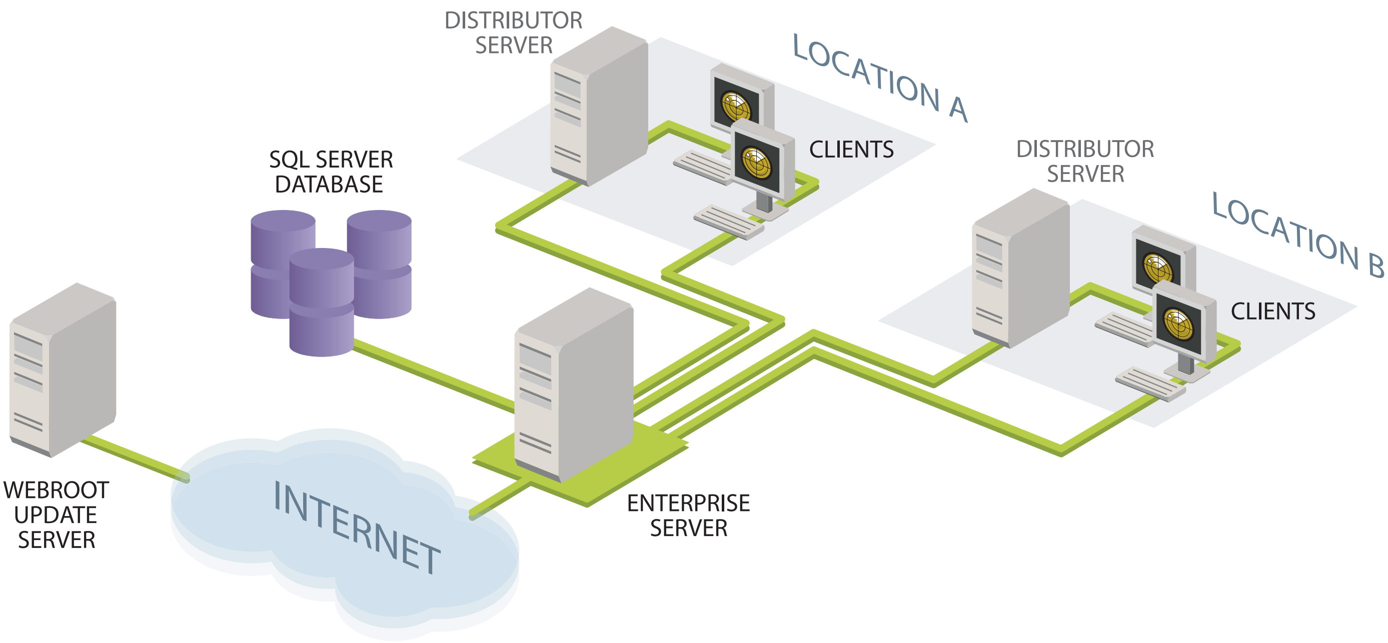
webroot® Spy Sweeper™ Enterprise

Technical Data Sheet

Completing the IT Security Solution

Webroot Spy Sweeper Enterprise is an award-winning, enterprise anti-spyware solution that provides centrally managed, desktop-level spyware protection. Offering the most thorough network-wide detection, removal and blocking of spyware available, Spy Sweeper Enterprise provides distributed spyware management using a client/server architecture. The optional deployment of distribution servers allow large organizations to balance the load of updating many clients quickly while also conserving the bandwidth of multi-site companies by distributing updates from servers located on the same LAN. Administrators have complete manual control over the system or the ability to configure for full autonomous operation.

The illustration below shows how Spy Sweeper Enterprise works in a network environment:



Comprehensive Removal Technology

The Webroot Comprehensive Removal Technology (CRT) is the backbone behind the most advanced spyware removal engine in the industry. CRT uses adaptive recognition practices to remove processes, applications or files that may have changed during the remediation process or may not have been previously detected.

This unique technology completely disables spyware programs detected on a system PC and sends them to quarantine, rendering them ineffective. Using CRT, Spy Sweeper Enterprise assures system stability during and after the spyware removal process.

Spy Sweeper Enterprise scans the client system using a constantly evolving database of hundreds of thousands of known spyware threats. If any files or traces of spyware match the definitions database, Spy Sweeper Enterprise immediately quarantines the identified threat and notifies the administrator.

Quarantining disables spyware functionality for immediate protection, while giving the administrator the option to review and permanently delete suspect files or safely restore them if they are essential to the operation of desirable applications. Desirable files that were sent to quarantine can be selected to "Always Keep" for specific users, groups or the entire enterprise.

webroot®

Spy Sweeper™ Enterprise

Technical Data Sheet

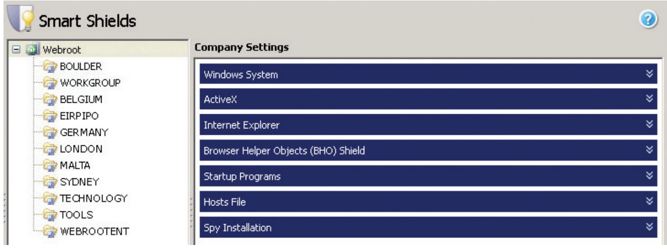
Webroot has combined its deep knowledge of spyware with years of research and development to create the most flexible, accurate and technically evolved detection, removal and blocking engine in the industry.

With increased capabilities, including the detection and removal of rootkit masked spyware, Spy Sweeper Enterprise removes and blocks the most persistent and powerful spyware programs today.

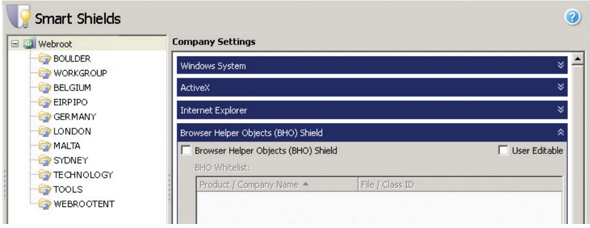
Malicious spyware programs can block certain windows API's in order to prevent removal from the operating system. To effectively remove these threats, Spy Sweeper Enterprise introduces kernel-level driver protection that allows for the deletion of files (locked or otherwise) directly off of the hard disk, bypassing the Windows system API's that are normally used to manage disk operations.

Advanced Proactive Protection

Spy Sweeper Enterprise provides Smart Shields that block spyware from installing and protects specific elements of the system that spyware attacks. The Startup, Spy Installation, Memory, Alternate Data Stream (ADS), ActiveX and Browser Helper Object (BHO) Shields block spyware before it can infect a protected workstation.



- The **Startup Shield** blocks spyware programs from writing critical registry keys for their operations. This shield is configurable to allow approved programs to be installed.
- The **Spy Installation Shield** detects spy processes trying to start and immediately terminates them. It also allows an administrator to block any unwanted executable (i.e. to stop unwanted game playing on the enterprise network) in addition to blocking spyware.
- The **Memory Shield** scans memory to catch spies that are currently loaded and terminates those processes.
- The **Alternate Data Stream Shield** prevents spies from executing from an alternate data stream. CoolWebSearch is known to exploit this vulnerability.
- The **ActiveX Shield** prevents the installation of any ActiveX components. This shield is configurable to allow for the installation of valid ActiveX components that an Administrator approves.
- The **Spy Communication Shield** blocks incoming and outgoing communication to malicious Web sites known to host potential spyware threats. This blocked list of URLs is updated via Webroot's daily definition releases.
- The **BHO Shield** stops the installation of unwanted toolbars that track Web site activities or install other add-ons without your consent. This shield is configurable to allow for the installation of valid BHOs that an administrator approves.



Additional Smart Shields in Spy Sweeper Enterprise defend critical areas from spyware attacks:

- The **IE Trusted Sites Shield** prevents spyware from modifying Internet Explorer's security zones settings.
- The **Messenger Shield** prevents spyware from exploiting the Windows Messenger service.
- The **Hosts File Shield** protects the hosts file from modifications by spyware.
- The **IE Hijack Shield** protects internal pages of Internet Explorer from spyware attacks.
- The **Favorites Shield** prevents spyware from adding unwanted favorites.
- The **Home Page Shield** protects the user's current home page or allows administrators to specify a corporate home page standard.
- The **Common Ad Sites/Blocked Web Sites Shield** prevents access to sites that are known to deliver spyware or advertisements from spyware. This list is updated in every definition file. Users also have the ability to add custom sites they wish to block.

Advanced Spyware Detection and Control

The **Spy Sweeper Enterprise Server** runs within the network to manage the enterprise clients. The features of the Enterprise Server are described below:

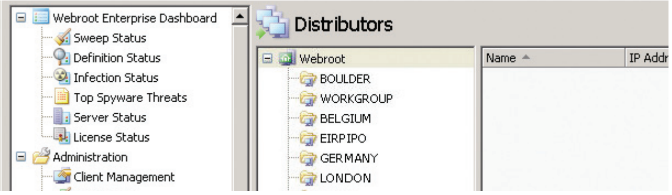
The **Admin Console** is Web-based and enables multiple simultaneous administrators with full audit logging of all user actions. The Admin Console is accessible from any Internet connected PC and provides the interface for configuring clients, managing updates, establishing alerts, viewing reports, and performing real-time scans of remote systems.

The **Database** stores the settings from the Admin Console. The database collects information from spyware sweeps as well as from the update and client services. Spy Sweeper Enterprise supports the use of a MS SQL Server (2000 and 2005) or MS SQL Server Express 2005 database.

The **Update Service** checks the Webroot Update Server for updates to software or threat definitions. This runs automatically on a scheduled basis without requiring any user interaction to ensure the latest updates are available. The update service can also be invoked from the Admin Console to manually check for updates. If distributed update servers are deployed, updates are automatically moved to local distribution servers. When a client polls for an update, it obtains a list of local distributors and will retrieve the update from one of the available local distributor servers.

The **Client Service** responds to client polling requests to receive results as well as to provide configuration settings and updates back to the clients. This component runs automatically to ensure that clients get the latest settings, software and definitions regardless of when clients are on the network.

The **Webroot Update Distribution Service** delivers software and threat definition updates to clients. This service runs on any Distributor Servers that may be installed throughout the enterprise to balance load and minimize WAN bandwidth consumption.



The **Spy Sweeper Enterprise Client** runs on user workstations and laptops. The client contains three major components deployed in a single installation:

The **Spy Sweeper Enterprise User Interface** provides access to a graphical user interface for end users to interact with the Spy Sweeper Enterprise service. The client can be deployed invisibly to end users, and provides user control over specific settings or runs in administrative mode with full control for advanced users.

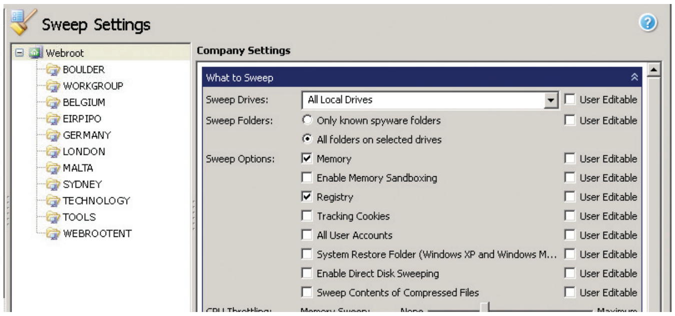
The **Spy Sweeper Service** does thorough sweeps of the system and uses proactive shields to protect against spies and their attacks. This component operates automatically so that scheduled sweeps or on-demand sweeps will run even when users are not logged into the system.

The **CommAgent Service** handles communication with the Client Service running on the Enterprise Server. It checks for configuration changes or updates as well as delivers client sweep results back to the server.

Client Management

Remote and Laptop Users

Spy Sweeper Enterprise maintains the enforcement of administrator-set policies for laptop and remote users while they are away from the network. When logged into the network, laptop and remote user machines automatically check with the Spy Sweeper Enterprise Server to download new definitions or product updates and send reports of spyware detected since last logging into the network. Additionally, the remote client sends report information, such as spyware detected and previous sweep date and time, which allows IT administrators to maintain accurate reporting capabilities. While disconnected from the network, laptop and remote users may be configured to check the Webroot Update Server directly so that they continue to receive the most up-to-date protection from spyware threats.



Sweep Drives: All Local Drives □ User Editable
Sweep Folders: ○ Only known spyware folders □ User Editable
● All folders on selected drives
Sweep Options: ☑ Memory □ User Editable
□ Enable Memory Sandboxing □ User Editable
☑ Registry □ User Editable
□ Tracking Cookies □ User Editable
□ All User Accounts □ User Editable
□ System Restore Folder (Windows XP and Windows M... □ User Editable
□ Enable Direct Disk Sweeping □ User Editable
□ Sweep Contents of Compressed Files □ User Editable

Schedule Spyware Sweeps

- Configure specific workstation drives to sweep for spyware
- Set sweeps to include or exclude memory and the registry
- Exclude files of a specific size from sweeps
- Determine spyware disposition by spyware category or by exact spyware name
- Enable Smart Shields to protect the common spyware entry points, including changes to system memory, registry entries, host files, startup processes, browser hijackings, alternate data streams and other security settings
- "Poll Now" command allows administrator to update workstation configuration, client software or spy definitions on demand
- Schedule sweeps by group; or if a critical situation arises, run a sweep instantly by individual workstation or group

- Client reboot notifications help with the full removal of persistent threats by prompting the end user to reboot if necessary to completely remove a detected threat
- Incremental Definitions allow organizations to download only the new or updated definitions from Webroot, significantly reducing the size of the definition packets that need to cross the network
- Memory Sandboxing permits compressed executables to unpack and execute in a protected memory space where they may be scanned and quarantined without compromising the integrity of the client workstation

Monitoring, Reporting and Alerts

- Configure who receives alerts when specific types of spyware are detected
- SNMP alerting for detected spyware at conclusion of sweeps
- View enterprise-wide graphical summaries of spyware detected by group or spyware category
- Display errors that occur during sweeps to aid technical support in resolving the problem
- Generate reports of alerts and spyware found
- Create custom reports if using SQL Server database and Crystal Reports

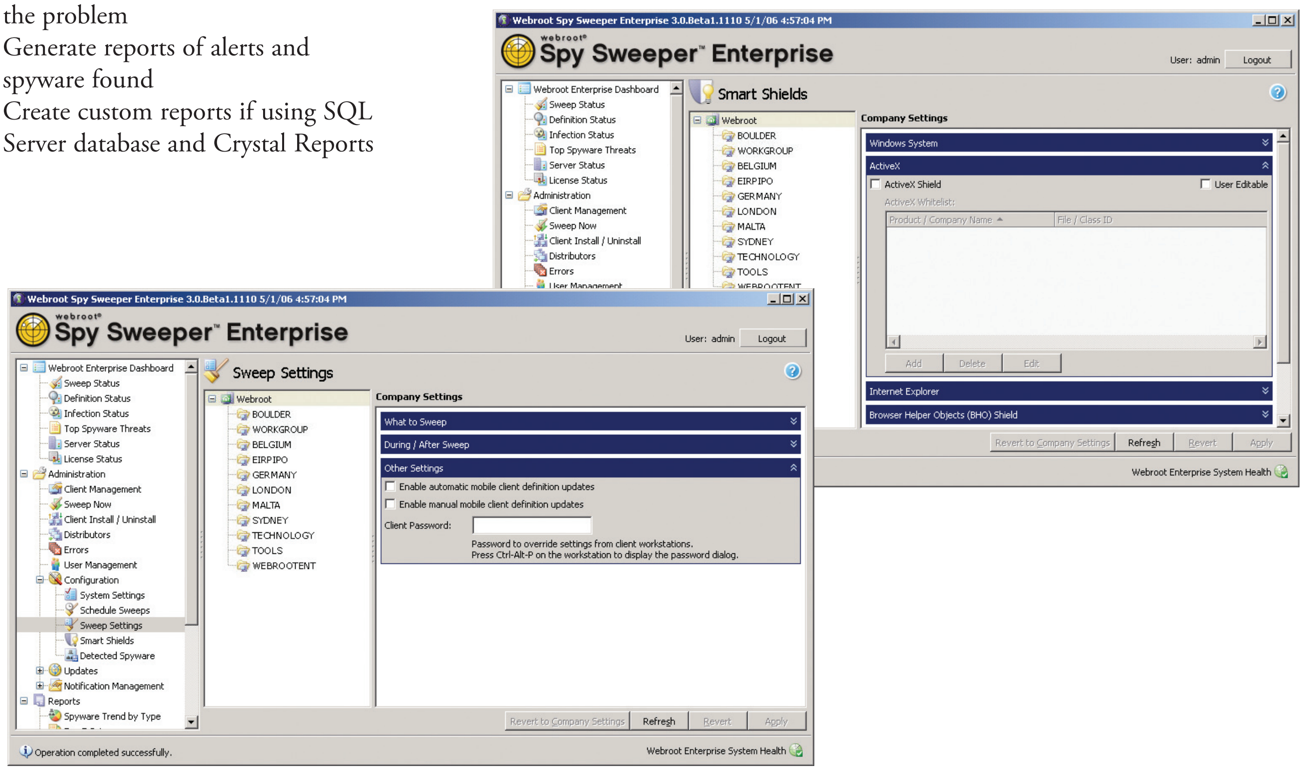
System Requirements

Server:

OS: Windows 2000 Pro/Server with SP4, Windows XP Pro with SP2, Windows 2003 Standard, Enterprise or SMB with SP1
CPU: 1 GHz Minimum
Memory: 1 GB Minimum
Disk Space: 1 GB Minimum
DB Support: Microsoft SQL Server 2005 Express (.NET 2.0, MDAC 2.8+), Microsoft SQL Server 2000 and 2005
IE: 6.0 SP1 or later

Client:

OS: Windows 2000 Pro/Server, Windows XP Home, Professional, Tablet, Windows 2003 Standard, Enterprise or SMB
CPU: 1 GHz Minimum
Memory: 128 Minimum, 256 MB or better recommended
Disk Space: 15 MB free space



☐ Enable automatic mobile client definition updates
☐ Enable manual mobile client definition updates
Client Password:

Password to override settings from client workstations.
Press Ctrl-Alt-P on the workstation to display the password dialog.

Operation completed successfully.

© 2006 Webroot Software, Inc. — All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior consent of Webroot Software, Inc. Webroot, Spy Sweeper, Spy Sweeper Enterprise and their logos are registered trademarks of Webroot Software, Inc.