

Azure Maintenance Mode Scheduler

Installation Guide

Server Requirements:

- The Azure Maintenance Mode Scheduler must be installed on a **Windows Server 2016, 2019, or 2022 server**. This can be **on-prem** or in **Azure**.

Accounts Required:

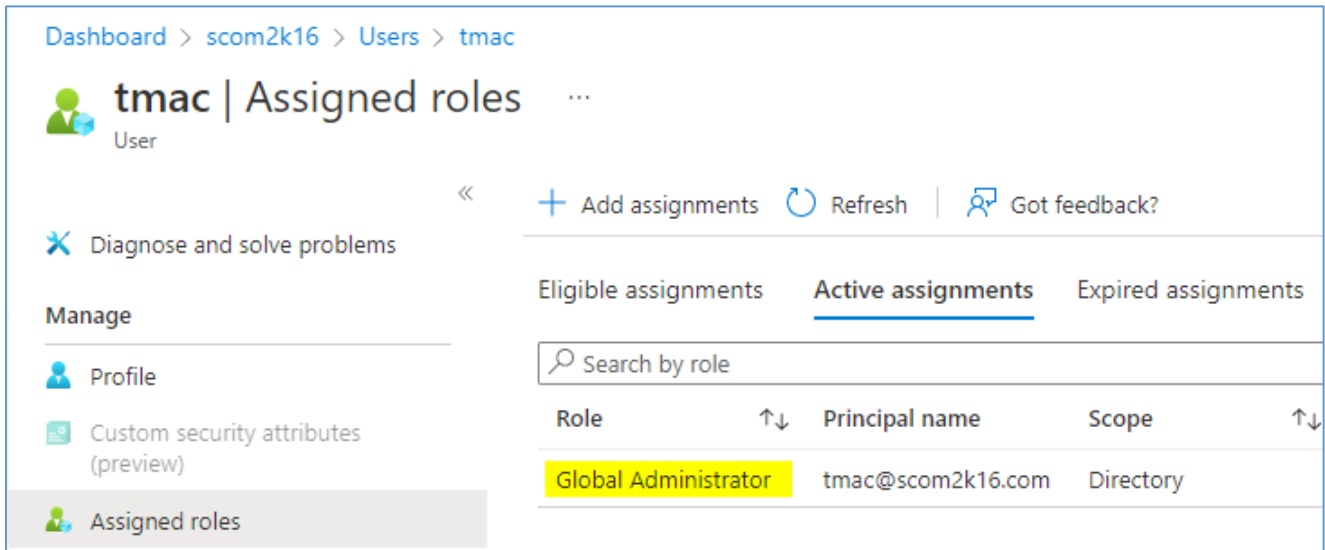
- **Application ID** (Client ID) created in Azure Active Directory with Client Secret. (Instructions below on how to create this account)
- **Local User Account or Domain User Account** with local admin rights to the Window Server.

Create the Application ID in Azure AD with PowerShell or Manually

- **Option 1: PowerShell (Recommended)**

1. Make sure you have an account with **Azure AD Global Admin Rights** and has **Owner or User Access Admin rights** to either your **Azure Management Group** or **one Azure Subscription**.

Azure Active Directory



The screenshot shows the Azure Active Directory portal interface. The breadcrumb navigation at the top reads: Dashboard > scom2k16 > Users > tmac. The main heading is 'tmac | Assigned roles' with a user icon and the label 'User'. Below this, there are links for 'Diagnose and solve problems', 'Manage', 'Profile', 'Custom security attributes (preview)', and 'Assigned roles' (which is highlighted). To the right, there are buttons for 'Add assignments', 'Refresh', and 'Got feedback?'. Below these buttons, there are tabs for 'Eligible assignments', 'Active assignments' (which is selected), and 'Expired assignments'. A search bar labeled 'Search by role' is present. A table with the following data is displayed:

| Role | Principal name | Scope |
|----------------------|-------------------|-----------|
| Global Administrator | tmac@scom2k16.com | Directory |

All services > Management groups > Tenant Root Group

Tenant Root Group | Access control (IAM) ...


Management group

Search (Ctrl+/) << + Add ↓ Download role assignments ≡ Edit columns ↻ Refr

Overview
Subscriptions
Activity Log
Access control (IAM)
Governance
Get started

Check access Role assignments Roles Deny assignments

2 items (2 Users)

| <input type="checkbox"/> | Name | Type | Role |
|--------------------------|---|------|-----------------------------|
| <input type="checkbox"/> | User Access Administrator | | |
| <input type="checkbox"/> |  tmac tmac@scom2k16.com | User | User Access Administrator ⓘ |

2. In the AzureMaintenanceModeScheduler.zip file there are two PowerShell scripts. You only need to run one of them.

AzMMforManagementGroup.ps1

AzMMforSubscription.ps1

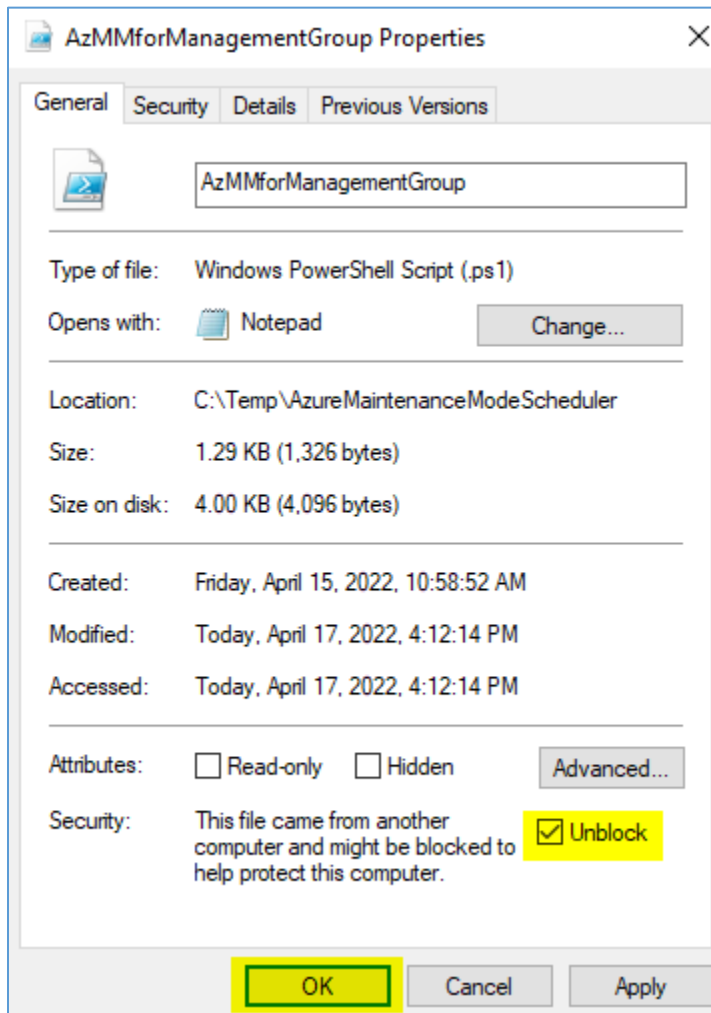
Run **AzMMforManagementGroup.ps1** if you have **alert rules** in **multiple subscriptions** and have an Azure Management Group that contains all the subscriptions.

Run **AzMMforSubscription.ps1** if you have all your **alert rules** in **one subscription** or if you only have access to one Subscription.

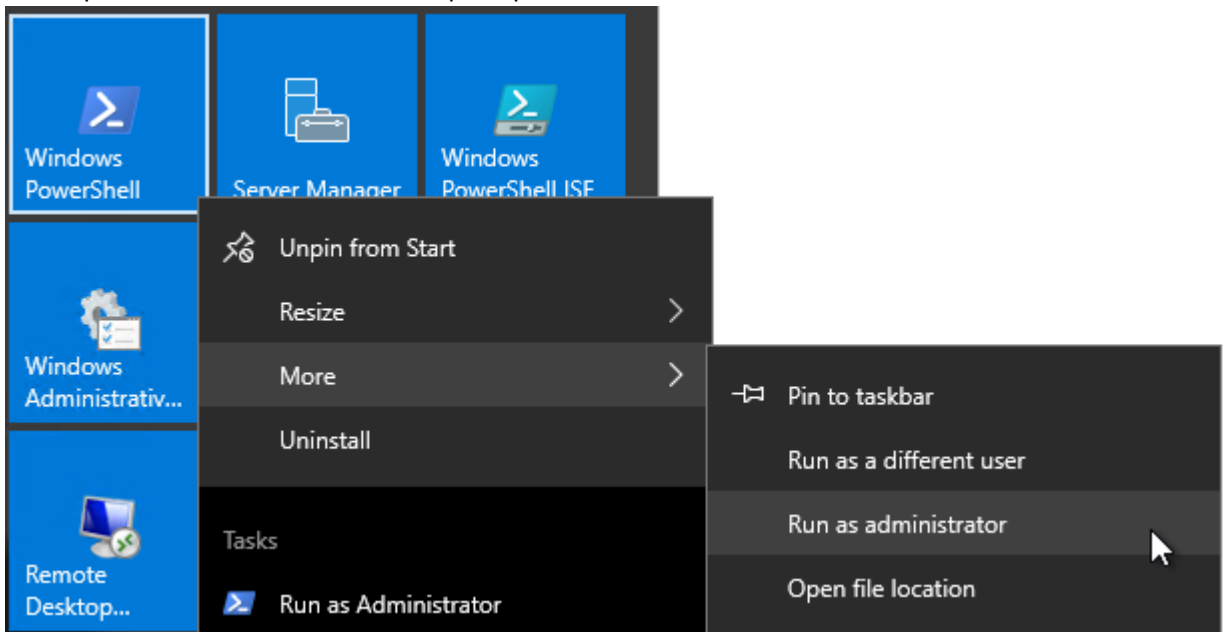
PowerShell Script Overview:

The script connects to azure. It creates an App Registration (AD Service Principal). It then creates an Azure Role Definition and sets minimal permissions. Then it assigns the App Registration to the role definition.

3. To Run the PowerShell Script, unblock the script by right clicking on the script and check Unblock.



4. Next open the PowerShell command prompt as administrator.



5. Type in: `Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser`

```
Administrator: Windows PowerShell
PS C:\> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

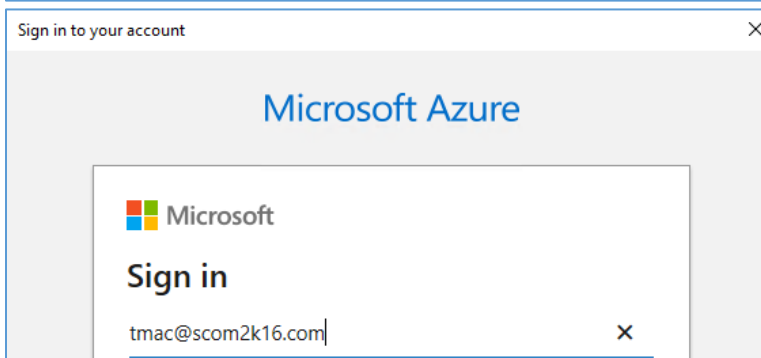
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the exe
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\>
```

6. `cd` (change directory) to the extracted zip files.
7. Run **one** of the PowerShell scripts (**Not Both**).

For Management Group: Type in: `.\AzMMforManagementGroup.ps1`

For Subscription: Type in: `.\AzMMforSubscription.ps1`

```
PS C:\Users\siteadmin> cd\
PS C:\> cd .\Temp\
PS C:\Temp> cd '.\Azure Maintenance Mode Scheduler\'
PS C:\Temp\Azure Maintenance Mode Scheduler> .\AzMMforManagementGroup.ps1
```



8. A window will pop up. Log on with your Azure Account with the rights described in step 1.

```
Please save the following information for the install
-----
Directory (tenant) ID: 016073f7-695b-4902-80a5-0846301c94db
Application (client) ID: 16727185-8259-4492-9925-ab3111342f69
Client Secret: ytF8Q~AHPZmRaPCFNFIiDEzZ6uQV_N1kBC4Uucrw
-----
```

Do not close the PowerShell window. Copy the Directory ID, Application ID, and Client Secret to a safe place. You will need to supply this information during the Installation of the Azure Maintenance Mode Scheduler.

If you get an error during this process. Please contact support@scm2k7.com and we will be happy to help you resolve any issues

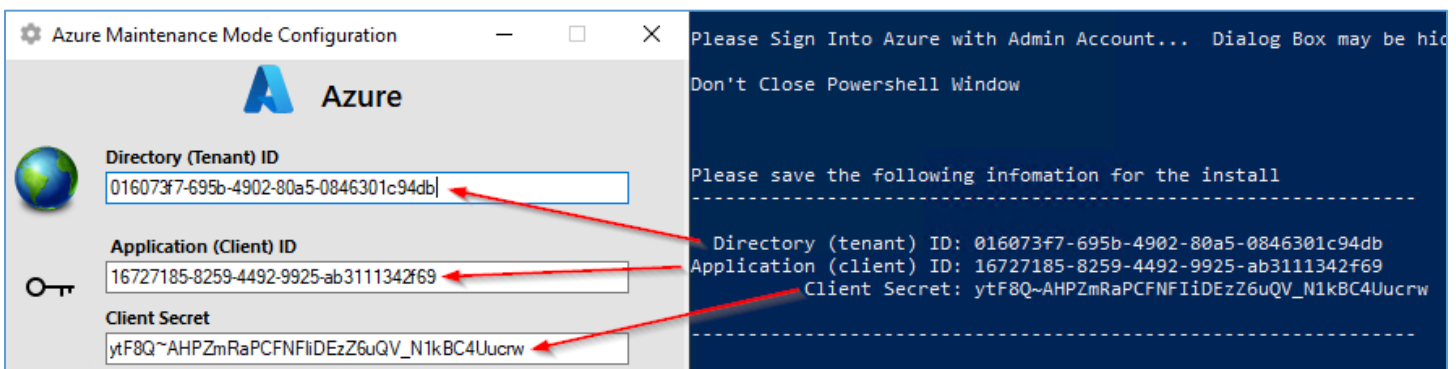
- a. Option 2: **Manually** (See [Appendix 1](#) Below)

- 2.) Next Double click on **Azure Maintenance Mode Scheduler.msi** file from the zip.
- 3.) Click **Next**
- 4.) **Read** and **Accept** the License Agreement, then click **Next**
- 5.) **Select** the location you want to install the application.
- 6.) On the **Ready to Install** screen click **Install**
- 7.) Click **Yes** on the next screen.
- 8.) Setup will take some time as it needs to install IIS.
- 9.) On the **Completing Setup Page** leave the Launch Azure Maintenance Mode Scheduler **checkbox checked** and **Click Finish**
- 10.) If you unchecked the Launch box on the last screen, you can also run it from the **Desktop** with the gear Icon

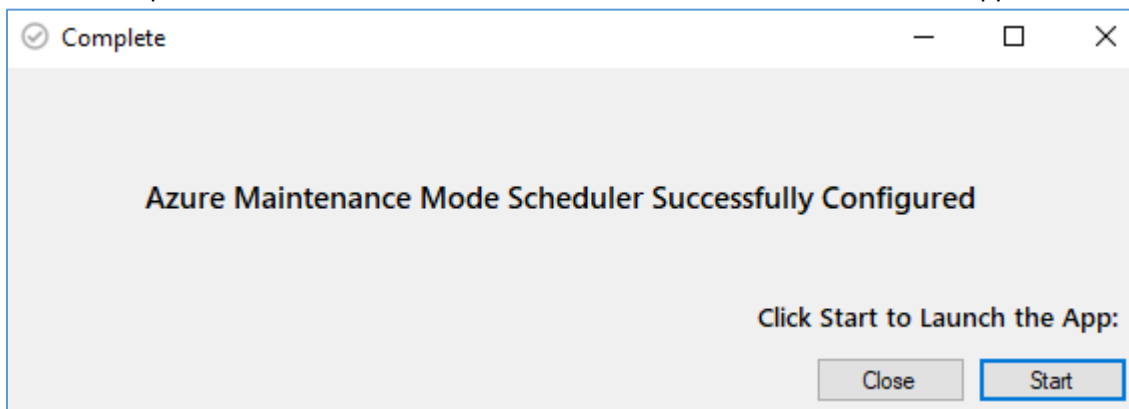


called **Azure Maintenance Mode Configuration**.

- 11.) **Copy and paste** the information generated from the PowerShell script into the dialog box **if it isn't automatically populated**.



- 12.) Type in the name and password of a **Local User Account** or **Domain User Account** with local admin rights to **the Window Server** you are installing on.
- 13.) Choose the **Date Format** you would like to use.
- 14.) Click **OK**
- 15.) On the complete screen click **Start** to Launch the Maintenance Mode Scheduler Application

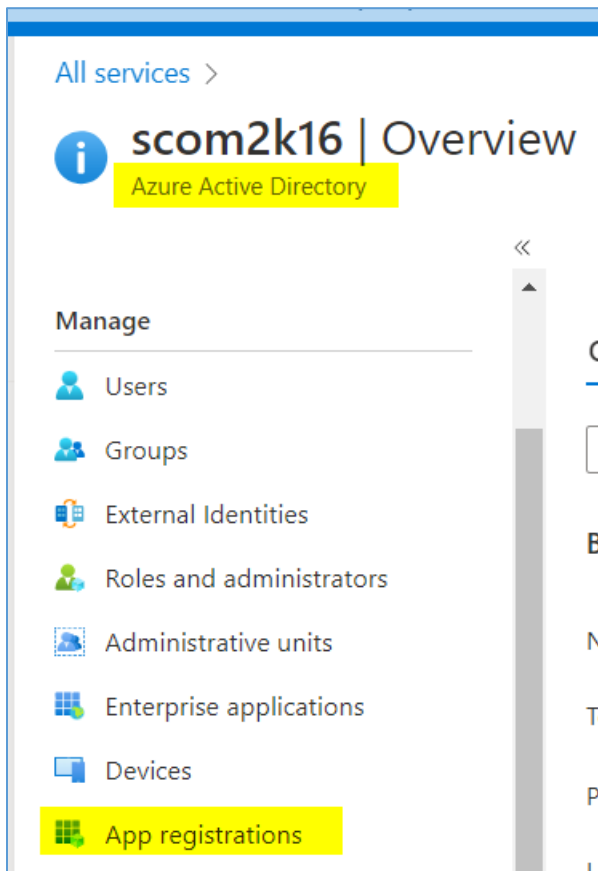


Appendix:

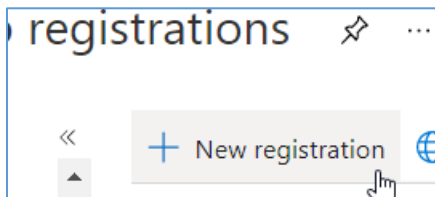
Option 2 - Manually creating an Application ID and assigning permissions:

In your Azure Subscription. Go to **Azure Active Directory**.

Under Manage click **App registrations**.



Click **New Registration**.



Under Name Type: **Azure Maintenance Mode Scheduler**

All services > scom2k16 >

Register an application ...

* Name

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

Azure Maintenance Mode Scheduler ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (scom2k16 only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼

e.g. https://example.com/auth


Leave all the rest the defaults.

Register


Then **Click Register**


On the next page. Under Essentials


Copy the Application (client) ID and the Directory (tenant) ID for use later in a text file.

 **Azure Maintenance Mode Scheduler** ✨ ...


<< 🗑️ Delete 🌐 Endpoints 🔍 Preview features


 Overview


 Quickstart


 Integration assistant


Manage

 Branding & properties

 Authentication

 Certificates & secrets

 Token configuration

 Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name
[Azure Maintenance Mode Scheduler](#)

Application (client) ID
f4e1c243-4cee-4312-b3b8-1ffe3cb219d2

Object ID
5f8aaf99-cc0d-4760-9df0-b01e4cef3087

Directory (tenant) ID
016073f7-695b-4902-80a5-0846301c94db

Client credentials
[0 certificate, 1 secret](#)

Redirect URIs
[Add a Redirect URI](#)

Application ID URI
[Add an Application ID URI](#)

Managed application in local directory
[Azure Maintenance Mode Scheduler](#)

Now under **Manage** Click **Certificates & secrets**

All services > scom2k16 >

Azure Maintenance Mode Scheduler

Search (Ctrl+/) << Delete Endpoints Preview feedback

- Overview
- Quickstart
- Integration assistant
- Manage**
- Branding & properties
- Authentication
- Certificates & secrets**

Got a second? We would love your feedback

Essentials

Display name
[Azure Maintenance Mode Scheduler](#)

Application (client) ID
f4e1c243-4cee-4312-b3b8-1ffe3cb219d2

Object ID
5f8aaf99-cc0d-4760-9df0-b01e4cef3087

Under Client secrets. Click **New client secret**.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token.

+ New client secret

| Description | Expires | Value ⓘ |
|-------------|---------|---------|
|-------------|---------|---------|

Type in **Azure Maintenance Mode**.

Select **Expires 12 months**

Add a client secret



DescriptionAzure Maintenance Mode

Expires12 months

Click **Add** at the bottom.

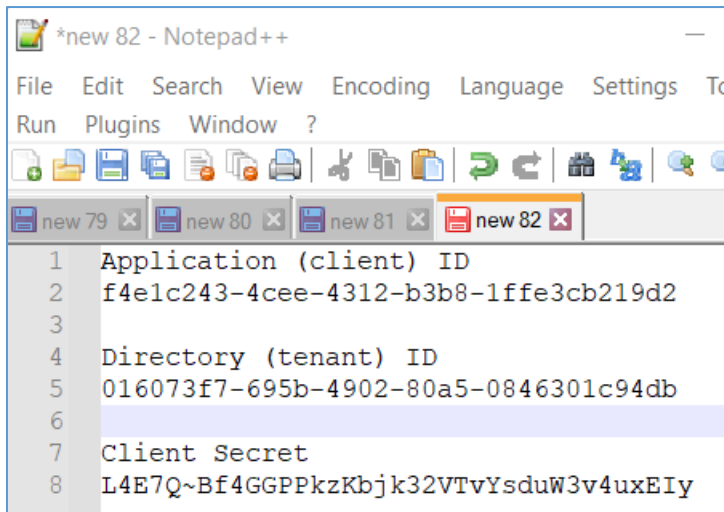
Add

Now on the next page. Don't leave this page until you copy the Value. If you leave you will have to create a new secret.

| Description | Expires | Value ⓘ | Secret ID |
|------------------------|-----------|-------------------------------|---|
| Azure Maintenance Mode | 3/10/2023 | L4E7Q~Bf4GGPPkzKbjk32VTvYs... | 8a4fea5b-8a28-4abe-af76-8975...   |

Click the **copy** button and **save** the secret for later in your text file.

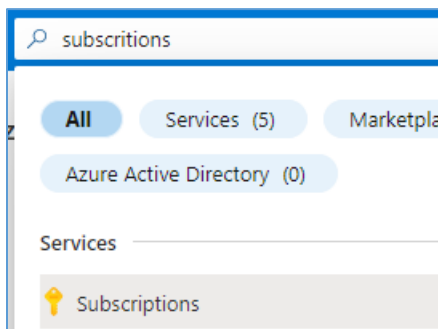
Now in my text file I have my **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** all saved for later.



```
*new 82 - Notepad++
File Edit Search View Encoding Language Settings To
Run Plugins Window ?
new 79 x new 80 x new 81 x new 82 x
1 Application (client) ID
2 f4e1c243-4cee-4312-b3b8-1ffe3cb219d2
3
4 Directory (tenant) ID
5 016073f7-695b-4902-80a5-0846301c94db
6
7 Client Secret
8 L4E7Q~Bf4GGPPkzKbjk32VTvYsduW3v4uxEIy
```

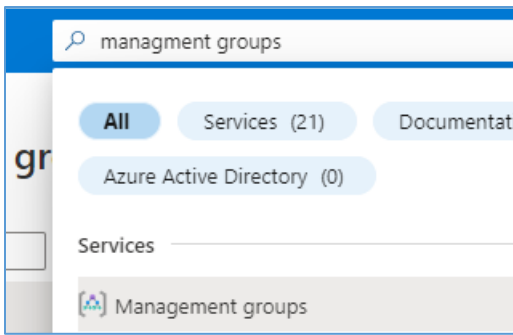
Now that we have an Application Account we now need to Assign it permissions to schedule the Alert Rules in Azure.

If you have one subscription in your tenant you can go to Subscriptions.

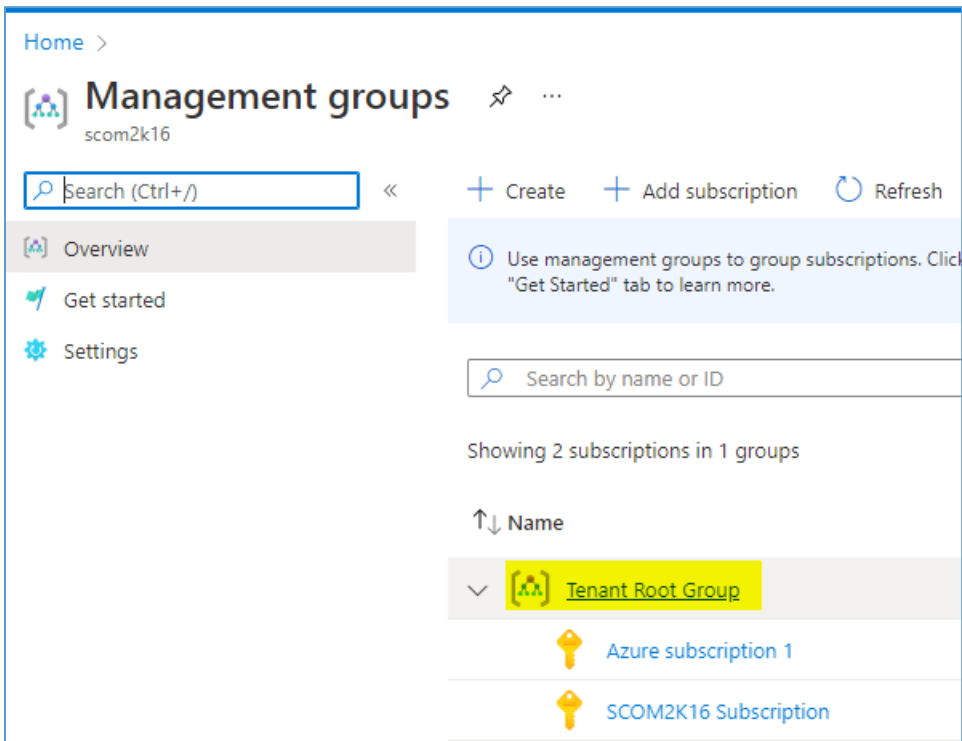


Most customers will have multiple subscriptions.

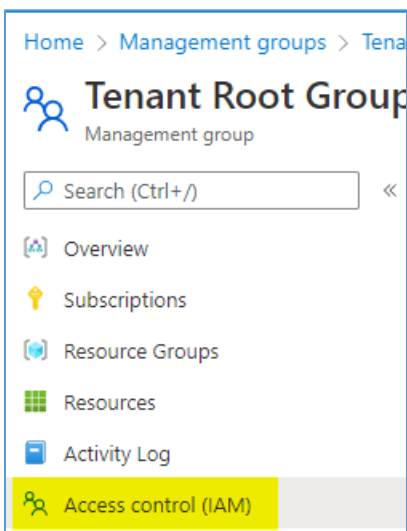
In that case go to Management Groups.



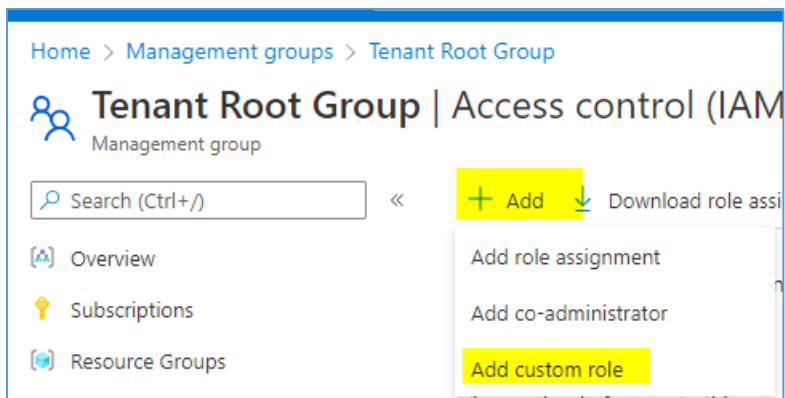
Click on the highest management group you want to schedule alerts for.



Now click **Access Control (IAM)**



Now click **Add**, Then Add custom role.



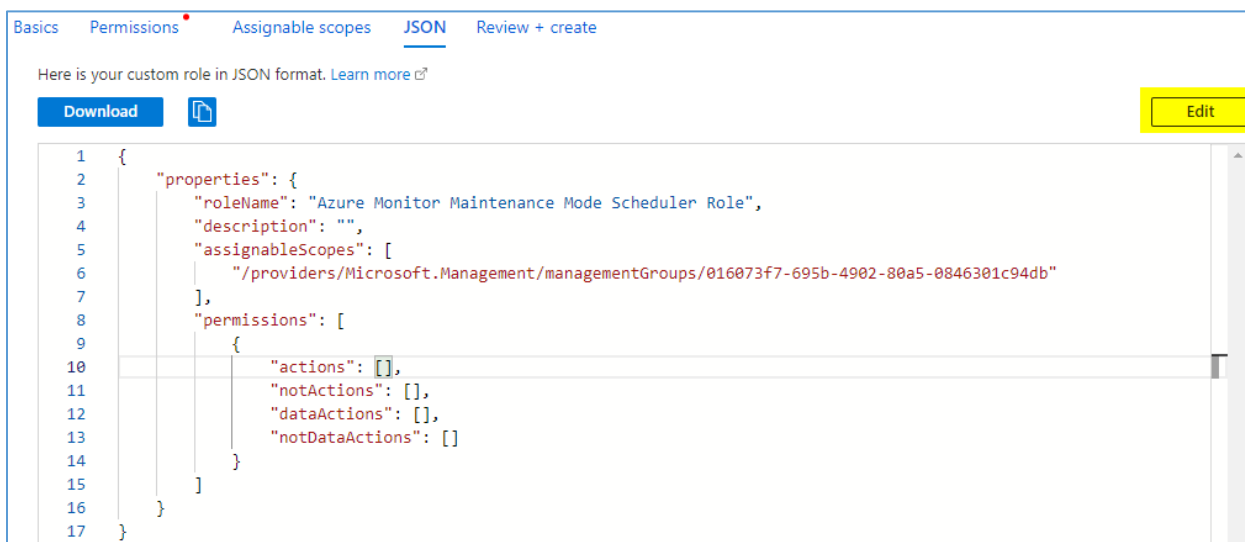
For Custom role name type : **Azure Monitor Maintenance Mode Scheduler**

The screenshot shows the 'Basics' tab of the 'Create custom role' wizard. The tabs at the top are 'Basics', 'Permissions', 'Assignable scopes', 'JSON', and 'Review + create'. The 'Basics' tab is active. Below the tabs, there is a text input field for 'Custom role name' containing 'Azure Monitor Maintenance Mode Scheduler Role' with a checkmark icon to its right. Below this is a larger text area for 'Description'. At the bottom, there are three radio buttons for 'Baseline permissions': 'Clone a role', 'Start from scratch' (which is selected), and 'Start from JSON'.

Now click JSON



Click Edit



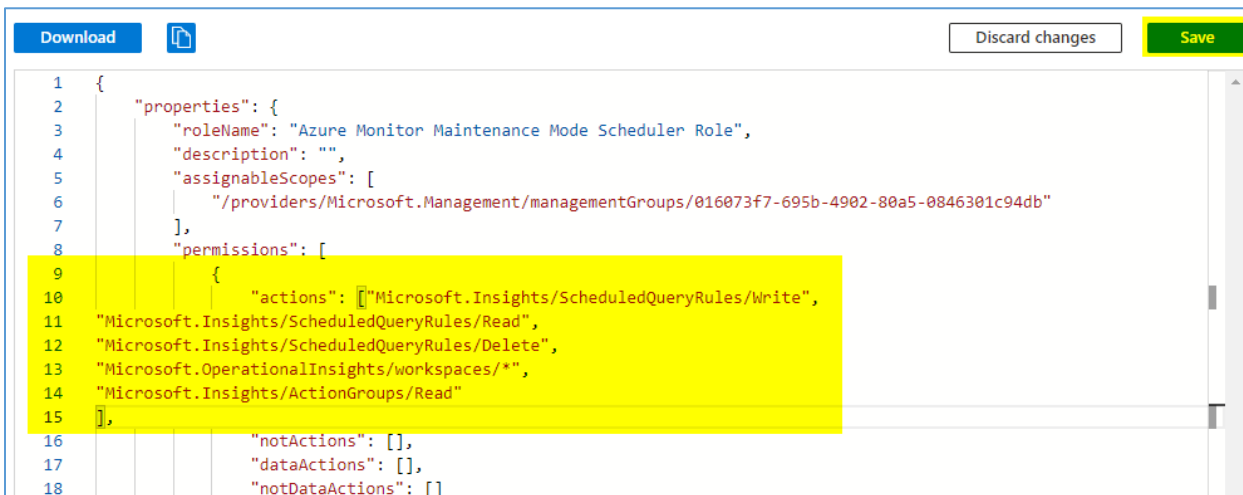
Put your cursor between the [] in actions:

```
1 {
2   "properties": {
3     "roleName": "Azure Monitor Maintainer",
4     "description": "",
5     "assignableScopes": [
6       "/providers/Microsoft.Manage
7     ],
8     "permissions": [
9       {
10        "actions": [],
11        "notActions": [],
12        "dataActions": [],
13        "notDataActions": []
14      }
15    ]
16  }
17 }
```

Now paste the following.

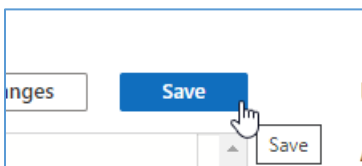
```
"Microsoft.Insights/ScheduledQueryRules/Write",
"Microsoft.Insights/ScheduledQueryRules/Read",
"Microsoft.Insights/ScheduledQueryRules/Delete",
"Microsoft.OperationalInsights/workspaces/*",
"Microsoft.Insights/ActionGroups/Read"
```

It should look like this when you are done. Don't worry about the formatting. As long as the text you pasted is between the [] it will work fine.



```
1 {
2   "properties": {
3     "roleName": "Azure Monitor Maintenance Mode Scheduler Role",
4     "description": "",
5     "assignableScopes": [
6       "/providers/Microsoft.Management/managementGroups/016073f7-695b-4902-80a5-0846301c94db"
7     ],
8     "permissions": [
9       {
10        "actions": ["Microsoft.Insights/ScheduledQueryRules/Write",
11        "Microsoft.Insights/ScheduledQueryRules/Read",
12        "Microsoft.Insights/ScheduledQueryRules/Delete",
13        "Microsoft.OperationalInsights/workspaces/*",
14        "Microsoft.Insights/ActionGroups/Read"
15        ],
16        "notActions": [],
17        "dataActions": [],
18        "notDataActions": []
19      }
20    ]
21  }
22 }
```

Make sure you hit **Save** in the top right when you are done.



Then click **Review + create** at the bottom of the page.

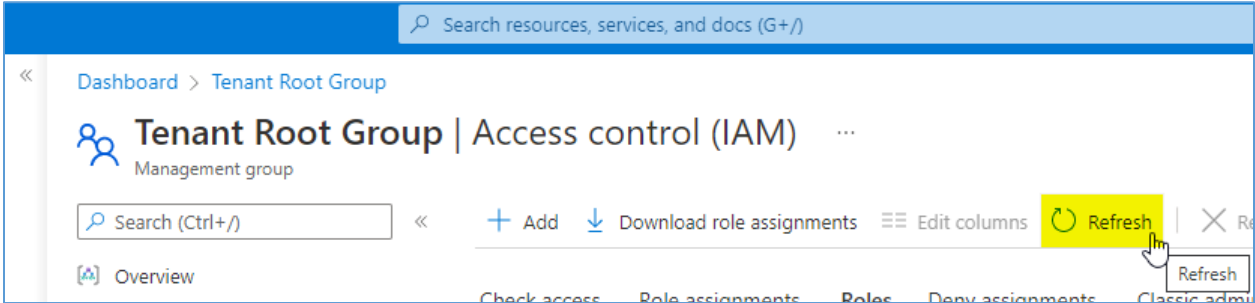


Then click Create



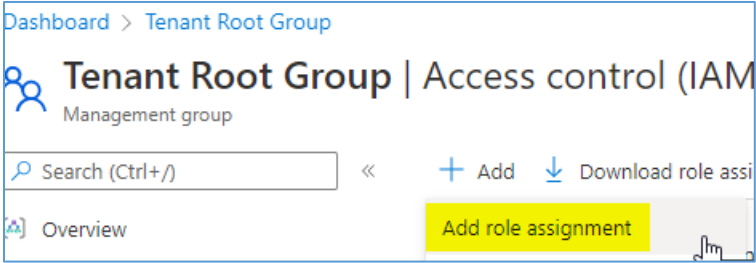
Then **OK**.

Now Click **Refresh**

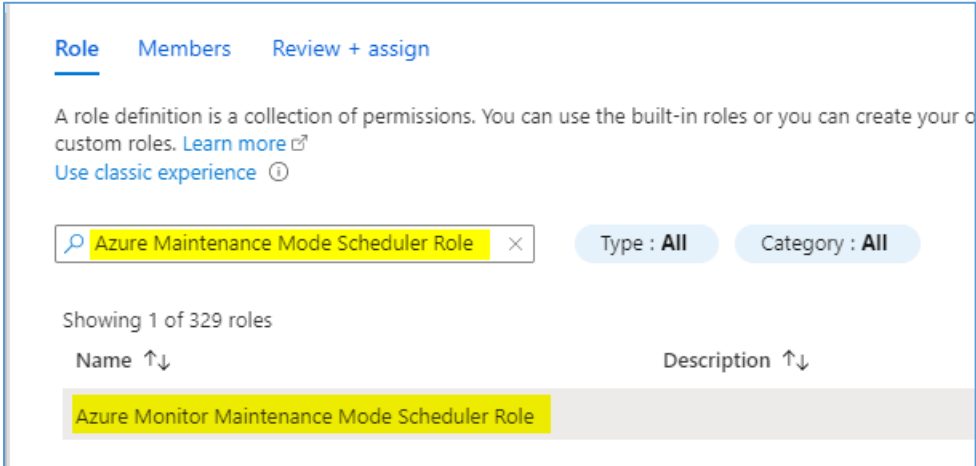


Now that we have a Custom Role called **Azure Maintenance Mode Scheduler Role**, we need to grant the Azure Maintenance Mode Scheduler to that role.

Click **Add role assignment**.



Under the Role Tab. Type in **Azure Maintenance Mode Scheduler Role** and select it



Click The **Member Tab** and **Select +Select Members**

Role **Members** Review + assign

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members **+ Select members**

| Name | Object ID |
|---------------------|-----------|
| No members selected | |

Description Optional

Type in **Azure Maintenance Mode Scheduler**.

Select members

Select ⓘ

Azure Maintenance Mode Scheduler

Azure Maintenance Mode Scheduler

Then select it and then click **Select** at the bottom of the screen.

Selected members:

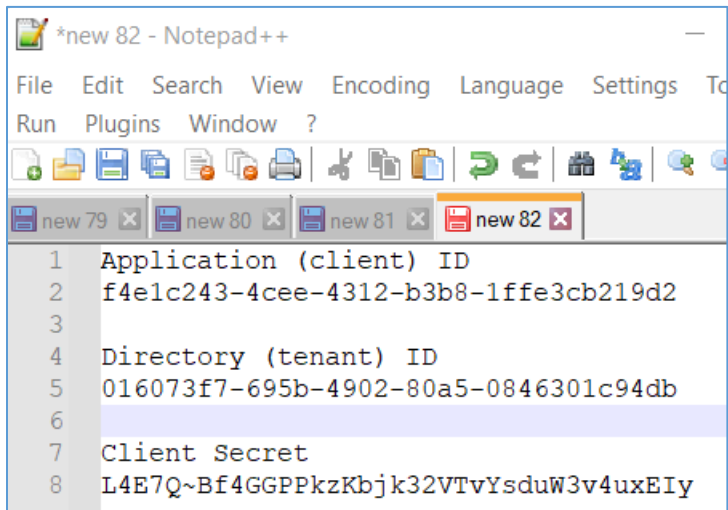
Azure Maintenance Mode Scheduler Remove

Select Close

Then Click **Review + assign** at the bottom of the screen. Then click **Review + assign** again.

Now we have the permission setup.

Make sure you still have your Notepad with the Client ID, Tennant ID and Secret as you will need this for the install.



The screenshot shows a Notepad++ window titled '*new 82 - Notepad++'. The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, and Tools. The toolbar contains various icons for file operations. The tab bar shows four tabs: 'new 79', 'new 80', 'new 81', and 'new 82' (which is the active tab). The text in the editor is as follows:

```
1 Application (client) ID
2 f4e1c243-4cee-4312-b3b8-1ffe3cb219d2
3
4 Directory (tenant) ID
5 016073f7-695b-4902-80a5-0846301c94db
6
7 Client Secret
8 L4E7Q~Bf4GGPPkzKbjk32VTvYsduW3v4uxEIy
```