

Guide to Office 365 Management Pack for System Center Operations Manager

**Microsoft Corporation**

Published: September, 2018

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](http://systemcenterom.uservoice.com/forums/293064-general-operations-manager-feedback/filters/top).

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.

© 2018 Microsoft Corporation. All rights reserved.

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

All other trademarks are property of their respective owners.

Contents

[Guide to Office 365 Management Pack for System Center Operations Manager 4](#_Toc523242771)

[Changes history 4](#_Toc523242772)

[Supported configurations 6](#_Toc523242773)

[Resource pools configuration 6](#_Toc523242774)

[Files in this Management Pack 6](#_Toc523242775)

[Get started 8](#_Toc523242776)

[Import the Management Pack 8](#_Toc523242777)

[Create a new management pack for customizations 8](#_Toc523242778)

[Manage Office 365 subscriptions 9](#_Toc523242779)

[Monitoring configurations: 9](#_Toc523242780)

[Register the application in Azure Active Directory 14](#_Toc523242781)

[Configure the Management Pack for Office 365 20](#_Toc523242782)

[Configure proxy connection 20](#_Toc523242783)

[Configure Run As profiles 21](#_Toc523242784)

[Understand the Office 365 Management Pack 22](#_Toc523242785)

[Management Pack classes hierarchy 22](#_Toc523242786)

[Office 365 subscriptions 23](#_Toc523242787)

[Services and Features discovery 23](#_Toc523242788)

[Connection State monitor 23](#_Toc523242789)

[Office 365 Incidents and Messages 23](#_Toc523242790)

[Alert Autoclose rule 24](#_Toc523242791)

[Use Office 365 Monitoring Dashboard 26](#_Toc523242792)

[Subscription Health 26](#_Toc523242793)

[Service Status 27](#_Toc523242794)

[Alert widgets 28](#_Toc523242795)

[Active Incidents 28](#_Toc523242796)

[Resolved Incidents 29](#_Toc523242797)

[Message Center 30](#_Toc523242798)

[Active Alerts 30](#_Toc523242799)

[Appendix: Known issues and troubleshooting 31](#_Toc523242800)

[Appendix: Management Pack contents 34](#_Toc523242801)

Guide to Office 365 Management Pack for System Center Operations Manager

This guide is based on version 7.2.0.0 of the Management Pack for Office 365.

Changes history

| **Release Date** | **Changes** |
| --- | --- |
| September, 2018 | The guide was updated to reflect the changes introduced with version 7.2.0.0 of this Management Pack:   * Fixed display strings. * Fixed links to the Office 365 Portal. * Minor guide fixes. |
| July, 2018 | The guide was updated to reflect the changes introduced with version 7.1.5140.0 (CTP) of this Management Pack:   * ADAL library update from 2.19.0.0 to 3.19.8.16603. * Fixed communication with Azure and appropriate requests. * Added support of multiple security protocol types. * Fixed issue: incorrect requests with client ids from the different subscriptions. * Fixed message for Connection State monitor in the case of invalid credentials. * Fixed saving authentication type in Run As Account. * Fixed updating Run As Account. * Fixed issue: user cannot save Auto-Created SPN data. * Added Retry button in the case of failed SPN creation. * Fixed navigation in O365 wizard. * Fixed error handling in wizard. * Fixed fields validation in wizard (added check for whitespaces). * Fixed links to the portal in the Display Strings. |
| March, 2017 | The guide was updated to reflect the changes introduced with version 7.1.5138.0 of this Management Pack:   * Automatically created SPN is never expired. * Fixed issue: no alerts were generated for identical feature names related to different services. * Improved discovery logic according to the latest version of Office 365 (support for services with similar display names). * Updated “Office 365 Incidents and Messages” section. * Updated “Import the Management Pack” section. * Updated “Specify permissions your app requires to access Office 365 Management APIs” section. * Updated “Appendix: Known issues and troubleshooting” section. |
| September, 2016 | The guide was updated to reflect the changes introduced with version 7.1.5134.0 of this Management Pack:   * Upgraded subscriptions authorization method: the monitoring is carried out by an Azure application, not a specific user. Introduced two options to create an application, essential for the monitoring: manual and automatic: Microsoft Office 365 Global Administrator credentials are required for the automatic option of Azure application creation, while Azure subscription can be used for the second (manual) option. See [Manage Office 365 subscriptions](#Managing_Office_365_Subscriptions) section for more details. * Added Message Center messages categorization (see “[Office 365 incidents and messages](#Incidents)” section for details). * Added a new Message Center messages type: Planned Maintenance. * The Management Pack now inquires Office 365 Service Communications API V2; added a possibility to customize the endpoints and resource URIs in advanced subscription settings of the Office 365 wizard while calling the API. The above changes are provided for further support of Chinese subscriptions. * Added “[Configure proxy connection](#Proxy)” section to the guide; * Fixed bug: if there were several locales (Australian, Russian, etc.) present on the workstation, the monitoring was stopping. * Updated “Known Issues” section of the guide. |
| February, 2015 | The guide was updated to reflect the changes introduced with version 7.0.5115.0 of this Management Pack:   * Fixed a bug that caused display of null values in “Display Name” column of Subscription Health box on Office 365 Monitoring Dashboard. This happens only in SCOM environments upgraded from 2007 to 2012. |
| January, 2015 | The guide was updated to reflect the changes introduced with version 7.0.5112.0 of this Management Pack:   * Alerting rules now have overridable parameters, which enable the customization of synchronization logics. * Alert Autoclose rule now has overridable parameters, which enable the customization of alert automatic closure logics. * Minor bug fixes. |
| June, 2014 | Original release of this management pack. |

Supported configurations

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

* System Center Operations Manager 2012 SP1
* System Center Operations Manager 2012 R2
* System Center Operations Manager 2016
* System Center Operations Manager 1807

The Operations Manager console used to configure the Management Pack requires .Net Framework 4.5 or higher.

Management Server Pool used to run Office 365 monitoring workflows requires .Net Framework 4.5 or higher.

Running Office 365 monitoring workflows on Windows Server 2008 R2 OS requires .Net Framework 4.5 or higher.

***Note:*** Microsoft Office 365 .Net Framework Rule is disabled by default in this Management Pack. Nevertheless, it is enabled for Microsoft Office 365 Resource Pool Computer Group by means of an override.

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

Resource pools configuration

Office 365 Management Pack uses agentless monitoring approach. All monitoring workflows that communicate with Office 365 Monitoring API are being executed on Management Servers only.

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

Files in this Management Pack

This release includes the following files:

| File | Description |
| --- | --- |
| Microsoft.SystemCenter.O365.mpb | This management pack will discover components of Office 365 subscription, and will provide synchronization between Office 365 and SCOM alerts. |
| Office 365 MP Operations Guide.docx | This document provides guidance to configuration and usage of Office 365 Management Pack for System Center Operations Manager |

Get started

Office 365 Management Pack can be used to:

1. Add Office 365 subscriptions and configure custom endpoints for them to be monitored in the Operations Manager
2. Proactively monitor connection health for the subscriptions and endpoints accessibility
3. Automatically discover services and features available for each subscription
4. Reflect Office 365 Incidents, Message Center, and Planned Maintenance messages for the subscription to the Operations Manager alerts
5. Visualize the subscriptions’ health and corresponding alerts via the dashboard and alert view.

Import the Management Pack

For general information about importing a management pack, see [How to Import a Management Pack in Operations Manager 2012](http://technet.microsoft.com/en-us/library/hh212691.aspx).

***Note:*** Upgrade from previous versions of the Management Pack is not supported out-of-the-box. Upon upgrade of the Management Pack, it is necessary to perform the following actions: restart the Operations Console, open “Office 365” Wizard in the Administration section of the Operations Manager, and re-enter the corresponding credentials for your subscriptions. Otherwise, certain errors in the event log may occur; refer to [Appendix: Known issues and troubleshooting](#KI) section for more details.

Please also note that upgrade to the latest version of the management pack requires the console cache clearance. To clear the cache, perform the following actions:

* copy the SCOM console shortcut to the desktop
* open the shortcut properties and add “ /clearcache” key to the target field
* start the SCOM using this shortcut

Create a new management pack for customizations

Office 365 Management Pack is sealed; therefore, you cannot save any changes of the original settings in the management pack file itself. 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 the best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

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

* It simplifies the process of exporting customizations that have been already 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 of 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)

Creating a New Management Pack for Customizations

|  |
| --- |
| 1. Open the Operations Console, and then click Administration button.  2. Right-click Management Packs, and then click Create New Management Pack.  3. Enter a name (for example, Office 365 Customizations), and then click Next.  4. Click Create. |

Manage Office 365 subscriptions

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

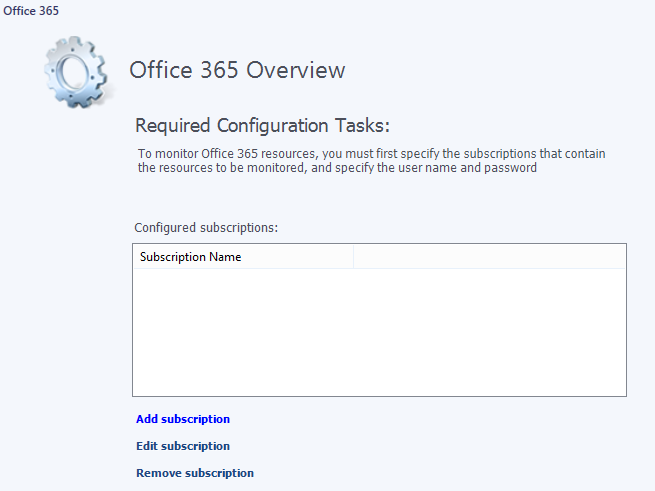
The first option (automatic) requires Global Administrator account of Microsoft Office 365 Subscription; therefore, one-time entering of the Global Administrator credentials is required, which provides access to Azure Active Directory for delegating the corresponding rights. Please note that the entered credentials 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 **Office 365** wizard.

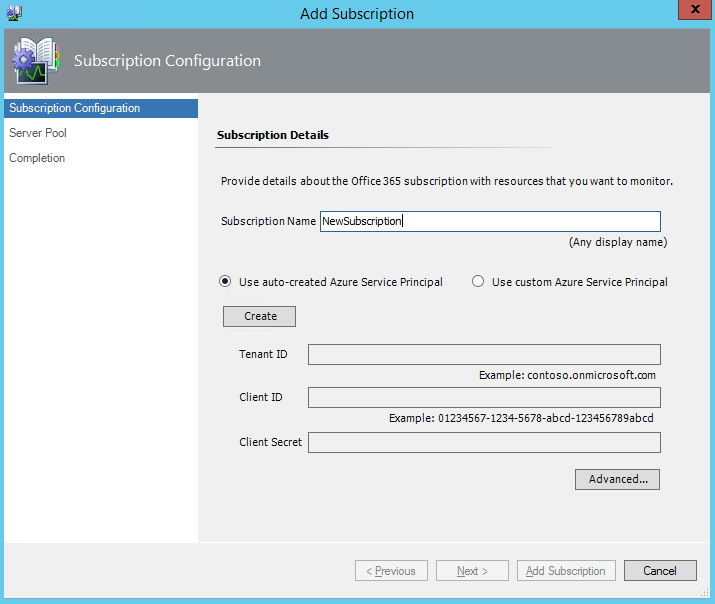


There are two options available for monitoring your subscriptions:

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

If you want to use auto-created Azure Service Principal to configure the monitoring, perform the following steps:

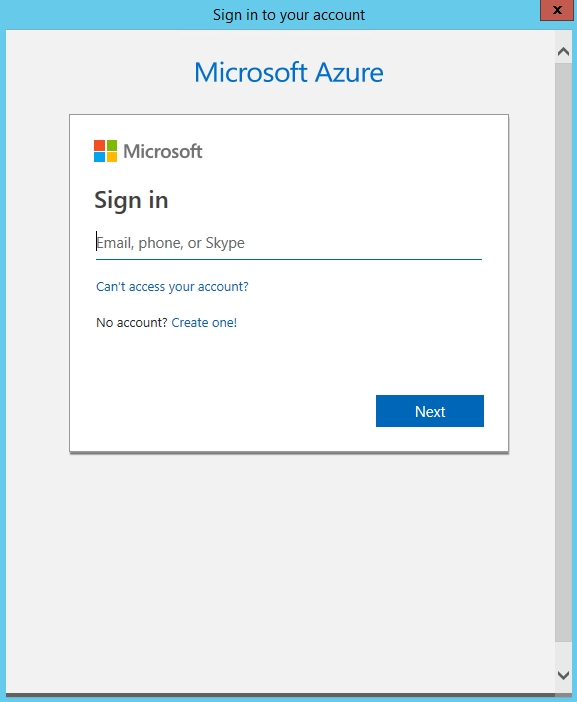
1. Click **Add subscription** to open “Add subscription” Wizard. Select “**Use auto-created Azure Service Principal**” option:



Enter a **Subscription Name** and click “**Create**”.

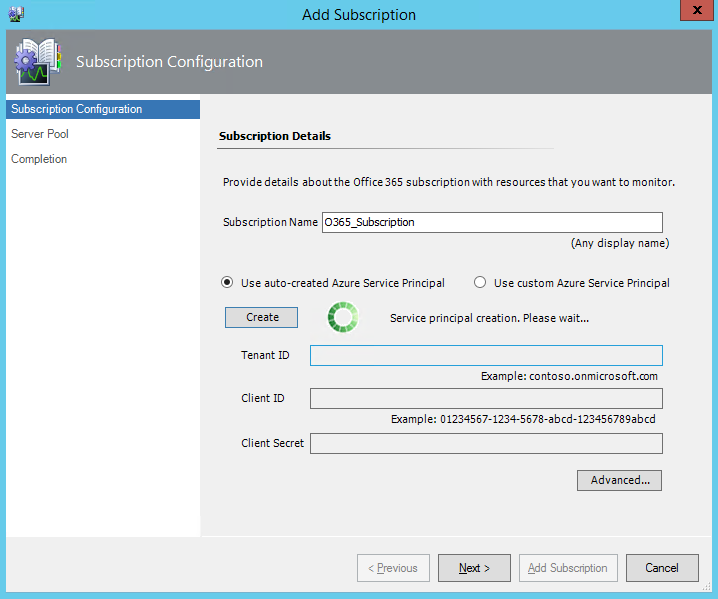
***Note:*** **Subscription Name** is a friendly name for the subscription; it will be used in the Operations Manager. Subscription Name should be descriptive and unique. Subscription Name cannot contain spaces.

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



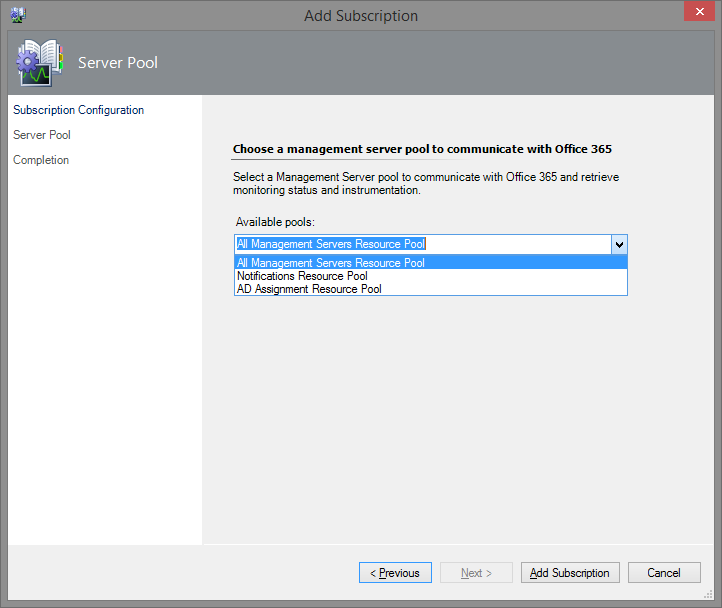
***Note:*** some browsers (e.g. Internet Explorer) may block the content coming from Office 365 Portal. In this case, add Office 365 Portal to the trusted sites zone.

1. Wait until Azure Service Principal will be created.



Upon successful creation of the application, the corresponding authentication data will be displayed in appropriated fields (Tenant ID, Client ID and Client Secret). It is strongly recommended to save this data for further usage! Click **Next**.

1. Choose a management server pool from the list of available pools. Click **Add Subscription**.

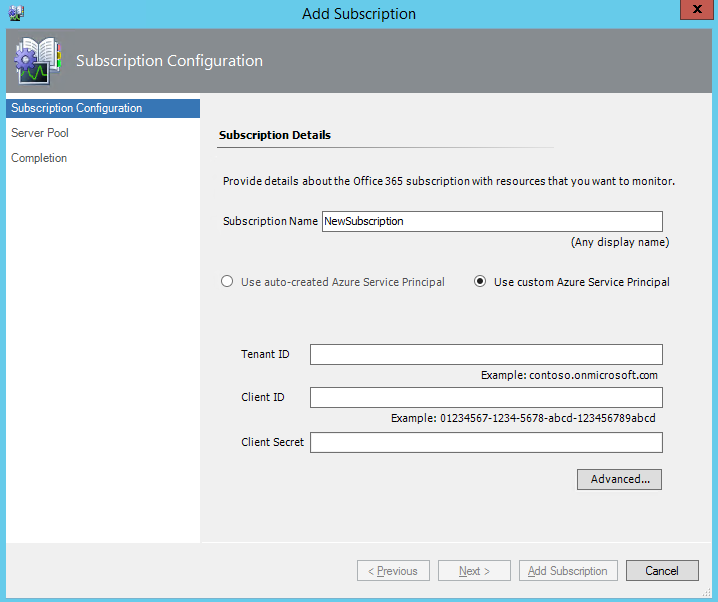


1. Click **Finish** to close the Wizard. The new subscription will be added to the Operations Manager, and will appear in Configured Subscriptions list.

#### **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:

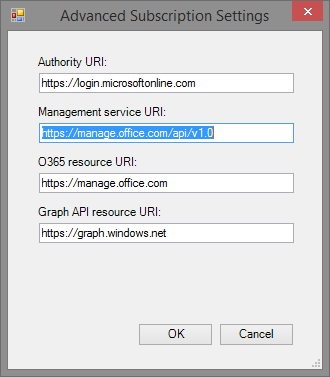
1. Click **Add subscription** to open “Add subscription” Wizard. Select “**Use custom Azure Service Principal**” option. Then enter a **Subscription Name, Tenant ID, Client ID and Client Secret** (see [Register the application in Azure AD](#AppReg) for more details). Click “Advanced…”.



***Note:***   
**Subscription Name** is a friendly name for the subscription; it will be used in the Operations Manager. Subscription Name should be descriptive and unique. Subscription Name cannot contain spaces.  
**Tenant ID (or Directory ID)** is a globally unique identifier that can be found in [Azure Management Portal](http://go.microsoft.com/fwlink/?LinkId=692045), when you browse to your Active Directory instance; for more details, see [Find your Office 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 [Generate a new key for your application](#Secret) section. Client Secret cannot contain spaces.

1. Verify the next URI endpoints for Authority, Management service, O365 and Graph API resource:



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

**Management service URI** is used to receive the data for the subscription monitoring upon successful authorization (default value: <https://manage.office.com/api/v1.0>).

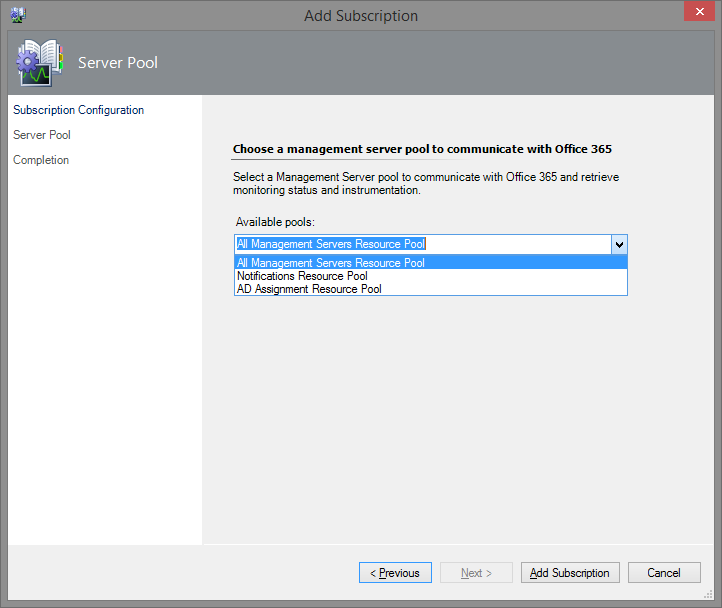
**O365 resource URI** is an identifier of the resource storing all Office 365 user data (default value: <https://manage.office.com>).

**Graph API** **resource URI** is an identifier of the REST API that provides programmatic access to directory objects in Azure Active Directory, such as users, groups, organizational contacts, and applications (default value: <https://graph.windows.net>).

**Please ensure that all this endpoints were added to whitelist!**

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 the endpoints are not specified clearly, the default values will be used.

1. Choose a **management server pool** from the list of available pools. Click **Add Subscription.**



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

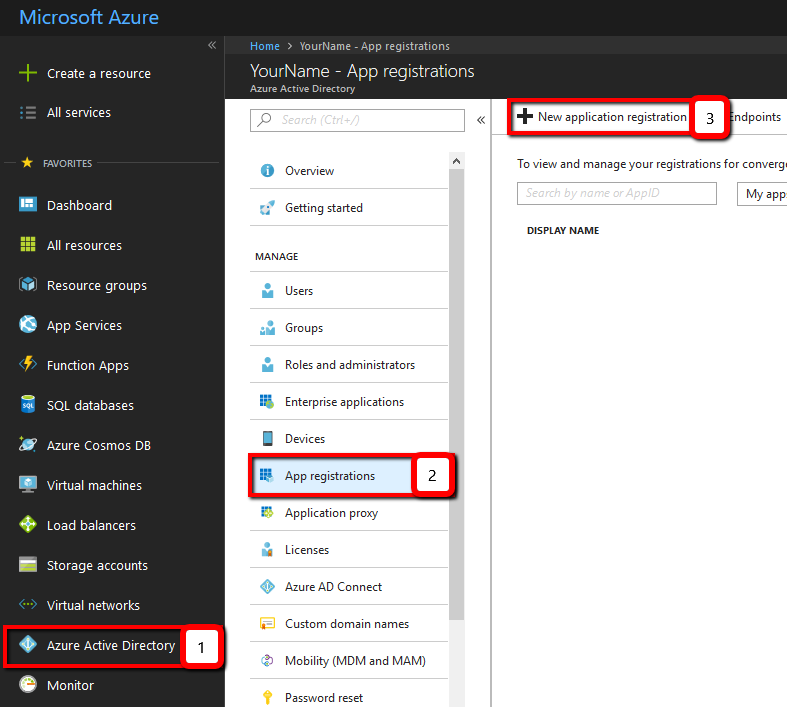
It is possible to modify credentials and resource pool for particular subscription. Select the subscription you want to edit, click **Edit subscription**, enter new credentials (or create the new ones) and select pool.

To remove a configured subscription: select it from the configured subscriptions list and click **Remove subscription**. All alerts related to the deleted subscription will be removed as well.

Register the application in Azure Active Directory

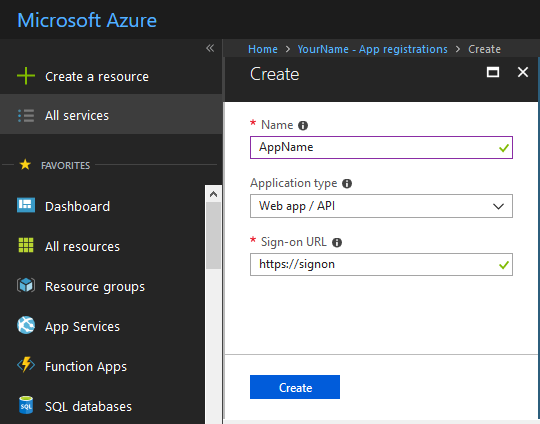
If you choose the second option requiring an Azure subscription, perform the following steps to register your application in Azure Active Directory:

1. Sign in to <https://portal.azure.com/>
2. In the left navigation panel, select «Azure Active Directory» (1). In the opened window click on «App registrations» (2) and click on «New application registration» (3).

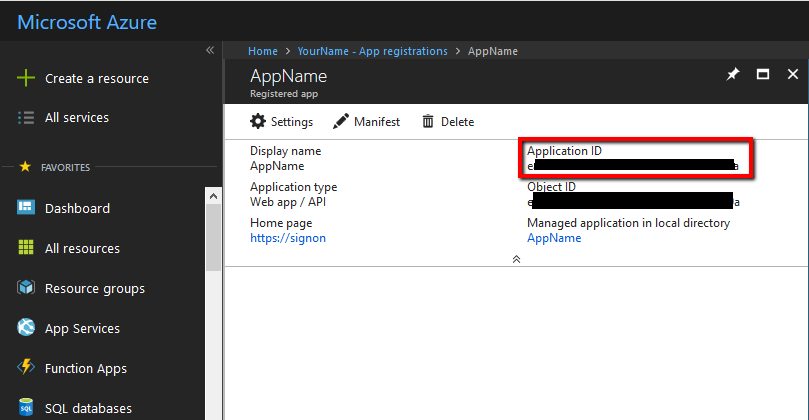


1. Create new application:

* Enter a friendly “**Name”** of your application
* Specify “**Application type”** as “Web app / API”
* Enter **“Sign-on URL”**: any valid URL starting with https://, e.g. **https://signon** (you can change this later as needed)
* Click **“Create”** button.



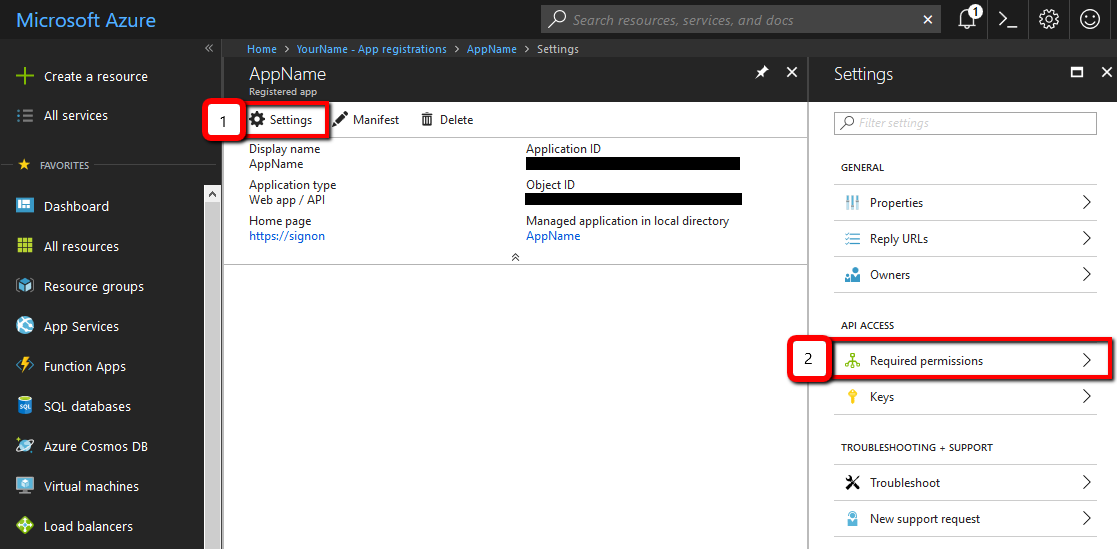
1. Your app is now registered with Azure AD, and has been assigned an Application ID. This value is used as “Client ID” in the Add Subscription window in SCOM, save it. However, there are several important aspects of your app left to configure.



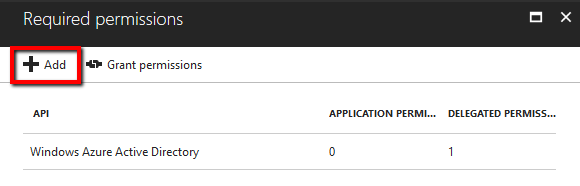
#### **Specify permissions your app requires to access Office 365 Management APIs**

Now, you need to specify exactly what permissions your app requires from Office 365 Management APIs. To do so, you add access to the Office 365 Management APIs to your app, and then you specify the permission(s) you need.

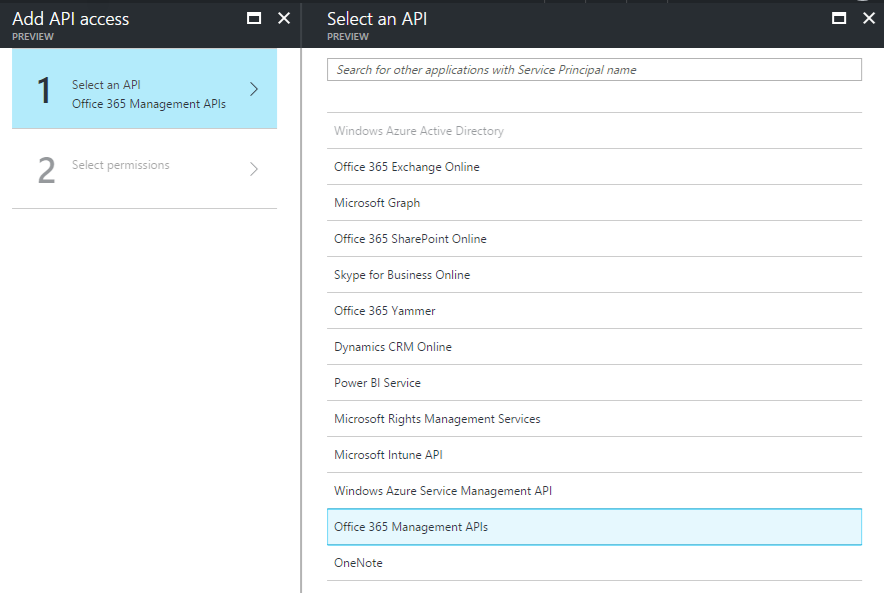
1. In your registered app window, click “Settings” button and click “Required permissions”.



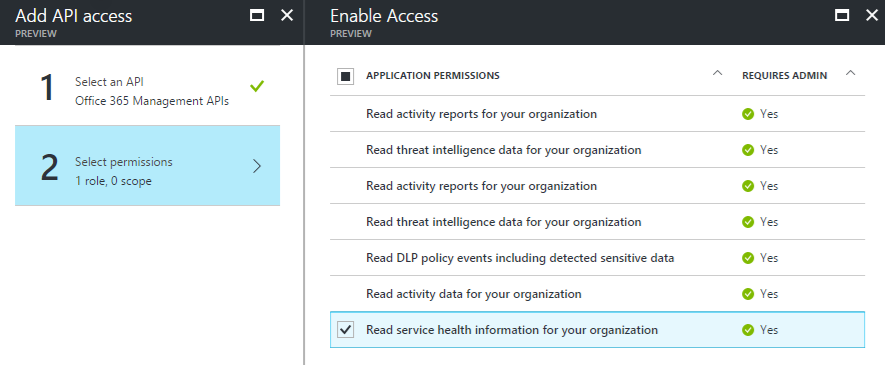
1. Click “Add” button in opened window.



1. Go to “Select an API” section (Settings > Required permissions > Add API access > Select an API).

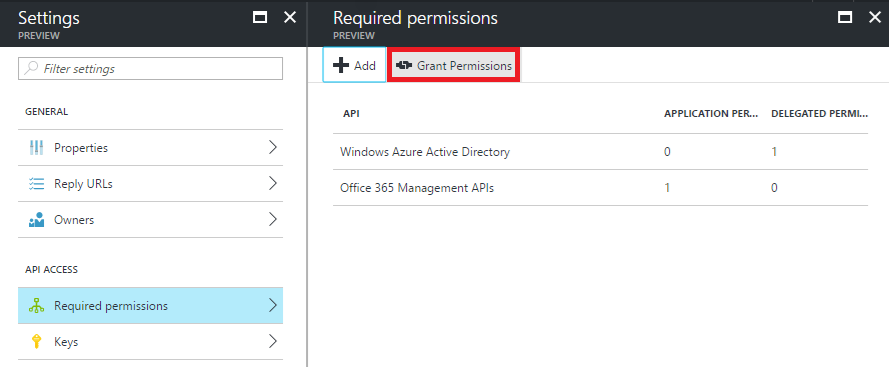


1. Check "Read service health information for your organization" item.



Then, click **Select** and **Done** buttons.

1. To finalize the settings, it is necessary to click **Grant Permissions** button:



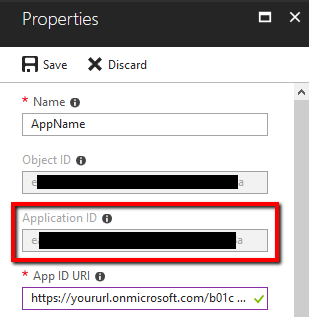
Note: if this button is disabled, your user account seems to be not of co-admin type.

#### **Configure your application properties in Azure Active Directory**

There are several important properties that determine, how your application functions within Azure AD, and how tenant admins will grant consent to allow your application to access their data by using the Office 365 Management APIs.

For more information about Azure AD application configuration in general, see [Application and service principal objects in Azure Active Directory](http://go.microsoft.com/fwlink/?LinkId=692046) article.

1. **CLIENT ID (or Application ID)**. This value is automatically generated by Azure Active Directory (Application ID). It represents a unique identifier for your application. You will need to use this, when your application accesses data from O365 API.



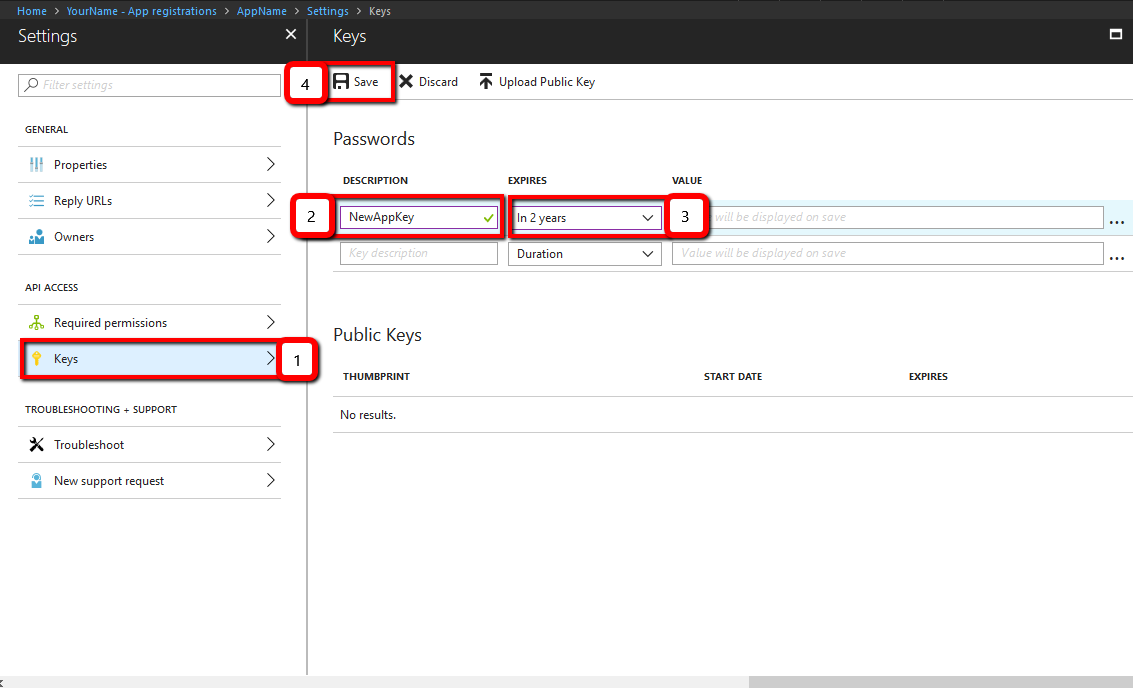
1. **CLIENT SECRET.** This is a key used, when exchanging an authorization code for an access token. **You have to generate a new key for your application**, see [Generate a new key for your application](#Secret) section.

Be sure to click **Save** after making any changes to these properties.

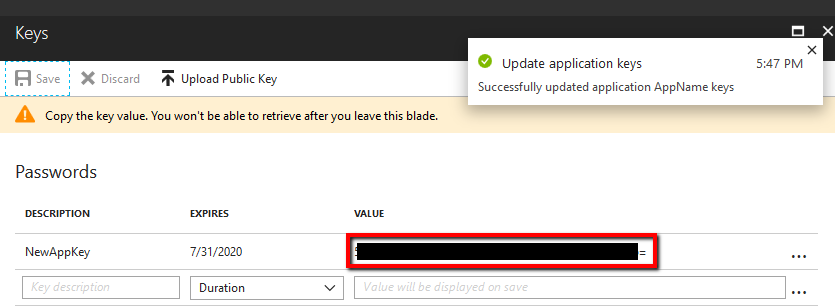
#### **Generate a new key for your application**

Keys, also known as **client secrets**, are used, when exchanging an authorization code for an access token.

1. In your Registered app window, click “Settings” button and click “Keys”(1).
2. Enter a friendly “**Description”** of your key (2), Select the duration for your key (3), and click “**Save” (4)**.



1. Azure displays the app secret only after saving it. Copy Value to the Clipboard. This is “Client Secret”, save it.



**Important!**

**Azure only displays the client secret at the time you initially generate it. You cannot navigate back to this page and retrieve the client secret later. If you did not save the client secret, you will have to regenerate it.**

Configure the Management Pack for Office 365

Configure proxy connection

To use a proxy server for the Office 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>

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 Azure Run As Profile Proxy.

To use a proxy server for the Office 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>

1. Restart the monitoring 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 Azure Run As Profile Proxy.

Configure Run As profiles

The Management Pack creates two Run As Profiles:

* Office 365 Subscription Password secure reference
* Office 365 Subscription Proxy secure reference

**Office 365 Subscription Password secure reference** Run As Profile is used to store Office 365 subscription credentials and should not be edited manually. See “[Manage Office 365 subscriptions](#Managing_Office_365_Subscriptions)” section for more details.

***Note:*** In dependence of the authentication method, there will be added postfix to the Run As Account Display Name and Description:  
 - For **Auto-created Azure Service Principal** postfix will be “\_AutoCreatedApp”  
 - For **Custom Azure Service Principal** postfix will be “\_CustomApp”



**Office 365 Subscription Proxy secure reference** Run As Profile 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 Office 365 portal endpoint. Please check firewall and proxy settings within your environment to ensure that aforementioned connection is allowed.

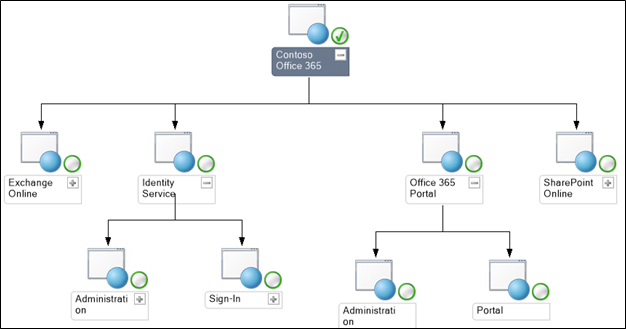
Understand the Office 365 Management Pack

Management Pack classes hierarchy

This Management Pack defines the following classes:

* Office 365 Subscription
* Office 365 Service
* Office 365 Feature

Each monitored Office 365 subscription hosts a set of services. Each service hosts a set of features.



Office 365 subscriptions

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

* Creates Run As Account that stores credentials for Azure application
* Adds a subscription object to the Operations Manager
* Creates a management pack with required internal overrides
* Specifies O365 and Azure URI endpoints as subscriptions' properties

For security reasons, the Wizard is the only way to configure the monitoring of Office 365 Subscriptions. See [Manage Office 365 subscriptions](#Managing_Office_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 and Features does not affect the health of the subscription object.

Office 365 monitoring is tenant-specific. Within the frames of a subscription, a certain set of services and corresponding features is provided. Therefore, adding a subscription to monitor, you add a specific tenant; multiple subscriptions of different tenants can be monitored simultaneously (tested up to 30 subscriptions)

Services and Features discovery

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

Connection State monitor

Office 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 Office 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.

Office 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 particular subscription service and feature. Each Incident provides a context, which contains a unique identifier, title, description, list of affected services, and features with their current operational states.

**Message Center messages** are not related to the operational state of services and features, but contain additional information about planned maintenance, updates, required actions, etc.

Office 365 Management Pack provides several alerting rules, targeted at the Subscription. These rules “replicate” Office 365 Incidents and Messages to the Operations Manager Alerts, which contain detailed information from related Office 365 events. Detailed information is stored in the alert’s context and custom fields. These fields are matching alerts to services and features to services.

**Note:** Do not change these fields in order to avoid incorrect alert display in the Dashboard.   
  
Rules update alert context and custom fields, if corresponding Office 365 Incident or Message has updated the information. Repeat count for the alert is increased in this case.

* **Office 365 Incidents alerting rule** generates and updates critical alerts for Incidents. Its behavior depends on the following overrideable parameters:
  + **Reopen closed alerts** – specifies, if the rule should create a new alert, when the new information arrives for the incident, which already has a corresponding alert with “Closed” status in the Operations Manager.
  + **Include resolved incidents** – specifies, if the rule should create a new alert for Office 365 incidents, which are marked as “Resolved”.
* **Office 365 Message Center planned maintenance rule** should raise Warning alerts instead of Informational.

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

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

Alert Autoclose rule

By default, “Alert Autoclose” rule runs once a day. This rule analyses the list of active alerts in the 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 Office 365 API any more), the rule automatically updates and closes corresponding alerts in the 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. 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 Office 365 API.

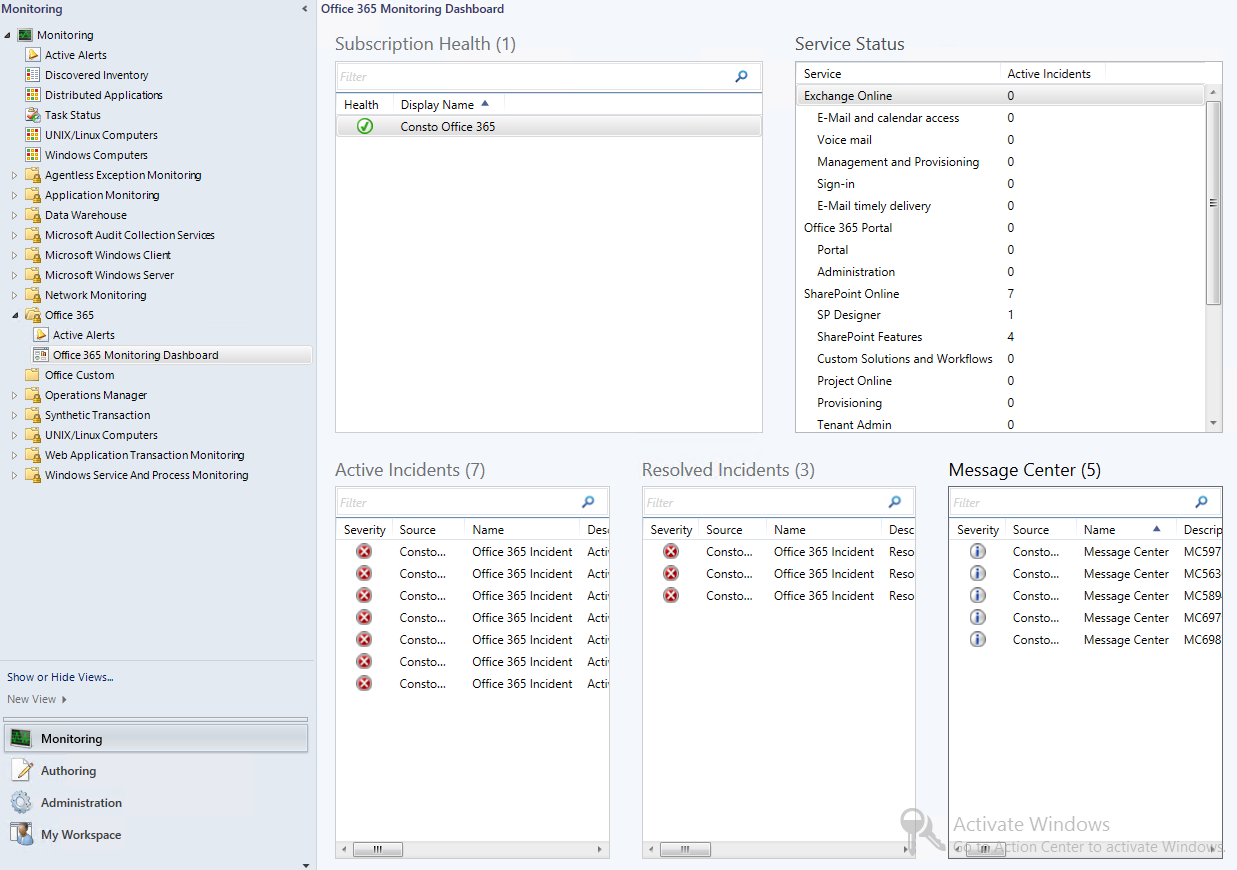
To enable this setting, the value of “Max Alert Age” parameter should be greater than zero. The threshold is measured in seconds. This parameter can be useful, if the user wants to receive timely notifications about new alert messages. To prevent confusion of new and old messages, the user can set autoclosing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

To avoid automated alerts resolution and closing, please disable this rule. In this case, alerts generated by alerting rules should be closed manually. “Alert Autoclose” rule does not affect alerts generated by “Office 365 Connection State” monitor.

Use Office 365 Monitoring Dashboard

The Monitoring Dashboard features are as follows:

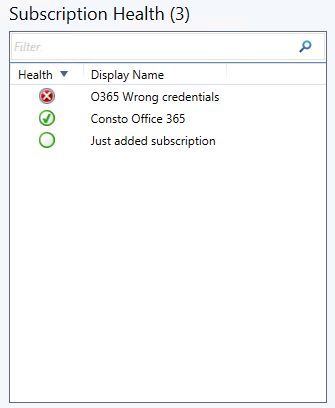
* Providing an overview of connection health for all configured subscriptions
* Displays the lists of active incidents, resolved incidents, Planned Maintenance messages, and informational messages for the selected subscription
* Displays a tree of Office 365 Services and Features available for the selected subscription, and the number of currently active incidents for each service or feature



Subscription Health

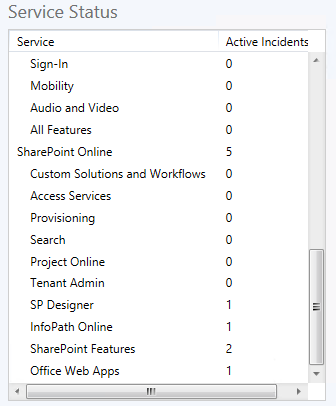
Subscription Health widget displays the list of Office 365 subscriptions configured with Add/Edit Subscription Wizard, as well as overall health state of each Subscription.

Subscription health state can be affected by Connection State monitor only. Healthy state means that subscription configuration is valid and connection to Office 365 Monitoring API is successful. Critical state means that Connection state monitor failed to connect the API using the provided credentails. 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.



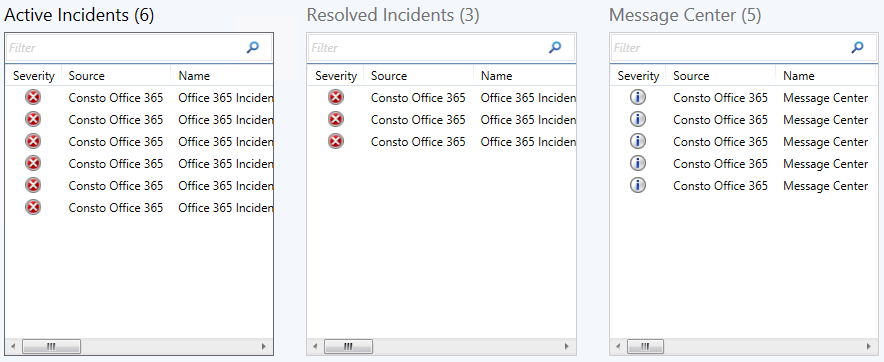
Service Status

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



Alert widgets

Three bottom controls (Active Incidents, Resolved Incidents, and Message 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.



Active Incidents

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

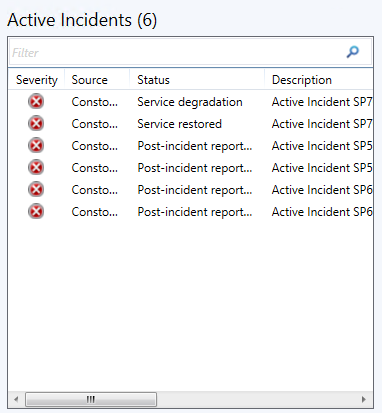
Each alert contains additional information in its context: the list of affected services, features and their current status. An incident (and the corresponding alert) is considered as active (and shown in Active Incidents list) if any of the affected services has one of the following states:

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

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

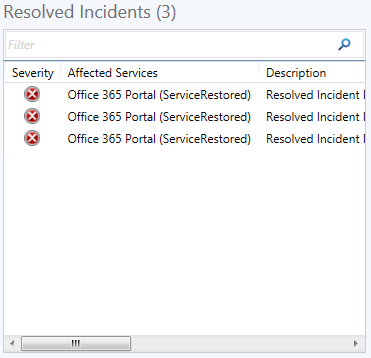
Note that each incident also contains “summary” status. In some cases, summary status can be updated to “Service Restored”, but internal status of the affected services is still non-operational. In such situation, the corresponding alert will be considered as active (in other words, service status has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

Alerts are being updated regularly by the corresponding rule. An alert can disappear from the list of Active Incidents and appear in Resolved Incidents list, when the status of the affected services changes.



Resolved Incidents

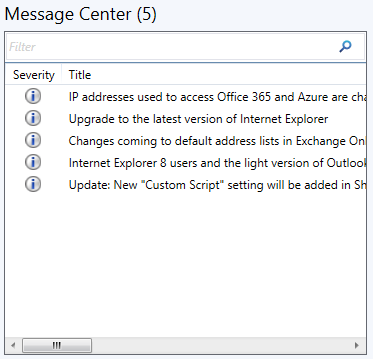
Resolved Incidents widget displays the list of the Operations Manager alerts generated for currently resolved Office 365 incidents for the selected subscription.



An incident (and the corresponding alert) is considered to be resolved (and shown in Resolved Incidents list) if there are no services having “active” incident states. Alerts are being updated regularly by the corresponding rule. An alert can disappear from the list of Active Incidents and appear in Resolved Incidents list, when the status of the affected services changes.

Message Center

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



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

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

Active Alerts

Active alerts view is located in Office 365 folder on the monitoring pane. It displays the cumulative list of all alerts targeted at all configured subscriptions (Active Incidents, Resolved Incidents, Message Center Messages, Connection State monitor alerts).

Appendix: Known issues and troubleshooting

#### **Management Pack upgrading issue**

**Issue:** after upgrading the Management Pack, the following errors may occur:   
  
*Property reference with id:"{66FF4067-B86D-37E2-7CD9-AE6B474AFD38}" in workflow "Microsoft.SystemCenter.O365.UnitMonitor.ConnectionState", running for instance "instance name" with id:"{C9CBAB71-51A8-9682-CAF6-974089E7425B}" cannot be resolved. Workflow will not be loaded. Management group "manage group name"*

*-----------------------------------------*

*Property reference with id:"{66FF4067-B86D-37E2-7CD9-AE6B474AFD38}" in workflow "Microsoft.SystemCenter.O365.Rules.PlannedMaintenanceAlertingRule", running for instance "instance name" with id:"{C9CBAB71-51A8-9682-CAF6-974089E7425B}" cannot be resolved. Workflow will not be loaded. Management group "manage group name"*

*-------------------------------------------*

*Property reference with id:"{66FF4067-B86D-37E2-7CD9-AE6B474AFD38}" in workflow "Microsoft.SystemCenter.O365.Rules.MessageCenterAlertingRule", running for instance "instance name" with id:"{C9CBAB71-51A8-9682-CAF6-974089E7425B}" cannot be resolved. Workflow will not be loaded. Management group "manage group name"*

*-----------------------------------------------*

*Property reference with id:"{66FF4067-B86D-37E2-7CD9-AE6B474AFD38}" in workflow "Microsoft.SystemCenter.O365.Rules.IncidentsAlertingRule", running for instance "instance name" with id:"{C9CBAB71-51A8-9682-CAF6-974089E7425B}" cannot be resolved. Workflow will not be loaded. Management group "manage group name"*

*--------------------------------*

*Property reference with id:"{66FF4067-B86D-37E2-7CD9-AE6B474AFD38}" in workflow "Microsoft.SystemCenter.O365.Rules.AlertAutoclose", running for instance "instance name" with id:"{C9CBAB71-51A8-9682-CAF6-974089E7425B}" cannot be resolved. Workflow will not be loaded. Management group "manage group name"*

*-------------------------------*

*Property reference with id:"{66FF4067-B86D-37E2-7CD9-AE6B474AFD38}" in workflow "Microsoft.SystemCenter.O365.Discovery.Service", running for instance "instance name" with id:"{C9CBAB71-51A8-9682-CAF6-974089E7425B}" cannot be resolved. Workflow will not be loaded. Management group "manage group name"*

**Resolution:** restart the Operations Console, open “Office 365” Wizard from Administration section, and edit credentials for your subscriptions correspondingly.

#### **Old URI values issue**

**Issue:** if subscription URI values were changed by the user, the subscription properties may still contain old URI values.

**Resolution:** restart the Operations Console to resolve the issue.

#### **Data displayed on Office 365 Portal may differ from data displayed in SCOM UI**

**Issue:** the data displayed in SCOM Operations Console is returned from Office 365 Portal by means of the Office 365 Management APIs. Therefore, sometimes it can differ from the data currently displayed on the Portal.

**Resolution:** no resolution available.

#### **User may receive errors in the log after changing subscription**

**Issue:** after changing subscription, the user may receive the following error in log:  
“*An Account specified in the Run As Profile "Microsoft.SystemCenter.O365.RunAsProfile.Password" cannot be resolved*”. The issue consists in a time lag between Run As account and corresponding Secure Reference Override changes.

**Resolution:** no resolution available.

#### **If the Firewall is enabled, some authorization issues may occur**

**Issue:** The Firewall may block some of the authorization requests, and Office 365 administrative wizard may not work.

**Resolution:** disable the Firewall or contact your network administrator and provide the corresponding [URIs](#URI) to resolve the issue.

#### **If several subscriptions added within a short period of time, monitoring can be stopped**

**Issue:** The monitoring can be stopped in case if a number of subscriptions added within a short period. The probability of occurrence depends on performance of the system and on the count of previously added subscriptions.

**Resolution:** Restart all SCOM services.

#### **The Dashboard displays incorrect data or no data at all**

**SCOM issue:** In some cases, the Dashboard may display incorrect data or no data at all.

**Resolution:** Clear the console cache. To clear the cache, perform the following actions:

• copy the SCOM console shortcut to the desktop

• open the shortcut properties and add “ /clearcache” key to the target field

• start the SCOM using this shortcut.

#### **Upon upgrade or reinstallation of the management pack, the number of active incidents may be excessive**

**SCOM console issue:** Upon upgrade or reinstallation of the management pack, the number of the displayed active incidents may be excessive, even if the console cache has been cleared before.

**Resolution:** Clear the console cache.

#### **Opened Fiddler can prevent Azure Service Principal creation**

**Issue:** In some cases, if “Fiddler" capture traffic, this makes it impossible to create a subscription.

**Resolution:** Close Fiddler application, and try adding a subscription again.

#### **Subscriptions Health State can became Critical after upgrading**

**Issue:** After upgrading the previous O365 Management Pack version subscriptions health state can became Critical.

**Resolution:** Close Operations manager Console and restart Microsoft Monitoring Agent Service on the machine with Management Server.

Appendix: Management Pack contents

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

**Rules (alerting)**

**Microsoft Office 365 .Net Framework Rule**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 2 | | Severity | Defines Alert Severity. | 2 | |  |
|  |  |  |

**Office 365 Feature Class - Discoveries**

**Office 365 Services and Features Discovery**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 14400 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | |  |
|  |  |  |

**Office 365 Subscription Class - Unit monitors**

**Office 365 Connection State monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | |  |
|  |  |  |

**Office 365 Subscription Class - Rules (alerting)**

**Office 365 Alert Autoclose rule**

The rule is used to process the list of all Events for the Subscription via Office 365 API and to close obsolete Alerts in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Max Alert Age (seconds) | Specifies the time the alert is active before being closed. | 0 | | Priority | Defines Alert Priority. | 0 | | Severity | Defines Alert Severity. | 0 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Office 365 Message Center Warning alerting rule**

When this rule receives a Message Center message of "Plan for change" category, it generates or updates a corresponding Warning Alert in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Office 365 Incidents alerting rule**

The rule is used to process the list of Active and Resolved Incidents for the Subscription via Office 365 API, and to generate or update corresponding Alerts in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Include resolved incidents | Creates an alert for a resolved incident if no active alert exists for the incident in SCOM. | true | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 1 | | Reopen Closed Alerts | Creates a new alert if a new information for a closed alert is received. | false | | Severity | Defines Alert Severity. | 2 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Office 365 Planned Maintenance Message alerting rule**

The rule is used to process the list of Planned Maintenance Messages for the Subscription via Office 365 API, and to generate or update corresponding warning Alerts in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Office 365 Message Center Critical alerting rule**

When this rule receives a Message Center message of "Prevent or fix issues" category, it generates or updates a corresponding Critical Alert in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 2 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Office 365 Message Center Informational alerting rule**

When this rule receives a Message Center message of "Stay informed" category, it generates or updates a corresponding Informational Alert in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates and Alert. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 0 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. | - | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |