
   2. Click on the hyperlinked **Display name**.
   3. Click on the **API permissions** link.



* 1. Click on **Add a permission**.



* 1. From the Request API permissions popup, select Microsoft Graph.

Text

Description automatically generated

* 1. Select Application permissions.

Graphical user interface, text, application

Description automatically generated

* 1. Type **service** in the **Start typing a permission to filter these results** box.
  2. From the filtered list, check **ServiceHealth.Read.All**, and **ServiceMessage.Read.All**.
  3. Click **Add permissions**.
  4. Click **Grant admin consent for** <<company name>>.



* 1. Optionally, you can remove the no longer required permission by clicking the … and selecting **Remove permission**.

Graphical user interface

Description automatically generated with medium confidence

* 1. Repeat for each application corresponding to an M365 subscription.

The final list of permissions should be the following:

Graphical user interface, text, application, email

Description automatically generated

Upgrading from Microsoft 365 MP Version 10.1.270.0

Updating from version 10.1.270.0 of the Microsoft 365 MP requires only a single simple manual step. If upgrading from version 10.1.100.0 or earlier, follow the steps in the previous section.

After upgrading from 10.1.270.0, using the Operations Manager console, open the **Administration** workspace and click on the **Microsoft 365** item. That is all. The first time this item is selected in the new management pack, it will automatically perform initialization to allow delegated authentication to work properly. Until this is done, existing workflows may fail.

After upgrading to version 10.1.270.0, old alerts from the Admin center will not show correct Alert Descriptions. New alerts will show correct Alert Descriptions, which will now include the Incident ID.

Manage Microsoft 365 subscriptions.

An Azure Service Principal (also Azure Active Directory Application or Azure SPN), not a specific user, conducts the monitoring and as a result an Azure Service Principal needs to be created. Accordingly, there are two options to create it: automatic and manual. Automatic option creates Azure Service Principal with Never expired key.

The first option (automatic) requires Global Administrator account of Microsoft 365 Subscription; therefore, one-time entering of the Global Administrator credentials is required, which provides access to Azure Active Directory for delegating the corresponding rights. **Please note that the credentials entered will not be stored**. In addition, changing the used Global Administrator password (or its expiration) will not affect the monitoring process.

For the second option (manual), an Azure subscription can be used, and this option does not suppose any further user actions during the process of monitoring. If you choose this option, you should register your created application in Azure Active Directory; for more details, see [Register the application in Azure Active Directory](#AppReg) section.

Monitoring configurations

To add, remove, or modify a monitored subscription, the Operations Manager Console must be run by a user belonging to the Operations Manager **Administrators** role.

To add and configure a subscription open the Operations Console, go to **Administration** section, and select **Microsoft 365:**

Graphical user interface, text, application

Description automatically generatedThere are two options available for monitoring your subscriptions:

#### **Monitoring configuration: Auto-created Azure Service Principal is used.**

If you want to use auto-created Azure Service Principal to configure the monitoring, which will completely create the subscription with all required permissions, perform the following steps:

1. Click **Add subscription** to open the **Add subscription** Wizard.

Graphical user interface, text, application, email

Description automatically generated

1. Enter a **Subscription Name**.

***Note:*** **Subscription Name** is a friendly name for the subscription; it will be used in Operations Manager. Subscription Name should be descriptive and unique. Subscription Name cannot contain spaces or single quote characters.

1. Select **Use auto-created Azure Service Principal** option:
2. Press **Next**.

Graphical user interface, text, application

Description automatically generated

1. Select whether to use Secret, Delegated, or Certificate authentication. See [Appendix: Certificates](#Appendix_Certificates) for more information.
2. If Certificate authentication is chosen, use the **Browse…** button to select a certificate file containing the public keys.
3. Press **Next**.

If using delegated authentication, the following page will be displayed. It will not be displayed if using Secret or Certificate authentication.

Graphical user interface, text, application, email

Description automatically generated

1. Select **Use same credentials for all services like M365 Mail, SharePoint/OneDrive, Teams**. The credentials entered will be used for all the services. Or:
2. Select **Use custom credentials for services**.

Graphical user interface, application

Description automatically generated

1. If you do not want to use certain synthetic transaction areas, you can uncheck the respective checkbox. Those transactions will be disabled in the watcher node wizard. There will be authentication errors on the watcher nodes if they were previously configured.
2. Press **Next**.Graphical user interface, text, application, email

   Description automatically generated
3. If using the GCC High cloud specify the GCC High endpoints. Refer to the section [GCC High Support for Subscriptions](#_GCC_High_Support) for the correct values.

**Authority Endpoint** is the URI used by the management pack to request the authorization for further monitoring of the subscription (default value: <https://login.microsoftonline.com>).

**Microsoft Graph Endpoint** is the URI for the REST API that provided programmatic access to Microsoft 365 objects (default value: <https://graph.microsoft.com/v1.0>).

If using the GCC High cloud, specify the GCC High endpoints. Refer to the section [GCC High Support for Subscriptions](#_GCC_High_Support) for the correct values.

**Please ensure that these endpoints are added to your organization’s AllowList.**

The Wizard does not validate credentials on this step! This allows the user to create a subscription object, even if the Internet connection is unstable. If the credentials are not valid, or the account does not have enough permissions, then a subscription object will be created, but Connection State monitor will change its health state to Critical and will raise a corresponding alert. If new endpoints are not specified, the default values will be used.

1. Choose a management server pool from the list of available pools.
2. Click **Next**.

***Note:*** The following page will differ, depending on the SPN creation method, the authentication method chosen, and whether the subscription is being created or edited. The images below represent only one of the possibilities.

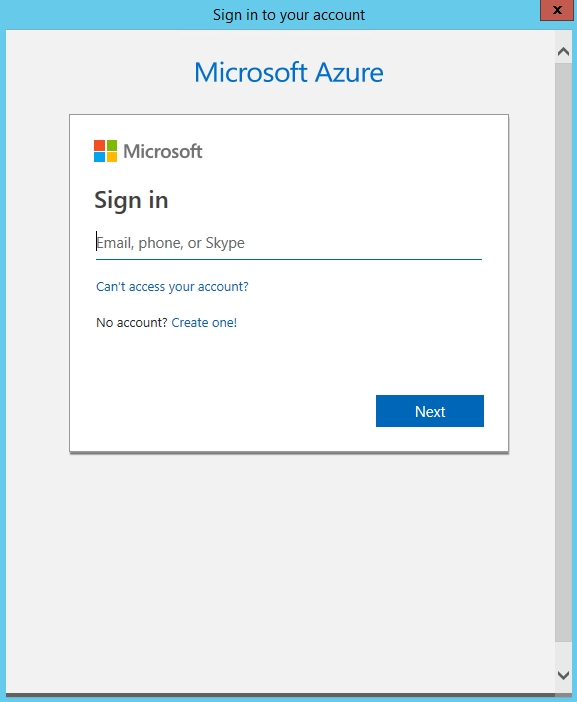
Graphical user interface, text, application, email

Description automatically generated

1. Click **Create**.

***Note:*** Once the Azure Service Principal is created, you cannot go back and change any of the previous settings. If changes are required to Endpoint Selection, complete the Add Subscription wizard, and then edit the new subscription. If other changes are required, delete the subscription, and create a new subscription with the correct values.

1. Enter Global Administrator account Login and click **Next**, then enter Password and click **Sign in**.



***Note:*** some browsers may block the content coming from Microsoft 365 Portal. In this case, add Microsoft 365 Portal to the trusted sites zone.

Graphical user interface, application

Description automatically generated

1. Wait until Azure Service Principal is created.

Graphical user interface, text, application, email

Description automatically generated

1. Upon successful creation of the application, the corresponding authentication data will be displayed in the appropriate fields (Tenant ID, Client ID, and Client Secret or Certificate Thumbprint).

***Note:*** It is strongly recommended to save this data for future reference!

1. Click **Add Subscription**.

Graphical user interface, text, application

Description automatically generated

1. Click **Finish** to close the Wizard. The new subscription will be added to Operations Manager and will appear on the Configured Subscriptions list.

#### **Monitoring configuration: Custom Azure Service Principal is used.**

If you want to use your custom Azure Service Principal for the monitoring, perform the following steps:

1. Click **Add subscription** to open the **Add subscription** Wizard.

Graphical user interface, text, application, email

Description automatically generated

1. Enter a **Subscription Name**.

***Note:*** **Subscription Name** is a friendly name for the subscription; it will be used in Operations Manager. Subscription Name should be descriptive and unique. Subscription Name cannot contain spaces or single quote characters.

1. Select **Use custom Azure Service Principal** option:
2. Press **Next**.

Graphical user interface, text, application

Description automatically generated

1. Select whether to use Secret, Delegated or Certificate authentication. See [Appendix: Certificates](#Appendix_Certificates) for more information.
2. Press **Next**.

If using delegated authentication, the following page will be displayed. It will not be displayed if using Secret or Certificate authentication.

Graphical user interface, text, application, email

Description automatically generated

1. Select **Use same credentials for all services like M365 Mail, SharePoint/OneDrive, Teams**. The credentials entered will be used for all the services. Or:
2. Select **Use custom credentials for services**.

Graphical user interface, application

Description automatically generated

1. If you do not want to use certain synthetic transaction areas, you can uncheck the respective checkbox. Those transactions will be disabled in the watcher node wizard. There will be authentication errors on the watcher nodes if they were previously configured.
2. Press **Next**.

Graphical user interface, text, application, email

Description automatically generated

1. If using the GCC High cloud specify the GCC High endpoints. Refer to the section [GCC High Support for Subscriptions](#_GCC_High_Support) for the correct values.

**Authority Endpoint** is the URI used by the management pack to request the authorization for further monitoring of the subscription (default value: <https://login.microsoftonline.com>).

**Microsoft Graph Endpoint** is the URI for the REST API that provided programmatic access to Microsoft 365 objects (default value: <https://graph.microsoft.com/v1.0>).

If using the GCC High cloud, specify the GCC High endpoints. Refer to the section [GCC High Support for Subscriptions](#_GCC_High_Support) for the correct values.

**Please ensure that these endpoints are added to your organization’s AllowList.**

The Wizard does not validate credentials on this step! This allows the user to create a subscription object, even if the Internet connection is unstable. If the credentials are not valid, or the account does not have enough permissions, then a subscription object will be created, but Connection State monitor will change its health state to Critical and will raise a corresponding alert. If new endpoints are not specified, the default values will be used.

1. Choose a **Management Server Pool**.
2. Click **Next**.

***Note:*** The following page will differ, depending on the SPN creation method, the authentication method chosen, and whether the subscription is being created or edited. The images below represent only one of the possibilities.

Graphical user interface, application

Description automatically generated

1. Then enter **Subscription Name, Tenant ID, Client ID,** and **Client Secret** or **Certificate Thumbprint** (see [Register the application in Azure AD](#AppReg) for more details).

***Note:* Tenant ID (or Directory ID)** is a globally unique identifier that can be found in [Azure Management Portal](https://portal.azure.com/), when you browse to your Active Directory instance; for more details, see [Find your Microsoft 365 tenant ID](https://support.office.com/en-us/article/Find-your-Office-365-tenant-ID-6891b561-a52d-4ade-9f39-b492285e2c9b) article. Please note that Tenant name can also be used in the corresponding Wizard field. Tenant ID cannot contain spaces.  
**Client ID (or Application ID)** is a GUID value automatically generated by Azure Active Directory for the application created in [Register the application in Azure Active Directory](#AppReg) section. You can find it in Azure management portal on the configuration page of your application. Client IDcannot contain spaces.

**Client Secret** is a key used when exchanging an authorization code for an access token; see the following section for details on the client secret. Client Secret cannot contain space characters.

**Certificate Thumbprint** is used to identify which certificate to use, when exchanging an authorization code for an access token. Certificate Thumbprint cannot contain spaces.

1. Click **Add Subscription**.

Graphical user interface, text, application

Description automatically generated

1. Click **Finish** to close the Wizard. The new subscription will be added to Operations Manager and will appear on the Configured Subscriptions list.

It is possible to modify credentials, endpoints, and resource pool for a particular subscription. Select the subscription you want to edit, click **Edit subscription**, enter new credentials (or create the new ones), endpoints, and select pool. The authentication method (Secret, Delegated or Certificate) cannot be changed by editing the subscription (create a new subscription if required).

To remove a configured subscription, select it from the configured subscriptions list and click **Remove subscription**.

Graphical user interface, text, application

Description automatically generated

When removing a subscription, you are given the option to delete the application from Azure AD as well. If the application was auto created and no other subscriptions are using it, you may want to delete it. All alerts related to the deleted subscription will be removed as well.

Register the application in Azure Active Directory

If you choose the **Use custom Azure Service Principal** option requiring an Azure subscription, perform the following steps to register your application in Azure Active Directory:

1. Sign in to <https://portal.azure.com/>
2. In the navigation panel, select **Azure Active Directory**.

Shape, company name

Description automatically generated with medium confidence

1. Next click on **App registrations**.

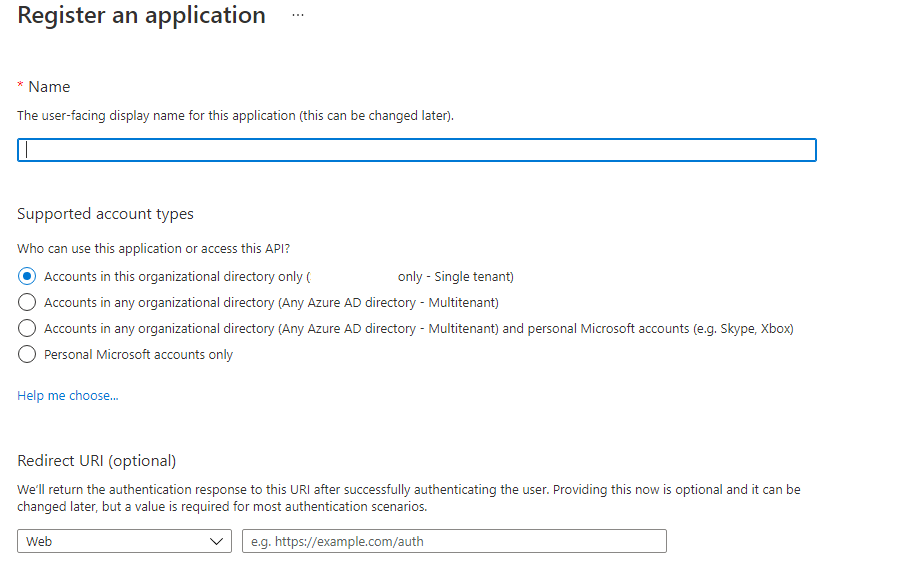


Graphical user interface, text, application, email

Description automatically generated

1. Next click **New registration** near the top of the screen:





1. Provide a Name for the application and select the appropriate support account types.
2. Click **Register**. The new application will be displayed:

Graphical user interface, text, application, email

Description automatically generated

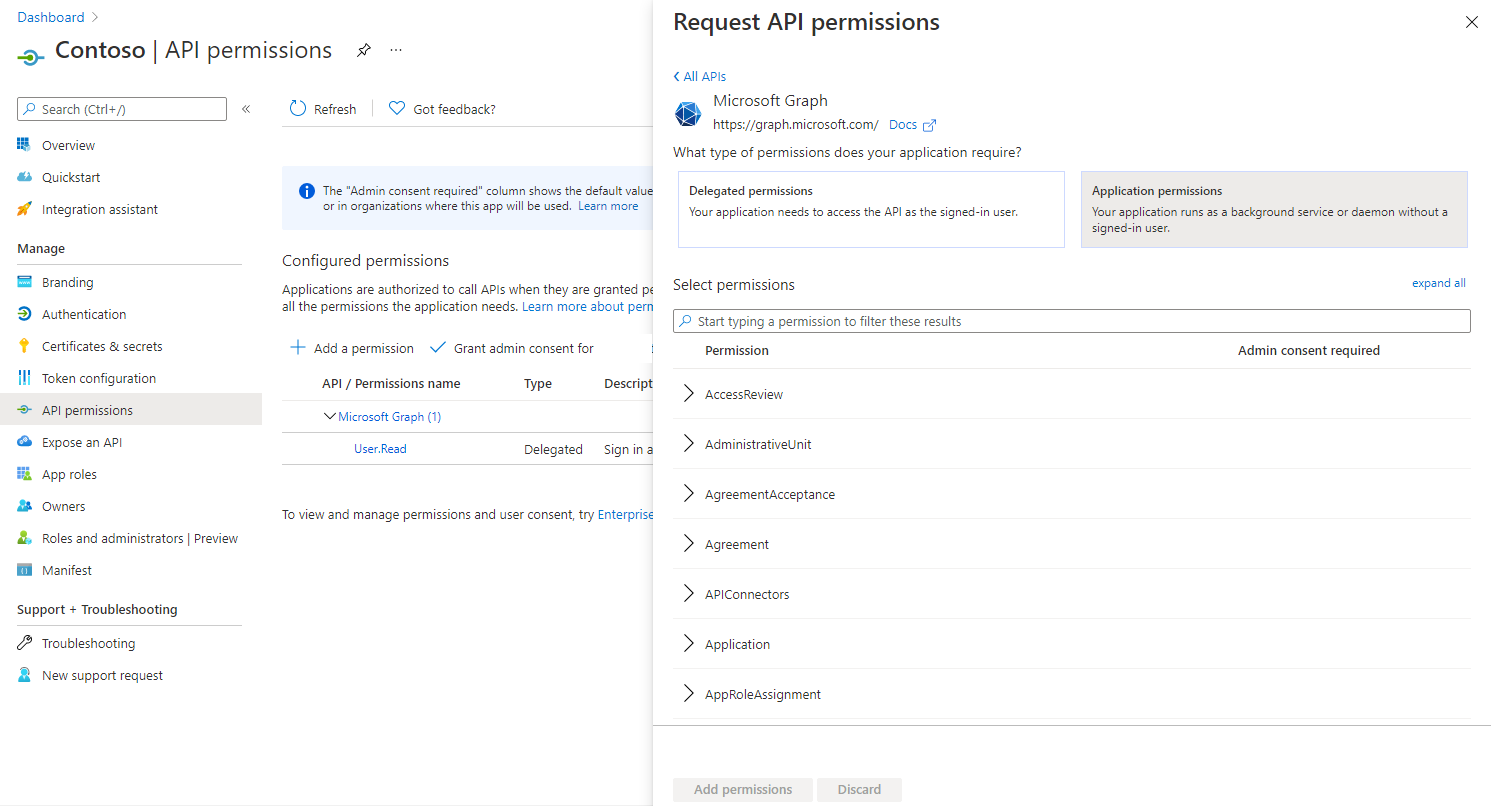
1. Next select **API permissions.**



1. Then click **Add a permission.**



1. Select **Microsoft Graph** then **Application permissions** (if using Secret or Certificate authentication) or **Delegated permissions** (if using Delegated authentication).



1. Depending on your monitoring scenario (see earlier table **Application Permissions**), add the following permissions:
   * Calendars – Calendars.Read
   * Channel – Channel.ReadBasic.All
   * Channel – ChannelMessage.Send2
   * Channel – ChannelMessage.Read.All2
   * Files – Files.ReadWrite.All
   * GroupMember – GroupMember.Read.All
   * Mail – Mail.ReadWrite
   * Mail – Mail.Send
   * Organization – Organization.Read.All
   * Reports – Reports.Read.All
   * ServiceHealth – ServiceHealth.Read.All
   * ServiceMessage – ServiceMessage.Read.All
   * Sites – Sites.Read.All
   * User – User.Read.All1
   * User – User.Read2

***Notes:***

1 Required only if using Secret or Certificate authentication (application permissions).

2 Required only if using Delegated authentication (delegated permissions).

***Note:*** To further restrict the Exchange Permissions, the application permissions can be scoped by creating an Application Access Policy as described in <https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access>.

1. Click **Add permissions**.
2. Next from the API permissions screen select **Grant admin consent for** <your organization name> and click **Yes**.

Graphical user interface, text, application

Description automatically generated

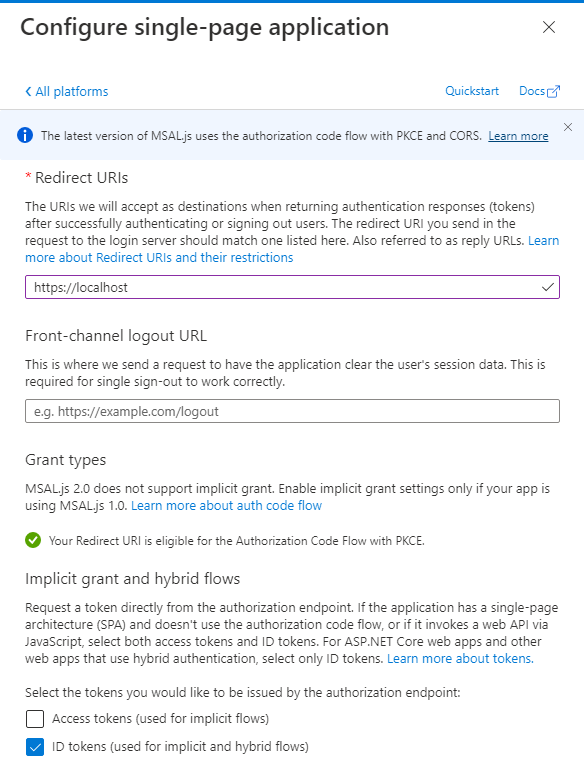
1. Confirm granting these permissions.
2. Next select **Authentication**



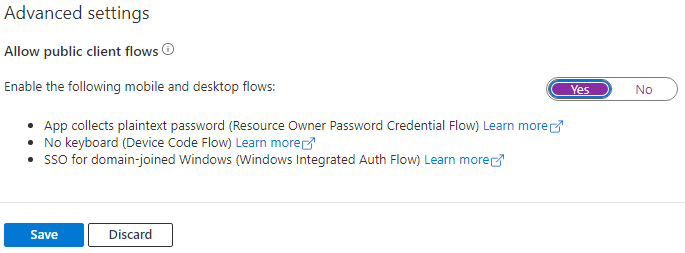
1. Under **Platform Configurations**, select **Add Platform**



1. Select **Single-page Application**
2. In the **Configure single-page application**, enter **Redirect URI** as <https://localhost>
3. Select the check box, **Implicit tokens (Used for implicit and hybrid flows)**



1. Next click **Configure** button at the bottom.
2. Under the **Advanced settings**, select **Yes** option for **Allow public client flows**.



1. Click Save.
2. Next select **Certificates & secrets** if using Secret or Certificate authentication. If using Delegated authentication, skip to step 29.

Graphical user interface, text, application, email

Description automatically generated

1. If using Secret authentication, select the **Client secrets** tab and click **New client secret**. Otherwise, skip to step 18 for Certificate authentication.

Graphical user interface, text, application

Description automatically generated

1. Provide a name and expiry timeframe and select **Add.**

Graphical user interface, text, application, email

Description automatically generated

1. **Please take note of the Value** (not the Secret ID). This is the only time which you will have access to this information. This needs to be copied into the **Client Secret** field of the **Add Subscription** page in the M365 Subscription Configuration wizard. Continue with step 21.
2. If using Certificate authentication, select the Certificates tab and click **Upload certificate**.

Graphical user interface, text, application, email

Description automatically generated

1. Select a file containing the certificate with public keys, add a description and select **Add.**

Graphical user interface, text, application, email

Description automatically generated

1. Please take note of the Thumbprint. This needs to be copied into the **Certificate Thumbprint** field of the **Add Subscription** page in the M365 Subscription Configuration wizard.
2. Next you will need the Tenant ID and Client ID. From the Azure Portal main menu select Azure Active Directory, App registrations, select the application, and copy and paste the **Directory (tenant) ID** into the Tenant ID field and the **Application (client) ID** into the Client ID fields of the **Add Subscription** page in the M365 Subscription Configuration wizard.

Graphical user interface, text, application

Description automatically generated

1. The results of this information provided to the wizard will appear like the following:

Graphical user interface, text, application

Description automatically generated

Select **Add Subscription** to complete adding the new subscription.

If you did not use the auto-created Azure Service Principal procedure above, you should verify the appropriate API permissions have been set in Azure. Open a browser and navigate to the Azure Portal **portal.azure.com** and login with the appropriate level of access to set API permissions. Next navigate to **Azure Active Directory** then to **App registrations**. Find and click on the appropriate M365 SCOM Monitoring application then click **API Permissions**.

Verify the following permissions have been granted to the organization:

For Secret and Certificate authentication (see below for Delegated):

Graphical user interface, text, application

Description automatically generated

For Delegated authentication (see above for Secret and Certificate):

Graphical user interface, application

Description automatically generated

Once this is verified click **Certificates & secrets** and verify **Client secret** or **Certificates:**

Graphical user interface, text, application, email

Description automatically generated

If using Secret or Certificate authentication, verify that a certificate or client secret exists (but you must have recorded the client secret value when created because you cannot reveal the value after creation). If using Delegated authentication, then no secret or certificate is required.

Configuring the Microsoft 365 Management Pack

This section will describe the various steps required to configure the Microsoft 365 Management Pack to begin monitoring your Microsoft 365 environment. The first step to using the Microsoft 365 Management Pack is to configure a watcher node to execute synthetic transactions as well as gather other information from your Microsoft 365 subscription.

Adding a Watcher Node

A watcher node is a system running a SCOM health service that executes synthetic transactions and other commands to gather information required by the management pack. To add a watcher node for the Microsoft 365 Management Pack, start the SCOM Operations console and select the Administration workspace. Next click the **Microsoft 365** menu item.

***Note****:* To monitor Teams network performance, the Teams Network Assessment Tool is required. The wizard can attempt to verify the presence of this prerequisite and install it if required.

Graphical user interface, application

Description automatically generated

Microsoft 365 watcher nodes that are currently configured will be displayed in the Watcher Node listbox. If there are no watcher nodes currently defined the list will be empty.

Step 1: Add Watcher Node

To add a new watcher node click on **Add watcher node**. The Add Watcher Node wizard will appear.

Graphical user interface, text, application

Description automatically generated

A list of systems with the SCOM health services will be displayed (systems already hosting a watcher node will not be listed). Select a system from the list to be used as a watcher node. This system must have the SCOM agent installed and running (or be a management server or gateway).

Click **Next** to continue.

Step 2: Select a Subscription

The Microsoft 365 Subscription page will be displayed.

Graphical user interface, application

Description automatically generated

If you have more than one subscription configured select the subscription which should be used by the watcher node.

Click **Next** to continue.

Step 3: Choose Optional Prerequisites

The Optional Prerequisites Setup page will be displayed.

Graphical user interface, text, application, email

Description automatically generated

If you are planning on monitoring Teams, select the **Install prerequisites for Teams network assessment.** This will attempt to install the Teams Network Assessment Tool on the watcher node if it is not already present.

Next select a user account with Administrator rights on the watcher node computer. The account must also have the **Logon as Service** permission. These credentials will only be used to verify and install (if required) the prerequisite software. These credentials will not be stored.

Click **Next** to continue.

Step 4: Set Up Watcher Node

The Watcher Node Setup page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Watcher Node Setup page will automatically attempt to check if the watcher node has the prerequisite software installed. The watcher node requires:

* PowerShell version 5 or higher.
* .NET version 4.7.2 or higher.
* To monitor Teams network performance, the Teams Network Assessment Tool is required.

Click the **Verify Prerequisites** button to run a script which will verify if these prerequisites are installed on the watcher node. The wizard will display the results of running the prerequisites script in the wizard page including showing if the script ran successfully and if it did, the status of the required prerequisites.

If one or more of these prerequisites are missing from the watcher node, click the **Install Prerequisites** to run a script which will attempt to install the Teams Network Assessment Tool (if it is required). The wizard will display the results of running the prerequisites installation script in the wizard page including showing if the script ran successfully and if it did, the status of the required prerequisites. If this step fails, you may need to manually install the prerequisites on the watcher node.

PowerShell version 5 or higher. It can be downloaded and installed as part of the Windows Management Framework 5.1:  
<https://www.microsoft.com/en-us/download/details.aspx?id=54616>

If the Network Assessment Tool needs to be installed manually, see the detailed instructions in [Appendix: Network Assessment Tools](#Appendix_Network_Assessment_Tools).

Click **Next** to continue.

Step 5: Set Up Subscription Endpoints

The Subscription Endpoints Setup page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Subscription Endpoints Setup page is used to determine where to collect information about your Microsoft 365 environment.

**Authority Endpoint** is the URL used to authenticate your Azure AD subscription. This needs to be changed if using one of Microsoft’s private Azure clouds.

**Graph API Endpoint** is the URL used to perform synthetic transactions. This needs to be changed if using one of Microsoft’s private Azure clouds.

If using the GCC High cloud, specify the GCC High endpoints. Refer to the section [GCC High Support for Watcher Nodes](#_GCC_High_Support_1) for the correct values.

The **Test Synthetic Transaction on Health Service** button is used to determine if the health service can connect to the endpoints defined and perform a synthetic transaction. It runs a task on the health service that makes GraphAPI calls to verify that synthetic transactions will work correctly on the health service. Note that the synthetic transaction attempts to read license information and if using a delegated subscription and licensing was not enabled, this test cannot succeed, and the button will be disabled.

Click **Next** to continue.

Step 6: Set Up Mail Flow Monitoring

The Mail Flow Setup page will be displayed.

Graphical user interface, text, application, email

Description automatically generated

The Mail Flow Setup page allows you to choose which mail flow transactions you want to run within your environment and the parameters required to run the mail flow transactions. Please note that depending on which synthetic transactions have been selected, not all properties may be required.

**M365 Sender email address** is the email address used to send Microsoft 365 email to measure synthetic email transactions. If using a subscription with delegated authentication, the email address will be specified by the subscription and not by the watcher node.

**M365 Receiver email address** is the email address used to receive Microsoft 365 email to measure synthetic email transactions. If using a subscription with delegated authentication, the email address will be specified by the subscription and not by the watcher node.

**Exchange URL** is URL used to perform synthetic transactions to a hybrid Exchange server. Note that if you are unsure of what to enter, this link might be used to help determine the URL:  
<https://autodiscover-s.outlook.com/autodiscover/autodiscover.json?Email=%3cuseremailaddress%3e&Protocol=EWS&RedirectCount=6>  
Replace **%3cuseremailaddress%3e** with an email address (this supports GCC environments as well as others). This URL will be used by the watcher node to communicate with the Exchange server, so if you have both *internal* and *external* URLs for Exchange, this will usually be the internal URL.

**Exchange Sender UPN** is the user principal name (looks like an email address and is often the same) used to send Exchange email to measure synthetic email transactions.

**Exchange Sender password** is the password for the Exchange Sender UPN account.

**Exchange Receiver UPN** is the user principal name (looks like an email address and is often the same) used to receive Exchange email to measure synthetic email transactions.

**Exchange Receiver password** is the password for the Exchange Receiver UPN account.

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

***Note:*** Exchange credentials (Exchange Sender UPN, Exchange Sender password, Exchange Receiver UPN, and Exchange Receiver password) are global. There is only one set of Exchange credentials, and they are used by all watcher nodes. If watcher nodes use different Exchange URL values, the credentials must be valid for all specified Exchange servers (which typically means all Exchange servers should be part of the same Active Directory Forest).

***Note:*** To further restrict the Exchange Permissions, the application permissions can be scoped by creating an Application Access Policy as described in <https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access>.

Click **Next** to continue.

Step 7: Set Up SharePoint/OneDrive Monitoring

The SharePoint/OneDrive Setup page will be displayed.

Graphical user interface, text, application, email

Description automatically generated

The SharePoint/OneDrive Setup page allows you to specify whether to use synthetic transactions to monitor SharePoint and OneDrive.

**SharePoint/OneDrive** verifies the ability to update and download files to SharePoint and measure performance.

**SharePoint Document Library** specifies the existing library (folder) in SharePoint which is used during the upload/download synthetic transaction.

**SharePoint Site** is the host name part of the URL used for the SharePoint synthetic transaction. It is not a URL but will be used as part of a GraphAPI query. Note that sub-sites and nested sites are supported. Do **not** include https://**.**

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

Click **Next** to continue.

Step 8: Set Up Teams & Network Monitoring

The Teams & Network Setup page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Teams & Network Setup wizard page allows you to enable Teams monitoring as well as Network monitoring. Please note that depending on which synthetic transactions have been selected, not all properties may be required.

**Teams** measures Teams network performance.

**Team Name** is the name of the team in Teams.

**Existing Channel Name** is the name of an existing Channel in a Team.

**Network** is used to monitor network performance and measures the Microsoft 365 login time and ping times. The values are collected only and there are no associated monitors.

To disable any of the synthetic transactions deselect the checkbox next to the synthetic transaction.

If using delegated authentication, Teams Chat messages will be sent to the specified channel to measure performance of chats. The channel should be a dedicated channel for synthetic transactions (or else users will see these test chat messages).

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

Click **Next** to continue.

Step 9: Set Up Licensing Monitoring

The Licensing Setup page will be displayed.

Graphical user interface

Description automatically generated

The Licensing Setup wizard page allows you to enable license monitoring.

**Licensing** enables / disables monitoring of M365 licenses which have been allocated.

**Sku Part Numbers** enumerates the specific SKUs to evaluate for license counts and availability. The watcher node wizard will attempt to retrieve information about SKUs in the subscription. Select at least one SKU. The color coding of the **Remaining** column shows the current state of a given SKU compared to the **Critical** and **Warning** threshold values on that same line.

When creating a new watcher node, the default suggested **Critical** and **Warning** threshold values for a given SKU are calculated as 5% and 10%, respectively, of the total number of licenses available. These can be modified to specify the remaining license count thresholds to use before a critical or warning alert is raised for a given SKU.

**License Verification UPN** specifies a user principal name (which looks like an email address and is often the same) to be verified as being licensed. If using a subscription with delegated authentication, the license verification UPN will be specified by the subscription and not by the watcher node.

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

Click **Next** to continue.

Step 10: Set Up Location

The Location Setup page will be displayed.

Graphical user interface, application

Description automatically generated

The Location Setup wizard page allows you to specify the location of the watcher node which is used in some of the dashboards.

**Location Name** is a friendly name of the location of the watcher node. This can be any name your organization uses but should be unique for each watcher node.

**Location Address to look up** is for the physical location of the watcher node and is used to position the watcher node status on a world map. This could be an address, a city name, office building, etc. Enter the name of the location then use the **Look Up** button to find its latitude and longitude. To use this capability please ensure the following URL is added to your organizations AllowList: <https://atlas.microsoft.com>. Follow this link for more information about this service. You can also enter latitude and longitude values manually, if needed. The location address is not stored and is only used for the lookup.

Click **Next** to continue.

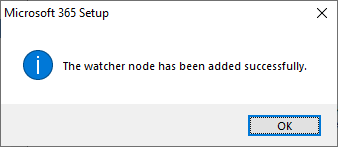
Step 11: Review Summary & Create

The Summary page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Summary wizard page will display a summary of the settings that will be used. Review and if needed go back to make any changes. Click **Finish** to create the watcher node and save these settings in the Microsoft 365 override management pack called **Microsoft.SystemCenter.M365.Overrides**. If these changes are saved successfully, a message like the following will be displayed:



You will be returned to the Microsoft 365 Overview page which should appear like this:

Graphical user interface, text, application

Description automatically generated

Once completed, the new watcher node will begin monitoring Microsoft 365 and the reports and dashboards will begin to display results after several minutes.

Editing a Watcher Node

A watcher node is a system running a SCOM health service that executes synthetics transactions and other commands to gather information required by the management pack. To edit an existing watcher node for the Microsoft 365 Management Pack, start the SCOM Operations console and select the Administration workspace. Next click the **Microsoft 365** menu item.

Graphical user interface, text, application, email

Description automatically generated

Microsoft 365 watcher nodes that are currently configured will be displayed in the Watcher node listbox.

Step 1: Edit Watcher Node

To edit an existing watcher node, click the watcher node you want to edit then select **Edit Watcher Node**. The Edit Watcher Node wizard will appear.

Step 2: Select a Subscription

The Microsoft 365 Subscription page will be displayed.

Graphical user interface, application

Description automatically generated

If you have more than one subscription configured select the subscription which should be used by the watcher node.

Click **Next** to continue.

Step 3: Choose Optional Prerequisites

The Optional Prerequisites Setup page will be displayed.

Graphical user interface, text, application, email

Description automatically generated

If you are planning on monitoring Teams, select the **Install prerequisites for Teams network assessment.** This will attempt to install the Teams Network Assessment Tool on the watcher node if it is not already present.

When editing a watcher node, the prerequisite check boxes will be checked by default if the corresponding synthetic transactions are enabled (because to enable them, the prerequisite software must have been installed previously). If Teams is enabled, the check box will be checked.

Next select a user account with Administrator rights on the watcher node computer. The account must also have the **Logon as Service** permission. These credentials will only be used to verify and install (if required) the prerequisite software. These credentials will not be stored.

Click **Next** to continue.

Step 4: Set Up Watcher Node

The Watcher Node Setup page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Watcher Node Setup page will attempt to check if the watcher node has the prerequisite software installed. The watcher node requires:

* PowerShell version 5 or higher
* .NET version 4.7.2 or higher
* To monitor Teams network performance, the Teams Network Assessment Tool is required.

Click the **Verify Prerequisites** button to run a script which will verify if these prerequisites are installed on the watcher node. The wizard will display the results of running the prerequisites script in the wizard page including showing if the script ran successfully and if it did, the status of the required prerequisites.

If one or more of these prerequisites are missing from the watcher node, click the **Install Prerequisites** to run a script which will attempt to install the Teams Network Assessment Tool (if it is required). The wizard will display the results of running the prerequisites installation script in the wizard page including showing if the script ran successfully and if it did, the status of the required prerequisites. If this step fails, you may need to manually install the prerequisites on the watcher node.

If the Network Assessment Tool needs to be installed manually, see the detailed instructions in [Appendix: Network Assessment Tools](#Appendix_Network_Assessment_Tools).

Click **Next** to continue.

Step 5: Set Up Subscription Endpoints

The Subscription Endpoints Setup page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Subscription Endpoints Setup page is used to determine where to collect information about your Microsoft 365 environment.

**Authority Endpoint** is the URL used to authenticate your Azure AD subscription. This needs to be changed if using one of Microsoft’s private Azure clouds.

**Graph API Endpoint** is the URL used to perform synthetic transactions. This needs to be changed if using one of Microsoft’s private Azure clouds.

If using the GCC High cloud, specify the GCC High endpoints. Refer to the section [GCC High Support for Watcher Nodes](#_GCC_High_Support_1) for the correct values.

The **Test Synthetic Transaction on Health Service** button is used to determine if the health service can connect to the endpoints defined and perform a synthetic transaction. It runs a task on the health service that makes GraphAPI calls to verify that synthetic transactions will work correctly on the health service. Note that the synthetic transaction attempts to read license information and if using a delegated subscription and licensing was not enabled, this test cannot succeed, and the button will be disabled.

Click **Next** to continue.

Step 6: Set Up Mail Flow Monitoring

The Mail Flow Setup page will be displayed.

Graphical user interface, text, application, email

Description automatically generated

The Mail Flow Setup page allows you to choose which mail flow transactions you want to run within your environment and the parameters required to run the mail flow transactions. Please note that depending on which synthetic transactions have been selected, not all properties may be required.

**M365 Sender email address** is the email address used to send Microsoft 365 email to measure synthetic email transactions. If using a subscription with delegated authentication, the email address will be specified by the subscription and not by the watcher node.

**M365 Receiver email address** is the email address used to receive Microsoft 365 email to measure synthetic email transactions. If using a subscription with delegated authentication, the email address will be specified by the subscription and not by the watcher node.

**Exchange URL** is URL used to perform synthetic transactions to a hybrid Exchange server. Note that if you are unsure of what to enter, this link might be used to help determine the URL:  
<https://autodiscover-s.outlook.com/autodiscover/autodiscover.json?Email=%3cuseremailaddress%3e&Protocol=EWS&RedirectCount=6>  
Replace **%3cuseremailaddress%3e** with an email address (this supports GCC environments as well as others). This URL will be used by the watcher node to communicate with the Exchange server, so if you have both *internal* and *external* URLs for Exchange, this will usually be the internal URL.

**Exchange Sender UPN** is the user principal name (looks like an email address and is often the same) used to send Exchange email to measure synthetic email transactions.

**Exchange Sender password** is the password for the Exchange Sender UPN account.

**Exchange Receiver UPN** is the user principal name (looks like an email address and is often the same) used to receive Exchange email to measure synthetic email transactions.

**Exchange Receiver password** is the password for the Exchange Receiver UPN account.

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

***Note:*** Exchange credentials (Exchange Sender UPN, Exchange Sender password, Exchange Receiver UPN, and Exchange Receiver password) are global. There is only one set of Exchange credentials, and they are used by all watcher nodes. If watcher nodes use different Exchange URL values, the credentials must be valid for all specified Exchange servers (which typically means all Exchange servers should be part of the same Active Directory Forest).

***Note:*** To further restrict the Exchange Permissions, the application permissions can be scoped by creating an Application Access Policy as described in <https://docs.microsoft.com/en-us/graph/auth-limit-mailbox-access>.

Click **Next** to continue.

Step 7: Set Up SharePoint/OneDrive Monitoring

The SharePoint/OneDrive Setup page will be displayed.

Graphical user interface, text, application, email

Description automatically generated

The SharePoint/OneDrive Setup page allows you to specify whether to use synthetic transactions to monitor SharePoint and OneDrive.

**SharePoint/OneDrive** verifies the ability to update and download files to SharePoint and measure performance.

**SharePoint Document Library** specifies the existing library (folder) in SharePoint which is used during the upload/download synthetic transaction.

**SharePoint Site** is the host name part of the URL used for the SharePoint synthetic transaction. It is not a URL but will be used as part of a GraphAPI query. Note that sub-sites and nested sites are supported. Do **not** include https://**.**

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

Click **Next** to continue.

Step 8: Set Up Teams & Network Monitoring

The Teams & Network Setup page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Teams & Network Setup wizard page allows you to enable Teams monitoring as well as Network monitoring. Please note that depending on which synthetic transactions have been selected, not all properties may be required.

**Teams** measures Teams network performance.

**Team Name** is the name of the team in Teams.

**Existing Channel Name** is the name of an existing Channel in a Team.

**Network** is used to monitor network performance and measures the Microsoft 365 login time and ping times. The values are collected only and there are no associated monitors.

To disable any of the synthetic transactions deselect the checkbox next to the synthetic transaction.

If using delegated authentication, Teams Chat messages will be sent to the specified channel to measure performance of chats. The channel should be a dedicated channel for synthetic transactions (or else users will see these test chat messages).

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

Click **Next** to continue.

Step 9: Set Up Licensing Monitoring

The Licensing Setup page will be displayed.

Graphical user interface, application

Description automatically generated

The Licensing Setup wizard page allows you to enable license monitoring.

**Licensing** enables / disables monitoring of M365 licenses which have been allocated.

**Sku Part Numbers** enumerates the specific SKUs to evaluate for license counts and availability. The watcher node wizard will attempt to retrieve information about SKUs in the subscription. Select at least one SKU. The color coding of the **Remaining** column shows the current state of a given SKU compared to the **Critical** and **Warning** threshold values on that same line.

When editing an existing watcher node, the values displayed in the **Critical** and **Warning** columns are calculated based on the threshold percentage values previously used if upgrading from a previous version of the Microsoft 365 management pack. These can be modified to specify the remaining license count thresholds to use before a critical or warning alert is raised for a given SKU.

**License Verification UPN** specifies a user principal name (which looks like an email address and is often the same) to be verified as being licensed. If using a subscription with delegated authentication, the license verification UPN will be specified by the subscription and not by the watcher node.

***Note:*** Values entered on this page are not validated by the wizard. Take care when entering values.

Click **Next** to continue.

Step 10: Set Up Location

The Location Setup page will be displayed.

Graphical user interface, application

Description automatically generated

The Location Setup wizard page allows you to specify the location of the watcher node which is used in some of the dashboards.

**Location Name** is a friendly name of the location of the watcher node. This can be any name your organization uses but should be unique for each watcher node.

**Location Address to look up** is for the physical location of the watcher node and is used to position the watcher node status on a world map. This could be an address, a city name, office building, etc. Enter the name of the location then use the **Look Up** button to find its latitude and longitude. To use this capability please ensure the following URL is added to your organization’s AllowList: <https://atlas.microsoft.com>. Follow this link for more information about this service. You can also enter latitude and longitude values manually, if needed. The location address is not stored and is only used for the lookup.

Click **Next** to continue.

Step 11: Review Summary & Create

The Summary page will be displayed.

Graphical user interface, text, application

Description automatically generated

The Summary wizard page will display a summary of the settings that will be used. Review and if needed go back to make any changes. Click **Finish** to create the watcher node and save these settings in the Microsoft 365 override management pack called **Microsoft.SystemCenter.M365.Overrides**. If these changes are saved successfully, a message like the following will be displayed:

Graphical user interface, text, application

Description automatically generated

Removing a Watcher Node

A watcher node is a system running a SCOM health service that executes synthetics transactions and other commands as needed by the management pack. To remove an existing watcher node for the Microsoft 365 Management Pack, start the SCOM Operations console and select the Administration workspace. Next click the Microsoft 365 menu item.

To remove a watcher node, click the watcher node you want to remove then select **Remove Watcher Node**. You will be asked to confirm the removal of the watcher node. The Microsoft 365 subscription being monitored by the watcher node will no longer be monitored.

***Note****:* It can take Operations Manager an indeterminate amount of time to completely remove a watcher node. Health services may appear to be unavailable until Operations Manager completes the remove operation. Health services that are not heart-beating (grey state) will not remove the watcher node until the health service begins heart-beating again.

***Note****:* Removing a watcher node does not uninstall prerequisite software (for example, Teams Network Assessment Tool). Administrators may wish to manually remove the prerequisite software, if no longer used by anything else.

Configure proxy connection.

To use a proxy server for the Microsoft 365 MP **wizard queries**, perform the following steps:

1. First, you will need to edit the Monitoring Console configuration file. It can be found in the following location:

*C:\Program Files\Microsoft System Center <SCOM Version>\Operations Manager\Console\Microsoft.EnterpriseManagement.Monitoring.Console.exe.config*

Add the following lines in the configuration section of the configuration file:

<system.net>

<defaultProxy enabled="true" useDefaultCredentials="true">

<proxy proxyaddress="*http://xxx.xx.x.xx:xxxx*" bypassonlocal="false" />

<bypasslist></bypasslist>

</defaultProxy>

</system.net>

***Note:*** proxyaddress value must be entered as follows: http://ProxyIPaddress:Port, for example <http://192.168.0.200:8080>

***Note:*** Secure proxy connections (https) are not supported. Disable SSL Intercept on the proxy, if required.

1. Restart the Operations Console.
2. Change IE settings to use the corresponding proxy.
3. Configure Management Server proxy settings: enable **Use a proxy server for communication with Microsoft** option, enter the corresponding address, and port values.
4. Create a Windows Run As Account with access to the proxy; add this account to Microsoft 365 Subscription Proxy secure reference.

To use a proxy server for the Microsoft 365 MP **monitoring queries**, perform the following steps:

1. You will need to edit the Monitoring Host configuration file. It can be found in the following location:

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

Add the following lines in the configuration section of the configuration file:

<system.net>

<defaultProxy enabled="true" useDefaultCredentials="true">

<proxy proxyaddress="*http://xxx.xx.x.xx:xxxx*" bypassonlocal="false" />

<bypasslist></bypasslist>

</defaultProxy>

</system.net>

***Note:*** proxyaddress value must be entered as follows: http://ProxyIPaddress:Port, for example <http://192.168.0.200:8080>

***Note:*** Secure proxy connections (https) are not supported. Disable SSL Intercept on the proxy, if required.

1. Restart the Microsoft Monitoring Agent service.
2. Configure Management Server proxy settings: enable **Use a proxy server for communication with Microsoft** option, enter the corresponding address, and port values.
3. Create a Windows Run As Account with access to the proxy; add this account to Microsoft 365 Subscription Proxy secure reference.

To use a proxy server for the Microsoft 365 MP **watcher node synthetic transaction**, perform the following steps:

1. For each watcher node, you will need to edit the Monitoring Host configuration file. It can be found in the following location:

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

Add the following lines in the configuration section of the configuration file:

<system.net>

<defaultProxy enabled="true" useDefaultCredentials="true">

<proxy proxyaddress=”*http://xxx.xx.x.xx:xxxx”* bypassonlocal="false" />

<bypasslist></bypasslist>

</defaultProxy>

</system.net>

***Note:*** proxyaddress value must be entered as follows: http://ProxyIPaddress:Port, for example <http://192.168.0.200:8080>

***Note:*** Secure proxy connections (https) are not supported. Disable SSL Intercept on the proxy, if required.

***Note:*** Watcher nodes are usually in different geographic locations and the proxy IP address will usually be different for each watcher node.

1. Restart the Microsoft Monitoring Agent service.

Run As Configuration

The Microsoft 365 Management Pack creates multiple Run As accounts including the following:

* Microsoft 365 Run As Account\_Credentials\_<<Subscription\_Id>> (there will be one account per configured subscription)
* Microsoft 365 Run As Account\_DelegatedLicensingUser\_<<Subscription\_Id>> (there will be one account per configured subscription using delegated authorization)
* Microsoft 365 Run As Account\_DelegatedMailReceiver\_<<Subscription\_Id>> (there will be one account per configured subscription using delegated authorization)
* Microsoft 365 Run As Account\_DelegatedMailSender\_<<Subscription\_Id>> (there will be one account per configured subscription using delegated authorization)
* Microsoft 365 Run As Account\_DelegatedServiceHealthUser\_<<Subscription\_Id>> (there will be one account per configured subscription using delegated authorization)
* Microsoft 365 Run As Account\_DelegatedSharePointUser\_<<Subscription\_Id>> (there will be one account per configured subscription using delegated authorization)
* Microsoft 365 Run As Account\_DelegatedTeamsUser\_<<Subscription\_Id>> (there will be one account per configured subscription using delegated authorization)
* Microsoft 365 Run As Account\_DelegatedPlaceholder
* Microsoft 365 Run As Account\_ExchangeEmailReceiver
* Microsoft 365 Run As Account\_ExchangeEmailSender

**Microsoft 365 Run As Account\_Credentials**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription) to collect information from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_DelegatedLicensingUser**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription using delegated authorization) to collect licensing information from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_DelegatedMailReceiver**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription using delegated authorization) to receive M365 mail from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_DelegatedMailSender**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription using delegated authorization) to send M36 mail from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_DelegatedServiceHealthUser**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription using delegated authorization) to collect service health and messages from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_DelegatedSharePointUser**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription using delegated authorization) to perform SharePoint uploads/download from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_DelegatedTeamsUser**\_**<<Subscription\_Id>>** is used by Watcher Nodes (configured to use this subscription using delegated authorization) to perform Teams uploads/downloads from Microsoft APIs. The description will include the name of the subscription.

**Microsoft 365 Run As Account\_Placeholder** is used by Watcher Nodes which are not configured to use delegated authorization to satisfy Operations Manager requirements. The actual credentials are dummy values and are never used.

**Microsoft 365 Run As Account\_ExchangeEmailReceiver** is used by all Watcher Nodes when receiving Exchange email. If you have not enabled M365 to Exchange Mail Flow, this Run As account will not be created.

**Microsoft 365 Run As Account\_ExchangeEmailSender** is used by all Watcher Nodes when sending Exchange email. If you have not enabled M365 to Exchange Mail Flow, this Run As account will not be created.

The Microsoft 365 Management Pack also creates multiple Profiles including the following:

* Microsoft 365 Exchange Receiver Profile
* Microsoft 365 Exchange Sender Profile
* Microsoft 365 Subscription Application Client Profile
* Microsoft 365 Subscription Password Profile
* Microsoft 365 Subscription Proxy secure reference
* Microsoft 365 Email Receiver Profile
* Microsoft 365 Email Sender Profile
* Microsoft 365 Licensing Profile
* Microsoft 365 Service Health Profile
* Microsoft 365 SharePoint Profile
* Microsoft 365 Teams Profile
* Microsoft 365 Teams NAT Profile

**Microsoft 365 Exchange Receiver Profile** is used by Watcher Nodes to login and receive email using Exchange.

**Microsoft 365 Exchange Sender Profile** is used by Watcher Nodes to login and send email using Exchange.

**Microsoft 365 Subscription Application Client Profile** is used to store Microsoft 365 subscription credentials to be used by Watcher Nodes and should not be edited manually. See [Manage Microsoft 365 subscriptions](#Managing_Office_365_Subscriptions) section for more details.

**Microsoft 365 Subscription Password Profile** is used to store Microsoft 365 subscription credentials to be used on the Management Server and should not be edited manually. See [Manage Microsoft 365 subscriptions](#Managing_Office_365_Subscriptions) section for more details.

**Microsoft 365 Subscription Proxy secure reference** should be configured manually. This profile is used by all rules and monitors defined in this management pack. All Run As Accounts mapped to this profile should have the following permissions:

* be a member of **Operations Manager Operators** System Center Operations Manager user role.
* be able to establish an HTTPS connection from the Management Server to Microsoft 365 portal endpoint. Please check firewall and proxy settings within your environment to ensure that connection is allowed.

**Microsoft 365 Email Receiver Profile** is used by Watcher Nodes to login and receive email using Microsoft 365 when using delegated authentication.

**Microsoft 365 Email Sender Profile** is used by Watcher Nodes to login and send email using Microsoft 365 when using delegated authentication.

**Microsoft 365 Licensing Profile** is used by Watcher Nodes to login and receive licensing information when using delegated authentication.

**Microsoft 365 Service Health Profile** is used by Watcher Nodes to login and receive service health and messages when using delegated authentication.

**Microsoft 365 SharePoint Profile** is used by Watcher Nodes to login and send/receive SharePoint files when using delegated authentication.

**Microsoft 365 Teams Profile** is used by Watcher Nodes to login and send/receive Teams files when using delegated authentication.

**Microsoft 365 Teams NAT Profile** is used by Watcher Nodes to run the Teams Network Assessment Tool if the default action account does not have sufficient permissions.

Management Pack Contents

This section describes the contents of the Microsoft 365 Management Pack.

This management pack defines the following classes:

* Microsoft 365 Subscription
* Microsoft 365 Service
* Microsoft 365 Feature (deprecated)
* Microsoft 365 Watcher Node
* M365 Licensing
* M365 Mail Flow
* Hybrid Mail Flow
* M365 Networking
* M365 SharePoint
* M365 Teams

Microsoft 365 subscriptions

There is no discovery workflow for Subscriptions; they should be added manually via Microsoft 365 Add Subscription wizard in the Administration section of the Operations Manager Console. The wizard performs the required configuration:

* Creates Run As Account that stores credentials for Azure application.
* Adds a subscription object to Operations Manager.
* Creates a management pack with required internal overrides.
* Specifies M365 and Azure URI endpoints as subscription properties.

For security reasons, the wizard is the only way to configure the monitoring of Microsoft 365 Subscriptions. See [Manage Microsoft 365 subscriptions](#Manage_Microsoft_365_subscriptions) for details.

As soon as a new subscription is configured, it appears in the subscriptions list. The subscription objects are monitored by the corresponding monitor regarding the connection health only. The health degradation of Services does not affect the health of the subscription object.

A single watcher node can only monitor a single Microsoft 365 subscription. If multiple subscriptions need to be monitored, multiple watcher nodes will need to be deployed.

Services discovery

The discovery workflow for Microsoft 365 Services is targeted at Microsoft 365 Subscription class. It automatically discovers all Microsoft 365 Services available for the given subscription. Services objects are not monitored, and do not roll up health to the subscription. The M365 Monitoring Dashboard uses these objects to build the list of services, and corresponding count of Active Incident Alerts.

Watcher Node discovery

The watcher node discovery is performed by the Watcher Node wizard. Depending on the features selected, the watcher node discovery may also create instances of:

* M365 Licensing (one per SKU being monitored)
* M365 Mail Flow
* Hybrid Mail Flow
* M365 Networking
* M365 SharePoint
* M365 Teams

Note that there is an existing watcher node discovery workflow, but it has been deprecated. The watcher node wizard is now the only way to discover watcher nodes. The deprecated discovery has been disabled with an override, so the **Remove-SCOMDisabledClassInstance** Operations Manager Shell (PowerShell) command can be used to clean up any old instances created by the discovery which cannot be removed automatically by the watcher node wizard.

Connection State monitor

Microsoft 365 Connection State monitor is targeted at the subscription. It is the only monitor which affects the health state of the subscription. This monitor checks the connection to Microsoft 365 Management API. If connection cannot be established (for example, API is unavailable, incorrect credentials or insufficient permissions), the monitor changes its health state and generates a corresponding alert. The monitor also queries Management service URI endpoints; if any of them returns error, the monitor changes the subscription state to unhealthy and generates a corresponding alert. See alert description for details.

Microsoft 365 Incidents and Messages

There are two main types of subscription-related events: Incidents and Messages.

**Incidents** provide information about operational state changes of the subscription service. Each Incident provides a context, which contains a unique identifier, title, description, list of affected services with their current operational states.

**Admin Center messages** are not related to the operational state of services, but contain additional information about updates, required actions, etc.

Microsoft 365 Management Pack provides several alerting rules, targeted at the Subscription. These rules replicate Microsoft 365 Incidents and Messages to the Operations Manager Alerts, which contain detailed information from related Microsoft 365 events. Detailed information is stored in the alert’s context and custom fields. These fields are matching alerts to services. By default, **these rules are disabled**, but can be re-enabled by creating an override in the Operations Manager Console.

***Note:*** Do not change the custom fields to avoid incorrect alert display in the Dashboard.

Rules update alert context and custom fields if corresponding Microsoft 365 Incident or Message has updated the information. Repeat count for the alert is increased in this case.

* **Microsoft 365 Incidents alerting rule** generates and updates critical alerts for Incidents. Its behavior depends on the following overridable parameters:
  + **Reopen closed alerts** – specifies if the rule should create a new alert, when the added information arrives for the incident, which already has a corresponding alert with Closed status in Operations Manager. The default value is false.
  + **Include resolved incidents** – specifies if the rule should create a new alert for Microsoft 365 incidents, which are marked as Resolved. The default value is false.

|  |  |
| --- | --- |
| Admin Center message Category field | Corresponding SCOM alert severity |
| Plan for change | Warning |
| Prevent or fix issues | Critical |
| Stay informed | Informational |

* **Microsoft 365 Admin Center alerting rules** will create alerts for Admin Center messages with categories based on the table below:

Alert Autoclose rule

By default, **the Alert Autoclose** rule runs once a day. This rule analyses the list of active alerts in Operations Manager and compares it to the actual list of Incidents and Messages for the given subscription. If some Incidents or Messages are out of date (i.e., they are not available via Microsoft 365 API anymore), the rule automatically updates and closes corresponding alerts in Operations Manager.

The following overridable parameters can be used to customize the behavior of this rule:

* **Max Alert Age** – specifies the maximum age for alerts, which correspond to **resolved** incidents. The default value is 7 days. If the alert represents a resolved incident and has not been updated during the period specified by the threshold, it will be forcibly closed, even if it is available via Microsoft 365 API.

To enable this setting, the value of **Max Alert Age** parameter should be greater than zero. The threshold is measured in seconds. This parameter can be useful if the user wants to receive timely notifications about new alert messages. To prevent confusion of new and old messages, the user can set auto closing of the latter after a certain period.

To avoid automated alerts resolution and closing, disable this rule or set the **Max Alert Age** to zero. In this case, alerts generated by alerting rules should be closed manually. **Alert Autoclose** rule does not affect alerts generated by **Microsoft 365 Connection State** monitor.

Management Pack Elements

The following section describes monitoring workflows provided by Microsoft 365 Management Pack.

In general Event Rules collect data when new events occur. License collection and Certificate Expiry monitor runs once every 6 hours and auto close runs once a day and all other rules run every 15 minutes. Overrides can be created to enable or disable rules, change data collection intervals and other configuration settings of the elements of the management pack.

**Management Pack Rules**

|  |  |  |
| --- | --- | --- |
| Display Name | Description | Enabled |
| Exchange Calendar Free/Busy Check Event Collection | The rule collects the Exchange Calendar Free/Busy Check event data from the Operations Manager event log. | true |
| Exchange to M365 Event Collection | This rule looks for and collects Exchange to M365 events in the Operations manager log. | true |
| Exchange to M365 Receive Duration Performance Collection | This rule measures the amount of time it takes to receive and verify a test email from Exchange to M365 and collects the time in milliseconds. | true |
| Exchange to M365 Send Duration Performance Collection | This rule measures the amount of time it takes to send a test email from Exchange and collects the time in milliseconds. | true |
| Exchange to M365 Total Duration Performance Collection | This rule measures the total amount of time it takes to send a test email from Exchange and verify receipt of a test email from Exchange to M365 and collects the time in milliseconds. | true |
| M365 (outlook.ha.office365.com) Response Time Performance Collection | This rule pings the address outlook.ha.office365.com and collects the time in milliseconds. ICMP and TCP pinging to specific ports is supported. | true |
| M365 (outlook.ms-acdc.office.com) Response Time Performance Collection | This rule pings the address outlook.ms-acdc.office.com and collects the time in milliseconds. ICMP and TCP pinging to specific ports is supported. | true |
| M365 (outlook.office365.com) Response Time Performance Collection | This rule pings the address outlook.office365.com and collects the time in milliseconds. ICMP and TCP pinging to specific ports is supported. | true |
| M365 Available License Count Event Collection | This rule looks for and collects License Count events (where SKU Part Number is found) in the Operations Manager Log. | true |
| M365 Calendar Free/Busy Check Event Collection | The rule collects the M365 Calendar Free/Busy Check event data from the Operations Manager event log. | true |
| M365 Consumed Units Collection | This rule collects the number of Consumed licenses. | true |
| M365 Mailbox Count M365 | This rule determines the number of mailboxes that exist under M365 and the associated organization's location. | true |
| M365 Mailbox Count M365 Event Collection | This rule looks for and collects Mailbox Count M365 events in the Operations Manager Log. | true |
| M365 Office Pro Plus License Verification Event Collection | This rule looks for and collects License Verification events in the Operations Manager Log. | true |
| M365 Portal Login Performance Collection | This rule connects to the Microsoft 365 Portal and logs in via synthetic transaction and collects the time in milliseconds. | true |
| M365 to Exchange Event Collection | This rule looks for and collects M365 to Exchange events in the Operations Manager log. | true |
| M365 to Exchange Receive Duration Performance Collection | This rule measures the amount of time it takes to receive and verify a test email from M365 to Exchange and collects the time in milliseconds. | true |
| M365 to Exchange Send Duration Performance Collection | This rule measures the amount of time it takes to send a test email from M365 and collects the time in milliseconds. | true |
| M365 to Exchange Total Duration Performance Collection | This rule measures the total amount of time it takes to send a test email from M365 and verify receipt of a test email from M365 to Exchange and collects the time in milliseconds. | true |
| M365 to M365 Event Collection | This rule looks for and collects M365 to M365 events in the Operations Manager log. | true |
| M365 to M365 Receive Duration Performance Collection | This rule measures the amount of time it takes to receive and verify a test email from M365 to M365 and collects the time in milliseconds. | true |
| M365 to M365 Send Duration Performance Collection | This rule measures the amount of time it takes to send a test email from M365 and collects the time in milliseconds. | true |
| M365 to M365 Total Duration Performance Collection | This rule measures the total amount of time it takes to send a test email from M365 and verify receipt of a test email from M365 to M365 and collects the time in milliseconds. | true |
| M365 Total Units Collection | This rule collects the number of Total licenses. | true |
| Microsoft 365 .Net Framework Rule | Microsoft 365 .Net Framework Rule. | false |
| Microsoft 365 Admin Center Critical alerting rule | When this rule receives an Admin Center message of "preventOrFixIssue" category, it generates or updates a corresponding Critical Alert in the Operations Manager. | false |
| Microsoft 365 Admin Center Informational alerting rule | When this rule receives an Admin Center message of "stayInformed" category, it generates or updates a corresponding Informational Alert in the Operations Manager. | false |
| Microsoft 365 Admin Center Warning alerting rule | When this rule receives an Admin Center message of "planForChange" category, it generates or updates a corresponding Warning Alert in the Operations Manager. | false |
| Microsoft 365 Alert Autoclose rule | The rule is used to process the list of all Events for the Subscription via Microsoft 365 API and to close obsolete Alerts in the Operations Manager. | true |
| Microsoft 365 Incidents alerting rule | The rule is used to process the list of Active and Resolved Incidents for the Subscription via Microsoft 365 API, and to generate or update corresponding Alerts in the Operations Manager. | false |
| Microsoft M365 Subscription Alert Telemetry Rule | Subscription alert telemetry rule for Microsoft M365 | true |
| Microsoft M365 Watcher Node Telemetry Rule | Watcher node telemetry rule for Microsoft M365 | true |
| SharePoint Connection Errors Rule | This event rule looks in the Operations Manager log for connection errors from the SharePoint Performance Monitor. | true |
| SharePoint Performance Download Rule | The rule measures the test file download time from SharePoint in milliseconds. | true |
| SharePoint Performance Event Collection | The rule collects the SharePoint Performance event data from the Operations Manager event log. | true |
| SharePoint Performance Total Rule | The rule measures the test file upload and download time to and from SharePoint in milliseconds. | true |
| SharePoint Performance Upload Rule | The rule measures the test file upload time to SharePoint in milliseconds. | true |
| Teams Connection Errors Rule | This event rule looks in the Operations Manager log for connection errors from the Teams Performance Monitor. | true |
| Teams Event Collection | This rule looks for and collects Teams Network Assessment events in the Operations Manager log. | true |
| Teams Network Assessment Average Jitter Performance Collection | This rule measures and collects the average jitter from the Microsoft Teams Network Assessment Tool. | true |
| Teams Network Assessment Packet Loss Rate Performance Collection | This rule measures and collects the packet loss rate from the Microsoft Teams Network Assessment Tool. | true |
| Teams Network Assessment Round Trip Latency Performance Collection | This rule measures and collects the round-trip latency from the Microsoft Teams Network Assessment Tool. | true |
| Teams Performance Event Collection | The rule collects the Teams Performance event data from the Operations Manager event log. | true |
| Teams Performance Upload Rule | The rule measures the test file upload time to Teams in milliseconds. | true |
| Teams Performance Download Rule | The rule measures the test file download time from Teams in milliseconds. | true |
| Teams Performance File Total Rule | The rule measures the test file upload and download time to and from Teams in milliseconds. | true |
| Teams Performance Chat Send Rule | The rule measures the time it takes to send a Teams Chat in milliseconds. | true |
| Teams Performance Chat Verify Rule | The rule measures the time it takes to verify a Teams Chat in milliseconds. | true |
| Teams Performance Chat Total Rule | The rule measures the total time it takes to send and verify a Teams Chat in milliseconds. | true |
| Teams Performance Total Rule | The rule measures the total Teams test file upload and download time and the Chat send and verify time in milliseconds. | true |

**Management Pack Monitors**

|  |  |  |
| --- | --- | --- |
| Display Name | Description | Enabled |
| Exchange Calendar Free/Busy Check Monitor | The monitor implements synthetic transactions to verify the ability to obtain free/busy status from Exchange. | true |
| Exchange to M365 Mail Flow Monitor | This monitor logs into Exchange using the OnPrem Sender Profile and sends a test message to the M365 Receiver Profile. It then logs into the account specified in the M365 Receiver Profile and verifies receipt of the email from the OnPrem Sender Profile. | true |
| Certificate Expiry Monitor | This monitor determines if the certificate used by a watcher node has expired or if the number of days until certificate expiry is lower than the set threshold. If the watcher node subscription is not using certificates, this monitor always succeeds. | true |
| M365 Available License Count Monitor | This monitor determines if the number of available M365 licenses is greater than the set warning and critical thresholds. | true |
| M365 Calendar Free/Busy Check Monitor | The monitor implements synthetic transactions to verify the ability to obtain free/busy status from M365. | true |
| M365 Connection State monitor | Microsoft 365 Connection State monitor | true |
| M365 Mailbox Count M365 Monitor | This monitor determines the number of mailboxes that exist under M365 and the associated organization's location. | true |
| M365 Office Pro Plus License Verification Monitor | This monitor determines if there are M365 licenses available and a connection can be made to retrieve licenses. | true |
| M365 Teams Network Assessment Average Jitter Monitor | This monitor evaluates whether the Microsoft Teams Network Assessment Tool reports an acceptable average jitter. | true |
| M365 Teams Network Assessment Packet Loss Rate Monitor | This monitor evaluates whether the Microsoft Teams Network Assessment Tool reports an acceptable packet loss rate. | true |
| M365 Teams Network Assessment Round Trip Latency Monitor | This monitor evaluates whether the Microsoft Teams Network Assessment Tool reports an acceptable round-trip latency. | true |
| M365 Teams Network Assessment Status Monitor | This monitor evaluates whether Teams can be successfully contacted using the Microsoft Teams Network Assessment Tool. | true |
| M365 to Exchange Mail Flow Monitor | This monitor logs into M365 using the M365 Sender Profile and sends a test message to the Exchange Receiver Profile. It then logs into the account specified in the Exchange Receiver Profile and verifies receipt of the email from the M365 Sender Profile. | true |
| M365 to M365 Mail Flow Monitor | This monitor logs into M365 using the M365 Sender Profile and sends a test message to the M365 Receiver Profile. It then logs into the account specified in the M365 Receiver Profile and verifies receipt of the email from the M365 Sender Profile. | true |
| Microsoft 365 MP WatcherNode Aggregate Monitor Availability | This availability aggregate monitor summarizes all availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Aggregate Monitor Performance | This performance aggregate monitor summarizes all performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Hybrid Mail Flow Aggregate Monitor Availability | This availability aggregate monitor summarizes all Hybrid mail flow availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Hybrid Mail Flow Aggregate Monitor Performance | This performance aggregate monitor summarizes all Hybrid mail flow performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Hybrid Mail Flow Dependency Monitor Availability | This availability dependency monitor rolls up Hybrid mail flow availability health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Hybrid Mail Flow Dependency Monitor Performance | This availability dependency monitor rolls up Hybrid mail flow performance health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Licensing Aggregate Monitor Availability | This availability aggregate monitor summarizes all licensing availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Licensing Aggregate Monitor Performance | This performance aggregate monitor summarizes all licensing performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Licensing Dependency Monitor Availability | This availability dependency monitor rolls up licensing availability health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Licensing Dependency Monitor Performance | This availability dependency monitor rolls up licensing performance health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode M365 Mail Flow Aggregate Monitor Availability | This availability aggregate monitor summarizes all M365 mail flow availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode M365 Mail Flow Aggregate Monitor Performance | This performance aggregate monitor summarizes all M365 mail flow performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode M365 Mail Flow Dependency Monitor Availability | This availability dependency monitor rolls up M365 mail flow availability health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode M365 Mail Flow Dependency Monitor Performance | This availability dependency monitor rolls up M365 mail flow performance health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Networking Aggregate Monitor Availability | This availability aggregate monitor summarizes all networking availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Networking Aggregate Monitor Performance | This performance aggregate monitor summarizes all networking performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Networking Dependency Monitor Availability | This availability dependency monitor rolls up networking availability health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Networking Dependency Monitor Performance | This availability dependency monitor rolls up networking performance health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode SharePoint Aggregate Monitor Availability | This availability aggregate monitor summarizes all SharePoint availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode SharePoint Aggregate Monitor Performance | This performance aggregate monitor summarizes all SharePoint performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode SharePoint Dependency Monitor Availability | This availability dependency monitor rolls up SharePoint availability health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode SharePoint Dependency Monitor Performance | This availability dependency monitor rolls up SharePoint performance health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Teams Aggregate Monitor Availability | This availability aggregate monitor summarizes all Teams availability monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Teams Aggregate Monitor Performance | This performance aggregate monitor summarizes all Teams performance monitors for the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Teams Dependency Monitor Availability | This availability dependency monitor rolls up Teams availability health to the Microsoft 365 Watcher Node. | true |
| Microsoft 365 MP WatcherNode Teams Dependency Monitor Performance | This availability dependency monitor rolls up Teams performance health to the Microsoft 365 Watcher Node. | true |
| SharePoint Connection Monitor | The monitor is an event monitor. It checks if a connection can be made to SharePoint Online. The monitor has two health states: healthy and critical. | true |
| SharePoint Performance Monitor | The monitor implements synthetic transactions to verify the ability to upload and download files to and from SharePoint. | true |
| Teams Connection Monitor | The monitor is an event monitor. It checks if a connection can be made to Teams Online. The monitor has two health states: healthy and critical. | true |
| Teams Performance Monitor | The monitor implements synthetic transactions to verify the ability to upload and download files to and from Teams. | true |
| Teams Performance Chat Total Time Monitor | This monitor evaluates whether the Teams Chat message takes an acceptable time to send and verify. | true |

**Overridable Parameters**

Many rules and monitors have common overridable parameters. The table below lists those overridable parameters along with a description of their purpose. After the overridable parameters used by several rules and monitors, those used by a single rule or monitor are listed below the display name of the rule or monitor. When creating overrides, pay attention to the potential to break cookdown. See [Appendix: Cookdown and Interval Overrides](#Appendix_Cookdown_and_Interval_Overrides) for details.

|  |  |
| --- | --- |
| Display Name | Description |
| Interval (seconds) | Specifies the frequency at which the rules or monitors will be run. |
| Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. |
| Match Count | Specifies the number of failures that must occur before an alert is raised. |
| Sample Count | Specifies the number of samples that should be considered for Match Count. |
| Synchronization Time | The synchronization time specified by using a 24-hour format. |
| Sleep Interval (seconds) | Specifies the number of seconds to wait between checking for incoming email. |
| Port Number | Specifies the TCP port number to use for pings. Can be numeric, or HTTP, HTTPS, RDP, SMB, WinRM, or UDP for ICMP pings. If ICMP is blocked, HTTPS is recommended for the Office endpoints. |
| SKU Part Number | SKU Part Number to query for license counts. |
| Threshold Value | The value to compare against. Healthy state means the sample value is less than or equal to the threshold value. |
|  |  |
| M365 Available License Count Monitor | |
| Critical threshold percentage | Deprecated; this license threshold value only exists to maintain backwards compatibility with previous versions of the management pack. This value is ignored once a pre-existing watcher node’s configuration has been modified by editing it using the watcher node wizard. |
| Warning threshold percentage | Deprecated (see **Critical threshold percentage** above) |
|  |  |
| Certificate Expiry Monitor |  |
| Warning Days | Specifies the value that is compared with the number of days remaining until a certificate expires to determine if a warning state should be generated. |
|  |  |
|  |  |
| Microsoft 365 Alert Autoclose rule | |
| Max Alert Age (seconds) | Specifies the time the alert is active before being closed. |
|  |  |
|  |  |
| Microsoft 365 Incidents alerting rule | |
| Include resolved incidents | Creates an alert for a resolved incident if no active alert exists for the incident in SCOM. |
| Reopen Closed Alerts | Creates a new alert if new information for a closed alert was received. |

Microsoft 365 Monitoring Dashboards

The Microsoft 365 Management Pack includes several dashboards designed to provide insights into the operation of the Microsoft 365 service. Dashboards are accessible via the SCOM console and there are additional HTML5 dashboards (requires SCOM 2019) which are accessible via the SCOM web console.

The following table lists the dashboards available in the Microsoft 365 Management Pack. If certain scenarios have not been enabled e.g., Teams monitoring then the corresponding dashboards will not have any data to display. To access these dashboards, navigate to the **Microsoft 365** folder.

|  |  |
| --- | --- |
| Report Name | Description |
| Active Alerts | Active Alerts view displays the cumulative list of all alerts targeted at all configured subscriptions (Active Incidents, Resolved Incidents, Admin Center Messages, Connection State monitor alerts) and alerts from synthetic transactions. |
| M365 Hybrid Mail Flow Performance Dashboard | Displays key performance measurements of the time to send mail from Exchange to M365 and from M365 to Exchange. |
| M365 Licensing Dashboard | Shows alerts and events related to M365 licenses. If the license thresholds are exceeded and alert will be raised and will be visible in this dashboard. |
| M365 Mail Flow Dashboard | Shows alerts and events related to the flow of mail in M365. |
| M365 Mail Flow Performance Dashboard | Shows the time to send and receive mail on M365. |
| M365 Monitoring Dashboard | Shows the overall health of the M365 subscriptions being monitored as well as any active incidents and messages. |
| M365 Network Performance Dashboard | Shows the M365 portal login times as well as ping response times to key services. |
| M365 SharePoint Dashboard | Shows alerts and events related to SharePoint and OneDrive. |
| M365 SharePoint Performance Dashboard | This dashboard included SharePoint upload times, SharePoint download times and the aggregate times. |
| M365 Teams Dashboard | Shows alerts and events related to Teams. |
| M365 Teams Network Assessment Dashboard | This dashboard shows alerts and events related to monitoring Teams network performance. |
| M365 Teams Network Assessment Performance Dashboard | Shows the performance details of key network metrics related to Teams including packet loss rate, round trip latency, and average jitter. |
| M365 Teams Performance Dashboard | This dashboard included Teams upload times, Teams download times, Chat send times, Chat verify times and the aggregate times. |
| M365 Watcher Nodes | This report shows the list of currently configured watcher nodes and the properties of each watcher node and the health state of each synthetic transaction area. |

Licensing Views Folder

|  |  |
| --- | --- |
| Report Name | Description |
| Consumed Licenses | This report will show the total number of consumed Microsoft 365 licenses. The rule that collects the license information runs once a day so until the watcher node has been running for 24-hours, there will be no data displayed in this report. |
| M365 Available License Count Alerts | Shows all alerts related to the M365 license count. |
| M365 Available License Count Errors | Shows all events related to the M365 license count. |
| M365 Office Pro Plus License Verification Alerts | Shows all alerts related to checking if the License Verification email address is valid. |
| M365 Office Pro Plus License Verification Errors | Shows all events related to checking if the License Verification email address is valid. |

Mail Flow Views Folder

|  |  |
| --- | --- |
| Report Name | Description |
| Exchange Calendar Free/Busy Check Errors | Shows events related to checking Exchange Free/Busy information. |
| Exchange to M365 Errors | Shows events related to the flow of email between Exchange and M365 |
| Exchange to M365 Mail Flow Alerts | Shows alerts related to the flow of email between Exchange and M365 |
| M365 Calendar Free/Busy Check Errors | Shows events related to checking M365 Free/Busy information. |
| M365 Mailbox Count | Shows a chart of the count of M365 mailboxes. |
| M365 Mailbox Count Errors | Shows events related to the collection of the count of M365 mailboxes. |
| M365 to Exchange Errors | Shows events related to the flow of email between M365 and Exchange |
| M365 to Exchange Mail Flow Alerts | Shows alerts related to the flow of email between M365 and Exchange |
| M365 to M365 Errors | Shows events related to the flow of email between M365 and M365 |
| M365 to M365 Mail Flow Alerts | Shows alerts related to the flow of email between M365 and M365 |

Performance Views Folder

|  |  |
| --- | --- |
| Report Name | Description |
| Exchange to M365 Receive Performance | Shows the time taken to send mail from Exchange to M365 |
| Exchange to M365 Send Performance | Shows the time taken for Exchange to accept a request to send mail. |
| Exchange to M365 Total Performance | Shows the total time taken to send mail from Exchange and receive it in M365 |
| M365 Portal Login Performance | Shows the time it takes to login to the Microsoft 365 portal |
| M365 to Exchange Receive Performance | Shows the time taken to send mail from M365 to Exchange |
| M365 to Exchange Send Performance | Shows the time taken for M365 to accept a request to send mail |
| M365 to Exchange Total Performance | Shows the total time taken to send mail from M365 and receive it in Exchange |
| M365 to M365 Receive Performance | Shows the time taken to send mail from M365 to M365 |
| M365 to M365 Send Performance | Shows the time taken for M365 to accept a request to send mail |
| M365 to M365 Total Performance | Shows the total time taken to send mail from M365 and receive it in Exchange |
| Ping Response Time (outlook.ha.office365.com) | Shows the time to ping the Outlook service outlook.ha.office365.com |
| Ping Response Time (outlook.ms-acdc.office.com) | Shows the time to ping the Outlook service outlook.ms-acdc.office.com |
| Ping Response Time (outlook.office365.com) | Shows the time to ping the Outlook service outlook.office365.com |
| SharePoint Download Performance | Shows the time to download from SharePoint |
| SharePoint Total Performance | Shows the total download and upload time from SharePoint |
| SharePoint Upload Performance | Shows the time to upload to SharePoint |
| Teams Download Performance | Shows the time to download from Teams |
| Teams Network Assessment Average Jitter | Shows the average jitter of a Teams call initiated on the watcher node |
| Teams Network Assessment Packet Loss Rate | Shows the packet loss rate of a Teams call initiated on the watcher node |
| Teams Network Assessment Round Trip Latency | Shows the round-trip latency of a Teams call initiated on the watcher node |
| Teams Total Performance | Shows the total download and upload time from Teams |
| Teams Upload Performance | Shows the time to upload to Teams |

SharePoint Views Folder

|  |  |
| --- | --- |
| Report Name | Description |
| SharePoint Connection Errors | Shows events related to SharePoint connection errors |
| SharePoint Connection Monitor Alerts | Shows alerts related to the connection to SharePoint |
| SharePoint Performance Errors | Shows events related to SharePoint performance |
| SharePoint Performance Monitor Alerts | Shows alerts related to SharePoint performance |

Teams Views Folder

|  |  |
| --- | --- |
| Report Name | Description |
| Teams Connection Errors | Shows any errors related to connecting to Teams. |
| Teams Connection Monitor Alerts | Shows alerts related to connecting to Teams. |
| Teams Network Assessment Alerts | Shows alerts related to Teams network assessment |
| Teams Network Assessment Errors | Shows events related to Teams network assessment |
| Teams Performance Errors | Shows events related to Teams performance. |
| Teams Performance Monitor Alerts | Shows alerts related to Teams network assessment |

M365 Dashboards Folder (Web Console)

|  |  |
| --- | --- |
| Report Name | Description |
| Active Alerts | Shows active alerts across all M365 services which are being monitored. |
| Exchange | Shows the status of Exchange and M365 mail flow including mail flow durations. |
| Geo View | Shows the state of the watcher nodes and the state of the M365 services from a geographic perspective. |
| License Status | Shows the status of licensing including used and total license counts. |
| Network | Shows the status of network traffic to various M365 services. |
| SharePoint | Shows the status of SharePoint including download and upload times. |
| Teams Network | Shows the status of Teams network including round trip latency, jitter, and packet loss rate. |
| Teams Synth Transactions | Shows the status of Teams synthetic transactions including download, upload, chat send, and chat verify times. |

**M365 Monitoring Dashboard**

The M365 Monitoring Dashboard is only accessible via the SCOM console. The features of this dashboard are as follows:

* Providing an overview of connection health for all configured subscriptions.
* Displays the lists of active incidents, resolved incidents, and informational messages for the selected subscription.
* Displays a list of Microsoft 365 Services available for the selected subscription, and the number of currently active incidents for each service.

Graphical user interface, application

Description automatically generated

Subscription Health

Subscription Health widget displays the list of Microsoft 365 subscriptions configured with Add/Edit Subscription Wizard, as well as overall health state of each Subscription.

Subscription health state can be affected by Connection State monitor only. Healthy state means that subscription configuration is valid and connection to Microsoft 365 Monitoring API is successful. Critical state means that Connection state monitor failed to connect the API using the provided credentials. This can be caused by various reasons including the following: incorrect credentials, insufficient permissions, firewall or proxy configuration or network problems. Accessability of all endpoints also affects subscription health state; if any of the endpoints does not respond (or responds incorrectly) during the check-up, subscription health state changes to critical.

Graphical user interface, text, application, email

Description automatically generated

Service Status

Service Status widget displays a tree of Microsoft 365 services discovered for the selected subscription. Each Service is attributed with a total number of active Incidents. Incidents count for a service is a sum of incidents counts for each service. The widget is designed to provide an overview of overall status for Microsoft 365 services. It does not allow you to perform any action against services, or related active incidents.

Graphical user interface, table

Description automatically generated

Alert widgets

Three bottom controls (Active Incidents, Resolved Incidents, and Admin Center) display filtered lists of alerts generated by the corresponding rules. Most generic data is displayed directly in the widget tables. Additional details can be found in alert context and custom fields available in the alert properties dialog. You may open the alert properties dialog by double-clicking the corresponding alert row, or via the context menu.

Graphical user interface, text, application

Description automatically generated

Active Incidents

Active Incidents widget displays the list of the Operations Manager alerts generated for currently active Microsoft 365 incidents for the selected subscription.

Each alert contains additional information in its context: the list of affected services, and their status. An incident (and the corresponding alert) is considered as active (and shown in Active Incidents list) if any of the affected services has one of the following states:

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

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

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

The corresponding rule is regularly updating alerts. An alert can disappear from the list of Active Incidents and appear in Resolved Incidents list when the status of the affected services changes.

Graphical user interface, text, application

Description automatically generated

Resolved Incidents

Resolved Incidents widget displays the list of the Operations Manager alerts generated for currently resolved Microsoft 365 incidents for the selected subscription.

Graphical user interface

Description automatically generated with low confidence

An incident (and the corresponding alert) is resolved (and shown in Resolved Incidents list) if there are no services having *active* incident states. The corresponding rule is regularly updating alerts. An alert can disappear from the list of Active Incidents and appear in Resolved Incidents list when the status of the affected services changes.

Admin Center

Admin Center widget displays the list of the Operations Manager alerts generated for informational messages for the selected Microsoft 365 subscription.

Graphical user interface

Description automatically generated

Admin Center messages contain additional information about updates, required actions, etc. Each Admin Center alert additionally contains an external link to the published article, or blog post with details. This hyperlink is included in the alert description text and the alert context.

It is also possible to get a detailed description of any message or incident in Microsoft 365 Administration Portal. Direct links to Microsoft 365 Admin Center and Incidents webpages are included to alerts’ Product Knowledge. Authorization for the subscription is required to view these pages.

Appendix: Troubleshooting the Watcher Node Setup

The watcher node is a critical component necessary for monitoring Microsoft 365. The watcher node is responsible for gathering important data from Microsoft 365 as well as executing synthetic transactions.

The Microsoft 365 Management Pack includes a wizard to help simplify the setup of the watcher node. The basic requirements of the watcher node are as follows:

* The watcher node requires the SCOM health service and that it is a member of the SCOM management group where the Microsoft 365 Management Pack is installed. Management servers and gateways always meet this requirement.
* PowerShell version 5 or higher. It can be downloaded and installed as part of the Windows Management Framework 5.1:  
  <https://www.microsoft.com/en-us/download/details.aspx?id=54616>
* .NET version 4.7.2 or higher
* The Teams Network Assessment Tool is required to evaluate network performance and network connectivity to determine how well the network would perform for a Microsoft Teams call. The watcher node setup wizard will attempt to install the Teams Network Assessment Tool, however if there are problems or if it needs to be installed manually see [Appendix: Network Assessment Tools](#Appendix_Network_Assessment_Tools).

If you experience errors when attempting to set up a new watcher node or if you are not seeing data in the Microsoft 365 reports and dashboards in the Operations Manager Console, then please check the following:

* On the watcher node system open the Event View and select the Operations Manager events. Look for event IDs in the range 900 – 999 for details about what might be going wrong.
* When installing a new watcher node, the wizard uses a SCOM task to install the necessary prerequisites. Ensure the SCOM agent account has enough privileges to install the required applications.

If attempting to open the Microsoft 365 item in the Administration workspace, you get an error like the following:

Could not load file or assembly ‘Microsoft.SystemCenter.M365.UI’, Version = ….

This most often occurs when an updated version of the management pack is imported, but the Operations Manager Console has not been restarted. The previous versions of the required assemblies are already loaded into the Operations Console and the new versions cannot be loaded. Restarting the Console will resolve this issue.

Appendix: Troubleshooting M365 Monitoring

There can be situations where monitoring M365 services is not behaving as expected. This section provides guidance on troubleshooting these scenarios.

In general terms, make sure the configuration of the subscriptions and the watcher nodes are correct by selecting the Administration tab in the SCOM Console then clicking on the Microsoft 365 item. Verify the settings for the monitored subscriptions as well as the watcher nodes.

The Windows Event Log is a useful source of information when troubleshooting. The Operations Manager folder is where all the specific events are logged. Check for events on the watcher node machine related to synthetic transactions and in particular look for any permissions-related messages which could prevent services from being monitored. Check for events on the local machine for issues with the Subscription or Watcher Node wizards.

If an alert is being raised, select the alert in the Alert View, and review the messages. For more information, click the **View additional knowledge…** link and select the **Alert Context** tab to see the raw data returned, which will often include a detailed error message.

When adding, removing, or editing watcher nodes including editing the monitoring configuration, make sure to wait for any updates to take effect. This can take an indeterminate period depending on several factors.

If using certificates for authentication, and errors are logged which include **Keyset does not exist**, the reason is that the Default Action Account, or Run As accounts being used by the health service, do not have Read permission for the certificate on the health service. See [Appendix: Certificates](#Appendix_Certificates) for instructions on setting the permissions.

Troubleshooting Mail Flow Monitoring

Start by checking your mail flow monitoring configuration. Open the Microsoft 365 item in the Administration workspace and edit the appropriate watcher node which is configured to monitor mail flow.

* The Subscription Endpoints wizard page has a Test Synthetic Transaction on Health Service button to ensure the watcher node can access the necessary Microsoft endpoints; verify the connection works and a synthetic transaction can be successfully completed.
* Next check the mail flow configuration:
* Ensure the M365-to-M365 Mail Flow option is selected.
* Verify the sender and receiver email addresses exist and are accessible.
* If monitoring Exchange
  + Ensure the Exchange URL is accessible, and the email addresses and password are correct.
  + If both internal and external URLs exist for Exchange, the internal URL is probably the correct one to use on the watcher node.

Troubleshooting SharePoint Monitoring

Start by checking your SharePoint monitoring configuration. Open the Microsoft 365 item in the Administration workspace and edit the appropriate watcher node which is configured to monitor SharePoint.

* The Subscription Endpoints wizard page has a Test Synthetic Transaction on Health Service button to ensure the watcher node can access the necessary Microsoft endpoints; verify the connection works and a synthetic transaction can be successfully completed.
* Next check the watcher node configuration specifically the SharePoint/OneDrive Setup:
* Ensure the SharePoint/OneDrive option is selected.
* Ensure the SharePoint Library exists and is accessible. If it is not, Event ID 961 **Unable to find Document Library named …** will be logged in the Operations Manager log on the watcher node.
* Ensure the SharePoint site is correct and note the site entered is not the URL. The URL will be built using the site name entered.
* The Operations Manager event log on the health service machine may report 961 events, with a message like:

Access to the path 'C:\Windows\TEMP\TestDoc-AgentComputerName.txt' is denied.

This can occur if the action account does not have permission to write to the temporary file folder. Add the action account to the Security settings for the folder and ensure it has permission to Read & execute, List folder contents, Read, and Write.

* The Operations Manager event log on the health service machine may report 961 events, with a message like:

Unable to connect to SharePoint site 'site name'.  
State: Critical.  
Exception: System.Exception: No subsites found under parent site 'site name'

This can occur if the SharePoint Site specified in the watcher node wizard was not a valid site or sub-site.

Troubleshooting Teams Monitoring

Start by checking your Teams monitoring configuration. Open the Microsoft 365 item in the Administration workspace and edit the appropriate watcher node which is configured to monitor Teams.

* The Subscription Endpoints wizard page has a Test Synthetic Transaction on Health Service button to ensure the watcher node can access the necessary Microsoft endpoints; verify the connection works and a synthetic transaction can be successfully completed.
* Next check the Teams configuration, specifically the Teams & Network Setup:
* Ensure the Teams option is selected.
* Ensure the Team Name provided already exists and is accessible.
* Ensure the Existing Channel Name provided exists and is accessible. If it is not, Event ID 966 **Unable to find Channel library named …** will be logged in the Operations Manager log on the watcher node.
* Note that Teams Chat transactions are only performed if using Delegated authentication (otherwise zero values are returned).
* If the Teams for Business Network Assessment Tool is reporting the following message (in an alert):

Invalid configuration detected: Failed to create/open directory for writing results: Microsoft Teams Network Assessment Tool\yyyymmddhhmmssffff\_service\_connectivity\_check\_results.txt.

(Where yyyymmddhhmmssffff is the date and time the tool ran.) Check the note under [Appendix: Network Assessment Tools](#Appendix_Network_Assessment_Tools) about installing the tool manually.

* If the Skype for Business Network Assessment Tool (which is still supported, but upgrading to the Teams Network Assessment Tool is recommended) is reporting the following message (in an alert):

Invalid configuration detected: Failed to open file for writing results. connectivity\_results.txt. Please check the NetworkAssessmentTool.exe.config file.

Check the note under [Appendix: Network Assessment Tools](#Appendix_Network_Assessment_Tools) about installing the tool manually.

* The Operations Manager event log on the health service machine may report 966 events, with a message like:

Access to the path 'C:\Windows\TEMP\TestDocTeams-AgentComputerName.txt' is denied.

This can occur if the action account does not have permission to write to the temporary file folder. Add the action account to the Security settings for the folder and ensure it has permission to Read & execute, List folder contents, Read, and Write.

Troubleshooting Licensing

Licensing information is only collected every 6 hours so viewing licensing information in the console as well as the dashboards and reports may be delayed.

Troubleshooting Microsoft 365 Incidents and Messages

If events having ID 26319 (Source: **OpsMgr SDK Service**) containing text: **The user** <yourDomain>\<yourOMActionAccount> **does not have sufficient permission to perform the operation.** appear in your Operations Manager event log on the Management Server, this is an indication that the Operations Manager Service Action Account has not been added to the Local Administrators group on the Management Server where this is logged.

Add the named account to the Local Administrators group on the Management Server to resolve the problem and allow the Microsoft 365 Incident and Message rules to operate. This should be done for all Management Servers in the Management Servers pool.

See this article for more information on correctly deploying SCOM (including adding the OM Server Action Account to Local Administrators group): <https://kevinholman.com/2019/03/14/scom-2019-quickstart-deployment-guide/>

If events having ID 1900 to 1999 (Source: **Health Service Modules**) containing text: **The user** <yourDomain>\<yourOMActionAccount> **does not have sufficient permission to perform the operation.** appear in your Operations Manager event log on the Management Server, this is an indication that either:

1. The correct permissions were not added to the application when upgrading from an earlier version of the management pack. See [Upgrading from Microsoft 365 MP Version 10.1.100.0](#Upgrading_From_Earlier_Version) for full instructions.
2. Or the account is not a member of the Local Administrators group as detailed above.

Appendix: Application Permission Requirements

The following table provides details of the modules defined within the Microsoft 365 Management Pack, the GraphAPI method called by the module and the minimum application permissions required.

|  |  |  |  |
| --- | --- | --- | --- |
| Synthetic Transaction | Minimum Application permission required | Graph API methods | Module |
| M365 Free/Busy Check | Calendars.Read | Get Schedule | CalendarFreeBusyCheckM365 |
| Admin Center | ServiceHealth.Read.All | Get Health Overviews | GetServices, ConnectionState |
| Admin Center | ServiceMessage.Read.All | Get Issues, Get Messages | ConnectionState, AlertAutoClose, GetAlerts |
| M365 Licensing, Network | Organization.Read.All | List Subscribed Skus | ConsumedUnits, GetAccountSku, LicenseCount, PortalLogin, TestConnection |
| M365 Licensing | User.Read.All1 User.Read2 | Get User License Details | LicenseVerification |
| M365 Mailbox Count | Organization.Read.All | Get Organization | MailboxCountM365 |
| M365 Mailbox Count | Reports.Read.All | Get Reports | MailboxCountM365 |
| M365 to M365 Mail Flow, M365 to Exchange Mail Flow | Mail.ReadBasic.All | List Mail Folders, List Messages | MailFlowExchangeToM365, MailFlowM365ToM365 |
| M365 to M365 Mail Flow, M365 to Exchange Mail Flow | Mail.ReadWrite | Delete Message | MailFlowExchangeToM365, MailFlowM365ToM365 |
| M365 to M365 Mail Flow, M365 to Exchange Mail Flow | Mail.Send | Send Mail | MailFlowM365ToExchange, MailFlowM365ToM365 |
| SharePoint / OneDrive | Sites.Read.All | List Sites | SharePointPerformance |
| SharePoint / OneDrive, Teams | Files.Read.All | List Drives, Download Content, Get Files Folder | SharePointPerformance, TeamsPerformance |
| SharePoint / OneDrive, Teams | Files.ReadWrite.All | Upload Content, Delete Drive Item | SharePointPerformance, TeamsPerformance |
| Teams | Channel.ReadBasic.All | List Channels | TeamsPerformance |
| Teams | GroupMember.Read.All | List Groups | TeamsPerformance |
| Teams | ChannelMessage.Send2 | Post Message | TeamsPerformance |
| Teams | ChannelMessage.Read.All2 | Get Message | TeamsPerformance |

Notes:

1 Required only if using Secret or Certificate authentication (application permissions).

2 Required only if using Delegated authentication (delegated permissions).

Appendix: Certificates

Authentication for GraphAPI, which is used by the Microsoft M365 management pack to perform many of the synthetic transactions, can use either Client Secrets, Delegated Authentication or Certificates. Client Secrets are like passwords, in they are “something you know.” Delegated authentication uses username and password to access specific resources. Client Secrets and Delegated authentication are easy to set up and use, but may be considered to not be secure enough, based on your organization’s policies. The alternative is Certificates, which are “something you have,” and are a more secure method of authentication. However, they are harder to set up and maintain.

The Microsoft 365 management pack supports Client Secrets, Delegated Authentication and Certificates. When a subscription is created, a choice must be made, and that choice cannot be changed after the subscription is created (but you can always create a new subscription and edit any watcher nodes using the old subscription).

Creation of certificates is beyond the scope of this document. Normally a corporate or commercial Public Key Infrastructure (PKI) would be used to generate the certificate. The following recommendations for creating the certificate may not be strictly required, but may be advisable:

|  |  |
| --- | --- |
| Hash Algorithm | SHA 512 |
| Key Length | 2028 |
| Key Export Policy | Exportable |
| Duration | 3 years |

Once the certificate is created, there will be two files required. The first contains the public key, will usually have a **.cer** extension, and will be used when creating new subscriptions. The second will contain the private keys, will usually have a **.pfx** extension, and will need to be installed on all computers which can run synthetic transactions using GraphAPI. Specifically, that means each watcher node and all management servers which are members of the pool selected for the subscription. The certificates will also have a thumbprint which should be noted (it is just a “name”).

Note that the private key file can be extracted from the **.cer** file using the Windows Certificate Manager. Follow these steps:

* Run **CertLM.msc** as an admin
* Select the just generated certificate file (**.cer**)
* Right-click and select **All Tasks**, **Export…**
* Choose **Yes, export the private key**
* Choose .PFX format

Graphical user interface, text, application

Description automatically generated

* Specify a password.

The private key certificate should be password protected and the two files should be stored securely where only authorized personnel have access to them.

The **.cer** (public key) file can be used when creating new subscriptions, simply by selecting the file when creating the subscription.

The **.pfx** (private key) file must be copied to each computer which will be used as a watcher node, as well as all computers in the management server pool being used by the subscription. After copying the private key file, it can be installed using PowerShell (run as an admin) with commands like the following:

$password = Read-Host 'Enter Password' -AsSecureString

Import-PfxCertificate -FilePath '<<pathToFile>>.pfx' -CertStoreLocation 'Cert:\LocalMachine\My' -Password $password

Note that the certificate store location (Cert:\LocalMachine\My) is important and must not be changed. The result will look something like this:

Graphical user interface, text, application

Description automatically generated

The certificate is now installed, but the Microsoft Monitoring Agent may not have permission to read the keys stored in the certificate. Follow these steps to review and set permissions:

* Run **CertLM.msc** as an admin
* Select the just imported certificate
* Right-click, and from **All Tasks**, select **Manage Private Keys…**
* If the list of accounts does not include accounts being used as the Agent Action account, or with run as credentials for Microsoft 365 workflows, add that account and give them Read access.
* It is not recommended to give **Everyone** Read access, although it will work.

Repeat the above procedure for each watcher node and management server that will be running synthetic transactions using the certificate-based subscription.

### Certificate Renewal

When a certificate being used for authentication is about to expire, a warning alert will be raised (by default 30 days before expiration). When that happens, a new certificate should be generated and installed on the watcher nodes and added to the application in Azure. Finally, the subscription should be edited, and the new thumbprint should be specified. If the certificate is not updated, the synthetic transactions using that certificate will fail as soon as it expires.

To create a new certificate, see the instructions [above](#Create_Certificate) in this appendix. Follow the instructions [above](#Install_Certificate) to install the certificate on the watcher nodes.

To add the new certificate to the Azure application, see the section on creating a custom application and adding [certificates](#Azure_Application_Adding_Certificate) above. Then edit the subscription using the old certificate and change the certificate thumbprint to the thumbprint for the new certificate.

When the new certificate is being used successfully (may take 15 minutes or more), the old certificate can be removed from the watcher nodes and the Azure application, if desired.

Appendix: Delegated Access

When using delegated permissions, access to Microsoft 365 resources is limited to only those resources permitted to the specific user credentials specified. The following resources may be helpful to establish the correct permissions to ensure the delegated users do not have access to any resources they are not supposed to have access to.

The following are provided as a courtesy. Support requests for Microsoft 365 users and permissions should not be directed to the SCOM Feedback site (which is only for issues with the management pack).

### SharePoint/OneDrive

[Customize permissions for a SharePoint list or library](https://support.microsoft.com/en-us/office/customize-permissions-for-a-sharepoint-list-or-library-02d770f3-59eb-4910-a608-5f84cc297782)

### Teams

[Assign policies to users and groups](https://docs.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups)

### M365 Mail

Normally the credentials used for mail (send or receive) would only have access to their own mailboxes. If access to other mailboxes is required, see the following:

[Give mailbox permissions to another user](https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/give-mailbox-permissions-to-another-user?view=o365-worldwide)

Appendix: Known Issues

This section will be updated as product issues are encountered.

Appendix: Event Log Entries

The watcher node may log one of more of these events in the local Event Log in the Operations Manager section.

|  |  |
| --- | --- |
| MP Element | Event ID |
| DiscoverM365WatcherNode | 900 |
| PortalLogin | 910 |
| PingRTTACDC | 915 |
| PingRTTHA | 916 |
| PingRTTO365 | 917 |
| ConsumedUnits | 920 |
| GetAccountSKU | 921 |
| LicenseCount (Error) | 930 |
| LicenseCount | 931 |
| LicenseVerification | 940 |
| CertificateExpiry | 945 |
| MailFlowExchangeToM365 | 950 |
| MailFlowM365ToExchange | 951 |
| MailFlowM365ToM365 | 952 |
| MailboxCountM365 | 955 |
| CalendarFreeBusyCheckM365 | 956 |
| CalendarFreeBusyCheckExchange | 957 |
| SharePointPerformance (Connect) | 960 |
| SharePointPerformance | 961 |
| TeamsPerformance (Connect) | 965 |
| TeamsPerformance | 966 |
| TeamsNetworkAssessment | 970 |
| VerifyPrerequisites | 980 |
| InstallPrerequisites | 981 |
| Watcher Node telemetry | 985 |
| Subscription Alerts telemetry | 986 |
| Watcher Node wizard (Info) | 990 |
| Watcher Node wizard (Warning) | 991 |
| Watcher Node wizard (Error) | 992 |
| Managed Module Exception | 999 |

The Management Server may log one or more of these events in the local Event Log in the Operations Manager section.

|  |  |
| --- | --- |
| MP Element | Event ID |
| GetServices (Info) | 1910 |
| GetServices (Error) | 1912 |
| ConnectionState (Info) | 1920 |
| ConnectionState (Error) | 1922 |
| AlertAutoclose (Info) | 1930 |
| AlertAutoclose (Error) | 1932 |
| GetAlerts (Info) | 1940 |
| GetAlerts (Error) | 1942 |

Appendix: Cookdown and Interval Overrides

Often rules and monitors share the same data source. For example, there are three rules and four monitors for Teams Network Assessment that all share a single data source. Operations Manager detects this situation and will only run a single copy of the data source and reuse the results for all seven rules and monitors. This decreases the load on a watcher node and ensures that all related workflows are working with a consistent set of data.

This process is called cookdown. The following web page describes the process and advantages of performing cookdown.

[Operations Manager Management Pack Authoring - Cookdown](https://social.technet.microsoft.com/wiki/contents/articles/15218.operations-manager-management-pack-authoring-cookdown.aspx)

As a result of cookdown, changing the interval at which synthetic transactions are executed suggests that all rules and monitors should be executed at the same rate. For instance, if the frequency that SharePoint is queried decreases, from the default once every 15 minutes to once every hour, all the rules and monitors must be overridden, or the synthetic transaction will still be run once every 15 minutes.

Monitors all allow suppression of alerts until multiple consecutive failures have occurred. The default value for this is one, meaning that an alert will be raised immediately upon the first detection of a problem. If the Match Count and/or Sample Count parameters are overridden, it will take multiple failures before an alert is raised. This will result in a longer delay between the first failure and notification of the failure. If the Interval Seconds parameter is decreased to reduce the notification delay, updating all the rules and monitors sharing the same data source may be desired.

***Note:*** Increasing the frequency of data sources too much can appear to Microsoft 365 as an attack and should be considered carefully.

The following table lists all the rules and monitors sharing the same data source. Overrides for any member of the group should usually be applied to all members of the group. Data source names which are **bold** have more than one rule and/or monitor.

|  |  |
| --- | --- |
| Data Source | Rule/Monitor Display Name |
| Alert Autoclose | Microsoft 365 Alert Autoclose rule |
| Exchange Calendar Free/Busy Check | Exchange Calendar Free/Busy Check Monitor |
| M365 Calendar Free/Busy Check | M365 Calendar Free/Busy Check Monitor |
| Consumed Units Collection | M365 Consumed Units Collection M365 Total Units Collection |
| Microsoft 365 Events | Microsoft 365 Incidents alerting rule |
| Exchange to M365 Mail Flow | Exchange to M365 Mail Flow Monitor Exchange to M365 Receive Duration Performance Collection Exchange to M365 Send Duration Performance Collection Exchange to M365 Total Duration Performance Collection |
| Available License Count | M365 Available License Count Monitor |
| Office Pro Plus License Verification | M365 Office Pro Plus License Verification Monitor |
| M365 to Exchange Mail Flow | M365 to Exchange Mail Flow Monitor M365 to Exchange Receive Duration Performance Collection M365 to Exchange Send Duration Performance Collection M365 to Exchange Total Duration Performance Collection |
| M365 to M365 Mail Flow | M365 to M365 Mail Flow Monitor M365 to M365 Receive Duration Performance Collection M365 to M365 Send Duration Performance Collection M365 to M365 Total Duration Performance Collection |
| Mailbox Count M365 | M365 Mailbox Count M365 Monitor M365 Mailbox Count M365 |
| Microsoft 365 Messages | Microsoft 365 Admin Center Critical alerting rule Microsoft 365 Admin Center Informational alerting rule Microsoft 365 Admin Center Warning alerting rule |
| Portal Login Performance | M365 Portal Login Performance Collection |
| ACDC Performance | M365 (outlook.ms-acdc.office.com) Response Time Performance Collection |
| HA Performance | M365 (outlook.ha.office365.com) Response Time Performance Collection |
| Office Performance | M365 (outlook.office365.com) Response Time Performance Collection |
| SharePoint Performance | SharePoint Performance Monitor SharePoint Performance Download Rule SharePoint Performance Total Rule SharePoint Performance Upload Rule |
| Teams Network Assessment | M365 Teams Network Assessment Status Monitor M365 Teams Network Assessment Average Jitter Monitor M365 Teams Network Assessment Packet Loss Rate Monitor M365 Teams Network Assessment Round Trip Latency Monitor Teams Network Assessment Average Jitter Performance Collection Teams Network Assessment Packet Loss Rate Performance Collection Teams Network Assessment Round Trip Latency Performance Collection |
| Teams Performance | Teams Performance Monitor Teams Performance Download Rule Teams Performance Total Rule Teams Performance Upload Rule Teams Performance Chat Total Time Monitor Teams Performance Chat Send Rule Teams Performance Chat Verify Rule Teams Performance Chat Total Rule Teams Performance File Total Rule |

Appendix: Network Assessment Tools

Teams network assessment is evaluated using the Teams Network Assessment Tool (NAT). In previous releases, the management pack used Skype for Business Network Assessment Tool (which is now deprecated). Version 3 of the Microsoft 365 management pack will continue to work correctly with either NAT but will install the Teams NAT from the watcher node wizard. This allows existing watcher nodes to continue to work with the previously installed S4B NAT, until the Teams NAT is installed.

### Teams NAT Manual Installation and Configuration

The Teams Network Assessment Tool is used to evaluate network performance and network connectivity to determine how well the network would perform for a Microsoft Teams call. The watcher node setup wizard will attempt to install the Teams Network Assessment Tool, however if there are errors, or it needs to be installed manually use the following link:  
<https://www.microsoft.com/en-us/download/details.aspx?id=103017>

***Note****:* A low privilege agent action account may not have permission to write the output file to the default location. In this case, the Microsoft 365 Teams NAT profile should have a higher privilege user assigned to it to allow the Teams NAT to work correctly.

1. Using the Operations Manager Console select the **Administration** workspace.
2. Select **Run As Configuration**, **Profiles** from the **Administration** tree.
3. Select the **Microsoft 365 Teams NAT profile**, right-click and select **Properties**.
4. Click **Next** to get to the Run As Accounts page.
5. Click the **Add** button to add a new account.
6. Select and existing **Run As account** or click **New** to create a new account.
7. Select the **All targeted objects** radio button.
8. Click **OK**, then **Save**, then **OK**.

### Skype for Business NAT Manual Installation and Configuration

The Skype for Business Network Assessment Tool is deprecated but was previously used to evaluate network performance and network connectivity to determine how well the network would perform for a Microsoft Teams call. The watcher node setup wizard no longer attempts to install the Skype for Business Network Assessment Tool, however if it needs to be installed manually use the following link:  
<https://www.microsoft.com/en-us/download/details.aspx?id=53885>

***Note****:* If installed manually, the agent action account may not have permission to write the output file to the default location. In this case, edit the configuration file (typically in this location):

C:\Program Files (x86)\Microsoft Skype for Business Network Assessment Tool\NetworkAssessmentTool.exe.config

Change the ResultsFilePath and OutputFilePath settings to include a folder which the default action account has permission to write. For example (underlined text was added):

<add key="ResultsFilePath" value="C:\ProgramData\Microsoft Skype for Business Network Assessment Tool\performance\_results.tsv"/>

And:

<add key="OutputFilePath" value="C:\ProgramData\Microsoft Skype for Business Network Assessment Tool\connectivity\_results.txt"/>

Appendix: Microsoft 365 Clouds (incl. GCC High)

The Microsoft 365 management pack supports the Microsoft 365 Worldwide, US Government GCC, and US Government GCC High clouds. Other clouds exist but have not been evaluated and are not officially supported.

There are currently five different Microsoft 365 clouds. This table takes you to the list of endpoints for each one. The scope of Office 365 Management Pack is limited to Worldwide, GCC and GCC High subscriptions only.

|  |  |  |
| --- | --- | --- |
| Cloud | Description | In scope of Microsoft 365 MP |
| [Worldwide endpoints](https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide) | The endpoints for worldwide Microsoft 365 subscriptions, which include the United States Government Community Cloud (GCC). | Yes |
| [U.S. Government DoD endpoints](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-u-s-government-dod-endpoints?view=o365-worldwide) | The endpoints for United States Department of Defense (DoD) subscriptions. | No |
| [U.S. Government GCC High endpoints](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-u-s-government-gcc-high-endpoints?view=o365-worldwide) | The endpoints for United States Government Community Cloud High (GCC High) subscriptions. | Yes |
| [Microsoft 365 operated by 21Vianet endpoints](https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges-21vianet?view=o365-worldwide) | The endpoints for Microsoft 365 operated by 21Vianet, which is designed to meet the needs for Microsoft 365 in China. | No |
| [Microsoft 365 Germany endpoints](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-germany-endpoints?view=o365-worldwide) | The endpoints for a separate cloud in Europe for the most regulated customers in Germany, the European Union (EU), and the European Free Trade Association (EFTA). | No |

Reference:

[Microsoft 365 endpoints - Microsoft 365 Enterprise | Microsoft Docs](https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-endpoints?view=o365-worldwide)

### GCC High Support for Subscriptions

When setting up a Subscription for GCC High, the Endpoint Selection should be set as follows (text follows the image):

Graphical user interface, text, application, email

Description automatically generated

<https://login.microsoftonline.us>

<https://graph.microsoft.us/v1.0>

### GCC High Support for Watcher Nodes

When setting up a Watcher Node to use a GCC High subscription, the Subscription Endpoints Setup should be set as follows (text follows the image):

Graphical user interface, text, application

Description automatically generated

<https://login.microsoftonline.us>

<https://graph.microsoft.us/v1.0>

### GCC High Limitations

Mailbox Count is not supported under GCC. Rule **M365 Mailbox Count M365** should be disabled on watcher nodes using GCC High subscriptions.

Any alerts raised by this rule cannot be resolved, as the features are not supported, disabling the workflows is recommended to avoid unnecessary events/alerts.