MPARR Quick installation guide (from scratch)

Welcome to this quick installation guide for MPARR 2, in this guide we will use all the online process to this activity.

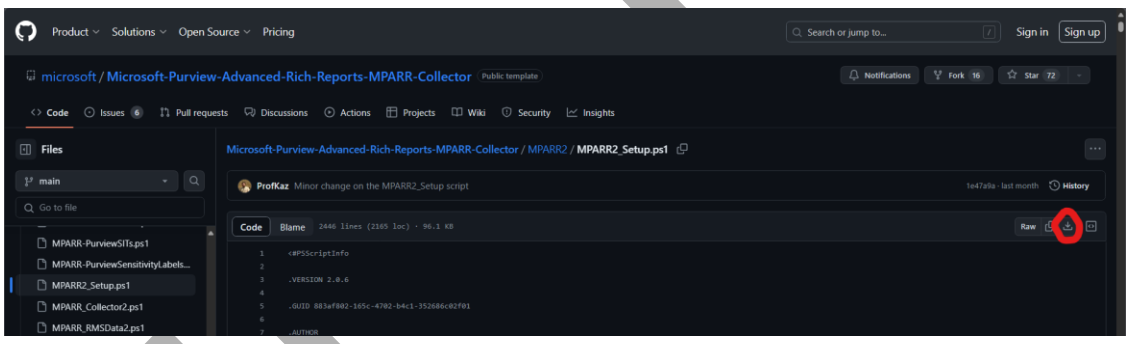
Requirements

To run MPARR 2 in a quick way you need to have these requirements:

- Azure subscription
- Owner or Contributor permissions over the Azure subscription
- Create a workspace in Logs Analytics
- Global Administrator role for your Microsoft 365 Tenant
- PowerShell 7
- Internet Access

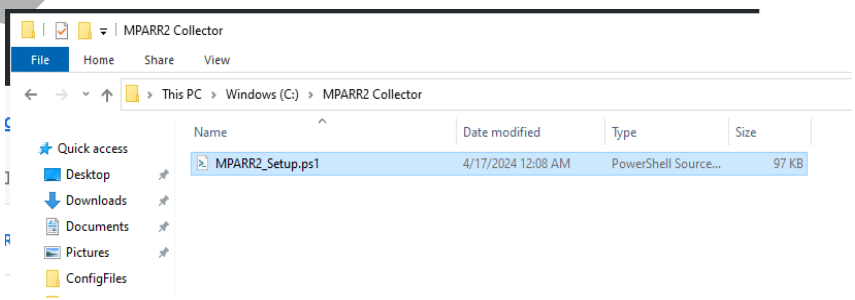
Get MPARR2 Setup Script

MPARR2_Setup.ps1 can help to you to do all the installation process, you need to get the file from [Microsoft-Purview-Advanced-Rich-Reports-MPARR-Collector/MPARR2/MPARR2_Setup.ps1 at main · microsoft/Microsoft-Purview-Advanced-Rich-Reports-MPARR-Collector · GitHub]



Screen Capture 1 Download MPARR2_Setup.ps1

To download the script, press the icon marked on the Screen Capture 1 and put in a folder on your local drive called “MPARR2 Collector” or any other name that can be work for you.



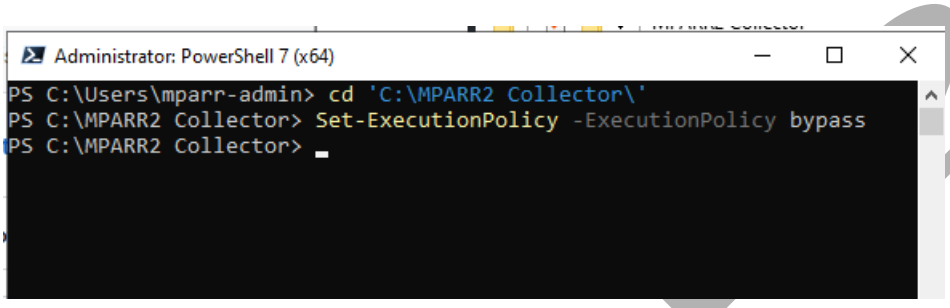
Screen Capture 2 MPARR2_Setup.ps1 on local drive

PowerShell Activities

To run all the scripts, it is required to use PowerShell 7, please open PowerShell 7 with Administrator permissions and set the Execution Policy to bypass. After the installation process this configuration will be change to remote signed.

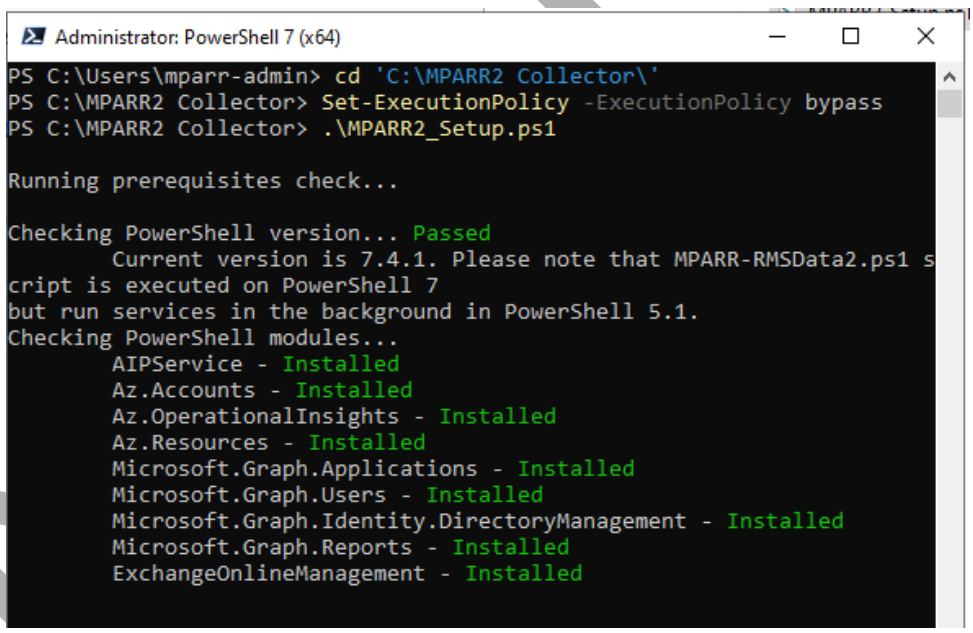
To change the Execution Policy to bypass, you need to execute:

PS C:\ > **`Set-ExecutionPolicy -ExecutionPolicy bypass`**



Screen Capture 3 PowerShell with Admin rights and setting Execution Policy on bypass

The next step is run MPARR2_Setup.ps1, the first time that is executed all the PowerShell modules required that are not installed will be installed, and the script will be exit, in that case will be required to execute once again.

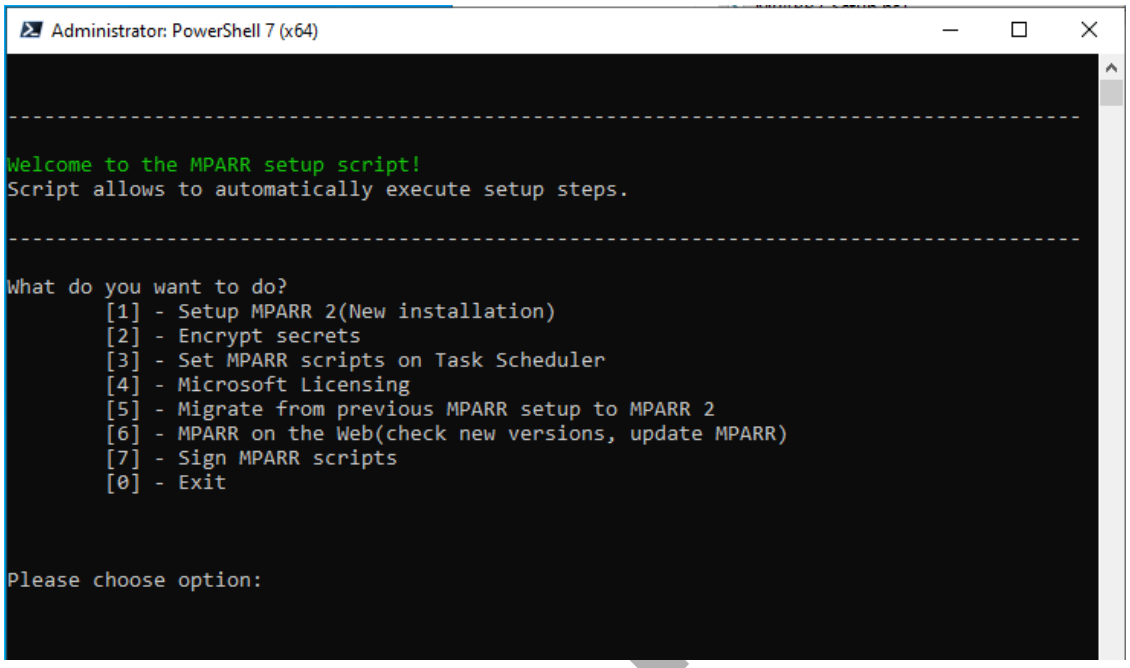


Screen Capture 4 Checking PowerShell modules installation status

Please accept all the modules that need to be installed.

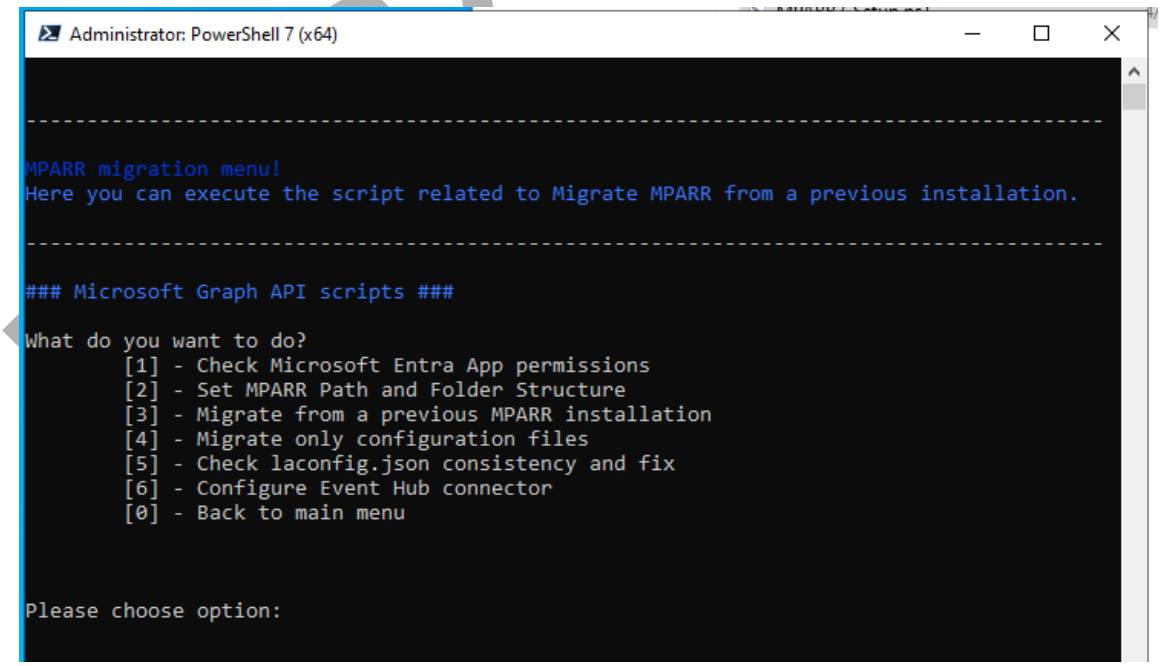
MPARR2 Setup quick process

Please remember that this guide is thought for a quick deploy of MPARR 2, if you need more details, you can check the online information, or request some additional data opening an issue request on GitHub.



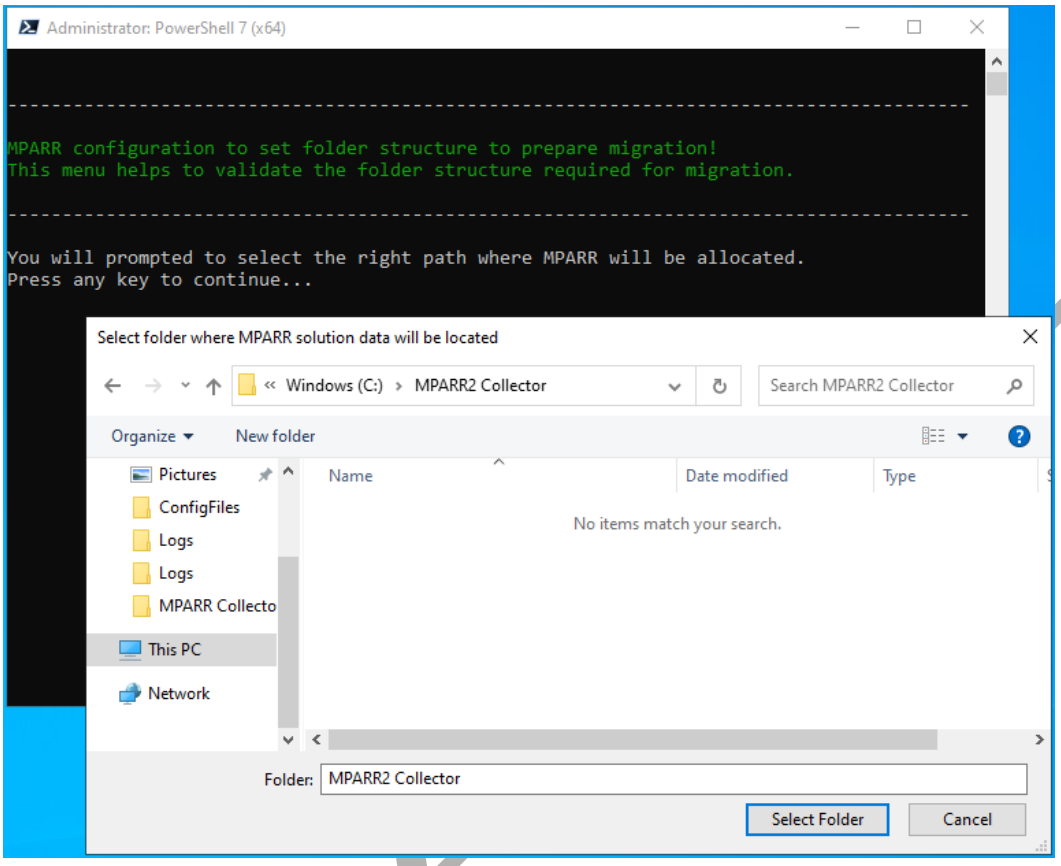
Screen Capture 5 Main setup menu

On the Main setup menu, please select option number 5 “Migrate from previous MPARR setup to MPARR 2”.



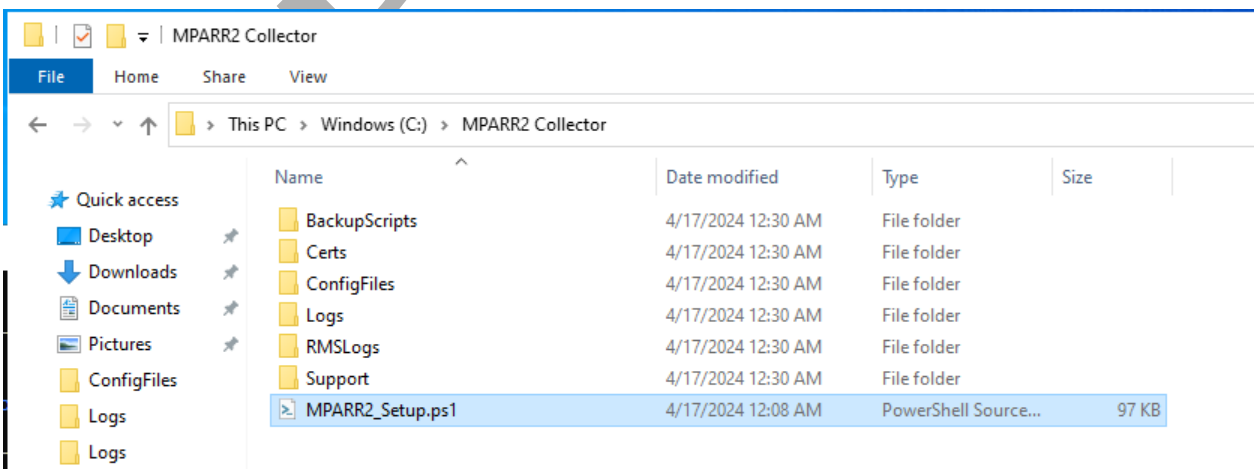
Screen Capture 6 MPARR migration menu

Under this new menu select option number 2 “Set MPARR Path and Folder Structure” and select your “MPARR2 Collector” folder.



Screen Capture 7 MPARR2 root folder selection

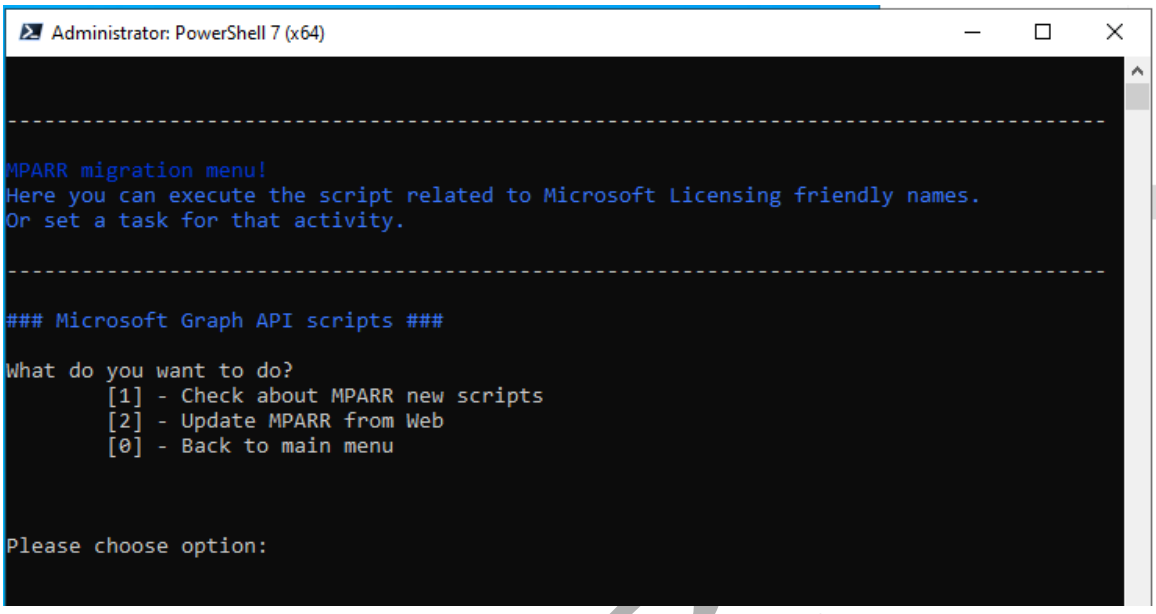
After the root folder is selected all the folder structure is created on that location.



Screen Capture 8 MPARR2 folder structure

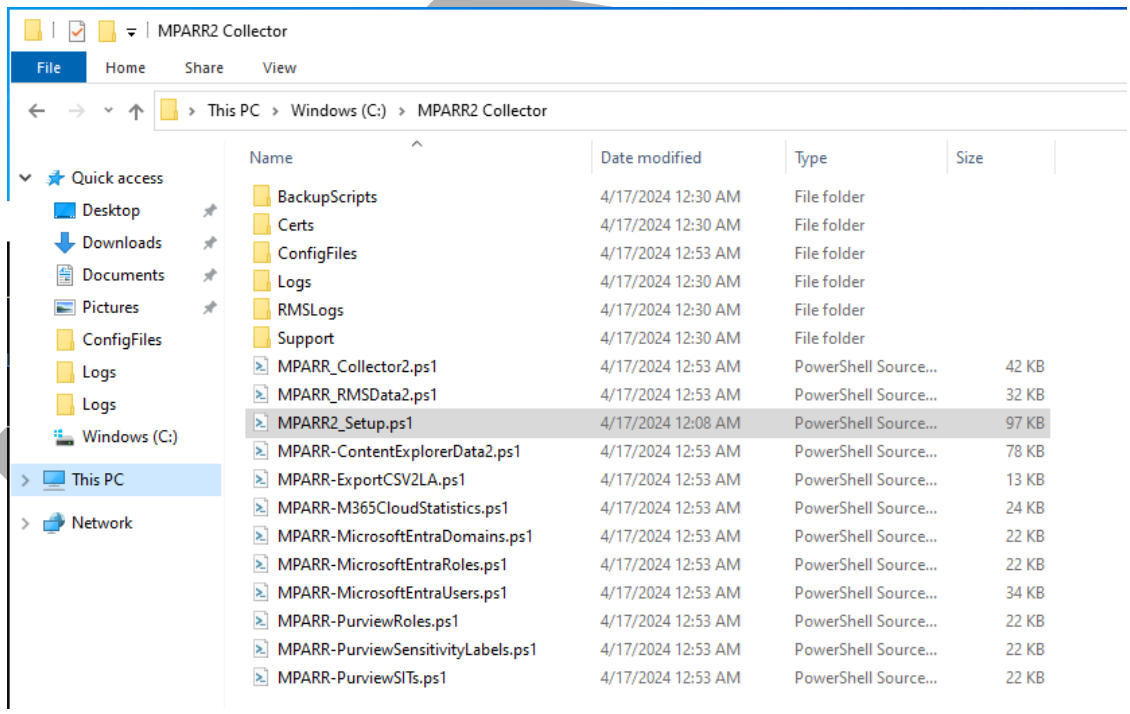
After finishing this process press on the PowerShell menu number 0 “Back to main menu”

Now on the Main setup menu select option number 6 “MPARR on the Web (check new versions, update MPARR)”



Screen Capture 9 MPARR 2 on the Web menu

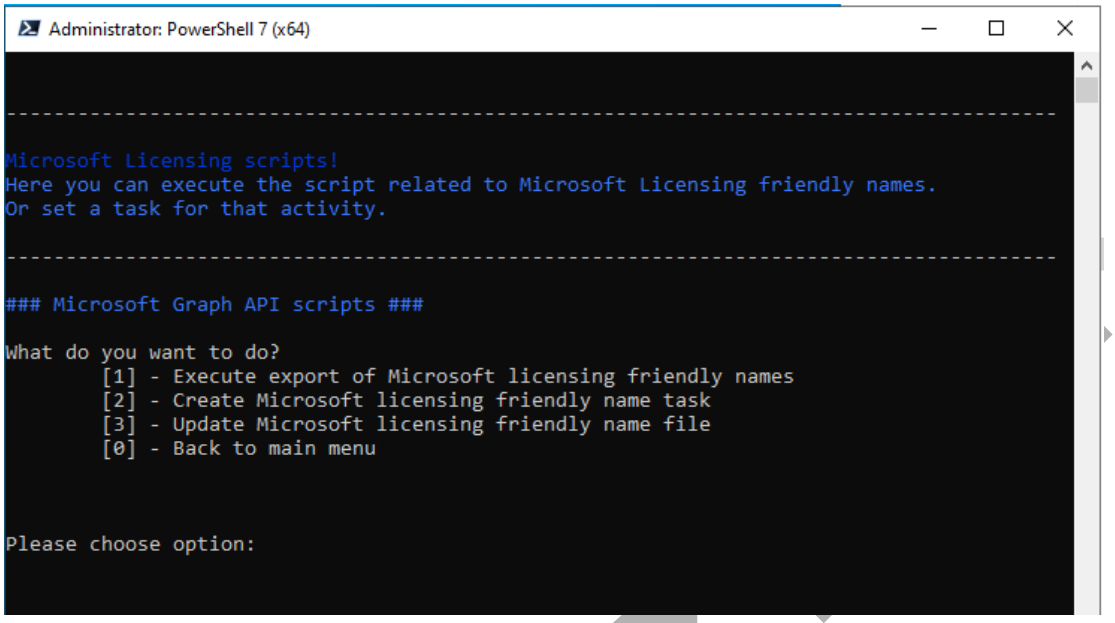
Under this menu select option 2 “Update MPARR from Web” all the MPARR components will be downloaded on the local “MPARR2 Collector” folder.



Screen Capture 10 MPARR 2 scripts downloaded to local folder

After scripts are downloaded to the local folder, please select option 0 “Back to main menu”

Now select under Main menu setup option number 4



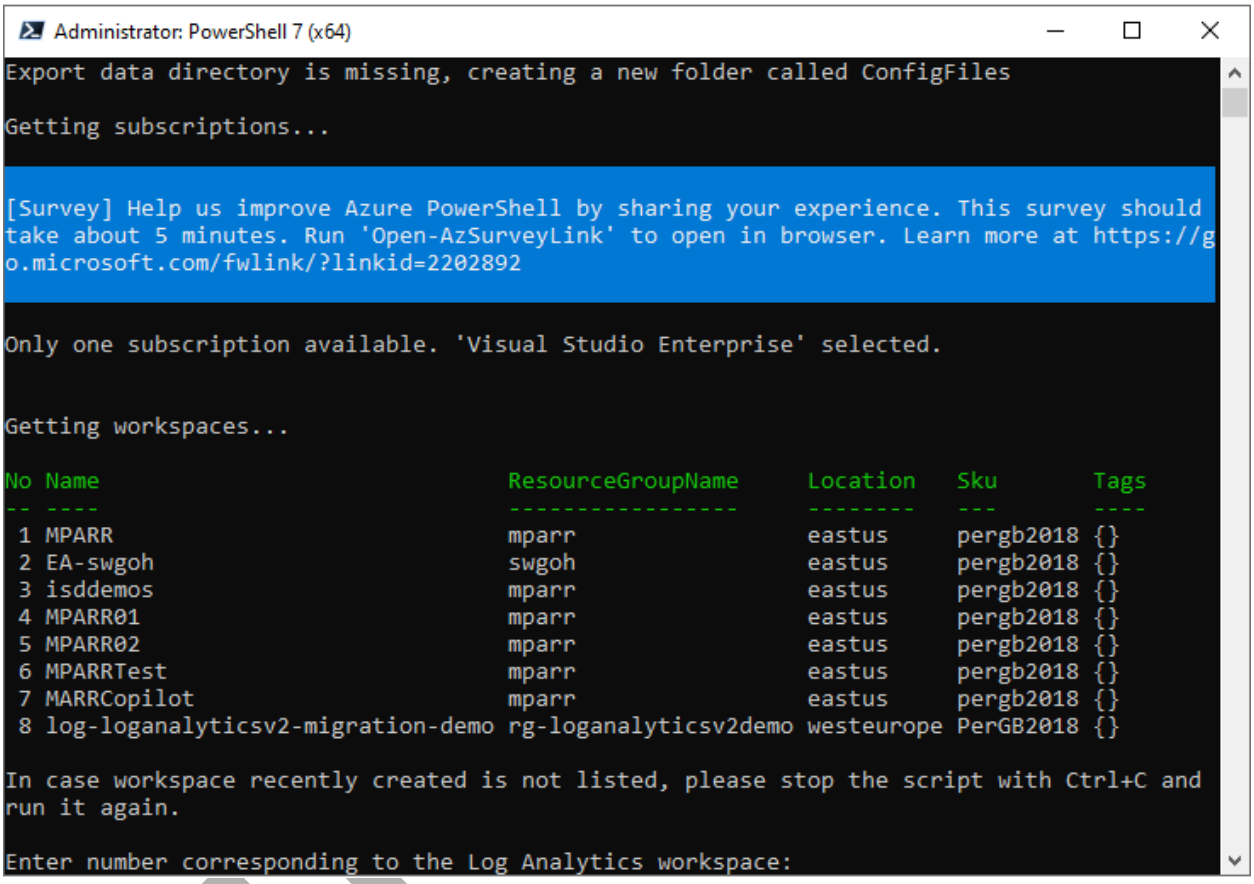
Screen Capture 11 Microsoft licensing menu

In this menu you need to select option 3 “Update Microsoft licensing friendly name file” a new CSV file will be downloaded under “Support” folder.

Next select the option 0 “Back to main menu”

MPARR 2 Configuration process

On the Main menu we will select option 1 “Setup MPARR 2(New installation)”. During this process your credentials will be required twice, the first login required is to connect to your Azure Subscription and select the Logs Analytics workspace, previously created under MPARR 2 requirements; the 2nd time to request credentials will be required to connect to your Microsoft 365 Tenant and create a Microsoft Entra App called “MPARR2’-Datacollector”.



Screen Capture 12 Logs Analytics workspace selection

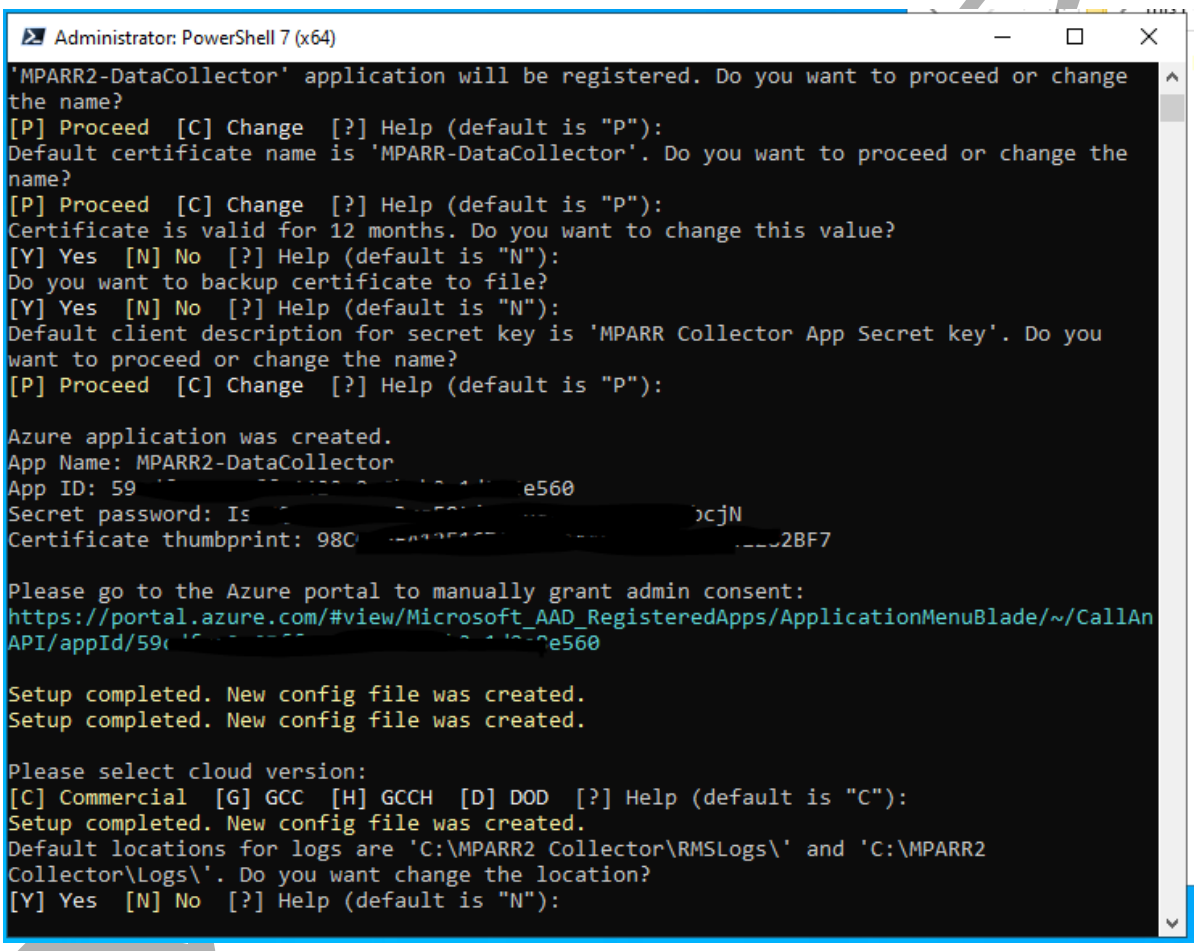
In this case, Screen Capture 12 Logs Analytics workspace selection, if you have more than one subscription you will be prompted to select the right subscription and then select the Logs Analytics workspace, you need to select the corresponding number.

After selecting your Logs Analytics workspace, you can be prompted to add your Global Administrator credentials for your Microsoft 365 Tenant.

Next you will need to use the default configuration, or make changes if it´s required, these are the points that you need to complete or accept:

- Application name, by default is called “MPARR2-Datacollector” the name can be changed
- App certificate, a local self-sign certificate will be created with the name “MPARR-DataCollector”, this certificate will be installed locally and imported to the previously Microsoft Entra App created.

- Certificate duration, by default the previous certificate will be created with 12 months' expiration, this value can be changed to set up until 36 months.
- Backup certificate, you can backup this certificate, in case that you want to backup you will be prompted to set a password for the PFX file that will be stored under "Certs" folder.
- App secret, under Microsoft Entra App a key is created and require a description, a default description related to MPARR will be added.
- Tenant Cloud version, in almost all the cases the Tenants are Commercial, in some cases, some Tenant can be located on other cloud services.
- Logs folders, use the default configuration.



Screen Capture 13 MPARR 2 configuration process

As last step in this configuration an additional configuration was added to setup the Event Hub connector, this configuration can be skipped pressing Enter or selecting "N"

MPARR 2 Post setup activities

Remaining at the Main setup menu, you can check in your "MPARR2 Collector" folder inside of the "ConfigFiles" folder that a new file was created called "laconfig.json", this file contains all your current configuration and the values can be changed in any moment, you can check that the passwords are stored in clear text, **option number 2 "Encrypt secrets"** on the Main menu permit to hash the passwords, in this hash process is used the logged user and the machine ID, other user cannot be able to use the configuration file after hash the password, or if you use the configuration file in another machine.

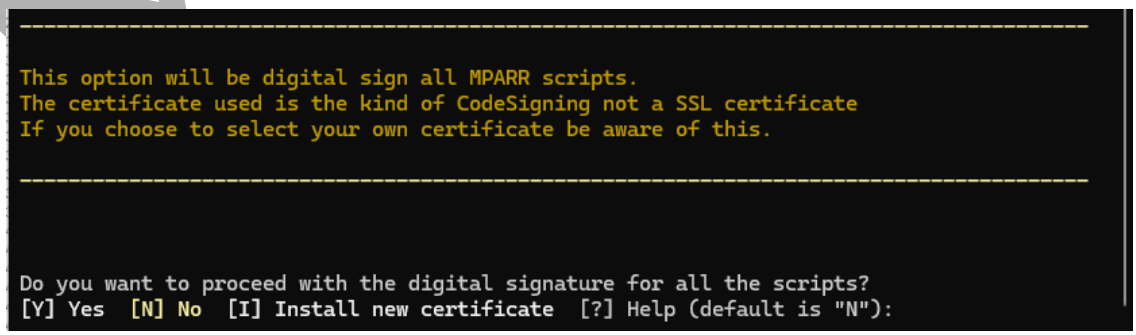
To set the tasks under the Task scheduler you need to go through these options, select the default options:

- Option 3 "Set MPARR scripts on Task Scheduler"
    - Option 1 "Create scheduled task for Core Scripts (MPARR Collector and MPARR RMS)"
        - Option 1 "Create MPARR Collector task"
        - Option 2 "Create MPARR RMS task"
    - Option 2 "Microsoft Graph API Scripts (Users, Domains, Roles, Cloud Statistics)"
        - Option 1 "Create Microsoft Entra Users task"
        - Option 2 "Create Microsoft Entra Domains task"
        - Option 3 "Create Microsoft Entra Roles task"
        - Option 4 "Create Microsoft 365 Cloud Statistics task"
    - Option 3 "Microsoft Purview API (Sensitivity Labels, Sensitive Info Types, Purview Roles, Content Explorer)"

      All these scripts need to have elevated privileges and can be executed manually in case the permissions cannot be assigned

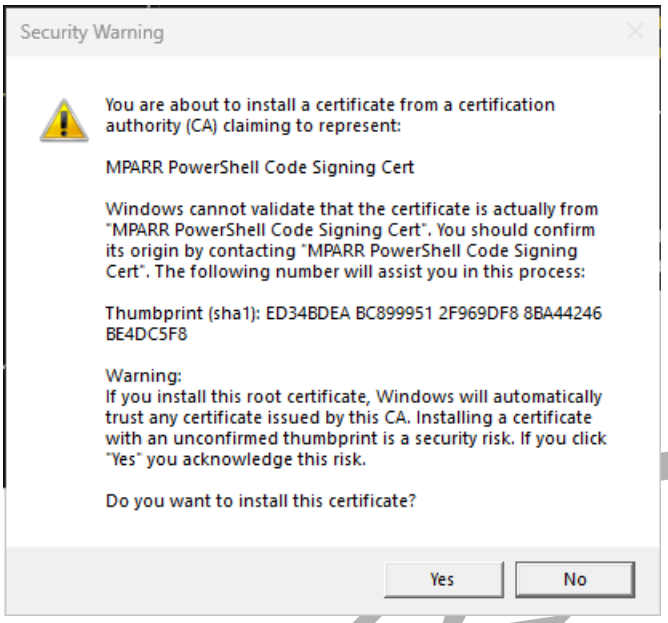
        - Option 1 "Create Microsoft Purview Sensitivity Labels task"
        - Option 2 "Create Microsoft Purview Sensitive Information Types task"
        - Option 3 "Create Microsoft Purview Roles task"
        - Option 4 "Create Microsoft Purview Content Explorer task"
- Option 4 "Microsoft Licensing"
    - Option 2 "Create Microsoft licensing friendly name task"

The last step in this menu is select option 7 "Sign MPARR scripts" this will permit to create a self-sign certificate for code or use an existing one. All the scripts will be sign and the Execution Policy can be set on Remote Signed.



Screen Capture 14 Sign MPARR scripts

When you select “Install new certificate” on the previous menu you need take care to select Yes when the prompt to install the certificate is show.



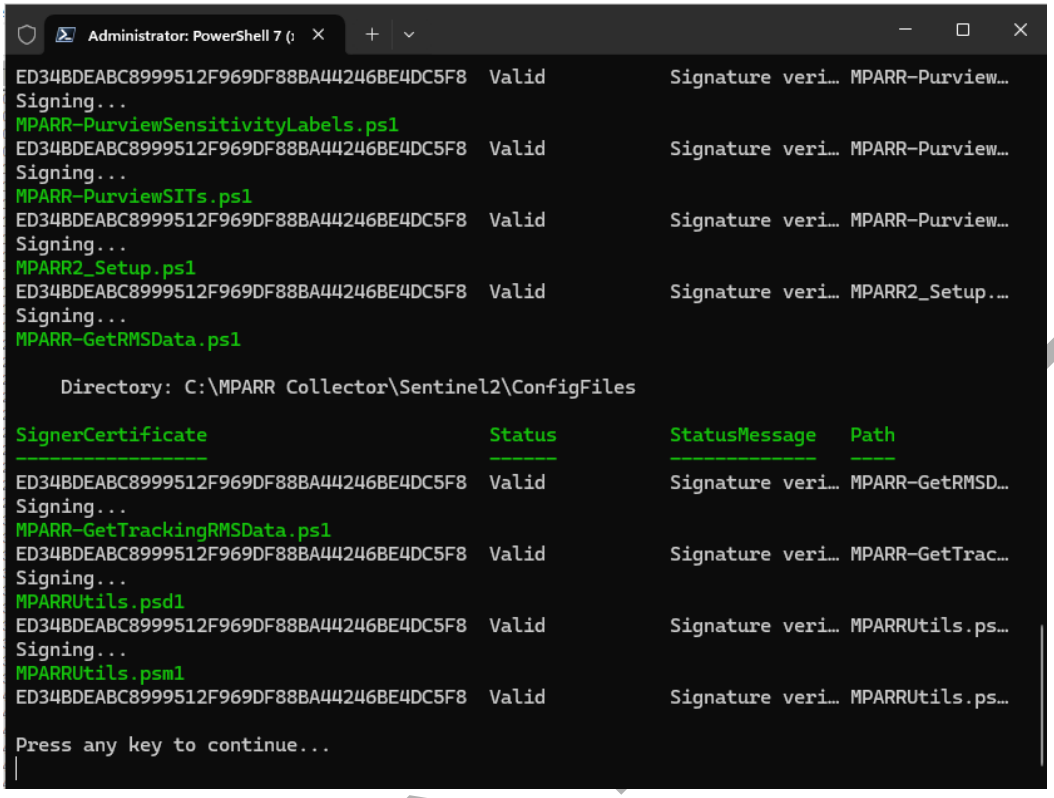
Screen Capture 15 Prompt to accept certificate installation

On the sign process now on the menu, Screen Capture 15 Prompt to accept certificate installation, you need to select Yes to finish the process a list of all the available certificates for coding will be listed, select the right certificate.

```
Do you want to proceed with the digital signature for all the scripts?
[Y] Yes  [N] No  [I] Install new certificate  [?] Help (default is "N"): y

Getting Code Signing certificates...

No Subject                                Thumbprint                                NotBef
                                                                                    ore
-- -------                                ----------                                ------
 1 CN=MPARR PowerShell Code Signing Cert ED34BDEABC8999512F969DF88BA44246BE4DC5F8 4/16/…
 2 CN=MPARR PowerShell Code Signing Cert 4DCE25FCC6B7EB2D27480A678A5EE1AC44B82544 4/12/…
 3 CN=MPARR PowerShell Code Signing Cert 4D858FB0FB899A2EF5447D142E8DD78FC334533C 4/2/2…
 4 CN=MPARR PowerShell Code Signing Cert 3C6171F92788CC69B794C2F356A2387261E66960 3/4/2…
 5 CN=MPARR PowerShell Code Signing Cert 12091541F28D9B35FE2530D520DE20F33D981A0D 2/23/…
 6 CN=EDM PowerShell Code Signing Cert   0233AFBBAAC735D2B306FA76481B616096791089 11/17…

Enter number corresponding to the certificate to use:
```

Screen Capture 16 Prompt to select certificate to sign the MPARR Scripts

After this process all the scripts are digital signed.



Screen Capture 17 MPARR 2 Scripts now are digital signed

Finally, you can select Option 0 to Exit.

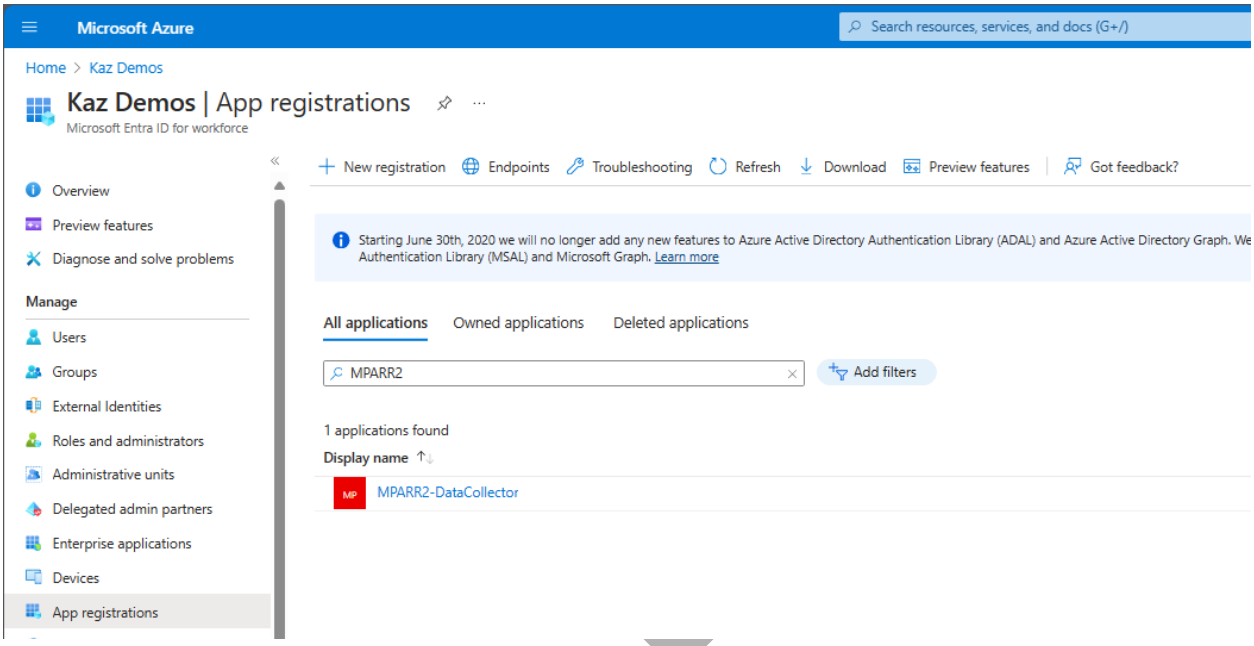
Signing the scripts is very important, on Windows Server it is mandatory to run PowerShell scripts under Task Scheduler.

Execution policy can be changed by executing the next cmdlet:

PS C:\ > **Set-ExecutionPolicy -ExecutionPolicy RemoteSigned**

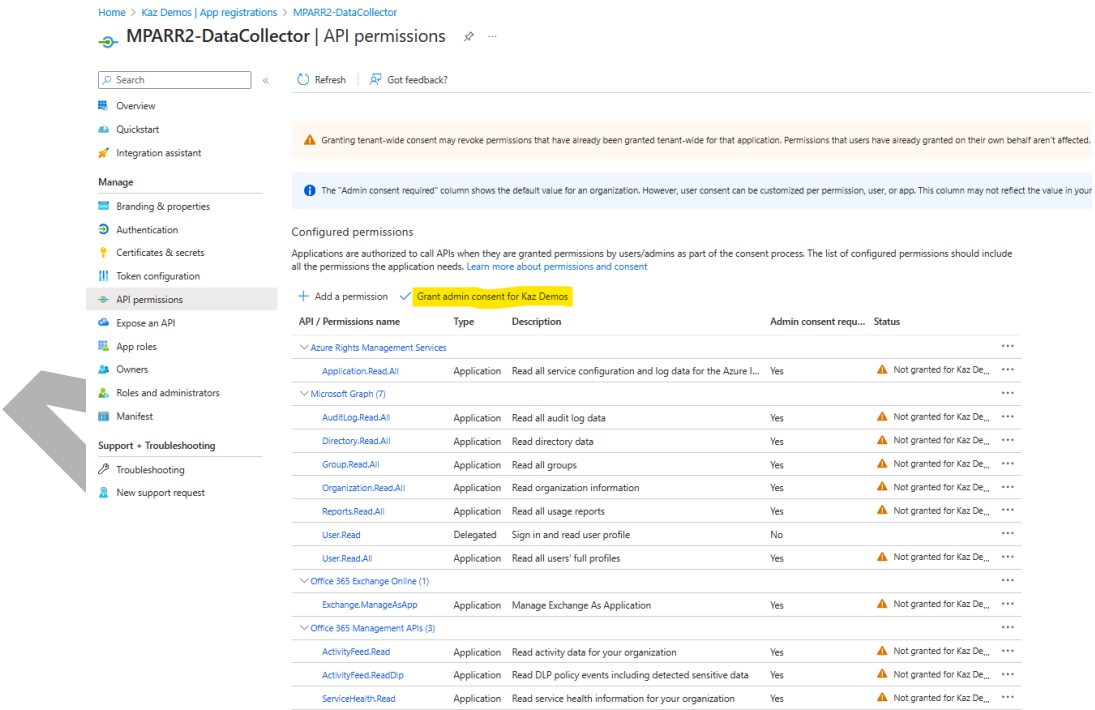
Screen Capture 18 Change execution policy to remote signed

Under Microsoft Entra Applications it´s required to “Grant access” to the API permissions, to do that you need go to Microsoft Entra ID, search under “App registrations” the “MPARR2-DataCollector” application created by MPARR2_Setup script.



Screen Capture 19 MPARR2-DataCollector application under Microsoft Entra ID

At MPARR2-DataCollector App go to menu API permissions and select “Grant admin consent…”

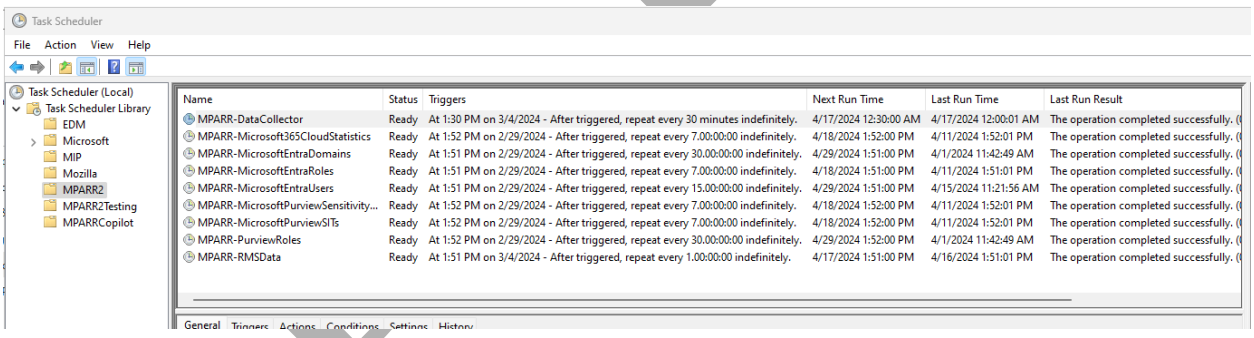


Screen Capture 20 MPARR2-DataCollector API permissions

After Grant the Admin Consent on the APP, it's recommended to start executing all the MPARR 2 scripts, one by one:

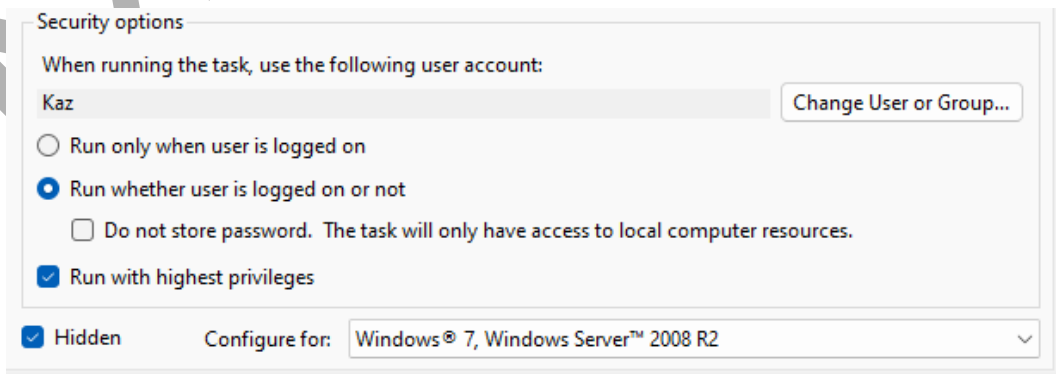
- MPARR-MicrosoftEntraUsers.ps1, in this one the first time that is executed ask if you want to get on licensed users or all users, including unlicensed or guests.
- MPARR-MicrosoftEntraDomains.ps1
- MPARR-MicrosoftEntraRoles.ps1
- MPARR-M365CloudStatistics.ps1
- MPARR-MSLicenses.ps1 (This one is created on the menu 4-2 under the Setup script)
- MPARR_RMSData2.ps1
- MPARR_DataCollector2.ps1
  The next scripts can be executed manually adding the attribute "-ManualConnection" in case to don´t want to add elevated privileges to the app. To execute manually someone with Compliance Administrator role is required to execute.
- MPARR-PurviewRoles.ps1 -ManualConnection
- MPARR-PurviewSITs.ps1 -ManualConnection
- MPARR-PurviewSensitivityLabels.ps1 -ManualConnection

To finish the Task Scheduler configuration, you need to open it, and extend MPARR2 folder, inside you will find all the tasks created.



Screen Capture 21 MPARR2 tasks under Task scheduler

To run MPARR2 scripts as a service on each task is required to change the way to run the script from "Run only when user is logged on" to "Run whether user is logged on or not"



Screen Capture 22 MPARR 2 running as a service