FWMON - ABOUT AND HOW TO START USING

The fwmon.ps1 powerShell script allows to monitor Windows OS network activity in real-time or retrieve data for a custom period. This script does not intercept traffic; instead, it displays network activities of applications and OS modules by protocols such as TCP, UDP, ICMP, etc., at the edge of the Windows Firewall and external networks.

The script is compatible with both server and desktop versions of Windows that have PowerShell version 5.1 onboard. Compatibility with later versions of PowerShell has not been tested yet.

The script's operation principle is based on real-time or on-demand reading of Windows Security log events related to Windows Firewall operations and presenting them to the user, either in the script console or in a text or Excel file. These events are not logged by default. To ensure the script works properly, you must perform some preparations, such as enabling Windows Firewall event logging and granting the user account running the script the right to read Security log events.

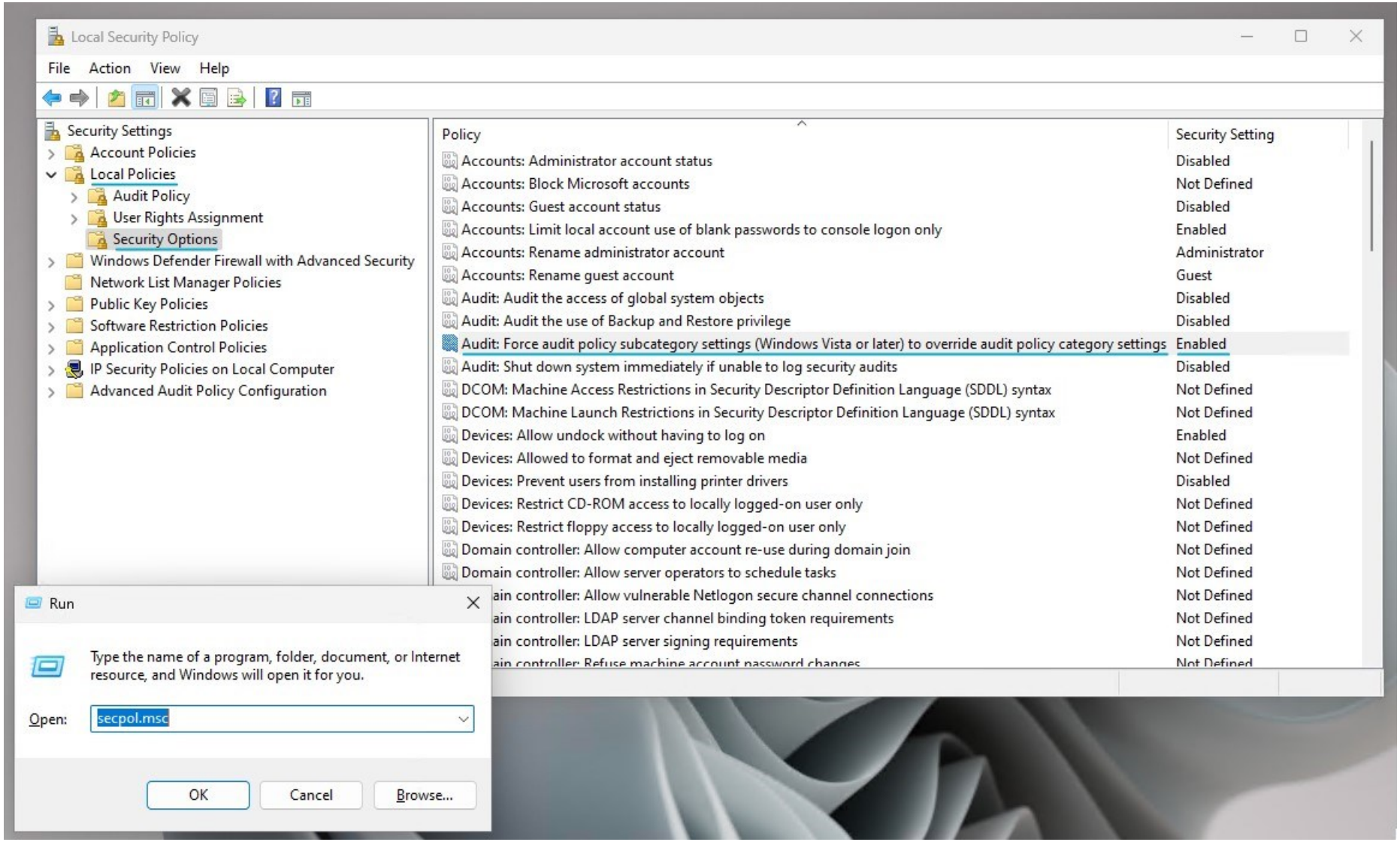
Automatic configuration:

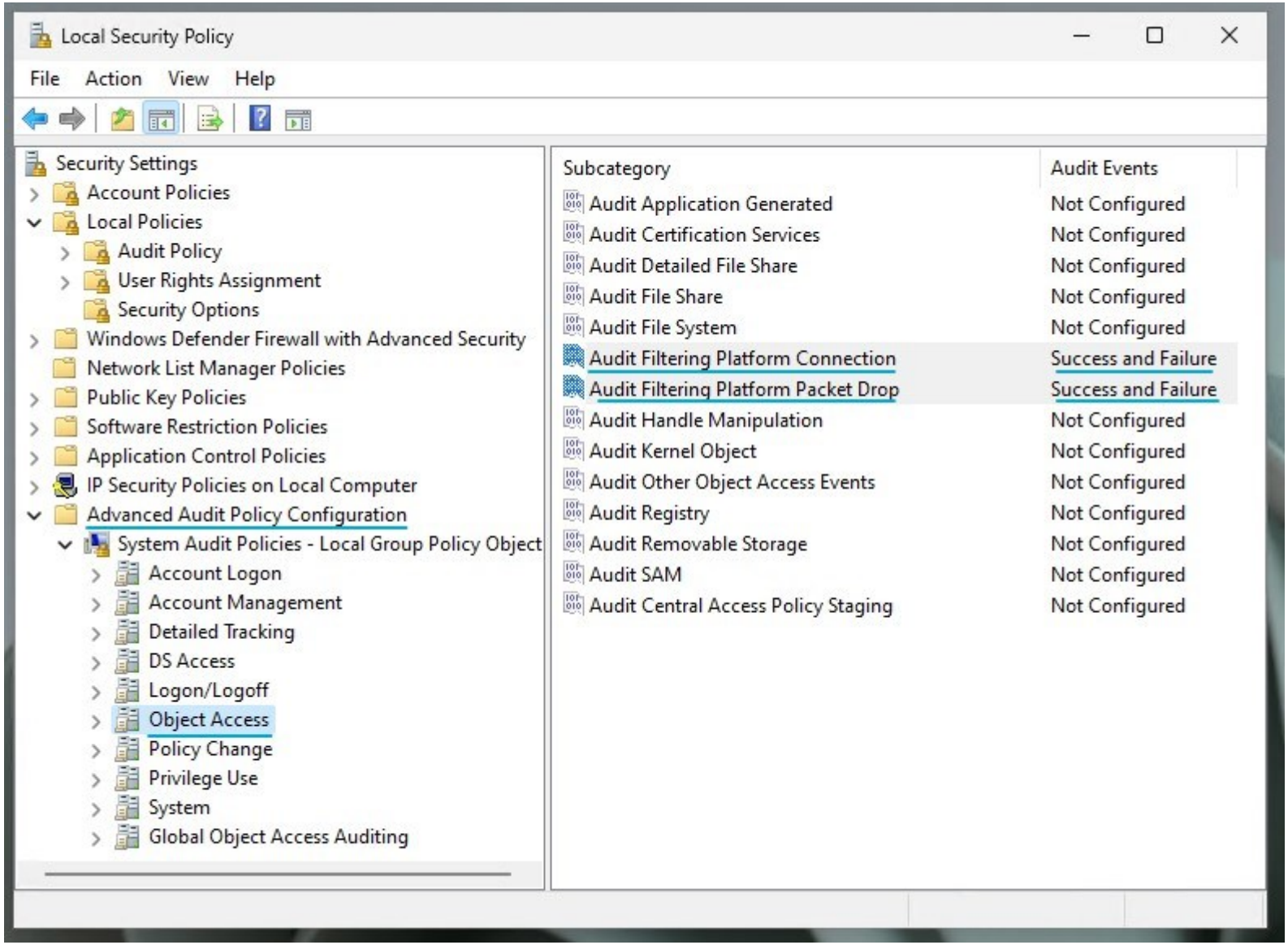
The automatic option is the only one available for Desktop versions of Windows with editions below Professional, such as Home and Starter. To enable it, run the file PrepOS.cmd with administrative rights; you can find it in a subdirectory with the same name. After executing the file, you must log out and log in again.

On advanced Windows Desktop Editions and Windows Server, the file PrepOS.cmd also configures the necessary settings automatically. However, you have another option to configure all settings manually to comply with your internal security policies. The section below describes the sequence of steps for manual operating system configuration.

Changing the settings manually

Launch the Local Security Policy MMC and configure the OS settings according to the screenshots below:





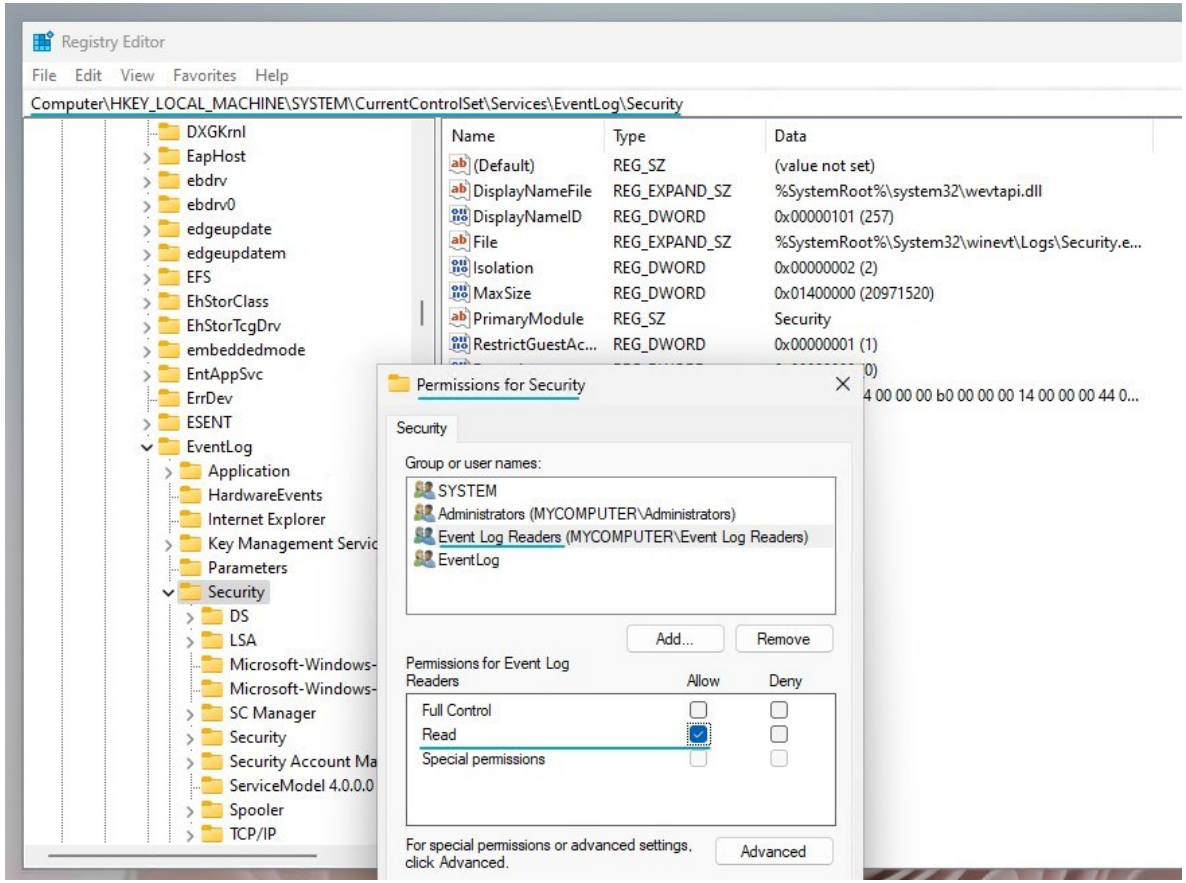
When finished, close MMC and run at elevated command prompt local computer policy update:

```
gpupdate /target:computer /force
```

Start with administrative rights Registry Editor.

Navigate to registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security

Change its permissions, add local security group "Event Log Readers" with READ permission as shown in the screenshot.



Include your own account in the "Event Log Readers" group with elevated cmd command:

```
net localgroup "Event Log Readers" %USERNAME% /add
```

Log out and log in again.

That's it, it's time to run fwmon.ps1. Enjoy!

THE END OF DOCUMENT