# Microsoft Forefront Client Security Privacy Statement

Last updated: April 2007

At Microsoft®, we're working hard to protect your privacy while delivering products that bring you the performance, power, and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of Microsoft Forefront™ Client Security (“Client Security”). This statement focuses on features that communicate with the Internet and is not intended to be an exhaustive list. It does not apply to other online or offline Microsoft sites, products, or services.

Microsoft Forefront Client Security provides unified malware protection for business desktops, laptops and server operating systems. Forefront Client Security helps guard against emerging threats such as spyware and rootkits, as well as traditional threats such as viruses, worms, and Trojan horses by delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities. There are two parts to the Microsoft Forefront Client Security solution. The first is the Client Security agent—installed on business desktops, laptops and server operating systems—that provides real-time protection from and scheduled scanning for threats such as spyware, viruses, and rootkits. The second is the central management server, which enables administrators to easily manage and update preconfigured or customized malware protection agents and generate reports and alerts about the security status of their environment.

**Collection and use of your personal information**

When we need information that personally identifies you or allows us to contact you, we will explicitly ask you for it. The personal information that we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to provide the service(s) or carry out the transaction(s) you have requested or authorized, and it may also be used to request additional information on feedback that you provide about the product or service that you are using; to provide important notifications regarding the software; or to improve the product or service (for example, bug and survey form inquiries).

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as answering customer questions about products or services, or performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may disclose personal information about you if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site; (b) protect and defend the rights of Microsoft (including enforcing our agreements), or (c) act in urgent circumstances to protect the personal safety of Microsoft employees, users of Microsoft products or services, or members of the public.

Personal information collected by Microsoft software, sites, and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or agents maintain facilities. By using Microsoft software, sites or services, you consent to any such transfer of information outside of your country. Microsoft abides by the safe-harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union.

**Collection and use of information about your computer**

This software contains Internet-enabled features that collect certain standard information from your computer ("standard computer information") and send it to Microsoft. Standard computer information includes certain information about your computer software and hardware, such as your IP address, operating system, and Web browser. The privacy details for each Client Security feature listed in this privacy statement disclose what additional information is collected and how it is used.

**Security of your information**

Microsoft is committed to protecting the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we protect the content of the reports submitted to the SpyNet AntiSpyware Community through the use of server authentication and encryption, such as the Secure Socket Layer (SSL) protocol.

**For more information**

If you have questions about this privacy statement, please contact us by e-mail at spypriv@microsoft.com

SpyNet
Microsoft Corporation
One Microsoft Way, Redmond, Washington 98052

## Specific features

The remainder of this document will address the following specific features:

**Microsoft SpyNet**

**What this feature does:** The online Microsoft SpyNet community is a voluntary, worldwide community of users. Through Microsoft SpyNet, managed Client Security users can report spyware and other forms of potentially unwanted software to Microsoft at their administrators’ discretion. The Client Security group policy allows your administrator to configure if managed clients will send a report to Microsoft whenever Client Security detects a program or program component that demonstrates suspicious activity but is not currently in the definition library.

**Information collected, processed, or transmitted:** Microsoft SpyNet reports include information about the files or programs in question, such as the file names, cryptographic hash, vendor, size, and date stamps. In addition, full URLs can be collected to indicate the origin of the file, and might occasionally contain personal information such as search terms or data entered in forms. Reports can also include the actions that you applied when Client Security notified you that software was detected (deny or permit). Microsoft SpyNet reports include this information to help Microsoft gauge the effectiveness of Client Security in detecting and removing malicious and potentially unwanted software. Reports also contain standard computer information, and are automatically sent to Microsoft when:

* Client Security detects software or changes to your computer by software that has not yet been analyzed for risks.
* You apply actions to software that Client Security has detected.
* Client Security completes a scheduled scan and automatically applies actions to software that it detects, according to your settings.

Your administrator can choose to have managed clients join Microsoft SpyNet with a basic or an advanced membership. Basic member reports contain the information described above. Advanced member reports are more comprehensive and might occasionally contain personal information from, for example, file paths and partial memory dumps. These reports, along with reports from other users who are participating in Microsoft SpyNet, enable Microsoft researchers to discover new threats more rapidly. Spyware definitions are then created for programs that meet the analysis criteria and the updated definitions are made available to all users through Microsoft Update.

If your administrator has decided to have your managed client join Microsoft SpyNet, Microsoft might request a Sample Submission report. This report contains specific files from your computer that Microsoft suspects might be potentially unwanted software. The report is used for further analysis. You will be asked each time if you want to send a Sample Submission report to Microsoft unless your administrator has chosen to have these reports sent automatically without bothering you. To help protect your privacy, the information sent to Microsoft is encrypted using SSL.

To the extent that any personal information is included in a report, Microsoft does not use the information to identify you or contact you.

**Use of information:** Microsoft SpyNet reports are used to improve Microsoft software and services. The reports may also be used for statistical or other testing or analytical purposes, trending, and definition generation. Report access is limited to Microsoft employees, contractors, and vendors who have a business need to use them.

**Choice/control:** Your Client Security administrator configures the behavior of the managed clients, including whether or not the managed client will participate in the SpyNet community. Based on the Client Security policy settings set by your administrator, you may or may not be presented with a prompt to send reports to Microsoft.

**History**
**What this feature does:** This feature provides a list of all detected programs on your computer and what actions Client Security took when the programs were detected. In addition, you can view a list of Allowed items, which are programs that Client Security does not monitor while they are running on your computer, and Quarantined items, which are programs that Client Security prevents from running until you choose to remove them or allow them to run again.

**Information collected, processed, or transmitted:** The list of detected programs and the actions taken are stored on your computer. These lists include Client Security activity for all users and are available to all users of your computer. The lists are sent to Microsoft only if your administrator has decided to have your managed client participate in Microsoft SpyNet.

**Choice and control:** Youmay be able todelete the History lists if your administrator has decided to allow access to this feature.

**Definition Updates**:

**What this feature does:** Client Security uses Windows Server Update Services (WSUS) and/or Microsoft Update to deploy software updates and patches to managed clients. When checking for updates is enabled, Client Security will automatically check for new spyware and virus definitions and software updates hourly, and, when available, download them. When enabled, this feature helps keep Client Security up-to-date.

**Information collected, processed or transmitted:** If you or your administrator choose to enable automatic updates, your computer will periodically communicate with Microsoft servers to determine whether your version of Client Security has the most recent software updates and spyware and virus definitions. Standard computer information will be sent to Microsoft, together with information about your version of Client Security. For more details on what information is collected, see the WSUS privacy statement at <http://go.microsoft.com/fwlink/?LinkId=78929> and the Microsoft Update privacy statement at <http://go.microsoft.com/fwlink/?LinkId=78930>.

If you or your administrator has enabled automatic updates, updates will be downloaded and installed automatically

**Use of information:** The information sent to Microsoft is used to provide and improve the update service. For more details on how this information is used, see the WSUS privacy statement at <http://go.microsoft.com/fwlink/?LinkId=78929> and the Microsoft Update privacy statement at <http://go.microsoft.com/fwlink/?LinkId=78930>.

**Choice/control:** Use of Update Services is optional. Your administrator can configure how Client Security uses WSUS and Microsoft Update. You or your administrator may also choose to manually update your version of Client Security. For more information, see the Microsoft Forefront Client Security Deployment Guide at <http://go.microsoft.com/fwlink/?LinkID=59684>.