

# O365 Supplemental Management Pack

## Advanced O365 Monitoring using SCOM

*Prepared for*

3/15/2019

Version 2 Final

*Created by*

**Taylor Blackwell and Brian Zoucha**

[Taylor.Blackwell@microsoft.com](mailto:Taylor.Blackwell@microsoft.com);

[Brianz@microsoft.com](mailto:Brianz@microsoft.com)

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

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

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

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

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

Microsoft Corp. is strictly prohibited.

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

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

## Contents

Foreword .....	4
What's New in V2.....	4
Overview.....	5
Prerequisites and Requirements.....	6
Management Pack .....	6
Support Files.....	6
Service Accounts.....	6
Watcher Node .....	7
Watcher Node Preparation.....	7
Management Pack Configuration .....	8
Deploy the O365 Supplemental management pack .....	8
Creating a new Management Pack for customizations.....	8
Create RunAs Accounts .....	9
Configuring RunAs Profiles .....	10
Enable and Configure Monitors .....	10
Enable and Configure Rules .....	20
Management Pack Contents.....	29
Monitors .....	29
Rules .....	30
Run as Profiles.....	31
Tasks .....	32
Dashboards .....	32
Executive Level Dashboard.....	33
Troubleshooting .....	35
Basic Troubleshooting .....	35
Event Log.....	37

## Foreword

We would like to thank the following colleagues for their contributions and time in making this management pack happen. When we hit roadblocks, you were always there to listen and assist with even the smallest details. Thanks!

Ismaen Aboubakare, James Harper, Kevin Holman, Stephen McComas and Tyson Paul

## What's New in V2

- SharePoint Online Monitoring
  - SPO Connection Monitor
  - SPO Synthetic Transaction Monitor
  - SPO Performance Collection
- Mail Flow Monitoring
  - Increased Error Checking in Mail Flow Monitors
  - Mail Flow Performance Collection
- License Monitoring
  - Updated O365 Available License Count Monitor
  - Consumed License Collection Rule
- Network Performance Collection Rules
  - Portal Login Performance Rule
  - PING Response Time Collection Rules

## Overview

The Office 365 Supplemental Management Pack includes synthetic transactions that provide an increased level of visibility into the health of the Office 365 environment. For customers that don't have an on-premises monitoring solution, they are limited to using the Admin Portal. We are providing this supplemental Management Pack for our customers leveraging System Center Operations Manager as their monitoring platform. There is a Microsoft System Center Management Pack for Office 365 available for download, the supplemental management pack described in this document provides a deeper view into the health of the on-premises and cloud environment. The following Office 365 components are monitored using this supplemental management pack:

- Mail flow – Validate mail flow by sending a test email from a sender mailbox and validating receipt in the receiver mailbox.
- Licensing – Verification that a single dedicated user can obtain a license, Monitoring the available pool of licenses for a given subscription.
- Performance – Collection of performance rules including Watcher Node connection to Office 365, Mail Flow send/receive and Document upload/download.
- SharePoint Online – Validate the ability to upload and download files to specific SharePoint Online sites.

The management pack will execute these synthetic transactions from a local point-of-presence within the customer network for a comprehensive view of service availability. This supplemental Management Pack is based off of the document previously provided by Microsoft Architect, Rob Rinear "Monitoring Office 365 – The DIY Approach".

## Prerequisites and Requirements

The O365 Supplemental Management pack requires a working SCOM environment as a base.

The solution consists of the following elements added to the SCOM environment:

### Management Pack

- **O365 Supplemental.mp**: Current version 2.311.4.0

### Support Files

- **Exchange Web Services**: EWS is used to perform all mail flow workflows within the management pack.
- **Microsoft Online Services Sign-In Assistant for IT Professionals**: MOS SIA is used to login to Azure with PowerShell for the licensing workflows.
- **Windows Azure Active Directory PowerShell Module (MSOnline v1.1.183.17)** : The Azure AD PowerShell module is used to run PowerShell scripts for the licensing tests.
- **Windows Azure Active Directory PowerShell Module (AzureAD v2.0.2.4)**: The Azure AD PowerShell module is used to run PowerShell scripts for the licensing tests.
- **SharePoint Client-side Object Model**: Install SharePoint client-side object model (CSOM) DLLs from the following link on the servers(s) that will run the synthetic tests

### Service Accounts

This solution utilizes SCOM's "RunAs" accounts to define credentials stored in SCOM and use them to execute the scripts within the workflows. A set of service accounts is required for on-premises and O365 based monitoring workflows.

- **On-Premises Workflows**
  - An Exchange username and password for *sending* email
  - An Exchange username and password for *receiving* email
- **O365 Mail flow Workflows**
  - An Office 365 username and password for *sending* email
  - An Office 365 username and password for *receiving* email
- **O365 Licensing Workflows**
  - An Office 365 username and password for connecting to and verifying O365 subscriptions.
- **O365 SPO Workflows**
  - An Office 365 username and password for connecting to SharePoint Online.

**Note:** User accounts can be shared across workflows to conserve O365 licenses.

## Watcher Node

- This Management Pack solution requires at least one agent managed to computer to perform the workflows.

## Watcher Node Preparation

The O365 Supplemental Management Pack requires watcher nodes with the SCOM agent installed to perform synthetic transactions and transmit results back to the management servers. These watcher nodes will need to have the prerequisite components installed for the synthetic transactions to work. Once you have located computers to work as watcher nodes you will need to make sure all the components below are installed on every watcher node.

- **SCOM Agent:** This SCOM agent needs to be a member of the SCOM management group that the O365 Supplemental MP is imported on.
- **Exchange Web Services:** Install EWS 2.2 from the following link on the server(s) that will run the mail flow synthetic test workflows:  
<https://www.microsoft.com/en-us/download/details.aspx?id=42951>
- **Microsoft Online Services Sign-In Assistant for IT Professionals:** Install on the server(s) that will run the licensing workflows.  
<https://www.microsoft.com/en-us/download/details.aspx?id=41950>
- **Windows Azure Active Directory PowerShell Module (MSOnline v1.1.183.17):** Install the azure PowerShell module on the server(s) that will run the licensing workflows.  
<https://www.powershellgallery.com/packages/MSOnline/1.1.183.17>
- **Windows Azure Active Directory PowerShell Module (AzureAD v2.0.2.4):** Install the azure PowerShell module on the server(s) that will run the licensing workflows.  
<https://www.powershellgallery.com/packages/AzureAD/2.0.2.4>
- **SharePoint Client-side Object Model:** Install SharePoint client-side object model (CSOM) DLLs from the following link on the servers(s) that will run the synthetic tests:  
<https://www.microsoft.com/en-us/download/details.aspx?id=35585>

## Management Pack Configuration

The steps below walk through the process to import and configure the O365 Supplemental Management pack into Operations Manager.

### Deploy the O365 Supplemental management pack

Import the O365Supplemental.mp management pack using the steps below.

1. Log on to the computer with an account that is a member of the **Operations Manager Administrators** role for the Operations Manager management group.
2. In the Operations console, click **Administration**.
3. Right-click the **Management Packs** node, and then click **Import Management Packs**.
4. The **Import Management Packs** wizard opens. Click **Add**, and then click **Add from disk**.
5. The **Select Management Packs to import** dialog box appears. If necessary, change to the directory that holds your management pack file. Click the O365 Supplemental management pack to import from that directory, and then click **Open**.
6. On the **Select Management Packs** page, the management packs that you selected for import are listed. An icon next to each management pack in the list indicates the status of the selection, click **Import**.
7. The **Import Management Packs** page appears and shows the progress for each management pack. Each management pack is downloaded to a temporary directory, imported to Operations Manager, and then deleted from the temporary directory. If there is a problem at any stage of the import process, select the management pack in the list to view the status details. Click **Close**.

### Creating a new Management Pack for customizations

The O365 Supplemental management pack is sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, the Operations Manager saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

1. Open the **Operations Manager** console, and then click **Administration** button.
2. Right-click **Management Packs**, and then click **Create New Management Pack**.
3. Enter a name (for example, **O365 Supplemental Overrides**), and then click **Next**.
4. Click **Create**.



## Create RunAs Accounts

The O365 Supplemental management pack utilizes RunAs Accounts to perform workflows to test the O365 environment. Run As accounts will need to be configured for all the Run As profiles. **Note:** You will need to logon and connect to the Operations Manager console with an account that is a member of the Operations Manager Administrators role to complete the following operations.

- Office 365 Supplemental O365 Sender Profile
  - Office 365 Supplemental O365 Receiver Profile
  - Office 365 Supplemental Exchange Sender Profile
  - Office 365 Supplemental Exchange Receiver Profile
  - Office 365 Supplemental License Verification Profile
  - Office 365 Supplemental SPO Profile
1. In the Operations console, click **Administration**.
  2. In the Administration pane, expand **Administration**, expand **RunAs Configuration**, right-click **Accounts**, and then click **Create RunAs Account...**
  3. In the **Create RunAs Account Wizard**, on the **Introduction** page click **Next**.
  4. On the **General Properties** page, do the following:
    1. Select **Basic Authentication** in the **RunAs Account type:** list.
    2. Type a display name in the **Display Name** text box,
    3. Optionally, type a description in the **Description** box.
    4. Click **Next**.
  5. On the **Credentials** page, type a username (Must use the format Username@domain.com), and its password, for the account that you want to use with this **RunAs Account**.
  6. Click **Next**.
  7. On the **Distribution Security** page, select the **More secure** option as appropriate.
  8. Click **Create**.
  9. On the **RunAs Account Creation Progress** page, click **Close**.

**Important Note:** For the mail flow monitors to work the RunAs username must be in the UPN format (Username@domain.com) and be a valid email address, as this is where the workflows get the addresses used to verify mail flow.

## Configuring RunAs Profiles

Run As profiles have been included with the O365 Supplemental management pack, once imported. Use this procedure to modify the properties of Run As profiles to use the RunAs Accounts created above.

**Note:** You will need to logon and connect to the Operations Manager console with an account that is a member of the Operations Manager Administrators role to complete the following operations.

1. Select the **Administration** view.
2. In the **Administration** view navigation pane, select the **Profiles** container.
3. In the results pane, double-click the profile whose properties you want to edit. This opens the **Run As Profile Wizard**, which contains the settings that were configured previously.
4. On the **General Properties** page, you can modify the value in the **Display name** and **Description** fields.
5. Click **Next**.
6. On the **Run As Accounts** page, you can add your Run As accounts, click **Next**.
7. When you have completed your modifications, click **Save**.
8. On the **Completion** page, in the **More-secure Run As accounts:** box, you must select each account in turn and configure the distribution of the credentials for each Run As account.
9. When you have completed configuring distribution, click **Close**.

## Enable and Configure Monitors

You will need to override monitors and rules for the workflows you intend to use in order to enable monitoring utilizing the synthetic transaction scripts and collections on watcher nodes. The steps below will walk you through the process of enabling and setting parameters through overrides for each monitor included in the management pack.

### O365 to O365 Mail Flow Monitor

This monitor utilizes synthetic transactions to verify the flow of email from an O365 email account to another O365 email account. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into a sender account using the "O365 Sender Profile" and sending a test email to the receiver account specified in the

"O365 Receiver Profile". The monitor then logs into the receiver account using the "O365 Receiver Profile" to verify the test email was received.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Sleep Int	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for:** box, type "O356 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the monitor **O365 to O365 Mail Flow Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.

10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
13. Set the override value to the O365 EWS URL.
14. Click **OK**

## O365 to Exchange Mail Flow Monitor

This monitor utilizes synthetic transactions to verify the flow of email from an O365 email account to an Exchange email account. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into a sender account using the "O365 Sender Profile" and sending a test email to the receiver account specified in the "Exchange Receiver Profile". The monitor then logs into the receiver account using the "Exchange Receiver Profile" to verify the test email was received.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Exchange URL*	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment.
SleepInt	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search

This monitor contains the following overridable parameters.

for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the monitor **O365 to Exchange Mail Flow Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
13. Set the override value to the O365 EWS URL.
14. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
15. Set the override value to the Exchange EWS URL.
16. Click **OK**

## Exchange to O365 Mail Flow Monitor

This monitor utilizes synthetic transactions to verify the flow of email from an Exchange email account to an O365 email account. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into a sender account using the "Exchange Sender Profile" and sending a test email to the receiver account specified in the "O365 Receiver Profile". The monitor then logs into the receiver account using the "O365 Receiver Profile" to verify the test email was received.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled	False	This need to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Exchange URL*	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment.
Sleep Int	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.

4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the monitor **Exchange to O365 Mail Flow Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
13. Set the override value to the O365 EWS URL.
14. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
15. Set the override value to the Exchange EWS URL.
16. Click **OK**

## O365 Available License Monitor

This monitor utilizes Azure Active Directory PowerShell Module to verify that number of available licenses for a particular SKU is greater than the set threshold. The "License Verification Profile" is used to run the workflow. This monitor has three health states, healthy, warning and critical. The health state is determined by running the **Get-AzureADSubscribedSku** and then we need to make sure we actually have a license to assign. To determine that, we take the value of **PrePaidUnits** property (25) and subtract the value of the **ConsumedUnits** (24) property:

$$25 - 24 = 1$$

The **PrePaidUnits** property tells us how many licenses we've purchased, and the value **ConsumedUnits** tells us how many licenses are currently in use. If we subtract the number of licenses already spoken for from the number of licenses we purchased, we'll know how many licenses are still available.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
-----------	---------------	---------

This monitor contains the following overridable parameters.

Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
Rem Licenses Error	5	This sets the critical alert threshold for the monitor if the number of available licenses is less the set value it will cause an alert to be generated. The default value can be left or can be adjusted to fit the environment.
Rem Licenses Warn	10	This sets the warning alert threshold for the monitor if the number of available licenses is less the set value it will cause an alert to be generated. The default value can be left or can be adjusted to fit the environment.
Sku Type*	None	This need to be overridden to the account sku you wish to monitor on all watcher nodes. The available SKUs for your environment can be found by running the Get Account SKU Task.

1. Log on to the computer with an account that is a member of the Operations Manager Advanced Operator role for the Operations Manager management group.
2. In the Operations console, click the **Authoring** button.
3. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
4. On the toolbar, click **Scope**.
5. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
6. Click the check box next to **O365 Watcher Node**.
7. Click **OK** to close the dialog box.
8. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.



9. Under **Availability**, right-click the monitor **O365 Available License Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
10. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
11. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
12. Set the override value to **True**.
13. In the **Override Properties** dialog box, select the **Override** check box next to **RemLicenses**.
14. Set the override value to **License Threshold** (any number you choose).
15. In the **Override Properties** dialog box, select the **Override** check box next to **SkuType**.
16. Set the override value to **Monitored Sku Type**.
17. Click **OK**

## O365 Office Pro Plus License Verification Monitor

This monitor utilizes Azure Active Directory PowerShell Module to verify that user specified in the "License Verification Profile" is able to obtain a license. This monitor has two health states, healthy and critical. The health state is simply determined by whether a license is obtained by the workflow.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled	False	This need to be overridden to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.

3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the monitor **O365 Office Pro Plus License Verification Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. Click **OK**

## SPO Connection Monitor

This event driven monitor determines if a connection can be made to SharePoint Online. This monitor has two health states, healthy and critical. The health state is determined by Event 45 found in the Operation Manager log. These events are generated by the workflows for the "SPO Synthetic Transaction Monitor" and requires the "SPO Synthetic Transaction Monitor" be enabled to work.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
Enabled	False	This need to be overridden to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.

7. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the monitor **SPO Connection Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.

## SPO Synthetic Transaction Monitor

This monitor utilizes synthetic transactions to verify the ability upload and download files to SharePoint Online. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into SharePoint Online using the "Office 365 Supplemental SPO Profile " uploading a test file then verifying the existence of the file in SharePoint Online.

This monitor contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled	False	This need to be overridden to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
SPODocLib	None	This is the document library that will be used to upload and download the test file. Ex. Documents
SPOSite	None	This is the SharePoint Online site you will be testing synthetic transactions with.
TempFolder	None	The is the path for the watcher node to temporarily store the test file for upload. Ex. C:\windows\temp

12. In the Operations console, click the **Authoring** button.
13. In the **Authoring** pane, expand **Management Pack Objects** and then click **Monitors**.
14. On the toolbar, click **Scope**.
15. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
16. Click the check box next to **O365 Watcher Node**.
17. Click **OK** to close the dialog box.
18. After the monitors have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
19. Under **Availability**, right-click the monitor **SPO Synthetic Transaction Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
20. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
21. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
22. Set the override value to **True**.
23. In the **Override Properties** dialog box, select the **Override** check box next to **SPODocLib**.
24. Set the override value to the O365 SPO Document library.
25. In the **Override Properties** dialog box, select the **Override** check box next to **SPOSite**.
26. Set the override value to the O365 SPO Site.
27. In the **Override Properties** dialog box, select the **Override** check box next to **TempFolder**.
28. Set the override value to the O365 SPO Temp Folder.
29. Click **OK**

## Enable and Configure Rules

You will need to override rules to for the workflows you intend to use in order to enable monitoring utilizing the synthetic transaction scripts on Watcher Nodes. The steps below will walk you through the process of enabling and setting parameters through overrides for each monitor included in the management pack.

**Important Note:** All Mail Flow and SPO performance rules must have identical overrides to their corresponding monitors. **If the overrides are not identical cookdown will fail, causing the rules and monitors to malfunction and cause the workflows error or unload.**

## O365 to O365 Mail Flow Monitor Performance Rules

- O365 to O365 Send Duration Performance Collection
- O365 to O365 Receive Duration Performance Collection
- O365 to O365 Total Duration Performance Collection

These rules collect performance metrics generated by synthetic transactions to verify the flow of email from an O365 email account to another O365 email account. The three rules measure email send, receive and total times, respectively. When the synthetic transaction for the “O365 to O365 Mail Flow Monitor” is performed the rules collect the time it takes to login to a sender account using the "O365 Sender Profile" and send a test email. Then the amount of time the receiver account specified in the "O365 Receiver Profile" takes to verify the test email was received. Finally adding the two times together to create a total duration.

This rule contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Sleep Int	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Rules**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the rules have loaded, right-click the rule **O365 to O365 Send Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
8. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
9. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
10. Set the override value to **True**.
11. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
12. Set the override value to the O365 EWS URL.
13. Click **OK**
14. right-click the rule **O365 to O365 Receive Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
15. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
16. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
17. Set the override value to **True**.
18. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
19. Set the override value to the O365 EWS URL.
20. Click **OK**
21. right-click the rule **O365 to O365 Total Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
22. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
23. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
24. Set the override value to **True**.
25. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
26. Set the override value to the O365 EWS URL.
27. Click **OK**

## O365 to Exchange Mail Flow Monitor Performance Rules

- O365 to Exchange Send Duration Performance Collection
- O365 to Exchange Receive Duration Performance Collection
- O365 to Exchange Total Duration Performance Collection

These rules collect performance metrics generated by synthetic transactions to verify the flow of email from an O365 email account to an Exchange email account. The three rules measure email send, receive and total times, respectively. When the synthetic transaction for the “O365 to Exchange Mail Flow Monitor” is performed the rules collect the time it takes to login to a sender account using the "O365 Sender Profile" and send a test email. Then the amount of time the receiver account specified in the "Exchange Receiver Profile" takes to verify the test email was received. Finally adding the two times together to create a total duration.

This rule contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled*	False	This needs to be overridden and set to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Exchange URL*	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment.
SleepInt	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Rules**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the rules have loaded, right-click the rule **O365 to Exchange Send Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
8. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
9. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
10. Set the override value to **True**.
11. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
12. Set the override value to the O365 EWS URL.
13. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
14. Set the override value to the Exchange EWS URL.
15. Click **OK**
16. right-click the rule **O365 to Exchange Receive Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
17. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
18. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
19. Set the override value to **True**.
20. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
21. Set the override value to the O365 EWS URL.
22. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
23. Set the override value to the Exchange EWS URL.
24. Click **OK**
25. right-click the rule **O365 to Exchange Total Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.



26. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
27. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
28. Set the override value to **True**.
29. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
30. Set the override value to the O365 EWS URL.
31. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
32. Set the override value to the Exchange EWS URL.
33. Click **OK**

## Exchange to O365 Mail Flow Monitor Performance Rules

- Exchange to O365 Send Duration Performance Collection
- Exchange to O365 Receive Duration Performance Collection
- Exchange to O365 Total Duration Performance Collection

These rules collect performance metrics generated by synthetic transactions to verify the flow of email from an O365 email account to another O365 email account. The three rules measure email send, receive and total times, respectively. When the synthetic transaction for the “Exchange to O365 Mail Flow Monitor” is performed the rules collect the time it takes to login to a sender account using the "Exchange Sender Profile" and send a test email. Then the amount of time the receiver account specified in the "O365 Receiver Profile" takes to verify the test email was received. Finally adding the two times together to create a total duration.

This rule contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.
Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.

This rule contains the following overridable parameters.

Enabled	False	This needs to be overridden and set to True for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
O365 URL*	None	This needs to be overridden and populated with the URL for the O365 EWS URL utilized in your environment.
Exchange URL*	None	This needs to be overridden and populated with the URL for the Exchange EWS URL utilized in your environment.
Sleep Int	5 Sec	This value determines how long the monitor waits between search attempts during each run of the synthetic transaction. The synthetic transaction will attempt to search for the received email 10 times. The default value can be left or can be adjusted to fit the environment.

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Rules**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O356 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the rules have loaded, right-click the rule **Exchange to O365 Send Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
8. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
9. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
10. Set the override value to **True**.
11. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
12. Set the override value to the O365 EWS URL.
13. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
14. Set the override value to the Exchange EWS URL.
15. Click **OK**
16. right-click the rule **Exchange to O365 Receive Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.

17. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
18. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
19. Set the override value to **True**.
20. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
21. Set the override value to the O365 EWS URL.
22. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
23. Set the override value to the Exchange EWS URL.
24. Click **OK**
25. right-click the rule **Exchange to O365 Total Duration Performance Collection**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 watcher Node**.
26. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
27. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
28. Set the override value to **True**.
29. In the **Override Properties** dialog box, select the **Override** check box next to **O365 URL**.
30. Set the override value to the O365 EWS URL.
31. In the **Override Properties** dialog box, select the **Override** check box next to **Exchange URL**.
32. Set the override value to the Exchange EWS URL.
33. Click **OK**

## SPO Synthetic Transaction Monitor Performance Rules

This monitor utilizes synthetic transactions to verify the ability upload files to SharePoint Online. This monitor has two health states, healthy and critical. The health state is determined if the synthetic transaction is or is not able to successfully complete for any reason. The synthetic transaction works by logging into SharePoint Online using the "Office 365 Supplemental SPO Profile " uploading a test file then verifying the existence of the file in SharePoint Online.

This rule contains the following overridable parameters.

Parameter	Default Value	Details
Script Timeout	300 Sec	This set the amount of time the synthetic transaction must complete before it errors out. The default value can be left or can be adjusted to fit the environment.

This rule contains the following overridable parameters.

Interval Seconds	900 Sec	This sets how long the monitor waits until running the synthetic transaction again. The default value can be left or can be adjusted to fit the environment.
Enabled	False	This need to be overridden to true for all watcher nodes. This allows the monitor to run the synthetic transaction workflows.
SPODocLib	None	This is the document library that will be used to upload and download the test file. Ex. Documents
SPOSite	None	This is the SharePoint Online site you will be testing synthetic transactions with.
TempFolder	None	The is the path for the watcher node to temporarily store the test file for upload. Ex. C:\windows\temp

1. In the Operations console, click the **Authoring** button.
2. In the **Authoring** pane, expand **Management Pack Objects** and then click **Rules**.
3. On the toolbar, click **Scope**.
4. In the **Scope Management Pack Target(s) by object** dialog box, in the **Look for** box, type "O365 Watcher".
5. Click the check box next to **O365 Watcher Node**.
6. Click **OK** to close the dialog box.
7. After the Rules have loaded, click **O365 Watcher Node > Entity Health > Availability > Office 365 Supplemental MP Watcher Node Aggregate Monitor Availability**.
8. Under **Availability**, right-click the monitor **SPO Synthetic Transaction Monitor**, and then click **Overrides > Override the Monitor > For a specific object of the Class: O365 Watcher Node**.
9. In the **Select Object dialog** box, select the watcher node, and then click **OK**.
10. In the **Override Properties** dialog box, select the **Override** check box next to **Enabled**.
11. Set the override value to **True**.
12. In the **Override Properties** dialog box, select the **Override** check box next to **SPODocLib**.
13. Set the override value to the O365 SPO Document library.
14. In the **Override Properties** dialog box, select the **Override** check box next to **SPOSite**.
15. Set the override value to the O365 SPO Site.
16. In the **Override Properties** dialog box, select the **Override** check box next to **TempFolder**.
17. Set the override value to the O365 SPO Temp Folder.

18. Click **OK**

## Management Pack Contents

This solution is powered by a custom management pack consisting of multiple workflows and run as profiles to monitor mail flow and licensing. This provides additional insight regarding the health of an organizations email infrastructure.

### Monitors

- **O365 to O365 Mail Flow Monitor**
  - This monitor logs into O365 using the O365 Sender Profile and sends a test message to the O365 Receiver Profile. It then logs into the account specified in the O365 Receiver Profile and verifies receipt of the email from the O365 Sender Profile.
- **Exchange to O365 Mail Flow Monitor**
  - This monitor logs into Exchange using the Exchange Sender Profile and sends a test message to the O365 Receiver Profile. It then logs into the account specified in the O365 Receiver Profile and verifies receipt of the email from the Exchange Sender Profile.
- **O365 to Exchange Mail Flow Monitor**
  - This monitor logs into O365 using the O365 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 O365 Sender Profile.
- **O365 Office Pro Plus License Verification Monitor**
  - This monitor uses PowerShell to determine if there are O365 licenses available and a connection can be made to retrieve licenses.
- **O365 Available License Count Monitor**
  - This monitor uses PowerShell to determine if the number of available of O365 licenses is greater than the set threshold.
- **SPO Connection Monitor**
  - This event driven monitor looks for event 45 in the operations manager log to determine if a connection to SPO can be made.
- **SPO Synthetic Transaction Monitor**
  - This monitor logs into SPO using the SPO Profile and creates a test file. It then logs into the account specified in the SPO Profile and verifies the file is in the specified folder.

## Rules

- **O365 to O365 Mail Flow Event Collection**
  - This rule looks for and collects the event ID 40 in the Operations Manager log.
- **O365 to Exchange Mail Flow Event Collection**
  - This rule looks for and collects the event ID 43 in the Operations Manager log.
- **Exchange to O365 Mail Flow Event Collection**
  - This rule looks for and collects the event ID 42 in the Operations manager log.
- **O365 Office Pro Plus License Verification Event Collection**
  - This rule looks for and collects the event 41 ID in the Operations Manager Log.
- **O365 Office Pro Plus License Verification Event Collection**
  - This rule looks for and collects the event 44 ID in the Operations Manager Log.
- **O365 Consumed Units Collection**
  - This rule collects the number of licenses consumed.
- **O365 Portal Login Performance Collection**
  - This rule connects to the Office 365 Portal and logs in via synthetic transaction and collects the Time in MS.
- **O365 Response Time Performance Collection Rule (outlook.office365.com)**
  - This rule pings the address outlook.office365.com and collects the Time in MS.
- **O365 Response Time Performance Collection Rule (outlook.ha.office365.com)**
  - This rule pings the address outlook.ha.office365.com and collects the Time in MS.
- **O365 Response Time Performance Collection Rule (outlook.ms-acdc.office.com)**
  - This rule pings the address outlook.ms-acdc.office.com and collects the Time in MS.
- **Exchange to O365 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 MS.
- **Exchange to O365 Receive Duration Performance Collection**
  - This rule measures the amount of time it takes to receive and verify a test email from exchange to O365 and collects the Time in MS.
- **Exchange to O365 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 O365 and collects the Time in MS.
- **O365 to Exchange Send Duration Performance Collection**
  - This rule measures the amount of time it takes to send a test email from O365 and collects the Time in MS.
- **O365 to Exchange Receive Duration Performance Collection**
  - This rule measures the amount of time it takes to receive and verify a test email from O365 to exchange and collects the Time in MS.
- **O365 to Exchange Total Duration Performance Collection**

- This rule measures the total amount of time it takes to send a test email from O365 and verify receipt of a test email from O365 to Exchange and collects the Time in MS.
- **O365 to O365 Send Duration Performance Collection**
  - This rule measures the amount of time it takes to send a test email from O365 and collects the Time in MS.
- **O365 to O365 Receive Duration Performance Collection**
  - This rule measures the amount of time it takes to receive and verify a test email from O365 to O365 and collects the Time in MS.
- **O365 to O365 Total Duration Performance Collection**
  - This rule measures the total amount of time it takes to send a test email from O365 and verify receipt of a test email from O365 to O365 and collects the Time in MS.
- **SPO Connection Event Collection**
  - This event driven rule looks for connection errors from the SPO Synthetic Transaction Monitor.
- **SPO Download Duration Performance Collection**
  - This rule measures the amount of time it takes to download a test file from SPO and collects the Time in MS.
- **SPO Synthetic Event Collection**
  - This rule looks for and collects the event ID 45 in the Operations Manager event log.
- **SPO Total Duration Performance Collection**
  - This rule measures the total amount of time it takes to upload a test file to SPO and verify download of a test file from SPO and collects the Time in MS.
- **SPO Upload Duration Performance Collection**
  - This rule measures the amount of time it takes to upload a test file to SPO and collects the Time in MS.

## Run as Profiles

When the O365 Supplemental Management Pack is imported for the first time, it creates five new Run As profiles:

- **Office 365 Supplemental O365 Sender Profile**
  - This profile is used to login and send email using O365.
- **Office 365 Supplemental O365 Receiver Profile**
  - This profile is used to login and receive email using O365.
- **Office 365 Supplemental Exchange Sender Profile**
  - This profile is used to login and send email using exchange.

- **Office 365 Supplemental Exchange Receiver Profile**
  - This profile is used to login and receive email using exchange.
- **Office 365 Supplemental License Verification Profile**
  - This profile is used to verify O365 Licensing information.
- **Office 365 Supplemental SPO Profile**
  - This profile is used to verify SPO information.

## Tasks

- **Get Account Sku**
  - This task outputs the SKUs associated with the license verification profile.
- **O365 SMP Prerequisite Verification**
  - This task outputs the install status of prerequisites required on watcher nodes.




## Dashboards

- **O365 Mail Flow Dashboard**
  - This dashboard displays all mail flow related alerts and events for the O365 Supplemental MP.
- **O365 Licensing Dashboard**
  - This dashboard displays all licensing related alerts and events for the O365 Supplemental MP.
- **O365 Hybrid Mail Flow Performance Dashboard**
  - This dashboard displays all hybrid mail flow performance metrics related for the O365 Supplemental MP.
- **O365 Mail Flow Performance Dashboard**
  - This dashboard displays all Office 365 mail flow performance metrics related for the O365 Supplemental MP.
- **O365 Network Performance Dashboard**
  - This dashboard displays all network performance related metrics for the O365 Watcher Nodes.
- **O365 SPO Dashboard**
  - This dashboard displays all SharePoint Online related alerts and events for the O365 Supplemental MP.
- **O365 SPO Performance Dashboard**
  - This dashboard displays all SharePoint Online performance related metrics for the O365 Supplemental MP.
- **O365 Executive Level Dashboard**
  - This dashboard has the ability to display all Office 365 related alerts, monitors and performance data for the O365 Supplemental MP.

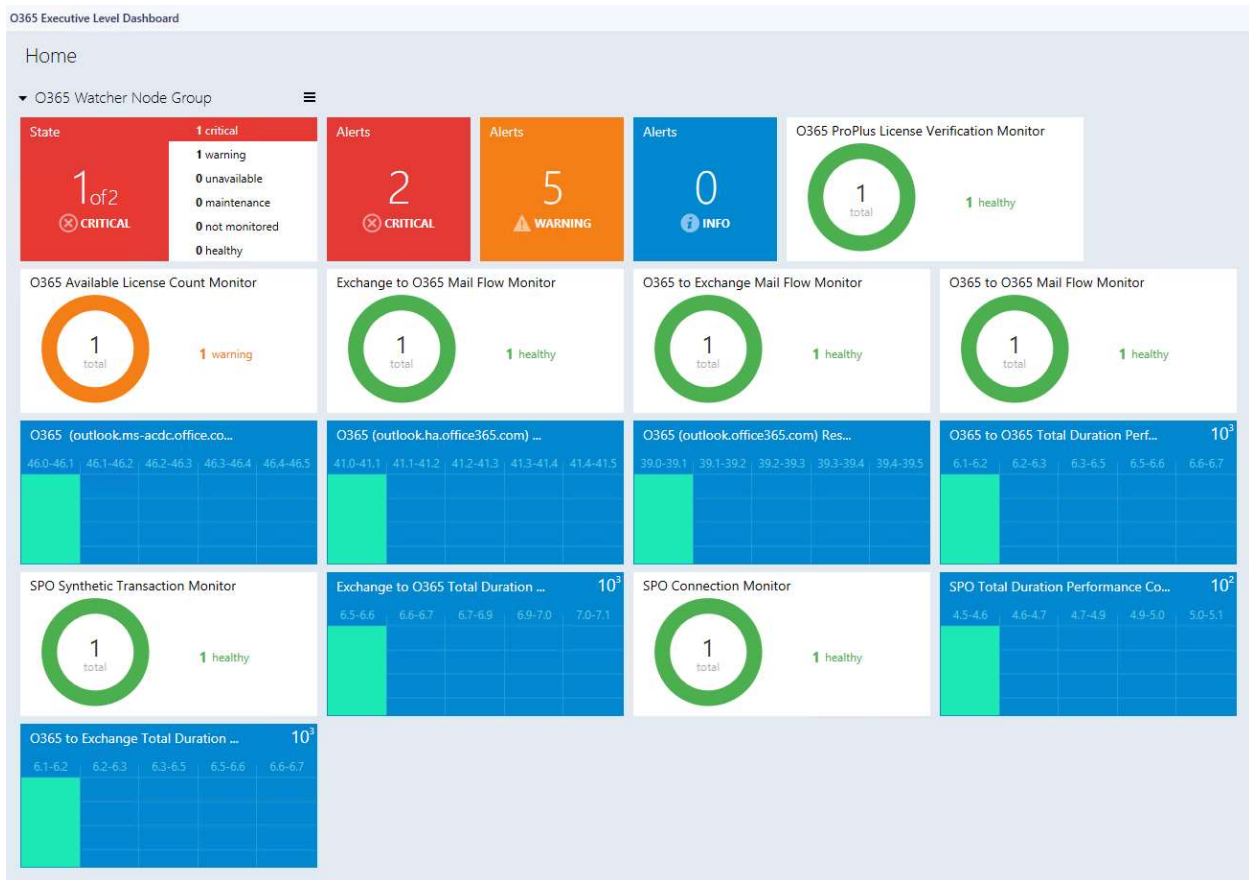


## Executive Level Dashboard

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

- 1.) Create a new **unsealed MP** for the **Dashboard**, you can use the same MP that you stored your overrides in when enabling the Performance Counters, Monitors and Rules.
- 2.) Click the **Monitoring Pane**, right click the folder for your new unsealed MP and choose **New Dashboard** view.
- 3.) In the **New Dashboard and Widget Wizard** click **SQL Server Dashboards**, then choose **Datacenter Dashboard template**.
- 4.) Provide a **Name** for your new Dashboard on the **General Properties** page, click **Next**
- 5.) Click **Create** on the **Summary** page, then click **Close** on the **Completion** page.
- 6.) In the **dashboard pane**, in the upper **right-hand** corner click the  to create a **Group**.
- 7.) Select **Add Virtual Group**, choose a **Display Name** and then select the **O365 Watcher Node** class and click **Add**
- 8.) Click the  and choose **Add Monitor Tile**, you can add a Monitor tile for each of the following:
  - i. O365 ProPlus License Verification Monitor
  - ii. O365 Available License Count Monitor
  - iii. Exchange to O365 Mail Flow Monitor
  - iv. O365 to Exchange Mail Flow Monitor
  - v. O365 to O365 Mail Flow Monitor
  - vi. SPO Connection Monitor
  - vii. SPO Synthetic Transaction Monitor
- 9.) Click the  and choose **Add Performance Tile**, you can add a **Performance** tile for each of the following:
  - i. O365 Portal Login Performance Collection
  - ii. O365 Response Time Performance Collection Rule (outlook.office365.com)
  - iii. O365 Response Time Performance Collection Rule (outlook.ha.office365.com)

- iv. O365 Response Time Performance Collection Rule (outlook.ms-acdc.office.com)
- v. Exchange to O365 Total Duration Performance Collection
- vi. O365 to Exchange Total Duration Performance Collection
- vii. O365 to O365 Total Duration Performance Collection
- viii. SPO Total Duration Performance Collection



## Troubleshooting

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

### Basic Troubleshooting

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

1. Check the Operations Manager Event Log on the Watcher Node, filter events ranging from 40-55. See table below.
2. O365 Connectivity from the Watcher Node workflow troubleshooting can be verified using the following Powershell code and the steps below.

2a. Open Windows Powershell ISE on the Watcher Node.

2b. Press Ctrl+N for a new session. Copy and Paste the following code sample into the new session

```
## Begin Code Sample ##  
  
Import-Module AzureAD  
# $UserCredential must be passed in correct format, @domain.com or  
# @tenant.microsoft.com or basic connectivity will fail.  
$UserCredential = "<username>@<tenant>.onmicrosoft.com"  
$UserPassword = ConvertTo-SecureString -String "<password>" -AsPlainText -Force  
$Credential = New-Object -TypeName "System.Management.Automation.PSCredential"  
-ArgumentList $UserCredential, $UserPassword  
$Service = Connect-AzureAD -Credential $Credential  
Get-AzureADSubscribedSku  
  
## End Code Sample ##
```

2c. Change the <username> and <password> credentials that you want to test connectivity with so that they match your subscription, Administrator credentials are not needed. A regular user account will work.

2d. Press F5 to execute the code snippet, when connected successfully you will be returned to the Powershell ISE prompt.

2e. Once connected you can execute any of the cmdlets that are included with Azure AD Powershell Modules, see the following link for reference.

#### Connect to Office 365 PowerShell

<https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell>

3. Troubleshooting Mail Flow, verify that you can login to the Office portal with the Run As Accounts and you can send/receive email successfully. If unable to send and receive mail successfully contact O365/Exchange Team. Attempt connection to the Office portal from the Agent Managed computer that you have designated as a O365 Watcher Node.
4. If needed, you can choose to install the required PowerShell modules manually, you can use Install-Module from within the PowerShell ISE.

#### **Install-Module**

<https://docs.microsoft.com/en-us/powershell/module/powershellget/install-module?view=powershell-6>

5. If you retire or decommission a watcher node, you can remove the watcher node by using the Remove-SCOMDisabledClassInstance cmdlet and target the O365 Watcher Node Discovery.

#### **Remove-SCOMDisabledClassInstance**

<https://docs.microsoft.com/en-us/powershell/module/operationsmanager/remove-scomdisabledclassinstance?view=systemcenter-ps-2016>

6. Why is using the correct account and or login/UPN important? By default, the Office 365 subscription uses the <company name>.onmicrosoft.com domain that was created with the account.\* You can add one or more custom domains to Office 365 rather than retaining the onmicrosoft.com domain, and can assign users to sign in with any of the validated domains. Each user's assigned domain is the email address that will appear on sent and received email messages.

For organizations using single sign-on, all users on a domain must use the same identity system: either cloud identity or federated identity. For example, you could have one group of users that only needs a cloud identity because they don't access on-premises systems, and another group of users who use Office 365 and on-premises systems. You would use add two domains to Office 365, such as contractors.contoso.com and staff.contoso.com, and only set up SSO for one of them.

**Note:** Using the incorrect login/UPN will affect the basic functionality of all workflows.

7. Cookdown refers to a feature of System Center Operations Manager where a single copy of a data source module is shared among multiple workflows to reduce overhead. The performance collection rules within this supplemental management pack leverage cookdown, when you enable them – the overrides for the performance collections rules **MUST MATCH EXACTLY** to the **MONITORS** or they will not work correctly.

## Event Log

Monitor/Rule	Event ID	Success	Error
<b>O365 Available License Count Monitor</b>	33		Problem getting O365 SKUs. \$Error
<b>O365 to O365 Mail Flow Monitor</b>	40	O365MailFlow SUCCESS: Mail flow completed for test ID \$TestID. Sender: \$SenderUser Receiver: \$ReceiverUser Send Duration: \$SWSDDTime Receive Duration: \$SWRDDTime TotalDuration: \$TotalDuration State: Healthy	O365MailFlow ERROR: Email NOT received for test ID \$TestID. Sender: \$SenderUser Receiver: \$ReceiverUser Send Duration: \$SWSDDTime Receive Duration: \$SWRDDTime TotalDuration: \$TotalDuration State: Critical
<b>Exchange to O365 Mail Flow Monitor</b>	42	O365MailFlow SUCCESS: Mail flow completed for test ID \$TestID. Sender: \$SenderUser Receiver: \$ReceiverUser Send Duration: \$SWSDDTime Receive Duration: \$SWRDDTime TotalDuration: \$TotalDuration State: Healthy	O365MailFlow ERROR: Email NOT received for test ID \$TestID. Sender: \$SenderUser Receiver: \$ReceiverUser Send Duration: \$SWSDDTime Receive Duration: \$SWRDDTime TotalDuration: \$TotalDuration State: Critical
<b>O365 to Exchange Mail Flow Monitor</b>	43	O365MailFlow SUCCESS: Mail flow completed for test ID \$TestID. Sender: \$SenderUser Receiver: \$ReceiverUser Send Duration: \$SWSDDTime Receive Duration: \$SWRDDTime TotalDuration: \$TotalDuration State: Healthy	O365MailFlow ERROR: Email NOT received for test ID \$TestID. Sender: \$SenderUser Receiver: \$ReceiverUser Send Duration: \$SWSDDTime Receive Duration: \$SWRDDTime TotalDuration: \$TotalDuration State: Critical
<b>O365 Office Pro Plus License Verification Monitor</b>	41	O365 License SUCCESS: Office Pro Plus License Status is Licensed. \$UserCredential Result:\$IsLicensed	O365 License ERROR: Office Pro Plus License Status is NOT Licensed. \$UserCredential Result:\$IsLicensed

<b>O365 Available License Count Monitor</b>	44	O365 License SUCCESS: \$AcctSkuld has remaining Licenses. Result: \$Units	O365 License Warning: \$AcctSkuld does NOT have enough Licenses. Result: \$Units
	44		O365 License Error: Problem getting SKUs.Contact Support:\$Error
	44		O365 License Error: Problem with AcctSku. Contact Support:\$Error
<b>SPO Synthetic Monitor</b>	45	SPO Synth Success: Document upload to SharePoint Online site \$SPOSite successful. State: Healthy	SPO Synth ERROR: Unable to connect to SharePoint Online site \$SPOSite. State: Critical. Error: \$ErrMsg
<b>O365 Portal Login Performance Collection</b>	50	O365 Connection Success: Connection established	O365 Connection ERROR: \$connectMSOLError
<b>O365 Response Time Performance Collection Rule (outlook.office365.com)</b>	51	O365 Connection Success: Connection established to \$ComputerName	O365 Connection ERROR: Unable to establish connection to \$ComputerName
<b>O365 Consumed Units Collection</b>	55		Problem getting O365 SKU. \$Error