Configure Microsoft SpyNet Reporting

Adjusts membership in Microsoft SpyNet.

Microsoft SpyNet is the online community that helps you choose how to respond to potential spyware threats. The community also helps stop the spread of new spyware infections.

Here's how it works. When Windows Defender detects software or changes by software not yet classified for risks, you see how other members responded to the alert. In turn, the action you apply help other members choose how to respond. Your actions also help Microsoft choose which software to investigate for potential threats. You can choose to send basic or additional information about detected software. Additional information helps improve how Windows Defender works. It can include, for example, the location of detected items on your computer if harmful software has been removed. Windows Defender will automatically collect and send the information.

If you enable this policy setting and choose "No Membership" from the drop-down list, SpyNet membership will be disabled. At this setting, no information will be sent to Microsoft. You will not be alerted if Windows Defender detects unclassified software running on your computer. Local users will not be able to change their SpyNet membership.

If you enable this policy setting and choose "Basic" from the drop-down list, SpyNet membership is set to "Basic". At this setting, basic information about the detected items and the actions you apply will be shared with the online community. You will not be alerted if Windows Defender detects software that has not yet been classified for risks.

If you enable this policy setting and choose "Advanced" from the drop-down list, SpyNet membership is set to "Advanced". At this setting, you send your choices and additional information about detected items. You are alerted so you can take action when Windows Defender detects changes to your computer by unclassified software. Your decisions to allow or block changes help Microsoft create new definitions for Windows Defender and better detect harmful software. In some instances, personal information may be sent but no information is used to contact you.

If you disable or do not configure this policy setting, by default SpyNet membership is disabled. At this setting, no information will be sent to Microsoft. You will not be alerted if Windows Defender detects unclassified software running on your computer. Local users will still be able to change their SpyNet membership.

Supported on: At least Windows Vista

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows Defender\SpyNet
Value Name	SpyNetReporting
Value Type	REG_DWORD
Enabled Value	1
Disabled Value	0

Microsoft SpyNet Membership

0. No Membership

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows Defender\SpyNet
Value Name	SpyNetReporting
Value Type	REG_DWORD
Value	0

1. Basic

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows Defender\SpyNet
Value Name	SpyNetReporting
Value Type	REG_DWORD
Value	1

2. Advanced

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows Defender\SpyNet
Value Name	SpyNetReporting
Value Type	REG_DWORD

Value	2

windowsdefender.admx

Administrative Templates (Computers)

- Control Panel
- Network
- Printers
- System
- Windows Components
  - Active Directory Federation Services
  - ActiveX Installer Service
  - Add features to Windows 8.1
  - Application Compatibility
  - AutoPlay Policies
  - Backup
  - Biometrics
  - BitLocker Drive Encryption
  - Credential User Interface
  - Desktop Gadgets
  - Desktop Window Manager
  - Digital Locker
  - Event Forwarding
  - Event Log Service
  - Event Viewer
  - Game Explorer
  - HomeGroup
  - Internet Explorer
  - Internet Information Services
  - Location and Sensors
  - NetMeeting
  - Network Access Protection
  - Network Projector

- Online Assistance
- Parental Controls
- Password Synchronization
- Presentation Settings
- Remote Desktop Services
- RSS Feeds
- Search
- Security Center
- Server for NIS
- Shutdown Options
- Smart Card
- Sound Recorder
- Tablet PC
- Task Scheduler
- Windows Calendar
- Windows Color System
- Windows Customer Experience Improvement Program
- Windows Defender
  - Check for New Signatures Before Scheduled Scans
  - Configure Microsoft SpyNet Reporting
  - Turn off Real-Time Monitoring
  - Turn off Routinely Taking Action
  - Turn off Windows Defender
  - Turn on definition updates through both WSUS and the Microsoft Malware Protection Center
  - Turn on definition updates through both WSUS and Windows Update
- Windows Error Reporting
- Windows Explorer
- Windows Installer
- Windows Logon Options
- Windows Mail
- Windows Media Center
- Windows Media Digital Rights Management
- Windows Media Player
- Windows Messenger
- Windows Mobility Center
- Windows Reliability Analysis

- Windows Remote Management (WinRM)
- Windows Remote Shell
- Windows SideShow
- Windows System Resource Manager
- Windows Update

Administrative Templates (Users)

- Control Panel
- Desktop
- Network
- Shared Folders
- Start Menu and Taskbar
- System
- Windows Components