



TechNet Home > Windows Vista Home > Technical Library > Security and Protection > Windows Defender

Search TechNet

TechCenters | Downloads | TechNet Program | Subscriptions | My TechNet | Sec

Windows Vista Home

Product Information

Technical Library

- Product Evaluation
- Planning & Architecture
- Deployment
- Security & Protection
- Management & Operations

Downloads

Learning

Community

Events & Webcasts

Scripting for Windows Vista

Windows Defender (Beta 2) Guide

Windows Defender Solution

Windows Defender Beta 2 is a free application that helps you stay productive by protecting your computer against pop-up windows, slow performance, and security threats caused by spyware and other potentially unwanted software. The application provides advanced system scanning and spyware removal technologies that simplify the removal of spyware existing on a system. Real-time protection helps prevent new spyware from installing while a streamlined alert mechanism minimizes interruptions. To help you make informed removal decisions, Microsoft analysts provide relevant information and guidance with each alert. From installation to maintenance, Windows Defender is easy to use and comes with pre-configured settings designed to help ensure security.

[Top of page](#)

Thorough Spyware Scanning and Removal

Windows Defender helps users detect and remove known spyware and other potentially unwanted software. To help automate spyware protection, Windows Defender includes automatic scanning options to provide regular spyware scanning in addition to on-demand scanning options. The spyware scan functionality has three options for detecting spyware including:

- **Quick Scan.** A quick scan rapidly checks the places on a hard disk that spyware is most likely to infect.
- **Full Scan.** A full scan will check all files on a hard disk, the registry, all currently running applications, and all other critical areas of the operating system.
- **Custom Scan.** A custom scan enables users to scan the drives and folders selected after performing a quick scan.

Note Windows Defender identifies and removes spyware using a definition database that details the characteristics of all known spyware. Each definition, commonly known as a spyware signature, is unique to the individual spyware. The definition detail includes the names and paths of the files that the spyware installs and the changes made to critical sections of the operating system including the Windows registry. In addition, the definitions contain expert advice and information to help users make informed removal decisions. The definition database is continuously updated to keep up with current threats.

The spyware scan uses an updated spyware definition database to identify installed spyware on a computer, provide threat descriptions, and suggest appropriate actions. As seen in Figure 1, the detected spyware listed in the scan results includes a threat description and a suggested action to help users make informed spyware removal decisions. If you wish to modify the actions before applying them, you might do so by using the drop-down list box in the **Action** column of the items list. After reviewing the list, you can take action on the listed spyware by either clicking the **Remove All** button, or apply the suggested actions by clicking the **Apply Actions** button.

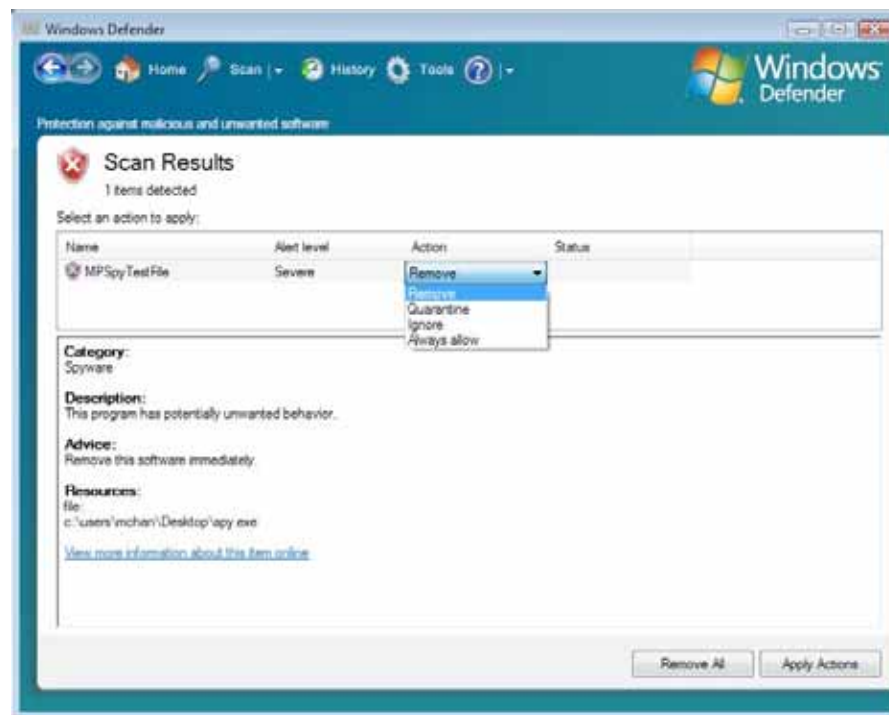


Figure 1 –Apply an action for each item

The available actions include:

- **Ignore.** Selecting **Ignore** will cause Windows Defender to not take immediate action, but the next scan will detect the item again.
- **Quarantine.** By placing an item in quarantine, you can test the item removal before deleting it from the system. After testing the removal, you can easily remove or restore the item from its quarantined state.
- **Remove.** This action removes the item from the system.
- **Always allow.** This action will stop Windows Defender from detecting the item in future scans by adding it to the **Allowed items** list. You can remove item from the **Allowed items** list at any time.

Windows Defender automates the removal process after an automatic scan by taking the default recommended action for all items detected. You can modify the default actions in the general settings to customize the automatic removal process. Windows Defender lists all other items as scan results on the Home Page to handle at your discretion.

[↑ Top of page](#)

Continuous Spyware Protection

Scanning and removal of known spyware that is already on your computer can help clean your system, but it will not keep new spyware from installing. To help protect you from new threats and even unknown threats, Windows Defender offers real-time protection using monitoring agents. These nine security agents monitor critical areas of your computer that spyware might attempt to modify. The agents monitor:

- **Auto Start.** This agent monitors the list of applications that you allow to run automatically when you start your computer. Spyware and other potentially unwanted software can be set to run automatically when Windows starts. That way, spyware can run without your knowledge and collect information. Spyware in your startup list can also make your computer start or run slowly.
- **System Configuration.** This agent monitors security-related settings in Windows. Spyware and other potentially unwanted software can change hardware and software security settings to collect information and use it to undermine your computer security further.
- **Internet Explorer Add-ons.** This agent monitors applications that automatically run when you start Internet Explorer. Spyware and other potentially unwanted software can masquerade as web browser add-ons and run without your knowledge.
- **Internet Explorer Configurations.** This agent monitors browser security settings, which are your first line of defense against harmful content on the Internet. Spyware and other potentially unwanted software can try to change these settings without your knowledge.
- **Internet Explorer Downloads.** This agent monitors files and applications designed to work with Internet Explorer, such as ActiveX controls and software installation applications. The browser can download, install, or run these files by itself. Spyware and other potentially unwanted software can be included with these files and be installed without your knowledge.
- **Services and Drivers.** This agent monitors services and drivers as they interact with Windows and your applications. Because services and drivers perform essential computer functions, such as allowing devices to work with your computer, they have access to important software in the operating system. Spyware and other potentially unwanted software can use services and drivers to gain access to your computer or to try to run undetected on your computer like normal operating system components.
- **Application Execution.** This agent monitors application execution activity and any operations they perform while running. Spyware and other potentially unwanted software can use vulnerabilities in applications that you have installed to run harmful or unwanted software without your knowledge. For example, spyware can run itself in the background when you start a frequently used application. Windows Defender monitors your applications and alerts you if it detects suspicious activity.
- **Application Registration.** This agent monitors tools and files in the operating system where applications can register to run at any time, not just when you start Windows or another application. Spyware and other potentially unwanted software can register an application to start without notice and run, for example, at a scheduled time each day. This allows the application to collect information about you or your computer or gain access to important software in the operating system without your knowledge.
- **Windows Add-ons.** This agent monitors add-on applications, also known as software utilities, for Windows. Add-ons enhance your computing experience in areas such as security, browsing, productivity, and multi-media. However, add-ons can also install applications that will collect information about you or your online activities and expose sensitive, personal information, often to advertisers.

These critical areas of the computer that the agents monitor represent the common entry points for spyware or potentially unwanted software. Typically, spyware will need to modify one of these areas in order to automatically start or monitor actions of the customer without proper consent. If any changes occur to these areas, Windows Defender will notify you with relevant information and options for appropriate actions. If a critical change triggers real-time protection, Windows Defender will enable you to allow or block those actions. This continuous protection can even detect and block unknown spyware ensuring that your computer stays safe.

[↑ Top of page](#)

Minimal Effort to Manage

Microsoft designed Windows Defender to require minimal effort to manage. It installs pre-configured to the optimal settings for a typical user. These settings automate the nightly spyware scanning and removal of high alert items, the downloading of spyware definition updates, and turns on real-time protection. The streamlined alert mechanism minimizes interruptions by limiting pop-up alerts to priority alerts, and consolidates multiple alerts to a single pop-up window. Windows Defender lists minor alerts in the scan results list on the Home page to handle at your discretion. Each alert item provides relevant information, expert guidance, and options that you can activate with a single click.

Pre-configured settings

To simplify the installation procedure, Windows Defender is pre-configured with optimal settings for detecting and removing spyware, eliminating any guesswork. However, if you are an advanced user, you can customize the general settings at any time. Some of the most important pre-configured settings provide:

- **Automated nightly scan.** By default, Windows Defender schedules a nightly scan of your computer at 2 A.M. The default configuration automatically downloads any new definitions before the scan and removes high alert items afterwards.
- **Real-time protection.** By default, real-time protection starts as soon as you install Windows Defender.
- **Automated spyware definition updates.** Because new or modified spyware is constantly emerging, anti-spyware software needs ongoing updates to combat the latest threats. At Microsoft, a dedicated spyware research team creates regular spyware definition updates for Windows Defender. By default, Windows Defender automatically downloads and installs the latest definitions nightly and before a scheduled scan to keep your protection up to date. Ongoing updates are available for no additional charge to Windows customers.

Minimized Alert Interruptions

Windows Defender alerts you when it detects suspicious behavior on a computer or discovers spyware during a regularly scheduled scan. To minimize interruptions, Windows Defender consolidates multiple alerts and adjusts its response to fit with the severity of the potential threat.

When innocuous changes occur, there is a small notification in the system tray. For moderate to severe threats, Windows Defender displays a yellow or red alert window as seen in Figure 2. From these alerts, you can take immediate action directly from the alert, or click **Review** to launch the user interface and get more information about the potential threat or threats detected. You can also pause over an item in the Alert window to get more information in a tool tip.

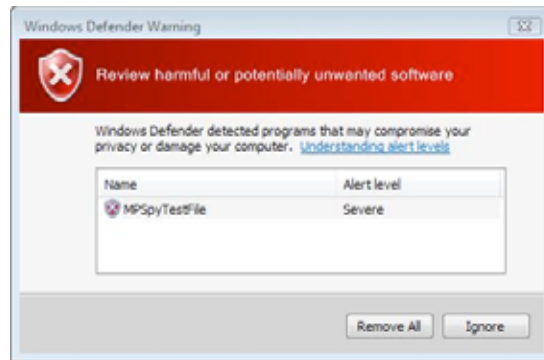


Figure 2 –Red Alert

Simplified Management

Windows Defender simplifies management by automating many of its services, minimizing required interactions, and simplifying the interaction process. To simplify the interaction process, Windows defender provides:

- **Single click access.** Windows Defender has a simple interface that does not bury its functionality. The toolbar across the top of every window enables single-click access to the five most important functions.
- **Simplified spyware removal process.** Scan results and real-time alerts list detected items that could potentially be spyware. To simplify the spyware removal process, Windows Defender provides:
 - **Default actions.** Every detected high threat item has a suggested resolution in the Action column that the Microsoft spyware research team determines to be the correct course of action. You can handle the removal process quickly and safely by applying these default actions.
 - **Actions taken directly from alerts.** To speed up the spyware removal process, the alerts provide actions that can be taken directly without requiring you to start the Windows Defender user interface.
 - **Relevant information and expert advice.** Every detected item provides relevant information about that item as well as expert advice on how to handle it. This allows advanced users to see the details before moving forward.

[Top of page](#)

Advanced User Options

Windows Defender provides you with visibility and control over your software. It provides visibility through the Software Explorer, scanning results, real-time protection alerts, event logs, and the history file. Windows Defender provides control by associating relevant information, guidance, and actionable choices to each item detected on your system. While the advanced user options are not necessary to keep your computer safe from spyware, they do enhance visibility and control.

Note Because you can prevent any software from installing itself on your system and any attempted changes made to critical settings, you are also protected from browser hijackings.

Software Explorer

To help you understand what software is currently running on your computer, automatically starting or communicating over the internet, Windows Defender has a feature called the Software Explorer. This feature lists applications in various categories including:

- **Startup Programs.** These applications run automatically with or without your knowledge when you start Windows.
- **Currently Running Programs.** These applications are currently running onscreen or in the background.
- **Network Connected Programs.** These applications or processes are currently connected to the Internet or to your home or office network.
- **Winsock Service Providers.** These applications perform low-level networking and communication services for Windows and applications that run on Windows. They often have access to important areas of the operating system.

The Software Explorer enables you to quickly discover and remove hidden or potentially unwanted applications that have been installed without your consent. It displays relevant information about each of these processes and provides options for stopping or disabling unwanted applications as seen in Figure 3 below.

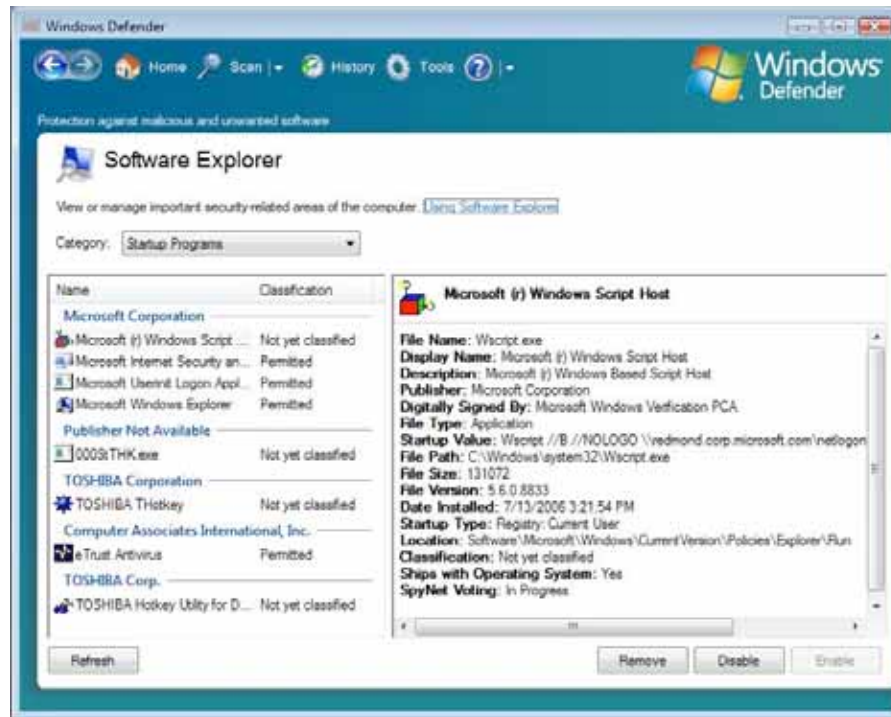


Figure 3 –Software Explorers

History

The History page displays the actions you have applied to spyware and other potentially unwanted software that Windows Defender has detected on your computer. The actions include Remove, Ignore, Always Allow, and Quarantine. The Always Allow and Quarantine actions list the items in other areas to be managed later. From the History page, you have access to:

- **Allowed Items.** If you trust the software that Windows Defender has detected, you can stop Windows Defender from alerting you to the risks by selecting the Always Allow action. This action lists these items on the Allowed Items page where they remain until removed. Removing a particular item from the Allowed Items list triggers Windows Defender to resume detection of this item.
- **Quarantined Items.** When Windows Defender quarantines software, it moves it to another location on your computer, and then prevents the software from running until you choose to restore it or remove it from your computer. This allows you to test the removal process before permanently removing the item from your computer.

Note History does not display the date, time, and details of every scan. It only lists information about the actions you have taken on the threats found.

Logged Events

Whenever Windows Defender takes a specific action like detecting or removing spyware, or when installing new definition updates, Windows Defender creates a new event in the Windows event log. As seen in Figure 4, the logs are located in the System Event folder with WinDefend as its source. You can review or audit previous actions later by searching for events created by Windows Defender in the Event Viewer.

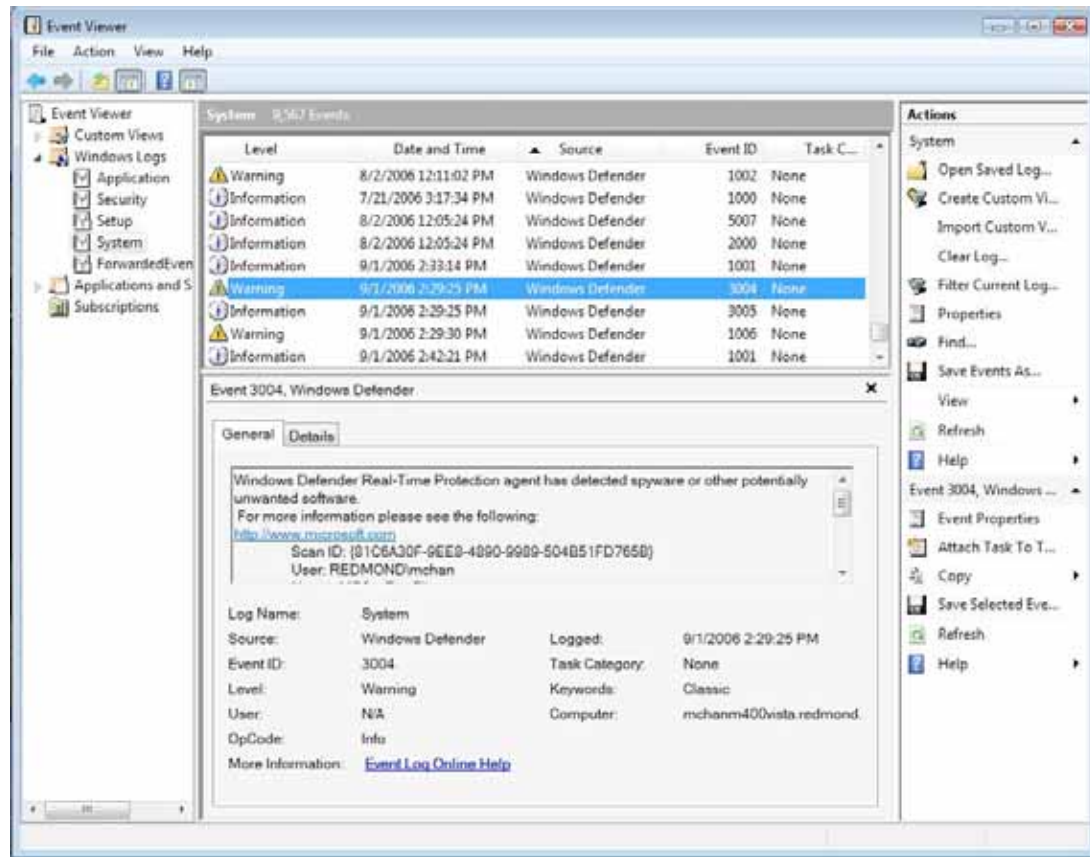


Figure 4 --Windows Defender Logged Events

SpyNet™ community

The Microsoft spyware research team bases the definitions they create on internal research as well as feedback from the SpyNet™ community. SpyNet is the voluntary worldwide community of Windows Defender users that helps determine which applications the research team classifies as spyware. Users participating in the SpyNet™ network help to discover new threats more quickly so all users are better protected.

Any user can choose to participate in SpyNet when they first install Windows Defender or later in the Microsoft SpyNet page from the tool options. Customers join on an opt-in basis and can select from one of three levels including:

- **Advanced Member.** Advanced participants always send a full report, even if personally identifiable information is present in the report. Advanced participants will also be alerted of unknown software that exhibits behaviors similar to spyware or potentially unwanted software.
- **Basic Member.** When basic members send spyware reports to Microsoft, their personally identifiable information is removed from the report. This can generate incomplete spyware reports.
- **Non Member.** If you choose not to be a member, no information will be sent to Microsoft.

[Top of page](#)

2 of 8

[Manage Your Profile](#)

© 2006 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Microsoft