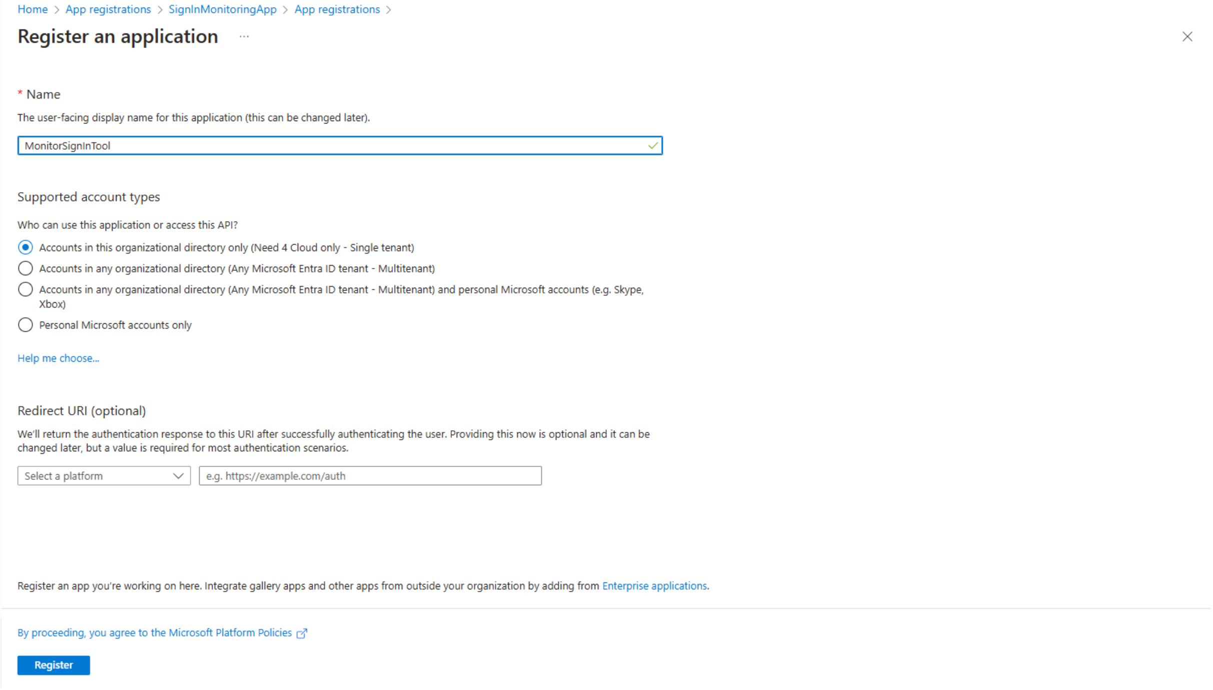
Setup MonitorSignInTool

Ensure that you have Powershell 7 installed on your endpoint and administrator rights first time you run this scripts

PS: Default location of all log files, certificates etc is C:\temp, edit this if you want to use another location

1. Download all files
2. Run CertCreator.ps1 to create public and private certificates and extract them to your endpoint's C:/temp , follow instructions in window or follow the below steps here
3. Log into entra.microsoft.com and register an application, call it for example MonitorSignInTool or something like that



Home > App registrations > SignInMonitoringApp > App registrations >

Register an application

* Name

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

MonitorSignInTool

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Need 4 Cloud only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

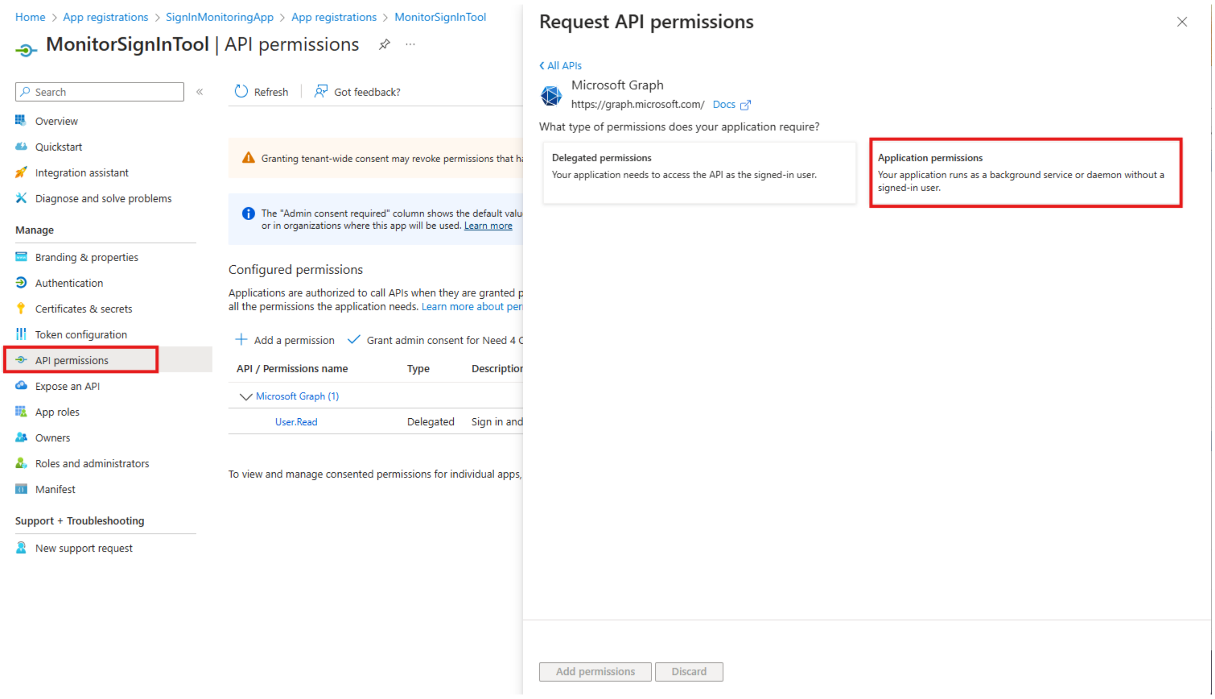
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

4. Go to API permissions -> Add a permission -> MS Graph -> Application permissions



Home > App registrations > SignInMonitoringApp > App registrations > MonitorSignInTool

MonitorSignInTool | API permissions

Search

Refresh | Got feedback?

Granting tenant-wide consent may revoke permissions that ha

The "Admin consent required" column shows the default valu or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted p all the permissions the application needs. Learn more about per

+ Add a permission ✓ Grant admin consent for Need 4 C

API / Permissions name	Type	Descriptior
Microsoft Graph (1)		
User.Read	Delegated	Sign in and

To view and manage consented permissions for individual apps,

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

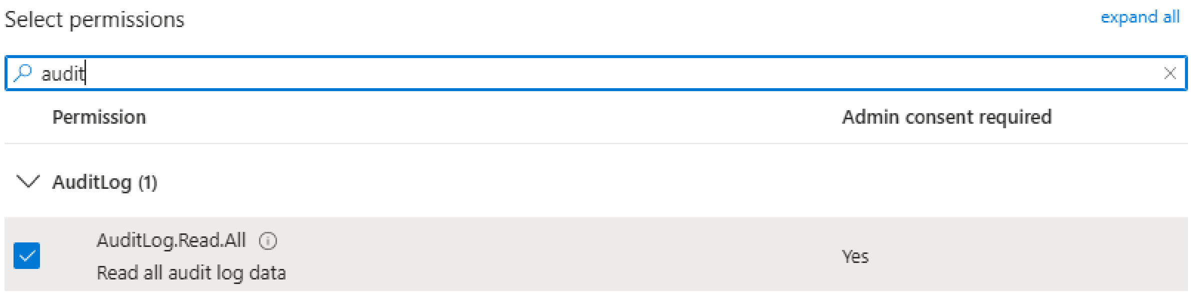
What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Add permissions | Discard

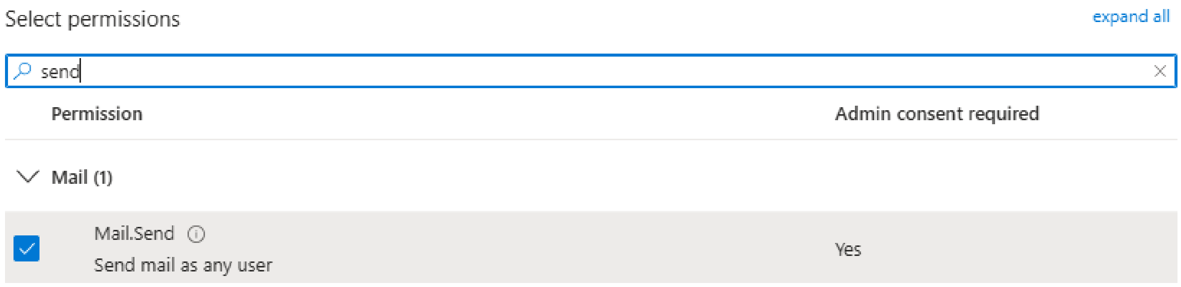
Select AuditLog.Read.All and Mail.Send



Select permissions expand all

audit

	Permission	Admin consent required
	AuditLog (1)	
☑	AuditLog.Read.All Read all audit log data	Yes



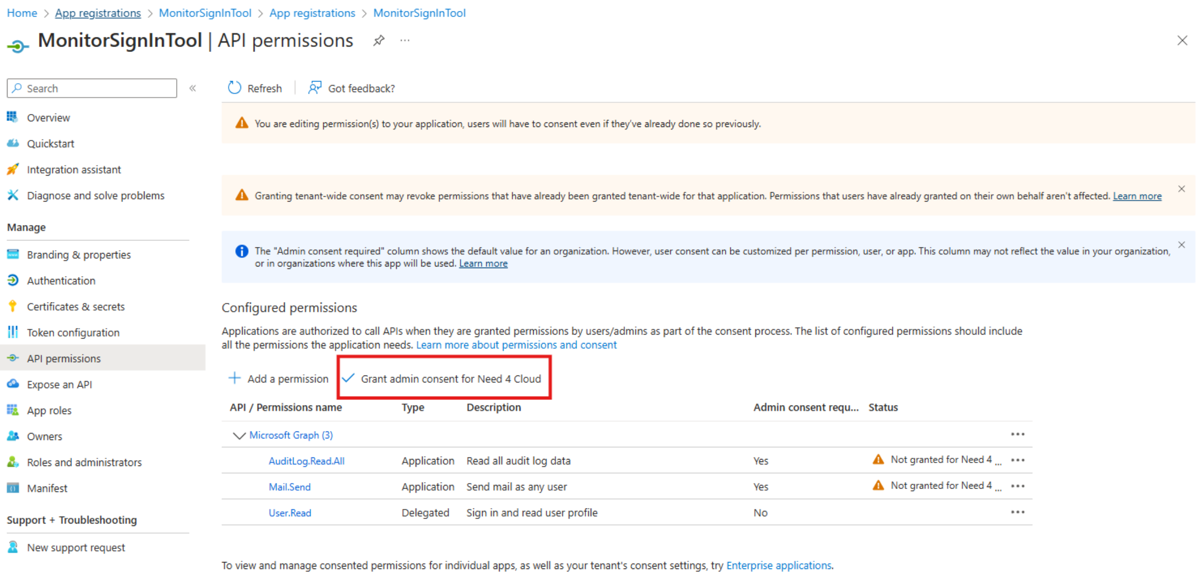
Select permissions expand all

send

	Permission	Admin consent required
	Mail (1)	
☑	Mail.Send Send mail as any user	Yes

And press Add permissions

5. Now grant permissions



MonitorSignInTool | API permissions

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

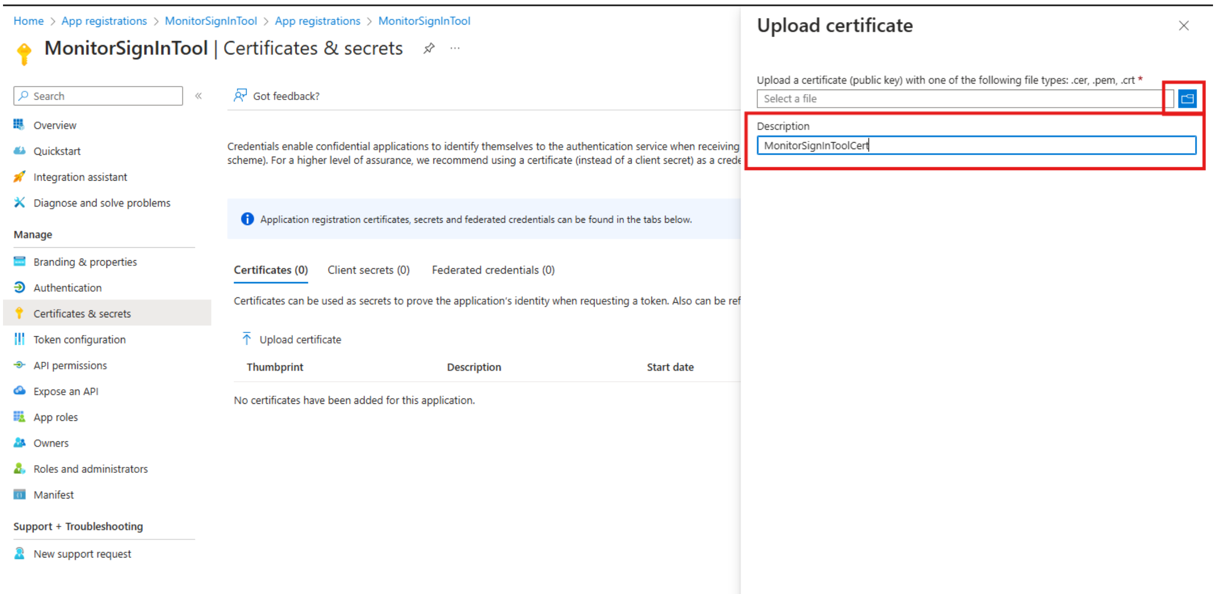
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
AuditLog.Read.All	Application	Read all audit log data	Yes	Not granted for Need 4 ...
Mail.Send	Application	Send mail as any user	Yes	Not granted for Need 4 ...
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

6. Now go to Certificates & Secrets, press Certificates and Upload certificate
   Give your certificate description and upload your public certificate from your endpoint
   PS: By default certificates validity is set to one year, this can be edited in CertCreator.ps1 script to for example 2 years. Remember to store your certificates in safe place and only allow authorized accounts to access them!



MonitorSignInTool | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a crede

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be ref

Thumbprint	Description	Start date

No certificates have been added for this application.

Upload certificate

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt *

Select a file

Description: MonitorSignInToolCert

7. When your certificate is uploaded , copy paste your certificate Thumbprint and copy paste it in MonitorSignIn.ps1 config
8. Edit all values in MonitorSignIn.ps1 to match your environment

ClientId = "Your Client ID" - can be found in Application -> Overview -> Application (client) ID

CertificateThumbprint = "Your Certificate Thumbprint" – can be found in Application -> Certificates -> or when generating Certificate with CertCreator.ps1 window

TenantId = "Your Tenant ID" – can be found in Application -> Overview Directory (tenant) ID

SenderEmail = "Sender Email upn" – need at least to have Exchange Online P1 license assigned

RecipientEmail = "RecipientEmail(s) UPN(s)" – separate with commas if you more recipients, need at least to have Exchange Online P1 license assigned

MonitoredAccount = "Object ID of monitored account" - can be replaced with UPN

MonitoredAccountName = "UPN monitored account when using ObjectID" – this is necessary to edit if you are using ObjectID in MonitoredAccount value to get account name in email messages

TimeWindowMinutes = 60 – scope of signin log check, edit this to TimeWindowHours to use hours instead of minutes

StateFilePath = "C:\temp\SignInMonitor_state.json" - feel free to edit this path, this file stores processed sign-in ID's to avoid checking duplicate sign ins

}

# Log file path

$logFile = "C:\temp\MonitorSignIn_log.txt" - feel free to edit this path, this file log's every step in the script to make it possible to troubleshoot

Edit this values to match your environment !

9. Run MonitorSignIn.ps1 to install all necessary MS Graph modules and test the connection
10. Create task schedule on your endpoint to run this script every X minutes to check sign ins

General:

Name**:** Give your task an understandable name

Choose Run whether user is logged on or not

Check Run with highest priviligies

Configure for: Windows Server XXXX or Windows X

Triggers:

On a schedule

One time, Start XX.XX.XXXX at XX.XX.XX

Select repeat task every X minutes for a duration of Indefinitely or at your choose

Select **Enabled**

Actions:

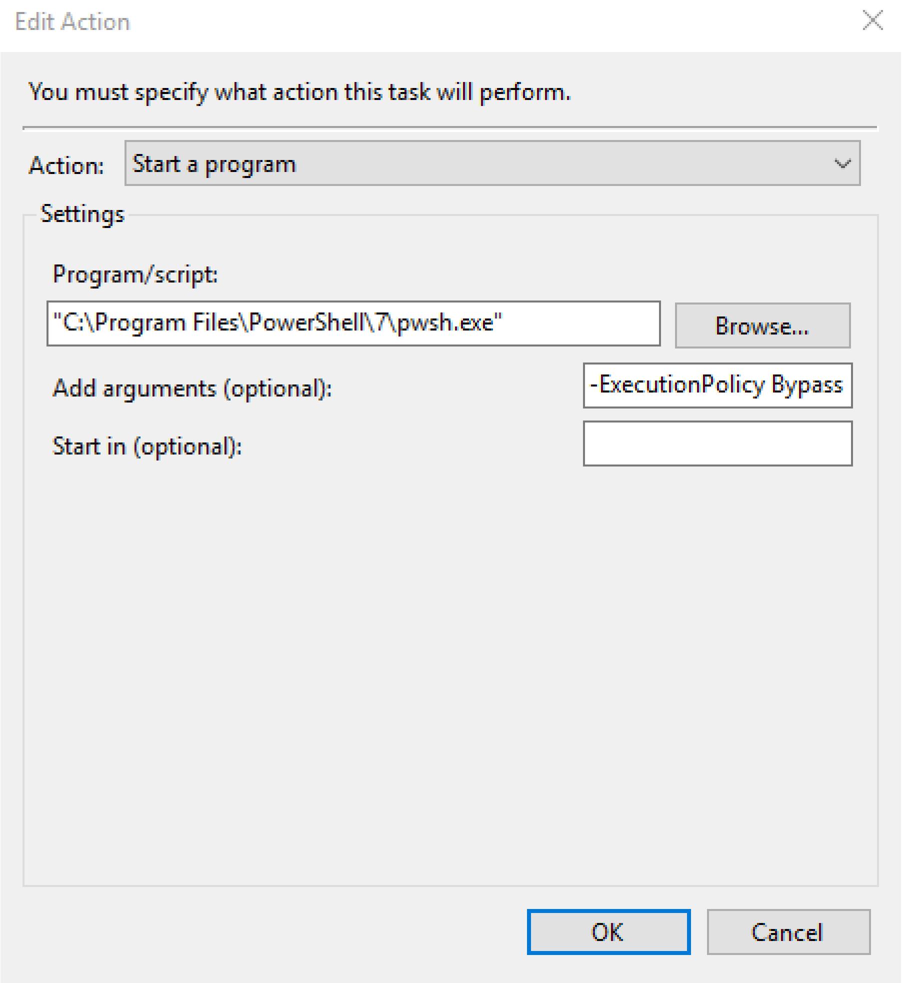
Action: Start a program

In Program/ Script: Find your path to Powershell 7 exe file which is pwsh.exe in Program Files, the default path should be

```
"C:\Program Files\PowerShell\7\pwsh.exe"
```

In Add arguments (optional): copy paste this path

```
-ExecutionPolicy Bypass -File "Your path\MonitorSignIn.ps1"
```



You must specify what action this task will perform.

Action: Start a program

Program/script: "C:\Program Files\PowerShell\7\pwsh.exe"

Add arguments (optional): -ExecutionPolicy Bypass

Start in (optional):

Conditions:

Uncheck: Start the task only if the computer is idle for

Uncheck: Start the task only if the computer is on AC power

Settings:

Check: Allow task to be run on demand

Check: Run task as soon as possible after as scheduled start is missed

Check: If task fails, restart every 1 minute

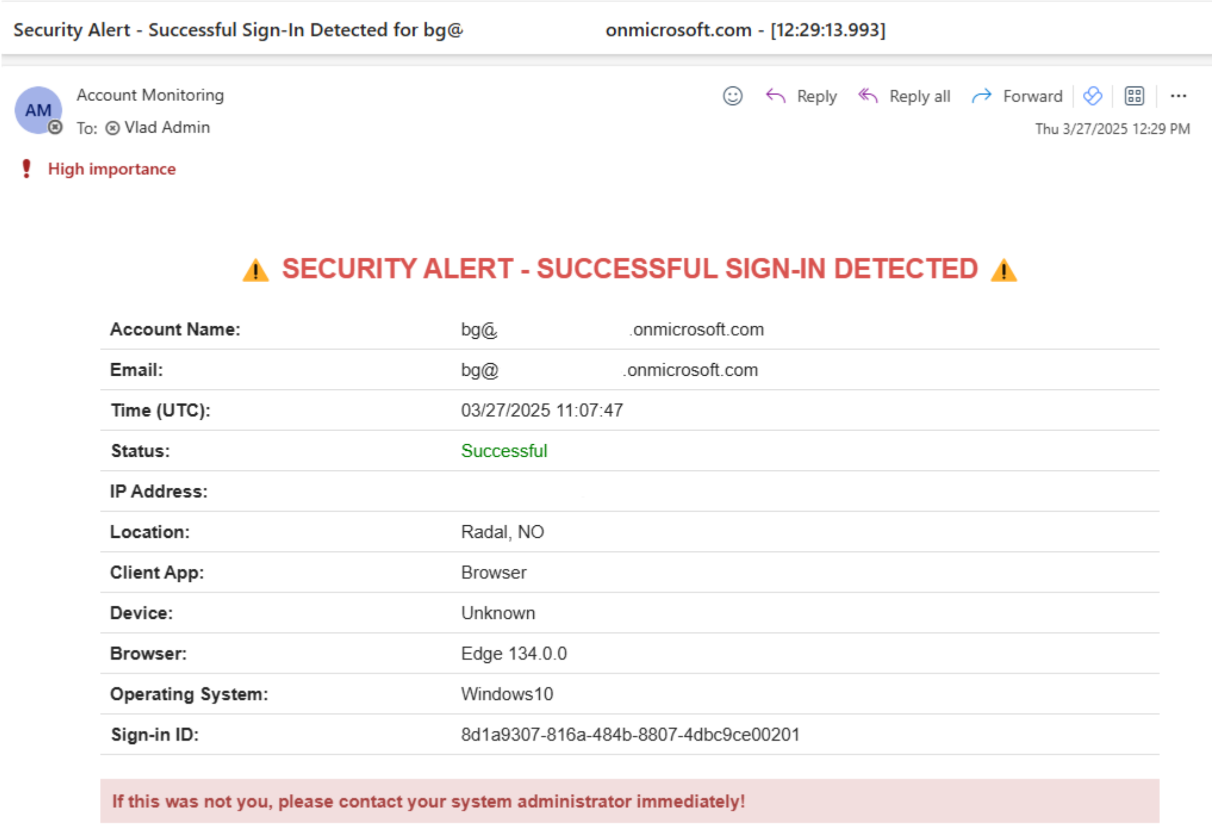
Now save everything and test with your account, sign in and see if your receive any email

There is 2 types of emails

1. Successful sign ins
2. Failed sign ins

You should get notified about both with 2 different mails templates

Successful



Security Alert - Successful Sign-In Detected for bg@ onmicrosoft.com - [12:29:13.993]

Account Monitoring

To: Vlad Admin

Thu 3/27/2025 12:29 PM

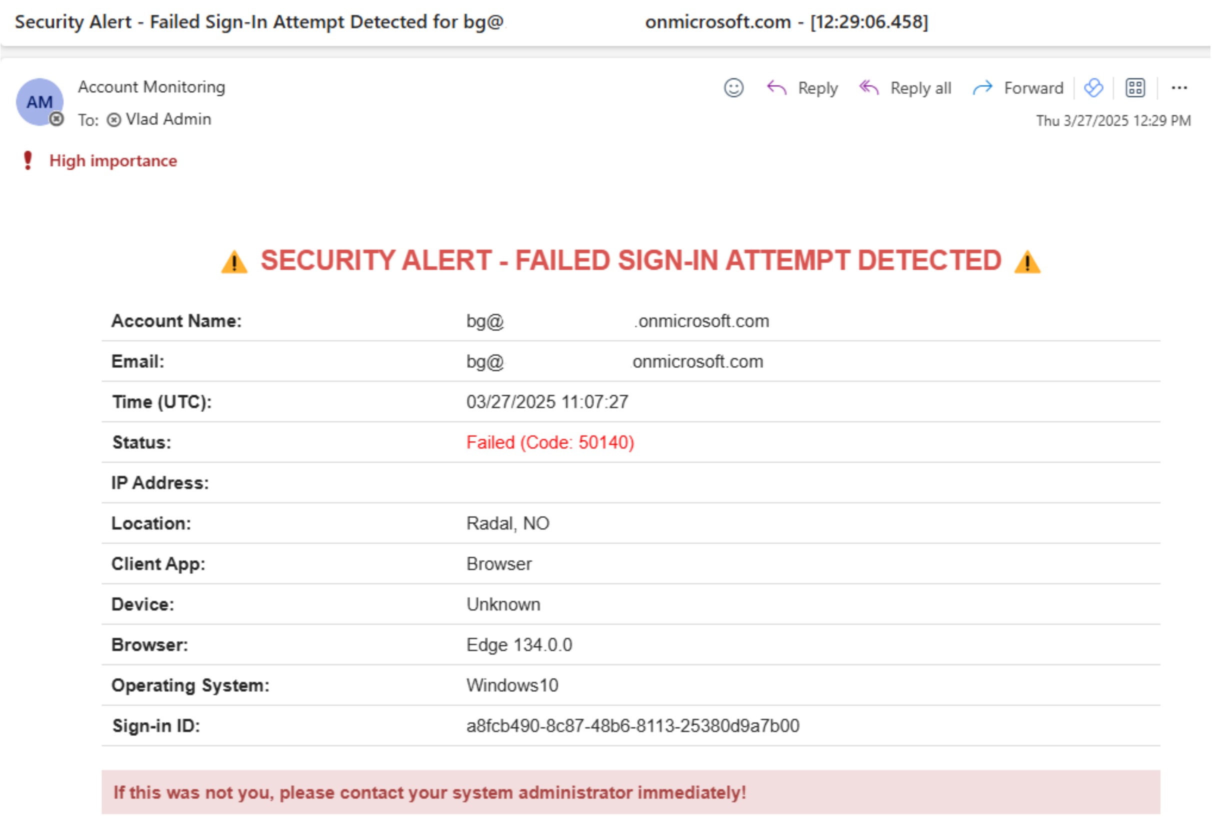
❗ High importance

⚠ SECURITY ALERT - SUCCESSFUL SIGN-IN DETECTED ⚠

Account Name:	bg@ .onmicrosoft.com
Email:	bg@ .onmicrosoft.com
Time (UTC):	03/27/2025 11:07:47
Status:	Successful
IP Address:	
Location:	Radal, NO
Client App:	Browser
Device:	Unknown
Browser:	Edge 134.0.0
Operating System:	Windows10
Sign-in ID:	8d1a9307-816a-484b-8807-4dbc9ce00201

If this was not you, please contact your system administrator immediately!

Failed



Security Alert - Failed Sign-In Attempt Detected for bg@ onmicrosoft.com - [12:29:06.458]

Account Monitoring

To: Vlad Admin

Thu 3/27/2025 12:29 PM

❗ High importance

⚠ SECURITY ALERT - FAILED SIGN-IN ATTEMPT DETECTED ⚠

Account Name:	bg@ .onmicrosoft.com
Email:	bg@ onmicrosoft.com
Time (UTC):	03/27/2025 11:07:27
Status:	Failed (Code: 50140)
IP Address:	
Location:	Radal, NO
Client App:	Browser
Device:	Unknown
Browser:	Edge 134.0.0
Operating System:	Windows10
Sign-in ID:	a8fcb490-8c87-48b6-8113-25380d9a7b00

If this was not you, please contact your system administrator immediately!