Instructions on how to activate the Sysmon tool on Windows 11

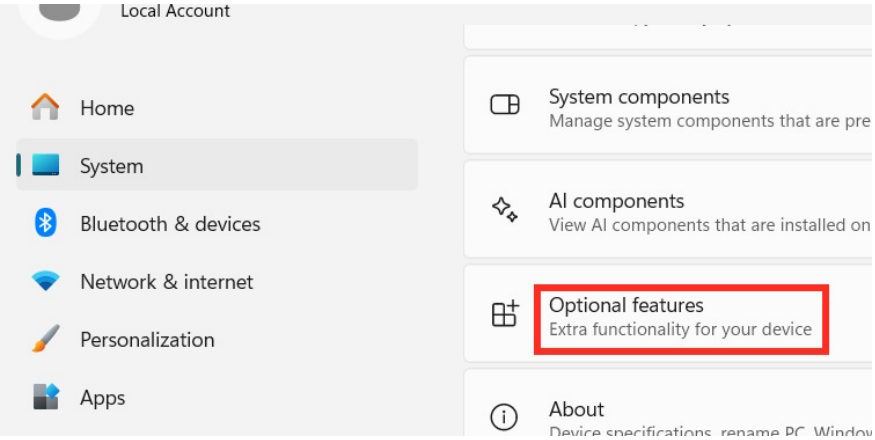
Sysmon helps administrators monitor processes, network connections, file changes, and other events to check for suspicious activity. Below are instructions on how to enable Sysmon on Windows 11.

Sysmon (System Monitor) is a powerful system monitoring utility that records detailed system activity and stores it in the Windows Event Log. Sysmon helps administrators monitor processes, network connections, file changes, and other events to check for suspicious activity. Below are instructions on how to activate Sysmon on Windows 11.

How to activate Sysmon via Windows 11 Settings

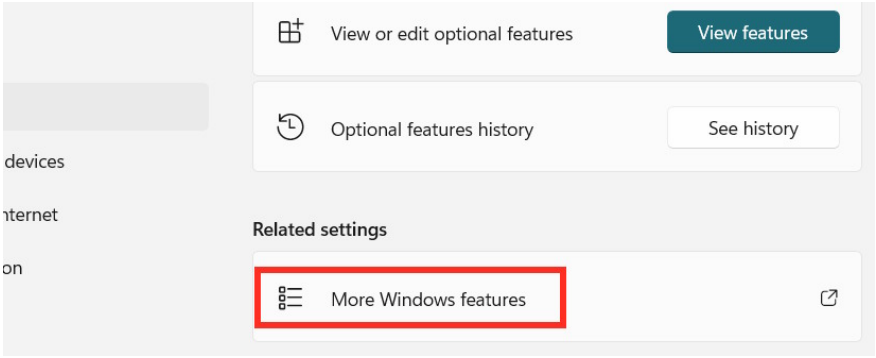
Step 1:

We open Settings, then **select System** , and then look to the side **and select Optional features** .

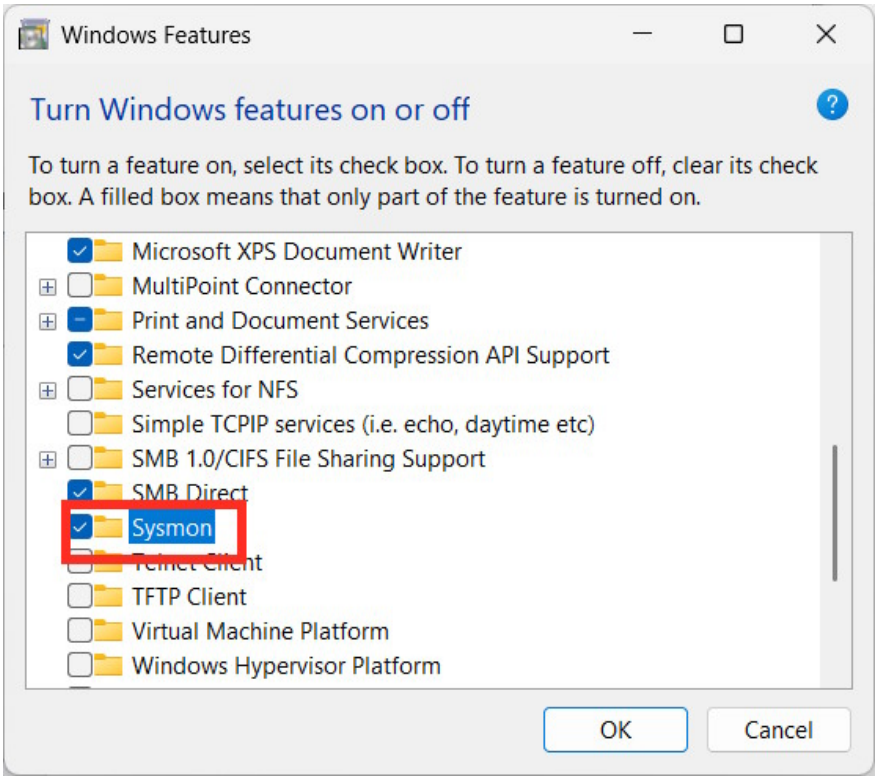


Step 2:

On the new interface, users **select "More Windows features"** to unlock more computer features.



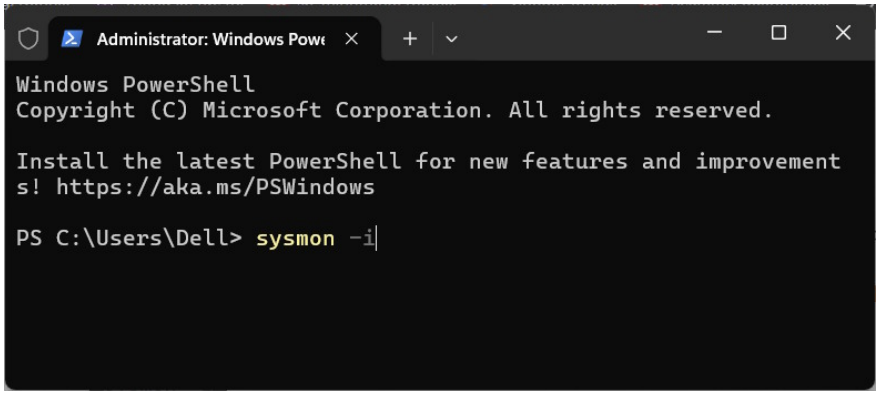
Then you will see new features for your computer; you need to **check the Sysmon box** to activate them.



Step 3:

After enabling the feature through Settings, you need to complete the installation process. **Open Terminal with administrator privileges** and then enter the command below.

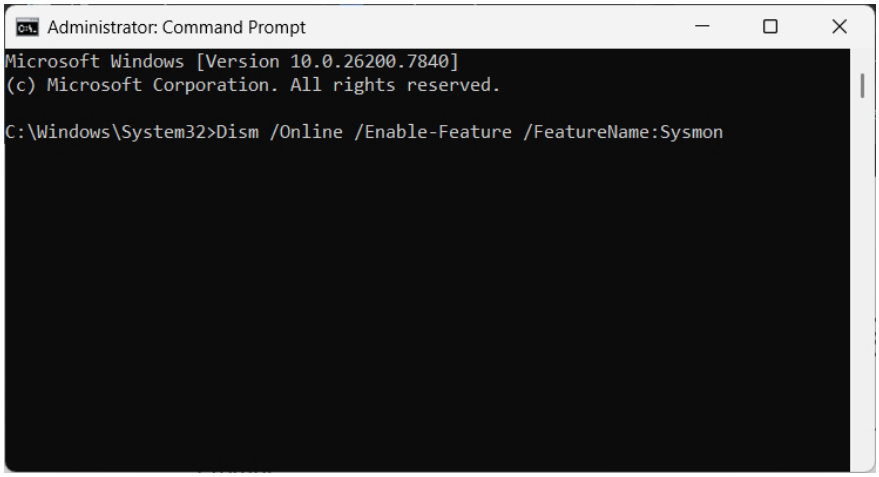
```
sysmon -i
```



Activate Sysmon via Command Prompt

First, we'll **open Command Prompt with the "Run as administrator" option** . Then, to enable this feature, enter the command below.

```
Dism /Online /Enable-Feature /FeatureName:Sysmon
```



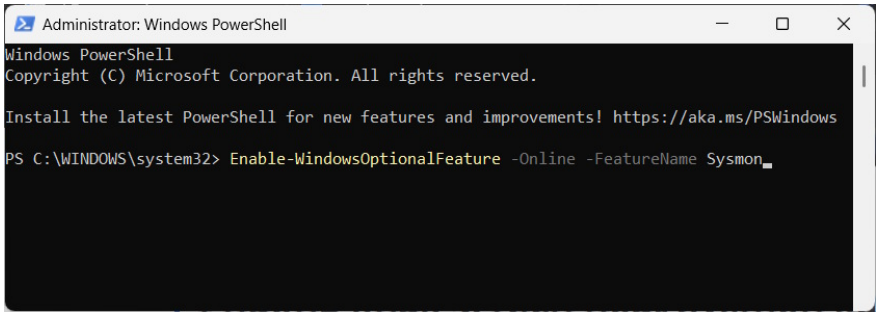
After you see the activation notification, enter **the following command** to install Sysmon on your computer.

```
sysmon -i
```

Activate Sysmon using PowerShell

We also **open Windows PowerShell with administrator privileges** and then enter the command below to activate it.

```
Enable-WindowsOptionalFeature -Online -FeatureName Sysmon
```



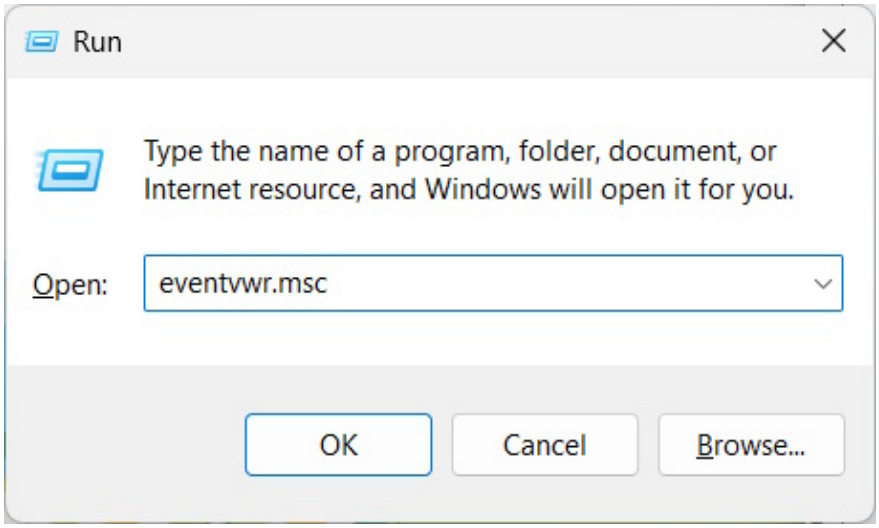
After successful activation, enter the command below to proceed with the installation.

```
sysmon -i
```

How to check if Sysmon is working.

After activating and configuring Sysmon, you can check if the tool is working correctly.

We **open the Run dialog box, then type eventvwr.msc** and press OK.



Then access the link below.

Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

If you see the events displayed in this interface, it means the Sysmon tool has been successfully activated.

You finished reading the article "**Instructions on how to activate the Sysmon tool on Windows 11**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.