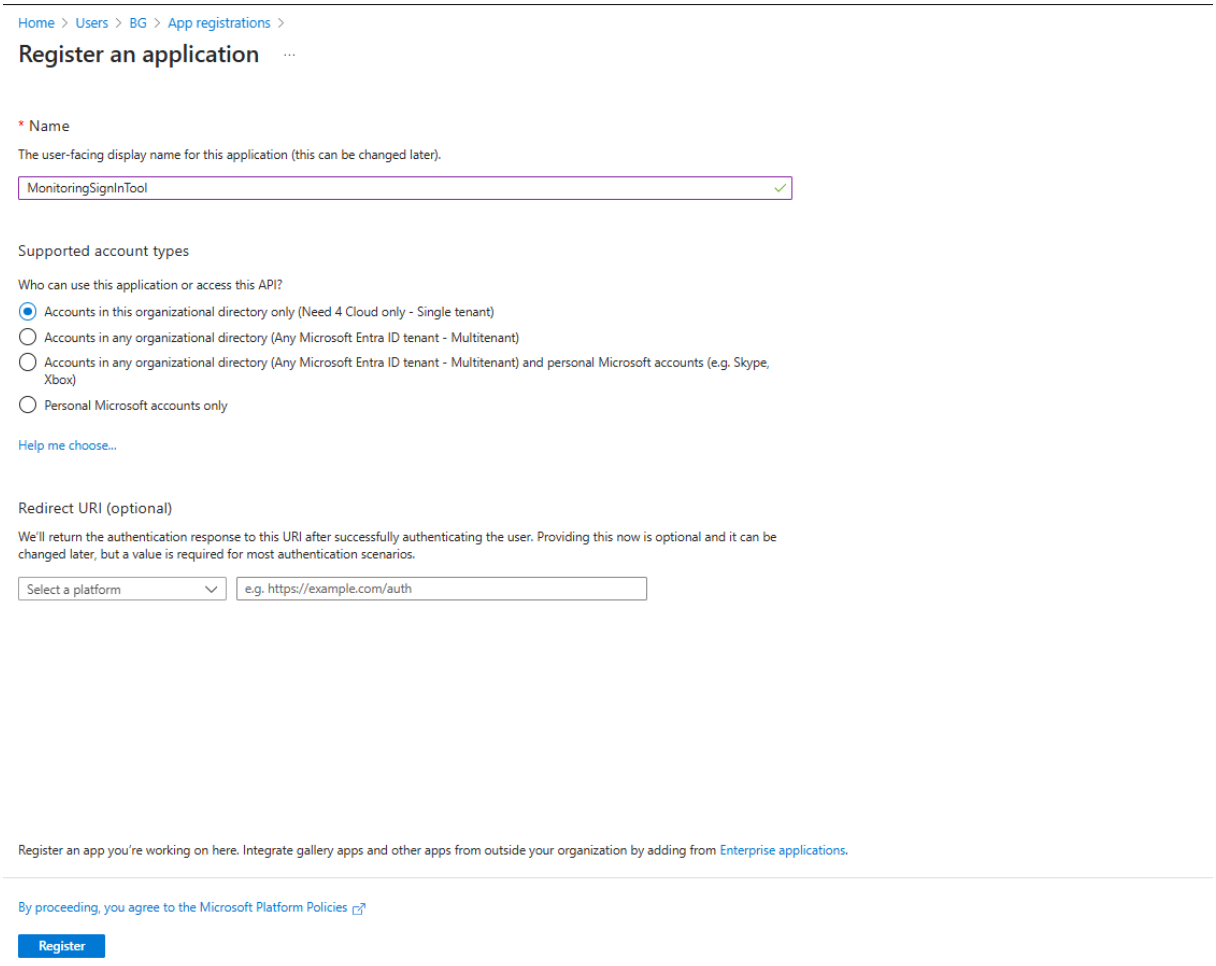
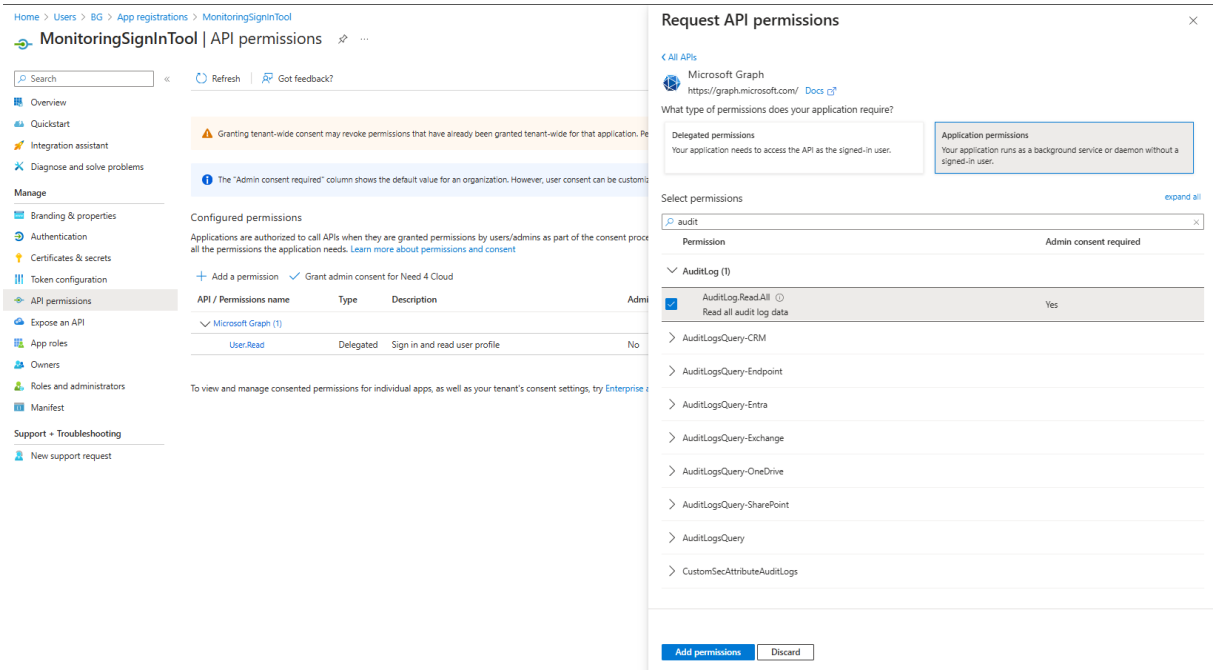
Setup guide Monitoring script

1. Create user which will send notification emails and assign Exchange online P1 license to this user, call this user for example Account Monitoring
2. Create or copy the recipient address(es) , they need at least to have Exchange online P1 license as well
3. Create app in Entra ID
   Entra.microsoft.com -> Applications -> App registration -> New registration

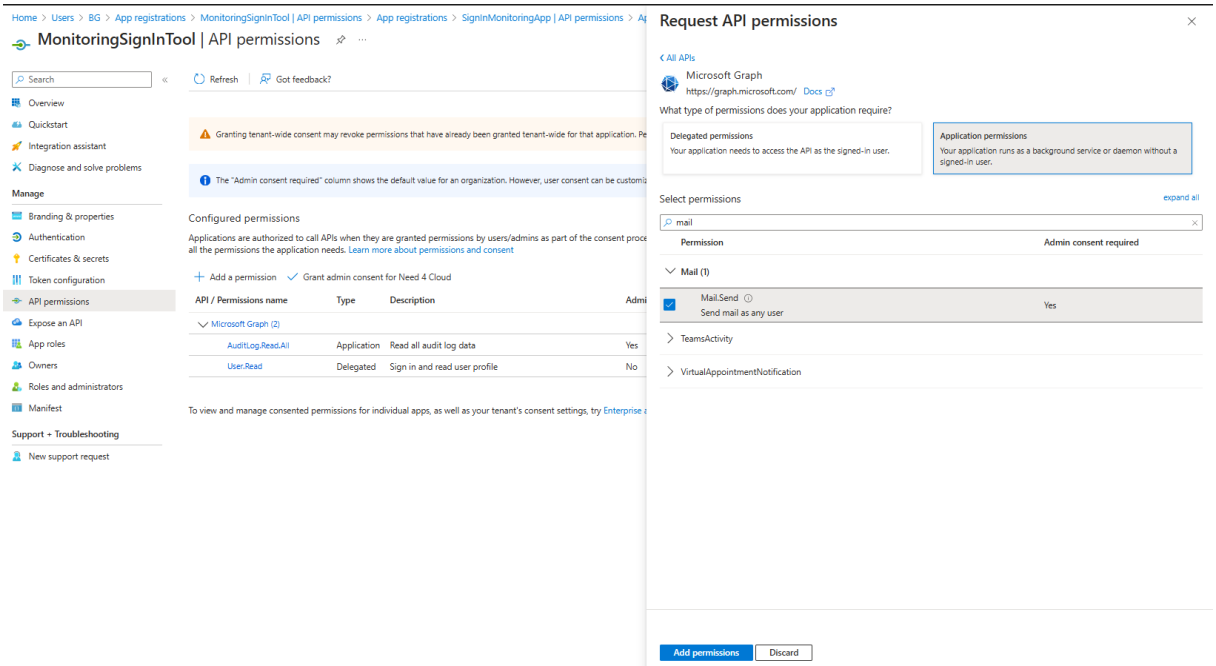
1) Give app a name for example MonitoringSignInTool
2) Choose Account in this organizational directory only



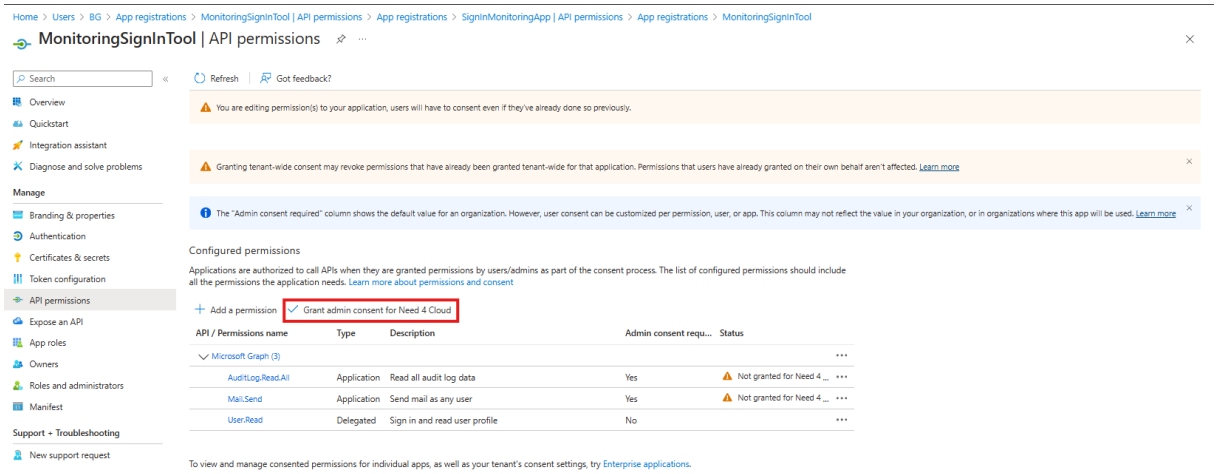
4. Now go to API Permissions -> Add a permission -> Microsoft Graph -> Application permissions -> Search for AuditLog.Read.All -> Select and choose Add permissions



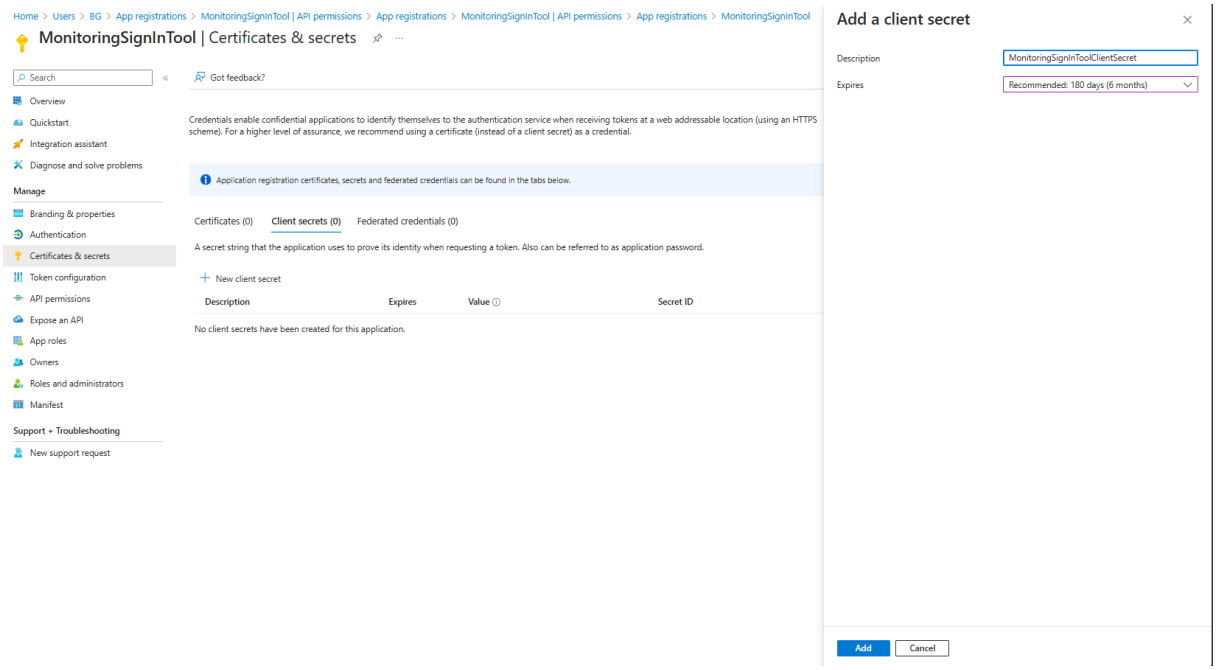
5. Now search for mail and select Mail.Send and press Add permissions



6. Press Grant admin consent for “Your org”

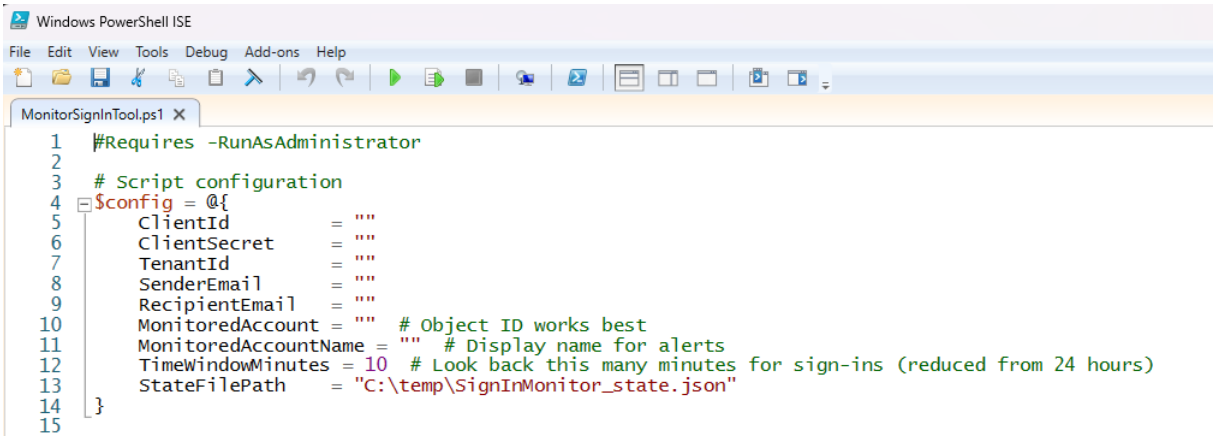


7. Confirm and check that Status says Granted on the right pane
8. Now go to Certificates & secrets and press New Client Secret
9. Give it a description, choose number of days and press Add



10. Copy the Value (not secret ID) and save it for later
11. Now go to Overview -> and copy Application (client) ID and Directory (tenant) ID and save it for later

12. Find downloaded MonitorSignInTool.ps1, right click and choose edit



Insert your values between columns

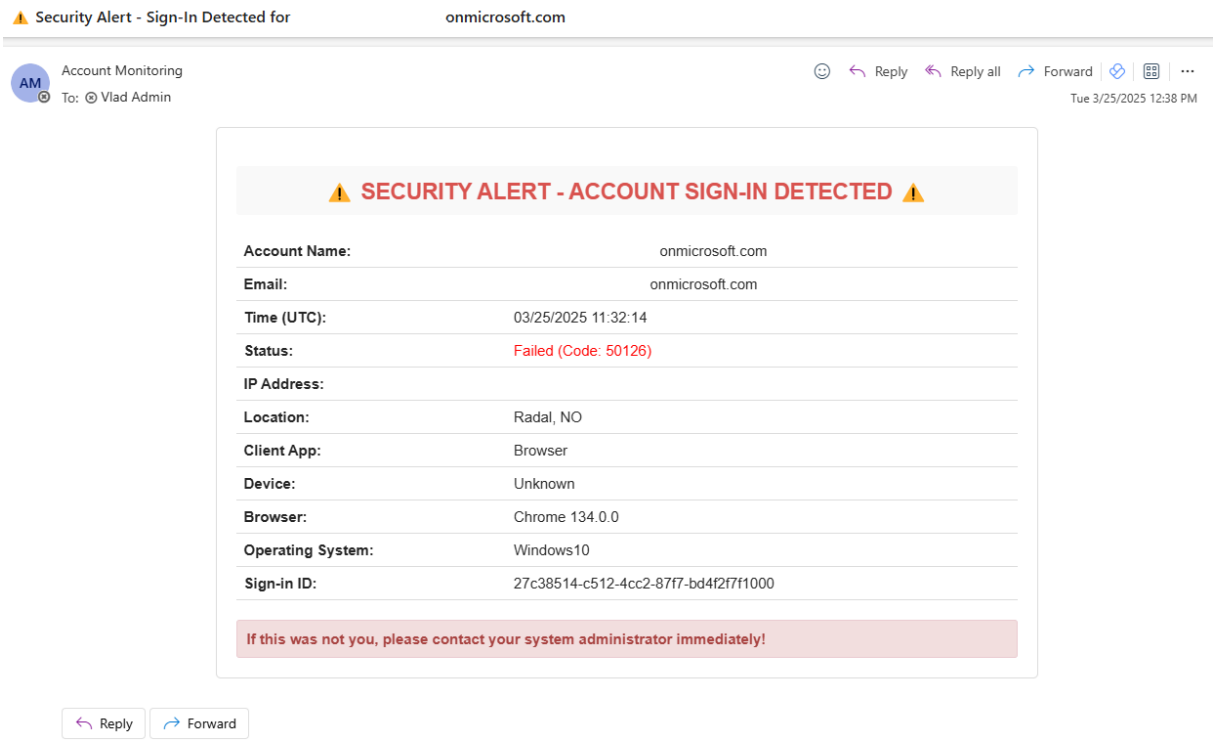
1) ClientId is your Application (client) ID
2) ClientSecret is your Value ID from Certificate & Secrets
3) TenantId is Directory (tenant) ID
4) SenderEmail is your sender email address
5) RecipientEmail is your recipient email address
6) MonitoredAccount is Object ID of account which you want to monitor (you can find in Entra -> Users. PS: It's best to use ObjectID instead of UPN to avoid big delays
7) MonitoredAccountName is the address or name of account which is monitored (this is optional if you don't want to get notified with objectID
8) TimeWindowMinutes is the scope for how many minutes back it should check sign in logs for the specific user. You can edit the value to TimeWindowHours if you prefer to use hours instead. Don't forget to edit file path if your script is located somewhere else and not in C:\temp

The script remembers last check time and saves ID's in SignInMonitor_state.json file which will be generated at first time you run the script, to avoid duplicate checks every time it runs.

It should also install all necessary modules from library and import them automatically.

Run this script from any endpoint and set up task schedule to run it every X minutes or hours.

Notification emails looks like this



Feel free to customize it / tweak it as you wan 😊