Webroot®
AntiSpyware®

CORPORATE EDITION

System Administrator Guide

webroot
SOFTWARE®

Webroot Software, Inc.
PO Box 19816
Boulder, CO 80308

www.webroot.com

Version 3.5.1

Webroot® AntiSpyware Corporate Edition System Administrator Guide

Version 3.5.1

Contents

1: Introduction

For an introduction to Webroot® AntiSpyware Corporate Edition and Webroot® AntiSpyware Corporate Edition with AntiVirus, see the following topics:

- Overview
- Admin Console Features
- Configuration Checklist

Note

Audience: This guide describes how to use the Admin Console interface to configure Webroot AntiSpyware components and to monitor and report on client workstation status. It assumes that you are a System Administrator who has a basic understanding of the Windows operating system and network communications.

Overview

Webroot AntiSpyware protects your business from a variety of online security risks, including viruses, spyware, and other potentially unwanted programs that may infiltrate company workstations.

To learn more about Webroot AntiSpyware, see the following topics:

- Product Versions
- Architecture and Communications
- Continuous Protection from Online Threats
- System-Wide Control

Product Versions

This guide describes how to use the features available for the following versions:

- **Webroot® AntiSpyware Corporate Edition**. Provides protection from spyware and other potentially unwanted programs.
- **Webroot® AntiSpyware Corporate Edition with AntiVirus**. Provides the same protection from spyware and other potentially unwanted programs as the regular edition, along with sophisticated Sophos® AntiVirus protection.

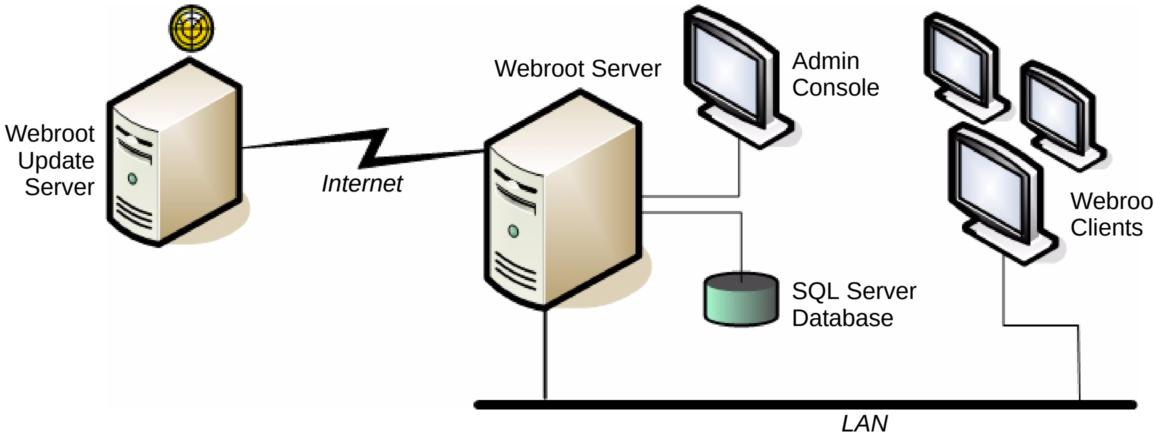
Note

In this guide, *Webroot AntiSpyware* refers to either version of the product.

Architecture and Communications

Using an architecture of a central server (Webroot Server) and multiple clients (Webroot Clients), Webroot AntiSpyware implements network-wide detection, removal, and blocking of security risks. The Webroot Server runs within your company network to manage Webroot Clients installed on each workstation. The Webroot Server is installed on one of your company servers and includes an Admin Console (a graphical user interface) and a SQL Server database.

To keep current with rapidly changing security risks, your Webroot Server communicates over the Internet with the Webroot Update Server™ to check for the latest spyware and virus definitions (the comprehensive database of online threats). If new threat definitions are available, the Webroot Server downloads them. During the next polling interval, the Webroot Clients receive those updates from the Webroot Server and can sweep workstations for any risks by checking against the latest definitions.



Continuous Protection from Online Threats

Online security threats come in many forms; the most common types come from spyware and viruses. The Webroot Clients installed on company workstations offer continuous protection from these threats by performing a sweep-and-quarantine process and by using Smart Shields to block potential threats from downloading before they can cause damage.

Types of Threats

The Webroot Clients protect workstations from a variety of threats that are specifically designed to infiltrate computers, including spyware, system monitors, Trojan horses, adware, and tracking cookies. While some of these programs may be harmless, others can steal personal information, slow down processing times, or cause system crashes. Spyware and other unwanted programs may install themselves as users visit Web sites, may arrive bundled with freeware or shareware, or may download through an e-mail attachment. These programs are difficult to detect, because they can hide in multiple locations and can reinstall if not removed properly with specialized anti-spyware software like Webroot AntiSpyware.

If you purchased the Webroot AntiSpyware with AntiVirus edition, workstations have added protection against viruses, as well as from spyware and other potentially unwanted programs. Viruses can arrive as file attachments to e-mail, as embedded files on a CD, and as clickable graphics in an e-mail. Virus creators constantly find new ways to distribute viruses by exploiting weaknesses in various programs and creatively duplicating themselves by using an e-mail address book or attaching themselves to legitimate files. Once on your hard drive, viruses are difficult to detect and remove, unless you have specialized antivirus software.

System Sweeps and Quarantine

To locate potential threats and protect workstations, you perform a three-step process:

1. **Sweep**. Webroot Clients search workstations for known threats, looking for any items that match definitions in the Webroot threat database. You can specify where Webroot Clients search (for example, search specific folders or file types) and the types of threats to detect (for example, locate viruses, but ignore tracking cookies).
2. **Quarantine**. After the search, detected items that match threat definitions are removed from their current locations and sent to a holding area (the Quarantine), where they are rendered inoperable and cannot harm workstations. You can control whether certain items are always quarantined, so you have a chance to review the list and take specific action, or whether certain items like viruses bypass the Quarantine and are always deleted. If a virus is detected, the Webroot Client removes the infected portions of a file in a “cleaning” process, then restores the file.
3. **Delete**. After detected items are quarantined, you can delete them permanently or can restore them to their original locations (if you later find that a certain piece of software will not work without an item). You should always leave an item in the Quarantine and test the workstation operations first, before deleting items permanently.

As an administrator, you can control which Webroot Client functions the user can access. For example, you can specify that users are able to sweep their own computers, but not change the sweep settings.

Smart Shields

For added protection, Webroot Clients include a shielding function called “Smart Shields” that protect workstations against unwanted programs that may change settings in browsers, operating systems, and in other areas. As users work, shields continuously monitor for suspicious activities and prevent potential threats from downloading. If Webroot AntiSpyware detects spyware or other potential threats attempting to download, it posts an alert message in the Admin Console.

System-Wide Control

You can control and monitor Webroot AntiSpyware operations by using an Admin Console installed on a company server. The Admin Console provides the following functions:

- **Monitoring**. The Dashboard shows the overall status of corporate workstations, including whether the sweeps have run on schedule and whether potential threats have been detected.
- **Administration**. The administration functions allow you to configure settings for the Webroot AntiSpyware components.
- **Reporting**. The reporting functions allow you to generate graphical executive summaries, threat reports, and status updates. You can customize reports to provide a detailed analysis of the threats by workstation, group, and threat type.

For more information, see the next section, “Admin Console Features” on page 4.

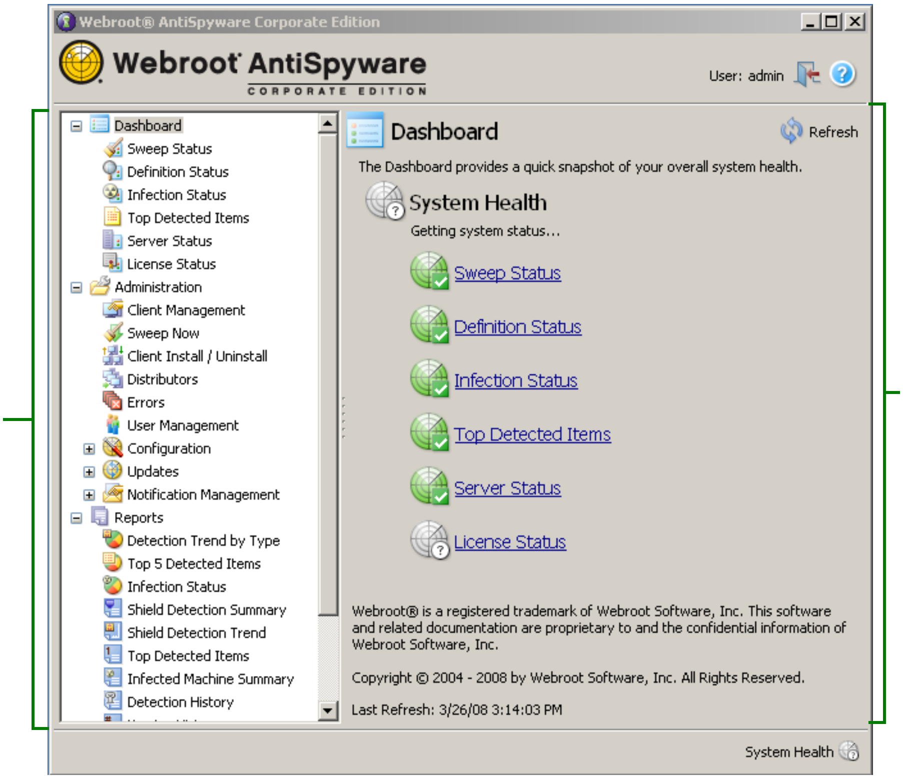
Admin Console Features

To perform most Webroot AntiSpyware tasks, you use the Admin Console. The Admin Console is installed along with the Webroot Server, as described in the *Webroot AntiSpyware Corporate Edition Installation Guide*.

To learn more about the Admin Console, read the following topics:

- Function Tree
- Main Panel

The following figure shows the Admin Console. When you first log in, the main Dashboard is open in the main panel to provide you with a quick glance at the status and health of your company workstations.



Dashboard

The Dashboard provides a quick snapshot of your overall system health.

System Health

Getting system status...

Webroot® is a registered trademark of Webroot Software, Inc. This software and related documentation are proprietary to and the confidential information of Webroot Software, Inc.

Copyright © 2004 - 2008 by Webroot Software, Inc. All Rights Reserved.

Last Refresh: 3/26/08 3:14:03 PM

Function tree: Expand and select nodes to see available settings and actions.

Main panel: Displays the settings and actions available for the selected function.

Function Tree

The Admin Console's function tree (on the left side) allows you to select and access tasks. When you select a task, the main panel on the right displays the settings and actions available.

Note

This guide uses the following notation for using the function tree: **Dashboard** > **Sweep Status**. This notation indicates that you should select "Sweep Status," below "Dashboard."

Use the function tree to navigate in the Admin Console. Do not use the **Back** button in your browser.

The following table describes each task available from the function tree.

Function tree options	
Dashboard	Quick snapshot of overall system health.
Sweep Status	Status of client workstations that have completed a sweep within the last week or within the last month.
Definition Status	Status of client workstations that do not have the current virus and spyware definitions installed.
Infection Status	List of workstations that have infections. (Threat types are assigned point values, based on severity.)
Top Detected Items	List of top threats found on workstations in the last 48 hours. (Threat types are assigned point values, based on severity.)
Server Status	Status of last downloaded software versions, ports, and services.
License Status	License information and expiration status.
Administration	Tasks for managing and configuring Webroot AntiSpyware.
Client Management	Tasks for creating workstation groups, polling workstations immediately, sweeping workstations immediately, and generating (exporting) reports.
Sweep Now	Tasks for sweeping selected workstations or groups.
Client Install/Uninstall	Tasks for installing and uninstalling the Webroot Client on workstations.
Distributors	Tasks for managing and assigning Distributors to Webroot Clients.
Errors	Error messages from the Webroot Clients and Webroot Server.
User Management	Tasks for creating and managing Admin Console users.
Configuration	Tasks for managing the Admin Console and Webroot Clients: • System Settings: Configure Webroot Server settings and Webroot Client communications. • Schedule Sweeps: Configure a schedule for workstation sweeps. • Sweep Settings: Determine what files and drives to sweep, as well as the types of threats to sweep for. Also enable options for allowing users some sweep controls and for obtaining definition updates. • Smart Shields: Configure shields that block potentially unwanted programs from downloading to workstations and configure whitelists for certain programs that users may need. • Detection Settings: Configure options for quarantining, deleting, or keeping items detected during sweeps. • Web Security: Enable the client proxy to redirect browser traffic through the Webroot Web SaaS Security service.

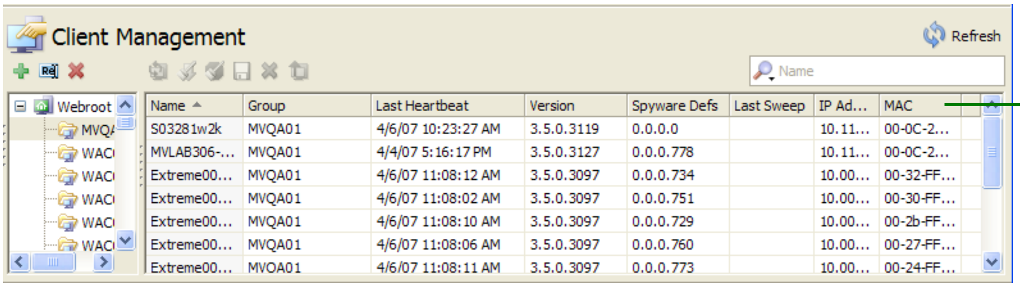
Function tree options *(continued)*	
Updates	Tasks for configuring component updates: • Update History: See a history of all downloaded updates. • Auto Install: Specify that updates install automatically. • Manual Install: Specify that updates be installed manually.
Notification Management	Tasks for configuring e-mail notifications and addresses: • E-Mail Notification Formats: Define text and format for update, alerts, and error messages. • E-Mail Addresses: Enter e-mail account information for the users who will receive notification. • Alert Notifications: Enter e-mail addresses of the users who should receive alert notifications. • Error Notifications: Enter e-mail addresses of the users who should receive error notifications. • Update Notifications: Enter e-mail addresses of the users who should receive update notifications.
Reports	Tasks for creating error and detection reports.
Detection Trend by Type	Trends over a selected period of time for adware, Trojans, system monitors, and viruses.
Top 5 Detected Items	Trends over a selected period of time for the five most prevalent threats detected on workstations.
Infection Status	Status of all workstations: either infected, clean, or never swept.
Shield Detection Summary	Summary of all the types and the amount of items blocked by shields.
Shield Detection Trend	Trends of the types and amount of items blocked by shields.
Top Detected Items	Prevalent threats for the entire company or for each group or workstation.
Infected Machine Summary	Summary about any infected workstations.
Detection History	History of detected threats by selected time frame and threat type.
Version History	History of Webroot Client versions installed on workstations.
Error Report	List of errors by time frame and workstation.
Detection Report	List of potential threats that have been detected and quarantined on workstations.
Single Detected Item Report	List of all clients that have been infected with a specific threat.
News and Docs	A link to the latest news from Webroot.

Main Panel

The main panel is a work area where you view status, enter configuration settings, and perform client functions such as polling and sweeping. The content that appears in this panel depends on what option you selected from the function tree. Depending on the content displayed, the main panel may include tabular columns, subpanels, commands, and a filter field.

Tabular Columns

Some panels display information in tabular columns, as shown in the example below. You can sort information by clicking on a column head at the top of the panel.

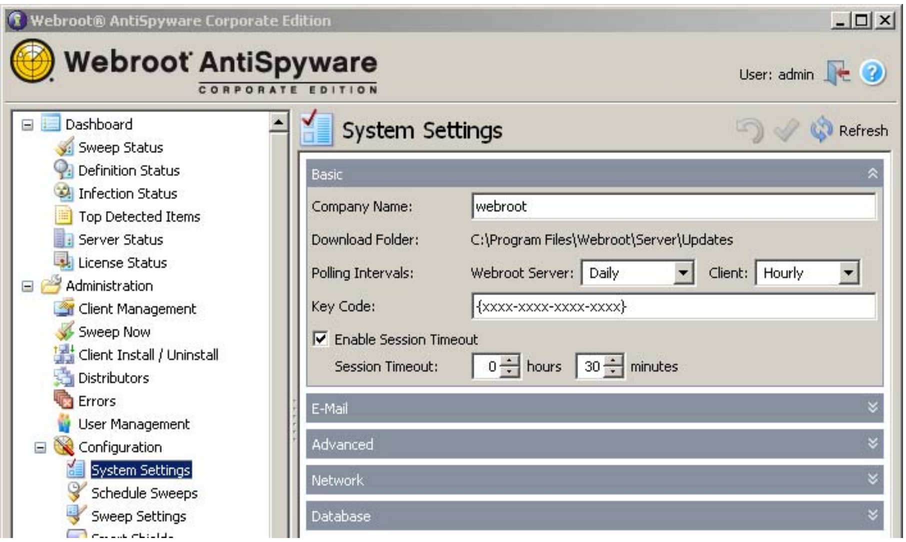


Name ▲	Group	Last Heartbeat	Version	Spyware Defs	Last Sweep	IP Ad...	MAC
S03281w2k	MVQA01	4/6/07 10:23:27 AM	3.5.0.3119	0.0.0.0		10.11...	00-0C-2...
MVLAB306-...	MVQA01	4/4/07 5:16:17 PM	3.5.0.3127	0.0.0.778		10.11...	00-0C-2...
Extreme00...	MVQA01	4/6/07 11:08:12 AM	3.5.0.3097	0.0.0.734		10.00...	00-32-FF...
Extreme00...	MVQA01	4/6/07 11:08:02 AM	3.5.0.3097	0.0.0.751		10.00...	00-30-FF...
Extreme00...	MVQA01	4/6/07 11:08:10 AM	3.5.0.3097	0.0.0.729		10.00...	00-2b-FF...
Extreme00...	MVQA01	4/6/07 11:08:06 AM	3.5.0.3097	0.0.0.760		10.00...	00-27-FF...
Extreme00...	MVQA01	4/6/07 11:08:11 AM	3.5.0.3097	0.0.0.773		10.00...	00-24-FF...

Click on a column head to sort data.

Subpanels

Subpanels include show/hide bars that you can click to open and close content in the main panel. When you are finished making changes to settings in every subpanel, you click **Apply** ✓ at the top right (it's not necessary to click **Apply** ✓ after changing information in each field or subpanel).



Company Name: webroot

Download Folder: C:\Program Files\Webroot\Server\Updates

Polling Intervals: Webroot Server: Daily Client: Hourly

Key Code: {xxxx-xxxx-xxxx-xxxx}

☑ Enable Session Timeout

Session Timeout: 0 hours 30 minutes

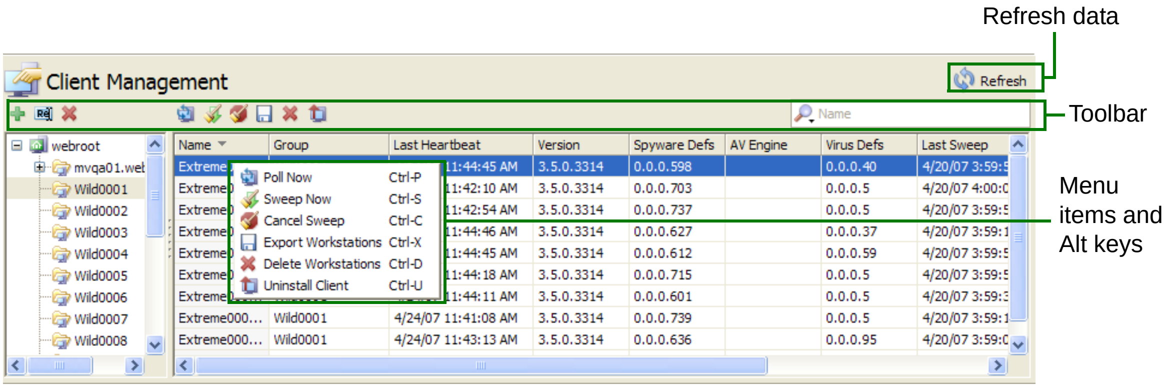
Subpanel (open)

Click on a Show/Hide bar to open or close a subpanel

Commands

Commands can include tasks such as client polling and sweeping. You can perform commands by using icons in the toolbar, menu items, and Alt key combinations. (The toolbar includes only the icons that apply to a current panel.)

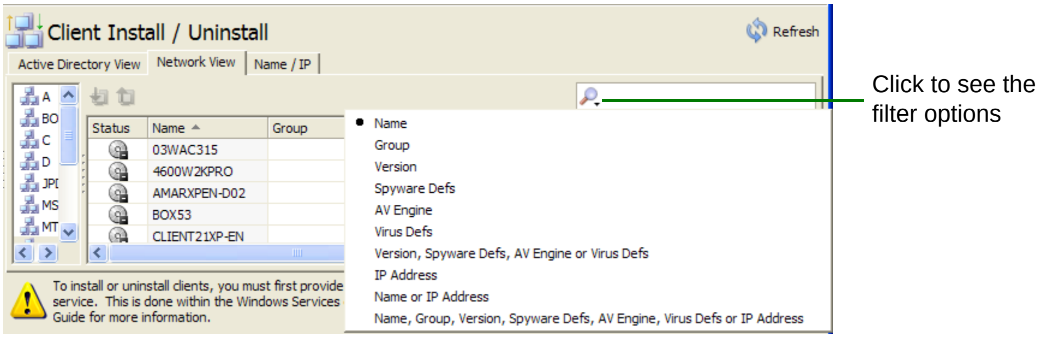
The Refresh icon appears on every panel and allows you to refresh the contents of the entire screen to display the most recent data. This is often helpful after you have requested a client polling and need to see updated information.



Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine	Virus Defs	Last Sweep
Extreme		11:44:45 AM	3.5.0.3314	0.0.0.598		0.0.0.40	4/20/07 3:59:5
Extreme		11:42:10 AM	3.5.0.3314	0.0.0.703		0.0.0.5	4/20/07 4:00:0
Extreme		11:42:54 AM	3.5.0.3314	0.0.0.737		0.0.0.5	4/20/07 3:59:5
Extreme		11:44:46 AM	3.5.0.3314	0.0.0.627		0.0.0.37	4/20/07 3:59:1
Extreme		11:44:45 AM	3.5.0.3314	0.0.0.612		0.0.0.59	4/20/07 3:59:5
Extreme		11:44:18 AM	3.5.0.3314	0.0.0.715		0.0.0.5	4/20/07 3:59:5
Extreme		11:44:11 AM	3.5.0.3314	0.0.0.601		0.0.0.5	4/20/07 3:59:3
Extreme000...	Wild0001	4/24/07 11:41:08 AM	3.5.0.3314	0.0.0.739		0.0.0.5	4/20/07 3:59:1
Extreme000...	Wild0001	4/24/07 11:43:13 AM	3.5.0.3314	0.0.0.636		0.0.0.95	4/20/07 3:59:0

Filter Field

The Filter field displays on the far right of the tool bar when there is content in a panel that can be filtered to meet your criteria. To see which filtering options are available, click the magnifying glass in the drop-down list, as shown below.


Click to see the filter options
Client Install / Uninstall
Refresh
Active Directory View
Network View
Name / IP
A
BO
C
D
JPI
MS
MT
● Name
Group
Version
Spyware Defs
AV Engine
Virus Defs
Version, Spyware Defs, AV Engine or Virus Defs
IP Address
Name or IP Address
Name, Group, Version, Spyware Defs, AV Engine, Virus Defs or IP Address

Status	Name	Group
	03WAC315	
	4600W2KPRO	
	AMARXPEN-D02	
	BOX53	
	CLIENT21XP-EN	

To install or uninstall clients, you must first provide service. This is done within the Windows Services Guide for more information.

To filter information:

1. From a panel that has the filter function, select your filter criteria from the drop-down list.
2. In the field, enter text to filter on.

You can use regular expressions. The following table summarizes the special characters you can use in regular expressions:

Character	Function
+	Repeats the previous item one or more times.
*	Repeats the previous item zero or more times.
?	Makes the preceding item optional.
. (period)	Matches any single character except line break characters \r and \n.
[ ]	Creates a character class. A character class matches a single character out of all the possibilities offered by the character class.
^	Matches characters at the beginning of the string. Matches a position rather than a character.
$	Matches characters at the end of the string. Matches a position rather than a character.
()	Used to create grouping. Typically used along with |.
{}	Repeats sets.
|	Logical “or.” Matches either the left side or the right side of the expression.
\	Escapes special characters so that they are taken literally.

As you enter filter criteria, the information in the table changes to show only the rows that match your criteria.

If desired, clear the filter by clicking the **Delete** ☒ icon at the right of the Filter field and to redisplay all rows.

Configuration Checklist

If you are configuring Webroot AntiSpyware for the first time, use the following checklist for an overview of configuration tasks.

Step	See...
1. Check system settings and notification settings.	"System Settings" on page 29 "Notification Management" on page 62
2. Create Webroot Client groups for easier administration.	"Manage Client Groups" on page 18
3. Configure sweep schedules and settings.	"Schedule Sweeps" on page 36 "Sweep Settings" on page 37
4. Run initial sweeps on client workstations.	"Sweep Now" on page 22 "Detection Settings" on page 51
5. Configure Smart Shields for continuous monitoring.	"Smart Shields" on page 42
6. View the Dashboard status for any detected threats.	"Dashboard" on page 11

▲

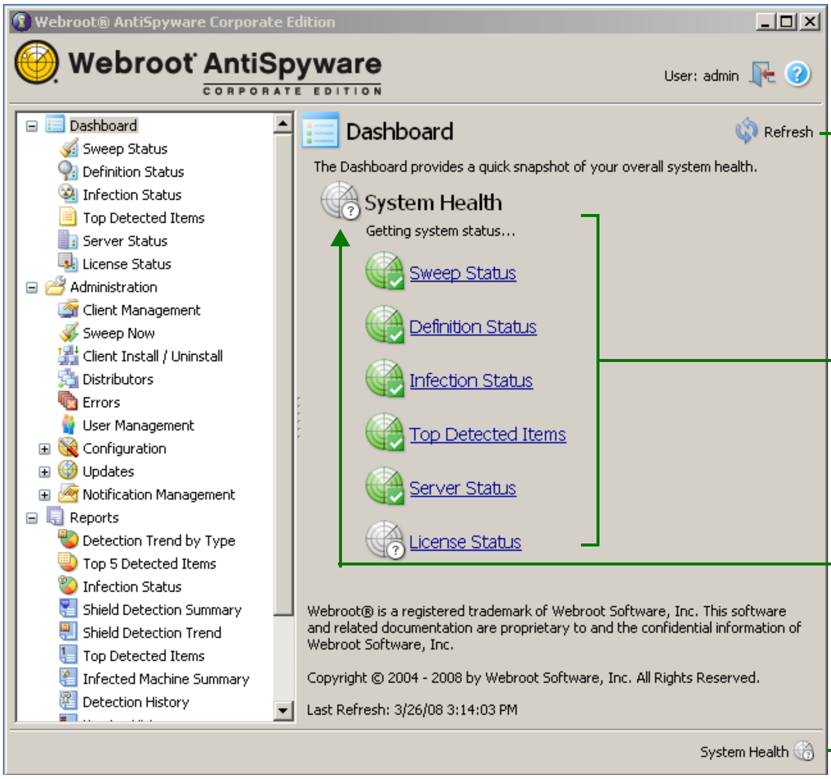
2: Dashboard

The Dashboard shows the overall health of your company workstations. From here, you can glance through categories of issues that may require your attention, such as whether sweeps have been performed on schedule and whether any threats have been detected.

The Dashboard includes the following status categories:

- Sweep Status. Shows whether client workstations have completed a sweep within the last week.
- Definition Status. Shows whether client workstations have the current threat definitions installed.
- Infection Status. Shows whether threats have been found on client workstations.
- Top Detected Items. Shows whether critical threats have been found on client workstations in the last 48 hours.
- Server Status. Shows the status of the last downloaded software versions, ports, and Webroot services.
- License Status. Shows the expiration status of your company license.

The following example shows the main Dashboard panel.



Dashboard

The Dashboard provides a quick snapshot of your overall system health.

System Health

Getting system status...

Webroot® is a registered trademark of Webroot Software, Inc. This software and related documentation are proprietary to and the confidential information of Webroot Software, Inc.

Copyright © 2004 - 2008 by Webroot Software, Inc. All Rights Reserved.

Last Refresh: 3/26/08 3:14:03 PM

Click **Refresh** to update all Dashboard information based on the latest poll from each client. (Otherwise, information refreshes hourly.)

Click a link to view more details.

Shows overall status. If any single category has a warning or critical status, this icon reflects the most serious status.

Displays on every screen. Click to return to the Dashboard.

Each category in the Dashboard can have one of the following status levels:

Icon	Description
✓	Good (green). There are no warnings or critical items
⚠	Warning (yellow). At least one item in the category has a warning status.
✖	Critical (red). At least one item in the category has a critical status.

Status information updates hourly. If you have just polled Webroot Clients (see “Poll Now” on page 20), click **Refresh** to see the most recent status.

Sweep Status

The Sweep Status panel lists client workstations that have not been swept in more than 7 days:

- **Critical Workstations**. Client workstations listed in this panel have not completed a sweep in the last 30 days or more. If no workstations meet Critical status, the panel displays “No Critical Workstations found.”
- **Moderate Risk Workstations**. Client workstations listed in this panel have not completed a sweep in the last 7 to 29 days. If no workstations meet Moderate Risk status, the panel displays “No Moderate Risk Workstations found.”

To manage items in the Sweep Status panel:

1. From the Admin Console function tree, select **Dashboard** > **Sweep Status**.

   The Sweep Status panel opens and shows any client workstations that have not been swept in more than 7 days.

2. From the Sweep Status panel, you can perform the following tasks:

Filter lists	To filter client workstations shown in the list, use the filter field (see “Filter Field” on page 8).
Report data	To export data for selected clients in either list, click the **Export Selected** icon. To export data from all clients in either list, click the **Export All** icon.
Poll	If you want to change sweep settings or other Admin Console settings for clients in either list, right-click on the client names, and select “Poll Now” from the menu or click the **Poll Now** icon. Click **Refresh** to update the status based on the latest polling data from each client.
Sweep	If you want to sweep clients in either list, select the clients. You can either right-click to select “Sweep Now” from the pop-up menu or click the **Sweep Now** icon.

Definition Status

The Definition Status panel lists client workstations that do not have the most recent versions of threat definitions:

- **Critical Workstations**. Client workstations listed in this panel have a definition version number that is five or more below the highest downloaded definition version. If no workstations meet Critical status, the panel displays “No Critical Workstations found.”
- **Moderate Risk Workstations**. Client workstations listed in this panel have a definition version number that is between one and four below the highest downloaded definition version. If no workstations meet Moderate Risk status, the panel displays “No Moderate Risk Workstations found.”

To manage items in the Definition Status panel:

1. From the Admin Console function tree, select **Dashboard > Definition Status**.

   The Definitions Status panel opens and shows any client workstations that do not have current threat definitions.

2. From the Definition Status panel, you can perform the following tasks:

Filter lists	To filter client workstations shown in the list, use the filter field (see “Filter Field” on page 8).
Report data	To export data for selected clients in either list, click the **Export Selected** icon. To export data from all clients in either list, click the **Export All** icon.
Poll	If you have automatic definition updates defined (see “Auto Install” on page 59) or have assigned a definition update to clients (see “Manual Install” on page 60), right-click on the client names, then select “Poll Now” from the menu or click the **Poll Now** icon. Click **Refresh** to update the status based on the latest polling data from each client.
Sweep	If you want to sweep clients in either list, select the client names. You can either right-click to select “Sweep Now” from the pop-up menu, or click the **Sweep Now** icon.

Infection Status

The Infection Status panel lists client workstations where threats have been detected during Webroot Client sweeps and threats blocked by Smart Shields:

- **Critical Workstations**. Client workstations listed in this panel have threats totalling 5 points or more. If no workstations meet Critical status, the panel displays “No Critical Workstations found.”
- **Moderate Risk Workstations**. Client workstations listed in this panel have threats totalling between 1 and 4 points. If no workstations meet Moderate Risk status, the panel displays “No Moderate Risk Workstations found.”

A client workstation remains listed on this panel until it has a clean sweep and the date changes to the next calendar day.

The following table shows the points assigned to found threats:

Threat	Points
Virus	5
Trojan horse	5
System monitor	5
Adware	1
Informational	0

For more information about sweeps and managing detected threats, see “Configuration” on page 29.

To manage items in the Infection Status panel:

1. From the Admin Console function tree, select **Dashboard** > **Infection Status**.

   The Infection Status panel opens and shows any client workstations with detected threats.

2. From the Infection Status panel, you can perform the following tasks:

Filter lists	To filter client workstations shown in the list, use the filter field (see “Filter Field” on page 8).
Report data	To export data for selected clients in either list, click the **Export Selected** icon. To export data from all clients in either list, click the **Export All** icon.
Poll	If you want to change any sweep settings or force clients to update definitions in either list, right-click the client names, then select “Poll Now” from the menu or click the **Poll Now** icon. Click **Refresh** to update the status based on the latest polling data from each client.
Sweep	If you want to sweep clients in either list, select the client names. You can either right-click to select “Sweep Now” from the pop-up menu, or click the **Sweep Now** icon.

Top Detected Items

The Top Detected Items panel lists the top threats found in the last 48 hours for client workstations:

- **Critical Workstations**. The Webroot Clients found threats totalling 5 points or more on the displayed workstations.
- **Moderate Risk Workstations**. The Webroot Clients found threats totalling between 1 and 4 points on the displayed workstations.

If no threats were found, the panel displays “No Items Detected.”

The following table shows the points assigned to found threats:

Threat	Points
Virus	5
Trojan horse	5
System monitor	5
Adware	1
Other	0

For more information about sweeps and managing detected threats, see “Configuration” on page 29.

To manage items in the Top Detected Items panel:

1. From the Admin Console function tree, select **Dashboard** > **Top Detected Items**.

   The Top Detected Items panel opens.

2. From the Top Detected Items panel, you can perform the following tasks:

View details	To see more information about a specific item online at the Webroot Threat Research Center, select it and click **Details**.
Filter list	To filter client workstations shown in the list, use the filter field (see “Filter Field” on page 8).
Report data	To export data for selected clients in either list, click the **Export Selected** icon. To export data from all clients in either list, click the **Export All** icon.

Server Status

The Server Status panel lists the following:

- **Latest Downloaded Versions**: The Webroot Server and Webroot Client versions downloaded and the version of spyware definitions downloaded. If you have Webroot AntiSpyware with AntiVirus, you can also see the AntiVirus Engine currently used and the version of virus definitions downloaded.
- **Webroot Port Status**: The ports used for the Webroot Update server, the Webroot Client service, and the update Distributor. Also indicates if the ports are open on the server.
- **Webroot Services**: The status of each Webroot Service (for example, “Running”).

To manage items in the Server Status panel:

1. From the Admin Console function tree, select **Dashboard** > **Server Status**.

   The Server Status panel opens.

2. If necessary, click **Refresh** to update the status.
3. If a service is not running, click **Start** to start it.

   All listed ports should be open. If a port is not open, check your firewall and proxy settings.

License Status

The License Status panel shows the number of Webroot Client licenses you have available, how many are in use, and license expiration information.

Note

The number of licenses in use updates every 24 hours, after the newly installed clients poll your company server and after your company server sends the number of used licenses once a day to the Webroot Update Server.

To view the License Status and renew licenses:

1. From the Admin Console function tree, select **Dashboard** > **License Status**.

   The License Status panel opens.

2. If necessary, click **Refresh** to update the status.
3. You can renew licenses by contacting Webroot at the contact information listed in this panel.

▲

3: Administration

The Administration features enable you to manage Webroot Clients installed on company workstations. From here, you can control all client polling, sweep schedules, shield settings, product updates, and sweep notifications.

To perform administration tasks, read the following topics:

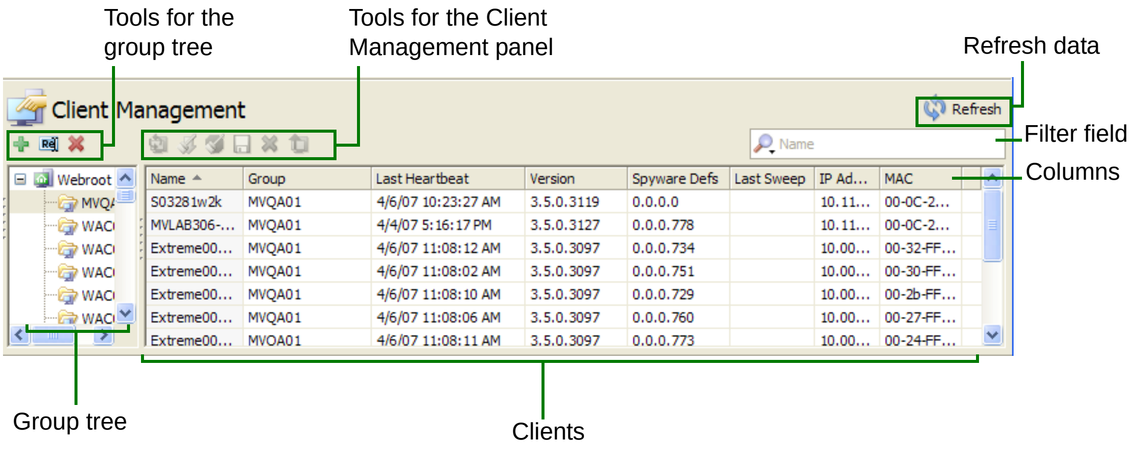
- Client Management. Create client groups for global management (installations, sweep scheduling, etc.), export client information to a spreadsheet, and poll clients for the latest information.
- Sweep Now. Perform an immediate sweep on selected clients (useful if an online threat has infiltrated company workstations and you do not want to wait until the next scheduled sweep).
- Client Install and Uninstall. Deploy the Webroot Clients to one or more company workstations.
- Distributors. Assign distributor servers to client groups (only necessary if you use additional distributors for load balancing in the Webroot architecture).
- Errors. View errors generated on client workstations related to Webroot software.
- User Management. Create user accounts for the Admin Console and view activity logs.
- Configuration. Modify Admin Console system settings, schedule sweeps for potential threats on client workstations, modify sweep settings, set shields that block potential threats from downloading to client workstations, manage the disposition of potential threats founds during sweeps, and enable a proxy connection to the Webroot Web Security SaaS service.
- Updates. Determine how often Webroot software and threat definitions are updated (automatically or manually).
- Notification Management. Configure a list of e-mail recipients for security alerts, errors, and updates.

Client Management

In the Client Management panel, you can perform the following functions:

- Define client groups for easier global administration, as described in "Manage Client Groups," below.
- Perform an immediate client poll on selected client workstations for the most updated information, as described in "Poll Now" on page 20.
- Sweep client workstations (or cancel sweeps) for spyware and other potential threats, as described in "Sweep Now" on page 22.
- Create and export client data to a comma-separated (CSV) file and load in a spread sheet, as described in "Export Webroot Client Data" on page 21.
- Delete a client workstation account from the Webroot database, if that client is no longer connected in the corporate network, as described in "Delete Workstations" on page 21.
- Uninstall the Webroot Client from workstations, as described in "Client Install and Uninstall" on page 24.

An example Client Management panel is shown below:



Name	Group	Last Heartbeat	Version	Spyware Defs	Last Sweep	IP Ad...	MAC
S03281w2k	MVQA01	4/6/07 10:23:27 AM	3.5.0.3119	0.0.0.0		10.11...	00-0C-2...
MVLAB306-...	MVQA01	4/4/07 5:16:17 PM	3.5.0.3127	0.0.0.778		10.11...	00-0C-2...
Extreme00...	MVQA01	4/6/07 11:08:12 AM	3.5.0.3097	0.0.0.734		10.00...	00-32-FF...
Extreme00...	MVQA01	4/6/07 11:08:02 AM	3.5.0.3097	0.0.0.751		10.00...	00-30-FF...
Extreme00...	MVQA01	4/6/07 11:08:10 AM	3.5.0.3097	0.0.0.729		10.00...	00-2b-FF...
Extreme00...	MVQA01	4/6/07 11:08:06 AM	3.5.0.3097	0.0.0.760		10.00...	00-27-FF...
Extreme00...	MVQA01	4/6/07 11:08:11 AM	3.5.0.3097	0.0.0.773		10.00...	00-24-FF...

Manage Client Groups

After Webroot Clients have been installed and configured (as described in the *Webroot AntiSpyware Corporate Edition Installation Guide* or "Client Install and Uninstall" on page 24), each client workstation is added to a default group named after the domain or workgroup where the client workstation is located. If desired, you can create your own client group structure to help save administration time. For example, by using client groups, you can perform the following tasks globally:

- Installing updates
- Managing detected items by threat type
- Managing sweep settings and shields
- Scheduling sweeps

When creating your own group structure, you can organize groups to distinguish between different types of users, such as system administrators who will test new product updates before distributing them throughout the company, and to distinguish between departments, geographic locations, or any other category you choose.

Client groups can be structured into subgroups, similar to Active Directory folders. This hierarchical group structure follows these rules:

- Each group can belong to only one parent group.
- A workstation can belong to only one group.
- Individual workstations take the settings of the nearest parent group.

See the following steps for creating, renaming, or deleting client groups.

To create client groups:

1. From the Admin Console function tree, select **Administration > Client Management**.

   The Client Management panel opens. Any previously defined groups are listed in the group tree and the assigned client workstations are shown at the right.

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see "Filter Field" on page 8).

2. Click the **Add** ✚ icon above the group tree.

   The Add Group window opens.

3. Enter a group name and click **OK**.

   The group name displays in the group tree. If necessary, click **Refresh** 🔄 to see the new groups.

4. To assign clients, drag client names from the list on the right to a group in the group tree. To reassign clients, drag it from the current group and drop it onto another group.

To rename groups:

1. From the Admin Console function tree, select **Administration > Client Management**.

   The Client Management panel opens, with a list of all existing groups in the group tree (middle panel).

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see "Filter Field" on page 8).

2. Right-click on the group name and select "Rename Group" from the menu or click the **Rename Group** icon above the group tree.

To delete groups:

1. From the Admin Console function tree, select **Administration** > **Client Management**.

   The Client Management panel opens. Groups are listed in the group tree and the assigned client workstations are shown at the right.

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see “Filter Field” on page 8).

2. If the group includes client assignments, reassign those clients to another group. To do this, drag and drop the client names to another group in the group tree.

   You cannot delete a group that still contains client assignments.

3. Right-click on the group name and select “Delete Group” from the menu or click the **Delete Group** ✖ icon above the group tree.

Poll Now

You can poll one or more client workstations on demand if you have changed some settings, such as shields, or you want to force a threat definition update immediately.

> **Note**
>
> To ensure that you do not overwhelm your network and servers, use this Poll Now feature selectively. You may notice slow performance if a large number of client workstations all request information from the server at the same time.

To poll client workstations immediately:

1. From the Admin Console function tree, select **Administration** > **Client Management**.

   The Client Management panel opens with a list of all existing groups in the group tree.

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see “Filter Field” on page 8).

2. From the group tree, click the group that includes the clients you want to poll.

   The clients that are assigned to that group appear in the client list.

3. From the client list, select the clients you want to poll. You can select multiple clients by using **Ctrl** or **Shift**.

4. Right-click and select “Poll Now” from the menu or click the **Poll Now** icon at the top of the list.

   The poll starts on the selected client workstations. A confirmation message opens, with the number of clients that will receive the polling message.

5. To check the status of the polling, click **Refresh** ⟳ and sort on the Last Heartbeat column to see that clients have updated.

Export Webroot Client Data

You can export the information shown in the Client Management columns to a comma separated (CSV) file. You can then load the file in a spreadsheet.

Note

To sort by column, click on a column head.

To create and export client data:

1. From the Admin Console function tree, select **Administration > Client Management**.

   The Client Management panel opens with a list of all existing groups in the group tree.

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see "Filter Field" on page 8).

2. From the group tree, click the group that includes the clients you want to include in the data.

   The clients that are assigned to that group appear in the client list.

3. From the client list, select the clients you want included in the export data. You can use **Ctrl** or **Shift** to select more than one client.

4. Right-click and select "Export Workstations" from the menu or click the **Export Workstations** 💾 icon at the top of the list.

   A File Download window opens.

5. Select where you want to save the CSV file, enter a file name, and click **Save**.

Delete Workstations

If a client workstation has not had a heartbeat for a long time or it no longer exists, you can delete its database entry from the Webroot database. Once deleted, the client name no longer appears in the Admin Console.

Note

If you delete a client workstation and it later reconnects to the network and contacts your company server, Webroot AntiSpyware creates a new database entry and adds the client workstation to a default group named after the domain or workgroup where the client workstation is located.

To delete a client workstation from the database:

1. From the Admin Console function tree, select **Administration > Client Management**.

   The Client Management panel opens with a list of all existing groups in the group tree.

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see "Filter Field" on page 8).

2. From the group tree, click the group that includes the clients you want to delete.

   The clients that are assigned to that group appear in the client list.

3. From the client list, select the clients you want to delete. You can select multiple clients by using **Ctrl** or **Shift**.
4. Right-click and select “Delete Workstations” from the menu or click the **Delete Workstations** icon at the top of the list.

   Webroot AntiSpyware deletes the client workstation from its database.

Sweep Now

If you learn about a critical threat, you can use the Sweep Now function to run an immediate sweep on one or more client workstations. The Sweep Now function is available from within the Client Management panel and directly from the function tree.

Before running a Sweep Now function, be aware of the following:

- Webroot AntiSpyware uses the current sweep settings during the sweep. For information about changing these settings, see “Sweep Settings” on page 37. If you want to change the settings, make the changes first and wait for the next polling interval or use the Poll Now function to ensure that client workstations receive the new settings.
- Port 50001 is used to communicate with client workstations. You can change the port from System Settings. (Go to **Administration** > **Configuration** > **System Settings**, **Network** section.)

Note

Running a sweep during business hours may slow performance for each affected client workstation.

To sweep from the Sweep Now panel:

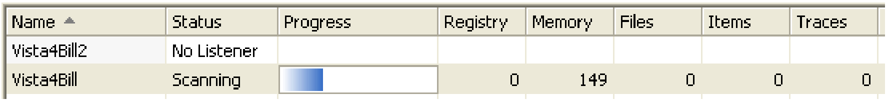
1. From the Admin Console function tree, select **Administration** > **Sweep Now**.

   The Sweep Now panel opens with a list of all existing groups in the group tree.

   If you want to run the sweep on all client workstations in the company, select the company at the top of the group tree. To filter the list of client workstations, use the filter field (see “Filter Field” on page 8).
2. From the group tree, click the group that includes the clients you want to sweep.

   The clients that are assigned to that group appear in the client list.
3. From the client list, select the clients you want to sweep. You can select multiple clients by using **Ctrl** or **Shift**.
4. Right-click and select “Sweep Now” from the menu or click the **Sweep Now** icon at the top of the list.
5. Select the group in the group tree to watch the sweep status.

   The Client panel shows the status for the affected workstations, similar to the following example.



Name	Status	Progress	Registry	Memory	Files	Items	Traces
Vista4Bill2	No Listener						
Vista4Bill	Scanning		0	149	0	0	0

To sweep from the Client Management panel:

1. From the Admin Console function tree, select **Administration** > **Client Management**.
2. Select the group or client workstation where you want to run the sweep. You can select more than one client workstation by using **Ctrl** or **Shift**.

   If you want to run the sweep on all client workstations in the company, select the company at the top of the group tree. To filter the list of client workstations, use the filter field (see "Filter Field" on page 8).
3. Right-click and select "Sweep Now" from the menu or click the **Sweep Now** icon at the top of the list.
4. To check the status of the sweeps, go to **Administration** > **Sweep Now** and click the client group.

To stop sweeps:

1. From the Admin Console function tree, select **Administration** > **Sweep Now**.

   The Sweep Now panel opens, with information about sweeps that are running.

   To filter the list of client workstations, use the filter field (see "Filter Field" on page 8).
2. Select a group to see which workstations in that group are currently running sweeps.
3. To cancel a sweep that is running, select the group or the client workstations (one or more) where you want to stop the sweep. Then click the **Cancel Sweep** icon at the top of the panel.

This stops the sweep regardless if is was started by an administrator or end user.

Client Install and Uninstall

You can install and update the Webroot Clients from the Client Install/Uninstall panel. You can also use this panel to determine the version of the Webroot Clients installed on each workstation and the last heartbeat from the workstation.

Note

If you are updating an existing installation, you do *not* need to uninstall the Webroot Client first.

Before installing the Webroot Client, be aware of the following requirements:

- Installing the Webroot Client from the Admin Console requires Windows networking, access to the admin share (admin$), and NetBIOS enabled on your network. (If you use Active Directory for the installation, NetBIOS does not need to be enabled.)
- If your client workstations are using Windows XP SP2 and the Windows Firewall, you must configure the firewall to have certain exceptions that permit installation from the Admin Console. For instructions, see the *Webroot AntiSpyware Corporate Edition Installation Guide*.

Caution

Do not install the Webroot Client on a file server.

To install and update Webroot Clients:

1. From the Admin Console function tree, select **Administration > Client Install/Uninstall**.

   The Client Install/Uninstall panel opens.

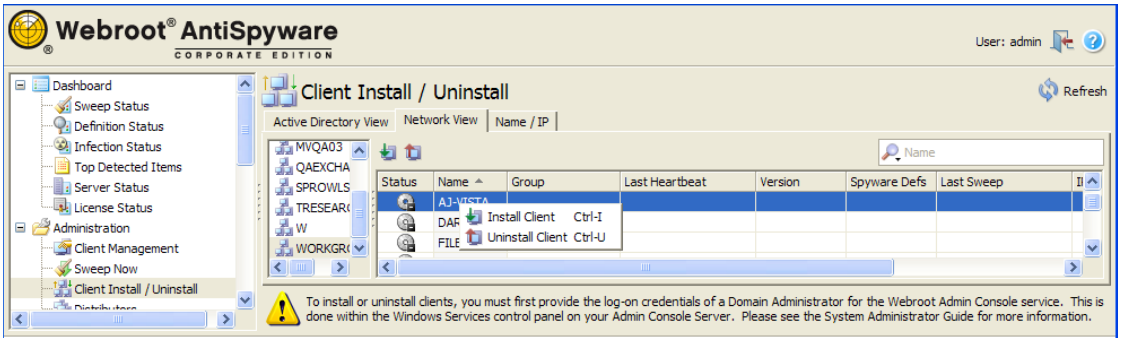
2. Select either the Active Directory View tab or the Network View tab to see a list of the domains or workgroups that exist on your network (middle panel).

   Note

   To view clients in the Active Directory View tab, you must be logged into the Admin Console as a domain user.

3. From the middle panel, select the domain or workgroup of the workstations.

   A list of workstations appears in the far right panel.



To install or uninstall clients, you must first provide the log-on credentials of a Domain Administrator for the Webroot Admin Console service. This is done within the Windows Services control panel on your Admin Console Server. Please see the System Administrator Guide for more information.

4. Select the client workstations where you want to install the Webroot Client. You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations. (The more clients installed at one time, the longer it may take for the operation to complete.)

   If you do not see some client workstations in the Network View tab, you can click the Name/IP tab. From this panel, you can install Webroot Clients using the host name, IP address, or an IP address range.

5. Right-click and select “Install Client” from the menu or click the **Install Client** icon at the top of the panel.

6. Click **Refresh** or go to the Client Management panel to see the status of the installation.

To remove a Webroot Client using the Client Install/Uninstall panel:

1. From the Admin Console function tree, select **Administration > Client Install/Uninstall**.

   The Client Install/Uninstall panel opens. A list of the domains or workgroups that exist on your network appear in the middle panel.

2. Select either the Active Directory View tab or the Network View tab to see a list of the domains or workgroups that exist on your network (middle panel).

3. On the right panel, select the client workstations where you want to uninstall the Webroot Client. You can select more than one workstation by using **Ctrl** or **Shift**.

   Note

   The uninstallation process permanently deletes any detected items, such as viruses and spyware, that were quarantined on the client workstation.

4. Right-click and select “Uninstall Client” from the menu or click the **Uninstall Client** icon at the top of the panel.

To remove a Webroot Client using the Client Management panel:

1. From the Admin Console function tree, select **Administration > Client Management**.

   The Client Management panel opens with a list of all existing groups in the group tree.

   To see all client workstations that have the Webroot Client installed, click the top (company) node of the group tree. To filter the list of client workstations, use the filter field (see “Filter Field” on page 8).

2. From the group tree, click the group with the Webroot Clients you want to remove.

   The clients that are assigned to that group appear in the client list.

3. From the client list, select the Webroot Clients you want to remove. You can select multiple clients by using **Ctrl** or **Shift**.

   Note

   The uninstallation process permanently deletes any detected items, such as viruses and spyware, that were quarantined on the client workstation.

4. Right-click and select “Uninstall Client” from the menu or click the **Uninstall Client** icon at the top of the panel.

Distributors

Webroot AntiSpyware includes a Distributor service component that you can install and run on additional servers to manage workstations in different geographical locations or to manage a large number of workstations. This Distributor service communicates periodically with the Webroot Server's Update service and with the Webroot Client's CommAgents.

Instructions for installing and assigning Distributors is provided in the *Webroot AntiSpyware Corporate Edition Installation Guide*. If you later add another Distributor Service on a company server, you must assign the server to client groups (groups are described in "Manage Client Groups" on page 18).

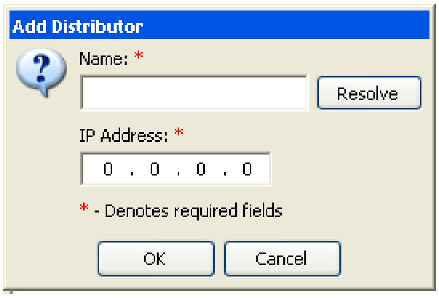
To assign a distributor server:

1. From the Admin Console function tree, select **Administration** > **Distributors**.

   The Distributors panel opens with a list of all groups in the group tree (middle panel).

2. Click **Add Distributor** ✚ at the top of the panel.

   The Add Distributor window opens.



0 . 0 . 0 . 0

* - Denotes required fields

3. Enter a name for the Distributor server.

   If you enter the DNS name of a server on your network, the IP address automatically populates when you tab to the second field.

4. If necessary, enter the IP address of the server.

5. Click **OK**.

   The server name now displays in the list on the right side of the panel.

6. Drag a server from the list to a group or to the company in the group tree.

   To remove a server assignment, select the server in the group tree, right-click, and select "Unassign Distributor."

   To remove the selected distributors from their assignments and from the list of distributors, click **Delete Distributor** ✖ . To update the status of the distributors, click **Refresh** ↻ .

   Your company server will automatically send copies of all updates to all Distributors. You still need to assign updates manually (from **Administration** > **Updates** >**Manual Install**) or set automatic installation rules (from **Administration** > **Updates** > **Auto Install**) to determine which updates should be applied to which groups.

Errors

You can view any errors that a Webroot application generates on a client workstation. You should review the error list periodically and then report any errors to Webroot.

To view errors:

1. From the Admin Console function tree, select **Administration** > **Errors** to open the Errors panel.

   To filter the list of errors, use the filter field (see "Filter Field" on page 8).

2. For more details about an error, click on the desired row.

   More information about the error appears in the Error Details pane below.

3. Contact Webroot Technical Support for assistance with the resolving the error.

User Management

During installation, a user account was defined for the Admin Console. If desired, you can define additional Admin Console users and view a daily audit log that lists actions taken by each user.

To add a new user account:

1. From the Admin Console function tree, select **Administration** > **User Management**.

   The User Management panel opens with a list of all existing user names.

2. Click **Add User/Group** ✚ at the top of the panel.

   The Choose Authentication Type window opens.

3. Click **Domain**, **Local**, or **Group** to enter a local user, or a user or user group from the Active Directory.

   The Add Admin Console User window opens. For Domain and Group authentication, you must enter the domain name. For Local authentication, you must enter a password.

4. Enter the user information click **OK**.

   The new user account displays in the User Management panel.

To edit a user account:

> **Note**
>
> You can only edit a local user account.

1. From the Admin Console function tree, select **Administration** > **User Management**.

   The User Management panel opens with a list of all existing user names.

2. Right-click on a user name and select "Edit User/Group" from the menu or click **Edit User/Group** ✎ at the top of the panel.

   The Edit User window opens.

3. Modify the user information and click **OK**.

To delete a user account:

1. From the Admin Console function tree, select **Administration > User Management**.

   The User Management panel opens with a list of all existing user names.

2. Right-click on a user name and select “Delete” from the menu or click **Delete** ✖ at the top of the panel.

3. From the confirmation box, select **Yes**.

To view audit logs:

1. Locate the logs (the name starts with `Webroot_Server_Audit`...) which are stored in your Webroot Server installation folder.

   The default location is: C:\Program Files\Webroot\Server\WebServer\logs.

2. Open the log in a text editor.

Note

You set how long to retain the daily audit logs from System Settings. (Go to **Administration** > **Configuration** > **System Settings**, **Advanced** section.)

Configuration

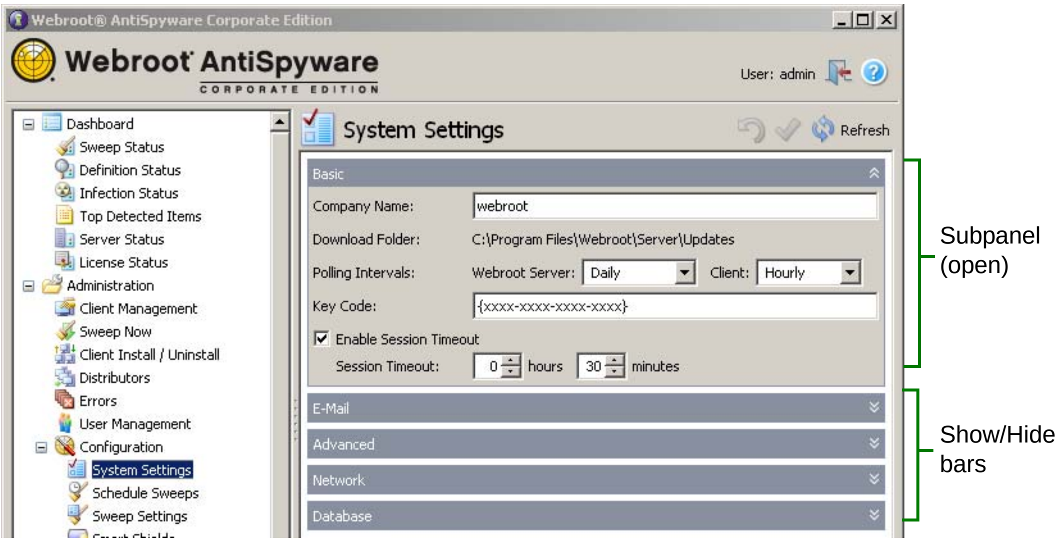
To perform configuration tasks, see the following topics:

- System Settings. Determine settings for the Admin Console, such as polling intervals, e-mail message settings, and port numbers for network communications.
- Schedule Sweeps. Set the weeks, days, and times to run sweeps on client workstations.
- Sweep Settings. Determine what types of potential threats the Webroot Client will locate during its sweeps.
- Smart Shields. Determine what types of threats the Webroot Client will block.
- Detection Settings. Determine how to handle the potential threats copied to the Quarantine.
- Web Security. Enable the Desktop Web Proxy to redirect browser traffic through the Webroot Web Security SaaS service.

System Settings

System settings determine Admin Console operations, including polling intervals, network port settings, e-mail addresses for alert notifications, and so on. Most of these settings were defined during installation (see the *Webroot AntiSpyware Corporate Edition Installation Guide*); however, if you need to modify any settings, you can follow the instructions in this section.

The System Settings panel is shown below. You can click on the show/hide bars to open and close subpanels. When you are finished changing *all* system settings, click **Apply** ✓ at the top right (it's not necessary to click **Apply** ✓ after changing information in each subpanel).



Company Name: webroot

Download Folder: C:\Program Files\Webroot\Server\Updates

Polling Intervals: Webroot Server: Daily Client: Hourly

Key Code: {xxxx-xxxx-xxxx-xxxx}

☑ Enable Session Timeout

Session Timeout: 0 hours 30 minutes

To change Basic settings:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **System Settings**.
2. Click the Basic show/hide bar, if it is not already open.
3. To edit settings, enter information in the appropriate fields.

4. When you are finished changing all system settings, click **Apply** ✓ at the top right.

Basic	
Field	**Description**
Company Name	Name of your company. This identifies your Webroot AntiSpyware product when your server looks for updates from the Webroot Update Server.
Download Folder	*You cannot edit this field; it is determined during installation.* Path to the folder where your company server stores the updates it downloads from the Webroot Update Server.
Polling Intervals:	
Webroot Server	Interval at which your Webroot Server checks for updates from the Webroot Update Server. If you select Manual Only, you must manually check for updates from **Administration > Updates > Update History**, then click **Check for Updates**.
Client	Interval at which the Webroot Clients (CommAgents installed on each workstation) check for updates and configuration changes from the Webroot Server. If you change this interval, each CommAgent will retrieve the new setting the next time it contacts the server. For example, if the polling interval is every hour and the last client heartbeat was 30 minutes ago, changes you make to polling intervals will be applied in 30 minutes. If all clients must receive updates or setting changes immediately, you can use the **Poll Now** button in the Client Management panel; however, you should use this option selectively to ensure that you do not overwhelm your network and servers. **Note:** Updates for Webroot Clients and spyware and virus definitions copy to the Download Folder whenever your company server contacts the Webroot Update Server, but these updates do *not install* automatically. You must either manually install them (see "Manual Install" on page 60) or configure automatic installation (see "Auto Install" on page 59).
Key Code	Unique code that identifies the rights and privileges associated with your installation, such as the number of licenses you have purchased for each client workstation application. If you purchased Webroot AntiSpyware online, you received your Key Code in an e-mail message. If you purchased Webroot AntiSpyware from a store or received it already installed on your computer, the Key Code is on the product packaging.
Enable Session Timeout	Amount of inactive time before the Admin Console session will time out. If you enable this option, enter the session timeout values in the fields that appear below.

To change E-Mail settings:

1. From the Admin Console function tree, select **Administration > Configuration > System Settings**.
2. Click the E-Mail show/hide bar.
3. To edit settings, enter information in the appropriate fields.
4. When you are finished changing all system settings, click **Apply** ✓ at the top right.

E-Mail

Field	**Description**
Message Settings:	
From Address	E-mail address that notification messages will come from. This must be a real e-mail address in the format: tom@webroot.com.
Message Timeout	Amount of time the Admin Console will wait to connect to the mail server before timing out.
Consolidate Alerts	Amount of time the Admin Console will wait to consolidate alerts into a single e-mail message, rather than sending each alert immediately. This reduces the number of e-mail messages recipients receive.
SMTP Settings:	
Server	Fully qualified domain name for your e-mail server used for outgoing mail (SMTP server).
Use SMTP Login	If you use a secure SMTP e-mail server, select this option and enter the user name and password in the fields that appear below. This is the name and password needed to log in to a secure SMTP server. **Note:** Webroot AntiSpyware only supports Auth-Login.
Send Test E-Mail:	
E-Mail Recipient	Select an e-mail address from the drop-down list and click **Send Message**. All e-mail addresses entered into **Administration > Notification Management > E-mail Addresses** are listed in the drop-down list. You can also enter an e-mail address to test it before adding it.

To change Advanced settings:

1. From the Admin Console function tree, select **Administration > Configuration > System Settings**.
2. Click the Advanced show/hide bar.
3. To edit settings, enter information in the appropriate fields.
4. When you are finished changing all system settings, click **Apply** ✓ at the top right.

Advanced	
Field	**Description**
Proxy Settings:	
Server User Name Password	If you use a proxy server to access the Internet, enter your proxy server name or IP address and port number in one of the following formats: • server_name.company.com:80 • 10.0.0.1:80 If you do not use a proxy server, leave the field blank. If you use a proxy server that requires authentication, enter your proxy server user name and password.
Poll Timeout Retries:	
Initial Interval Min & Max	Minimum and maximum time a rejected client workstation should wait before trying to connect again. The actual retry time is a randomly generated time between the minimum and maximum. If the client workstation is rejected again, it doubles the retry time. A rejected client continues to double the retry time until it connects successfully or until it reaches the final retry time. It then continues at the final retry interval until it is successful.
Maximum Interval	Amount of time between retries after the client workstation has been rejected several times. The rejected client continues to retry to connect at this interval until it is successful.
Audit Logging:	
Logs Expire After	Number of days to store the audit log of actions taken by Admin Console users.
E-Mail Recipient	E-mail address that will receive notifications that log information is about to expire. All e-mail addresses entered into **Administration > Notification Management > E-mail Addresses** are listed in the drop-down list.

To change Network settings:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **System Settings**.
2. Click the Network show/hide bar.
3. To edit settings, enter information in the appropriate fields.
4. When you are finished changing all system settings, click **Apply** ✓ at the top right.

Network	
Field	**Description**
Client Service Settings:	
IP/Host Name	The IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, use the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, select or enter the fully qualified domain name of your server (requires a properly configured DNS environment). ⚠ For these changes to take effect, the Clients must poll the Server on their normal interval (see the Client Polling Intervals field on page 30). If a client does not poll on its regular schedule (for example, for mobile clients or off-line clients), you must manually change the following key on the client workstation: HKEY_LOCAL_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\su.
Ports: No SSL SSL	Port on your company server that the Client Service uses to communicate with your client workstations. The default port is 50003 for Client versions 3.5 (prior versions use 50000). If you want to edit this setting, fill in one or both fields with the port you want to use. Be sure that the port you specify is not used to communicate with another system. If you want to use SSL, you must also select the Use SSL option at the bottom of the Network section. ⚠ For Client versions prior to 3.5, the Clients must poll the Server for the changes to take effect (see the Client Polling Intervals field on page 30 or “Poll Now” on page 20). If a client does not poll on its regular schedule (for example, for mobile clients or off-line clients), you must manually change the following key on a client workstation: HKEY_LOCAL_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\su. After all clients have polled, you must restart the Server’s client service.
Admin Server/ Distributor Settings:	

Network	
Field	**Description**
Ports: No SSL SSL	Port on your company server that the Distributor Service uses to distribute updates to distributor servers and client workstations. The default port is 50003. If you want to edit this setting, fill in one or both fields with the port you want to use. Be sure that the port you specify is not used to communicate with another system. The Admin Console service on your company server also uses the port you configure here. If you want to use SSL, you must also select the Use SSL option at the bottom of the Network section. ⚠ For Client version 3.5, the Clients must poll the Server for the changes to take effect (see the Client Polling Intervals field on page 30 or "Poll Now" on page 20). If a client does not poll on its regular schedule (for example, for mobile clients or off-line clients), you must manually change the following key on a client workstation: HKEY_LOCAL_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\su. After all clients have polled, you must restart the Webroot Admin Console service. You must also complete the instructions for changing the distributor service port on the company server, as described in "Installing and Assigning Distributors" in the *Webroot AntiSpyware Corporate Edition Installation Guide*. The port on each distributor server must be the same as the port defined in this field.
Client Settings:	
Sweep Now Ports: No SSL SSL	Port on your company server used to start a sweep of the selected client workstations from the Admin Console. The default port is 50001. If you want to edit this setting, fill in one or both fields with the port you want to use. Be sure that this port is not used to communicate with another system. If you want to use SSL, you must also select the Use SSL checkbox, located at the bottom of the Network section.
Poll Now Ports: No SSL SSL	Port on your company server used to poll the selected client workstations from the Admin Console to update their heartbeat and status. The default port is 50002. If you want to edit this setting, fill in one or both fields with the port you want to use. Be sure that the port you use is not used to communicate with another system. If you want to use SSL, you must also select the Use SSL checkbox, located at the bottom of the Network section.
Use SSL	If you want to use SSL connections for the ports listed above, select this option at the bottom of the panel. **Note:** Selecting this option means that all of the ports with the SSL field will use SSL. Be sure to fill in the SSL field for each port above.

To change Database settings:

1. From the Admin Console function tree, select **Administration > Configuration > System Settings**.
2. Click the Database show/hide bar.
3. To edit settings, enter information in the appropriate fields.
4. When you are finished changing all system settings, click **Apply** ✓ at the top right.

Database	
Field	**Description**
Server Type Database Version	*You cannot edit these fields.* Type and version of the SQL server you are using.
Server	Name of the server that is running MS SQL Server or SQL Server Express.
Database	Name of the database you configured for the Webroot AntiSpyware data.
Username	User name you defined for the Webroot AntiSpyware database in SQL Server or SQL Server Express.
Password	Password you defined for the Webroot AntiSpyware database in SQL Server or SQL Server Express.

Schedule Sweeps

You can schedule sweeps to run on specific days and times. Before you create sweep schedules, you might consider:

- Scheduling different client groups to sweep at different times to reduce load on the company server when clients report their results.
- Scheduling clients to sweep during off-hours as long as the system remains powered on (even with the user logged out). You need to let users know when their sweep is scheduled to make sure they leave their computer on for the sweep to run.

To schedule sweeps:

1. From the Admin Console function tree, select **Administration > Configuration > Schedule Sweeps**.

   The Schedule Sweeps panel opens.

2. Select the group or client workstation where you want to schedule the sweep. If you want these settings to apply to the whole company, select the company at the top of the group tree.

   The Schedule Sweeps panel shows the current settings for the selected group or company.

3. Select the options you want.
4. When you are finished changing all settings, click **Apply** ✓ at the top right.

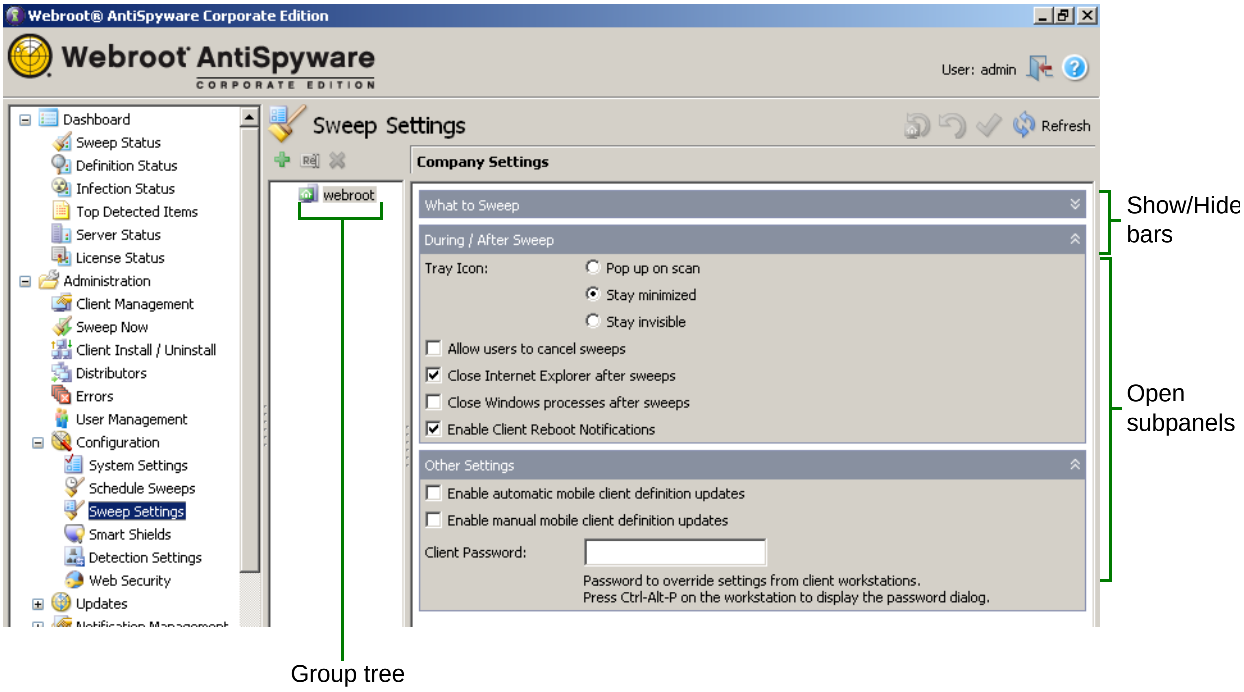
Option	Description
Allow user to modify settings	If you want end users to be able to change these settings, select this option. If you set this option, any changes you attempt to make will be ignored. If you need to change the schedule, you must deselect the option, wait for the clients to poll, then change the schedule.
Every: <number> weeks	Select the weekly interval.
Sweep Days Sweep Time	Select the day of the week and the time you want to run the sweep. The schedule uses the 24-hour clock.
Run missed sweeps at startup	Select this option if you want to run a missed sweep at Windows startup.
Sweep known folders on startup	Select this option to scan only the folders (with previously detected items) at Windows startup, so the sweep runs quickly. Using this option helps to ensure that sweeps run periodically, even if the computer is turned off when regular sweeps are scheduled.
Enable Deep Memory Scan	Select this option if you want the startup sweep to do an in-depth memory sweep. This option may delay Windows startup for a few minutes.
Delay startup sweeps by	Select this option if you want to delay any startup sweep after the client workstation starts Windows. Use the Minutes field to enter how soon the sweep should begin after Windows starts up.

To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Revert to Inherited Settings** at the top right.

Sweep Settings

You can configure settings that control how the Webroot Client sweeps workstations to detect viruses, spyware, and potentially unwanted programs. You can update sweep settings for the entire company or by specific group. We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

The Sweep Settings panel is shown in the example below. You can click on the show/hide bars to open and close subpanels. The fields in the subpanels include a User Editable check box. You can select this option to allow users the ability to change that particular settings. (After you make a settings user editable, any future changes you attempt to make from the Admin Console to that setting will be ignored. To change it, you must deselect the User Editable option, wait for the clients to poll or poll them immediately, then change the setting.)



Sweep Settings

Company Settings

What to Sweep

During / After Sweep

Tray Icon: ○ Pop up on scan
● Stay minimized
○ Stay invisible

□ Allow users to cancel sweeps

☑ Close Internet Explorer after sweeps

□ Close Windows processes after sweeps

☑ Enable Client Reboot Notifications

Other Settings

□ 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.

To configure the What to Sweep settings:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Sweep Settings**.
2. Click the What to Sweep show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To edit settings, select the desired option. If you want end users to be able to change a setting, select the User Editable option next to the desired field.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Revert to Inherited Settings** at the top right.

What to Sweep

Option	Description
Sweep Targets:	Specifies the drives for Webroot Clients to sweep. Typically, most spyware installs on the C: drive, but you should sweep all hard drives periodically.
Only known folders	Makes the sweep run faster by specifying that Webroot Clients only look in the folders where spyware is typically found. Using this option performs a less thorough sweep. You should periodically sweep all folders.
All folders on selected drives	Specifies that Webroot Clients look in all folders on the drives you select. This type of sweep will take longer to run. Using this option performs a more thorough sweep.
Sweep Options:	
Memory	Sweeps computer memory. Typically, you want to sweep memory each time a sweep runs because spyware commonly loads into memory.
Memory Sandboxing	Performs a thorough analysis of executable programs by running them in a protected memory area.
Registry	Sweeps computer registries. Typically, you want to sweep the registry each time a sweep runs, since some unwanted programs commonly create entries in a computer registry.
All User Accounts	Sweeps all registry entries, even those related to another user account or login ID on the computer, since spyware commonly creates entries in a registry. Using this option makes sure all registry entries are swept. If you deselect this option, Webroot Clients only sweep the account used for logging in.
Tracking Cookies	**Note:** To access this option, select All User Accounts (above). Includes known tracking cookies (from the spyware and virus definitions) in the sweep. You may want to remove tracking cookies. Some Web sites now issue tracking cookies that allow multiple Web sites to store and access cookies that may contain personal information (including surfing habits, user names and passwords, and areas of interest), then share the information they contain with other Web sites.
System Restore Folder (Windows XP only)	Sweeps the folder where Windows stores System Restore files. If a restore point contains spyware, Webroot Clients find them and let you remove them from the restore point.
Direct Disk Sweeping	Permits Webroot Clients to bypass the Windows operating system during sweeps and detect the newest strains of spyware that hide themselves from the operating system.

What to Sweep	
Option	**Description**
Rootkit Detection	**Note:** To access this option, select Direct Disk Sweeping (above). Includes rootkits in sweeps. Rootkits use file-obfuscation techniques to allow spyware and other malicious software to avoid detection and removal. Rootkits typically hide in logins, processes, files and logs, and may include software to capture information from desktops or a network. However, some legitimate programs use rootkits. If your company systems use these types of programs with rootkits, or use hidden files or partitions that would look like a rootkit, you can create a whitelist so they are ignored in the sweep. To create a rootkit whitelist, see “Detection Settings” on page 51 and “Gather Information for Whitelists” on page 57. Webroot strongly suggests that you **do not enable** the Rootkit Detection option in your production environment, unless you have properly tested how it will affect your hardware and software in a controlled environment using standard machine images. This testing will allow you to identify any valid hidden partitions and directories so you can include them in the whitelist before performing sweeps. Be aware that using the Rootkit Detection option extends the duration of the sweep function.
Sweep Contents of Compressed Files	Sweeps compressed files such as .zip, .rar, .lzh, and .cab files. Unwanted programs can hide inside these types of files. You may want to use this option after you have found spyware and want to be sure it is removed. **Note:** Using this option may significantly increase the time required for a sweep the first time you use it. After the first sweep with this option, Webroot AntiSpyware will skip compressed files that have not changed, thereby saving time.
Antivirus Options:	(Only available if you have Webroot AntiSpyware with AntiVirus.)
Sweep for Viruses	Sweeps for viruses, which are self-replicating programs that can infest computer code, documents, or applications.
Behavioral Genotype Detection	Enables additional protection (available with Sophos® AntiVirus) by analyzing programs for behavior typical of malware before the program’s code can execute. This option can locate many emerging threats, but on very rare occasions, a legitimate program could be classified as malicious because it shows malware-like behavior.
Sweep Throttling:	
Memory Sweep	Controls how much a memory sweep affects CPU usage. To reduce the impact on CPU usage, move the slider toward the High setting; however, this also causes memory sweeps to take longer. The actual setting you need depends on your hardware. Older hardware may require a setting closer to High. Newer hardware may not need this setting adjusted at all.

What to Sweep	
Option	**Description**
File System Sweep	Controls how much a file system sweep affects CPU usage. To reduce the impact on CPU usage, move the slider toward the High setting; however, this also causes memory sweeps to take longer. The actual setting you need depends on your hardware. Older hardware may require a setting closer to High. Newer hardware may not need this setting adjusted at all.

To configure the During/After Sweep settings:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Sweep Settings**.
2. Click the During/After Sweep show/hide bar.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To edit settings, select the desired option. If you want end users to be able to change a setting, select the User Editable option next to the desired field.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

   To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Revert to Inherited Settings** at the top right.

During/After Sweep	
Option	**Description**
Tray Icon:	Allows you to select how you want the Webroot Client to appear on client workstations as described below.
Pop up on scan	Displays a system tray icon that end users can double-click to display the Webroot Client window and automatically pops up the window whenever a sweep starts, whether scheduled or using Sweep Now.
Stay minimized	Default and recommended setting. Displays a system tray icon that end users can double-click to display the Webroot Client window, but does *not* pop up the window whenever a sweep starts. From this interface, end users can start their own sweeps and adjust any allowable settings. When a sweep is running, the tray icon will animate to show that Webroot Client is sweeping their system.
Stay invisible	Does not display a system tray icon and does not do anything when a sweep starts. End users have no access to the Webroot Client window to use options that are set as editable in the Admin Console.
Allow users to cancel sweeps	Allows you to permit end users to stop a sweep, regardless of how the sweep was started.

During/After Sweep	
Option	**Description**
Close Internet Explorer after sweeps	Allows you to close Internet Explorer after a sweep if the sweep found spyware or other threats that Webroot Clients could not delete with Internet Explorer open. If you have users who work in Internet Explorer regularly, *deselect* this option. Deselecting the option leaves Internet Explorer open after a sweep.
Close Windows processes after sweeps	Allows you to specify that Windows processes close after a sweep, if the sweep found spyware or other threats that Webroot AntiSpyware could not delete with a Windows process running.
Enable Client Reboot Notifications	If Webroot Clients need to restart Windows to completely remove one or more items found, this option will display a small message near the system tray telling users that they need to restart Windows. This option does *not* force a restart, but lets users know that they should restart Windows when they can. If you do not select this option, users will not be notified that a restart is needed. Webroot Clients will wait until the next restart to fully remove found items. However, the more time that passes until the next restart, the greater the risk that Webroot Clients will not be able to fully remove the found item.

To configure the Other settings:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Sweep Settings**.
2. Click the Other Settings show/hide bar.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To edit settings, select the desired option. If you want end users to be able to change a setting, select the User Editable option next to the desired field.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

   To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Revert to Inherited Settings** at the top right.

Other Settings	
Option	**Description**
Enable automatic mobile client definition updates	Select this option if you have end users who use laptops and travel a lot. This option lets them receive spyware and virus definition updates directly from Webroot automatically when they are connected to the Internet. For more information, see "Auto Install" on page 59.

Other Settings ***(continued)***	
Option	**Description**
Enable manual mobile client definition updates	Select this option if you have end users who use laptops and travel a lot. This option lets them receive spyware and virus definition updates directly from Webroot by clicking a button when they are connected to the Internet. For more information, see "Manual Install" on page 60.
Client Password	Enter a password that lets system administrators access and change Webroot AntiSpyware settings when you are working at a client workstation.

Smart Shields

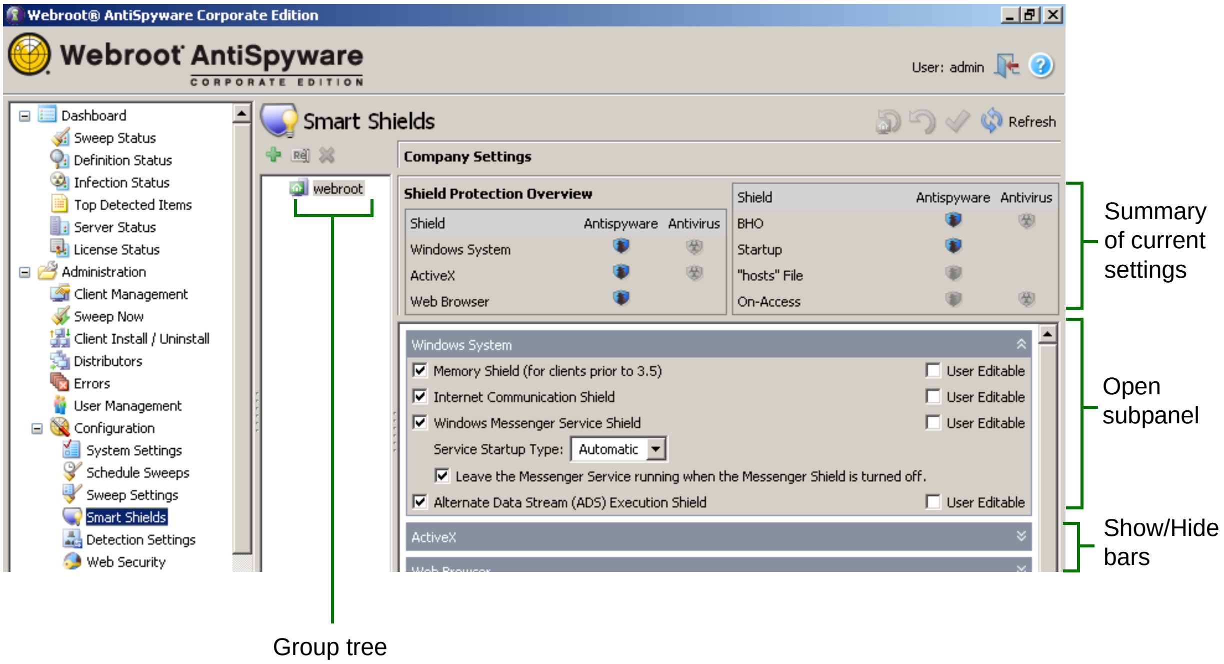
You can configure Smart Shields to continuously monitor common activities and block infections from downloading to workstations. Smart Shields protect your systems against viruses and unwanted programs that may change settings in your Web browser, on Windows, and in certain files and programs. You can update shield settings for the entire company or by specific group. We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

Note

If you have the AntiVirus edition and you want real-time virus protection, you must enable the On Access shields.

The Smart Shields panel is shown in the following example. A summary of the current shield settings is shown at the top of the panel.

You can click on the show/hide bars to open and close subpanels. The fields in the subpanels include a User Editable check box. You can select this option to allow users the ability to change that particular setting. (After you make a setting user-editable, any future changes you attempt to make from the Admin Console to that setting will be ignored. To change it, you must deselect the User Editable option, wait for the clients to poll or poll them immediately, then change the setting.)



Shield Protection Overview

Shield	Antispyware	Antivirus
Windows System	●	●
ActiveX	●	●
Web Browser	●	

Shield	Antispyware	Antivirus
BHO	●	●
Startup	●	
"hosts" File	●	
On-Access	●	●

Windows System

☑ Memory Shield (for clients prior to 3.5) □ User Editable

☑ Internet Communication Shield □ User Editable

☑ Windows Messenger Service Shield □ User Editable

Service Startup Type: Automatic

☑ Leave the Messenger Service running when the Messenger Shield is turned off.

☑ Alternate Data Stream (ADS) Execution Shield □ User Editable

To configure Windows System shields:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
2. Click the Windows System show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

Windows System Options	
Option	**Description**
Memory Shield (for clients prior to 3.5)	Searches memory every hour looking for potentially unwanted programs. **Note:** This shield manages only Webroot Client versions prior to 3.5. In versions 3.5 and above, the enhanced protection from the OnAccess shields supersedes this Memory shield.
Internet Communications Shield	Watches for communication from your computer to known Web sites that are related to potentially unwanted programs, such as adware and spyware. Webroot AntiSpyware includes a list of known sites with its spyware and virus definitions. If Webroot Clients detect an attempt to communicate with a site on the list, it will block access to the site.

Windows System Options	
Option	**Description**
Windows Messenger Service Shield	(Applies only to Windows 2000 and XP.) Turns off and actively watches the Microsoft Messenger Service. This service is not an instant messaging program and does not affect your use of instant messaging. This service is often used for sending spam and creating pop-up ads. Turning off the service stops these types of spam and pop-ups. If you use this service to broadcast information to your users, do not turn on this shield.
Service Startup Type	Controls the state of the Messenger Service Startup Type when the Messenger Shield is off (applies if you turn the Messenger Shield off, after having turned it on). Select one of the following: • Automatic—The service starts when Windows starts or when the service is called for the first time. • Manual—You must start the service manually before the operating system can load it and make it available for use. • Disabled—You cannot start the service automatically or manually.
Leave the Messenger Service running...	Controls the status of the Messenger Service when the Messenger Shield is off.
Alternate Data Stream (ADS) Execution Shield	Actively watches for programs that try to start from an alternative data stream (ADS). ADS is a highly technical way to hide images, data, or code in a file and can be used to hide malicious code. The hidden content is impossible to detect using regularly available tools, such as Windows Explorer. Turning on this shield stops a program from starting if it tries to start from an ADS.

To configure ActiveX shields:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
2. Click the ActiveX show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

ActiveX Options

Option	Description
ActiveX Shield	Actively watches for programs that install ActiveX technology on workstations. Whenever a program tries to install ActiveX technology, the Webroot Client blocks the installation. ActiveX technology is a group of functions developed by Microsoft that let programs share information. Many legitimate programs use ActiveX, but some spyware programs also use ActiveX to install themselves.
ActiveX Whitelist	Allows you to create a whitelist of applications that use ActiveX if end users need these applications. Webroot Clients will not block the applications in the whitelist. To add an application to the whitelist: 1. Click **Add** ✚. 2. In the dialog box, enter the product or company name to identify the product. (This is purely for informational purposes.) Then enter the file or class ID of the executable file associated with the application. You can also enter the entire run key that will be added to the registry for the application. 3. Click **OK**. To change or delete an application, select it and click **Edit** ✎ or **Delete** ✖. For information about gathering what you need for the whitelist, see "Gather Information for Whitelists" on page 57.

To configure Web Browser shields:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
2. Click the Web Browser show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

Web Browser Options

Option	Description
Tracking Cookie Shield	Actively watches for tracking cookies as end users visit Web sites and removes them. Tracking cookies are cookies that can track Web activities. These *may* include cookies that contain user names, passwords, or similar information entered on some Web sites.
Send Cookie Events	Sends cookie removal information to the Console.

Web Browser Options	
Option	**Description**
Internet Explorer Hijack Shield	Actively protects various Internet Explorer functions, such as the home page, search page, error pages, and other default pages that the browser opens. Some spyware programs change (“hijack”) these pages without warning. Whenever spyware programs try to change these pages, Webroot Clients blocks the change.
Protected Home Page	Allows you to enter the address of the Web site you want as the home page in the format: http://www.webroot.com. When you enter a home page, the address you enter will replace the end user’s existing home page. End users will only be able to change their home page through the **Smart Shields >Web Browser** panel. If the Tray Icon Setting (**Administration > Configuration > Sweep Settings**) is set to Stay Invisible, end users will not be able to change their home page.
Internet Explorer Favorites Shield	Actively protects your Internet Explorer favorites. Whenever a Web site tries to change favorites, Webroot Clients block the change. Some Web sites add entries to favorites without warning. This option ensures that changes are not made. Even if Webroot Clients are not open when a change is attempted, they will block the change.
Internet Explorer Secured Zones Shield	Actively protects the Internet Explorer security settings (select **Tools > Internet Options** and click the **Security** tab). Whenever a program tries to change these settings, Webroot Clients block the change. Some programs change these options without warning.

To configure Browser Helper Objects (BHO) shields:

1. From the Admin Console function tree, select **Administration > Configuration > Smart Shields**.
2. Click the Browser Helper Objects (BHO) show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

Browser Helper Objects (BHO) Shield Options

Option	Description
Browser Helper Objects (BHO) Shield	Actively watches workstations for the installation of Browser Helper Objects (BHOs). Whenever a BHO tries to install itself, Webroot Clients block the installation. BHOs are add-on programs that work with a browser. Some spyware programs add BHOs without warning. This shield ensures that programs do not add a BHO without end users being aware of it.
BHO Whitelist	Allows you to define a whitelist of BHOs that your users need to install. Webroot Clients will not block the applications in the whitelist. To add an application to the whitelist: 1. Click **Add** ✚. 2. In the dialog box, enter the product or company name to identify the product. (This is purely for informational purposes.) Then enter the file or class ID of the executable file associated with the application.You can also enter the entire run key that will be added to the registry for the application. 3. Click **OK**. To change or delete an application, select it and click **Edit** ✎ or **Delete** ✖. For information about gathering what you need for the whitelist, see "Gather Information for Whitelists" on page 57.

To configure Startup Programs Options shields:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
2. Click the Startup Programs Options show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

Startup Programs Options	
Option	**Description**
Startup Shield	Actively watches startup items for any known spyware that tries to change startup items. Some spyware programs will add startup items, so that they will always start. This shield ensures that known spyware programs do not add something to the startup items.
Startup Shield Whitelist	Allows you to define a whitelist of applications that your users need to start with Windows. Webroot Clients will not block the applications in the whitelist. To add an application to the whitelist: 1. Click **Add** ➕. 2. In the dialog box, enter the file name of the executable file associated with the application. You can also enter the entire run key that will be added to the registry for the application. 3. Click **OK**. To change or delete an application, select it and click **Edit** ✏ or **Delete** ✖.

To configure “Hosts” File shields:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
2. Click the “Hosts” File show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

“Hosts” File Options	
Option	**Description**
“hosts” File Shield	Actively prevents changes to the Hosts file. Some spyware programs will add or change the IP address for a Web site in the Hosts file. When you try to access the added or changed Web site, you will be sent to a different Web site, such as an advertising site. This shield ensures that spyware programs do not change an IP address in the Hosts file. If end users are permitted to edit the Hosts file, do not turn this shield on.
Keep “hosts” file read-only	Controls the state of the Hosts file when the Hosts File Shield is off (applies if you turn the Hosts File Shield off, after having turned it on).
Common Ad Sites Shield	Sets the IP address for known advertising sites to the IP address for your computer. This blocks banner and other advertising from these sites. When you go to a Web site that has advertising from one of the blocked sites, you may see a small graphic that indicates a broken link to a graphic (typically a red X in a box). This just shows where the blocked ad would display.
Use Definitions	Enables the list of known advertising sites that come as part of the spyware and virus definitions to block banner and other advertising from the sites on the list.
Use Custom List Blocked Websites	Allows you to create a list of Web sites to block banner and other advertising from those sites. To add a Web site to the “blocked” list: 1. Click **Add** ➕. 2. In the dialog box, enter the site address. Include “WWW” in this address. 3. Click **OK**. To change or delete a site, select it and click **Edit** ✎ or **Delete** ✖.

To configure On Access shields:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
2. Click the On Access show/hide bar, if the subpanel is not already open.
3. From the group tree, select the company node or specific group for which you want to apply the settings.
4. To turn settings on or off, select the desired fields. If you want end users to be able to change a setting, select the User Editable checkbox next to the desired options.
5. When you are finished changing all shields, click **Apply** ✓ at the top right.

On Access Options	
Option	**Description**
On Write Shield	Actively watches for known spyware and viruses during write operations.
On Read Shield File Types to Scan	Actively watches for known spyware and viruses during read operations. The file types shown in the File Types to Scan list will be included in the shields. To add to the scan list: 1. Click **Add** ✚. 2. In the dialog box, enter a file extension. 3. Click **OK**. To change or delete a file type, select it and click **Edit** ✎ or **Delete** ✖. To revert back to the original list, select **Restore Default List** ↖.
On Execute Shield Additional Blocked Applications	Allows you to block files from executing on the client workstation when a user tries to start a specific application. For example, you could add a file sharing application that you do not want to let company personnel use. To add file types to the “blocked” list: 1. Click **Add** ✚. 2. In the dialog box, enter the file name of the executable file associated with the application. 3. Click **OK**. To change or delete a file type, select it and click **Edit** ✎ or **Delete** ✖.

Note

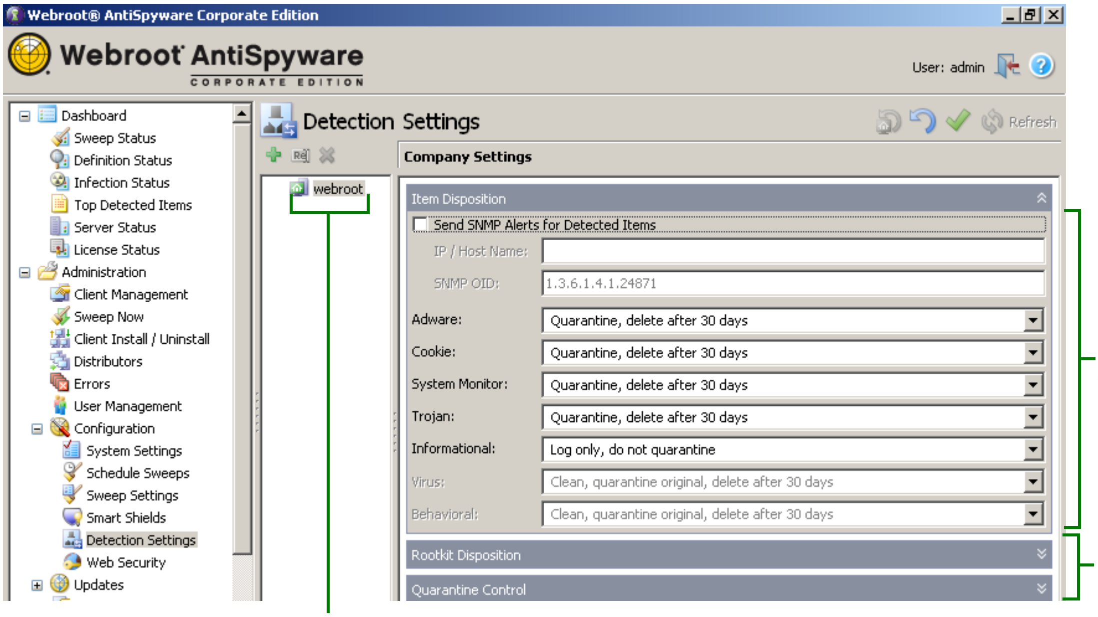
If you have the AntiVirus edition and you want real-time virus protection, you must enable the On Access shields.

Detection Settings

Before running sweeps, you should determine the disposition (for example, log or quarantine) of any detected spyware and viruses. By default, Webroot AntiSpyware quarantines most types of items and deletes them after 30 days. You can change the default settings for each type: adware, tracking cookies, system monitors, Trojan horses, informational items, and viruses. You can also create a whitelist of items you want the sweep to exclude.

You can update detection settings for the entire company or by specific group. We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

The Detection Settings panel is shown in the example below.



☐ Send SNMP Alerts for Detected Items

IP / Host Name:

SNMP OID: 1.3.6.1.4.1.24871

Adware: Quarantine, delete after 30 days

Cookie: Quarantine, delete after 30 days

System Monitor: Quarantine, delete after 30 days

Trojan: Quarantine, delete after 30 days

Informational: Log only, do not quarantine

Virus: Clean, quarantine original, delete after 30 days

Behavioral: Clean, quarantine original, delete after 30 days

Open subpanel

Show/Hide bars

Group tree

To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Revert to Inherited Settings** .

To configure Item Disposition:

1. From the function tree, select **Administration** > **Configuration** > **Detection Settings**.
2. From the group tree, select the group for which you want to apply the settings. If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. Click the Item Disposition show/hide bar, if the subpanel is not already open.
4. Select each option you want.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

Item Disposition

Option	Description
Send SNMP Alerts for Detected Items	Select this option to send Simple Network Management Protocol (SNMP) alerts when Webroot Clients detect items such as viruses or spyware on a client workstation. Then fill in the fields below to identify the SNMP server.
IP/Host Name	DNS name or IP address of your management server. This is the server where your SNMP management software is installed.
SNMP OID	SNMP object identifier (OID) assigned to Webroot Software, Inc.
Adware Cookie System Monitor Trojan Informational	Select how you want Webroot Clients to manage adware, cookies, system monitors, Trojans, and informational items: • Log only, do not quarantine (default for Informational type) • Quarantine, delete after 2 days • Quarantine, delete after 7 days • Quarantine, delete after 30 days (default for most types) • Quarantine, delete after 365 days • Do not quarantine, delete right away
Virus	**Note**: To access this option, you must first select the Sweep for Viruses option in the Sweep Settings panel. Select how you want Webroot Clients to manage viruses: • Log only, do not clean or quarantine • Clean, quarantine original, delete after 2 days • Clean, quarantine original, delete after 7 days • Clean, quarantine original, delete after 30 days (default) • Clean, quarantine original, delete after 365 days • Clean, delete original right away **Note**: “Cleaning” is the process of removing infected portions of a file, then restoring the file.
Behavioral	**Note**: To access this option, you must first select the Behavioral Genotype Detection option in the Sweep Settings panel. Select how you want Webroot Clients to manage viruses detected with the Behavioral Genotype Detection option: • Log only, do not quarantine • Quarantine, delete after 2 days • Quarantine, delete after 7 days • Quarantine, delete after 30 days (default) • Quarantine, delete after 365 days • Do not quarantine, delete right away

To configure Rootkit Disposition:

1. From the function tree, select **Administration** > **Configuration** > **Detection Settings**.
2. From the group tree, select the group for which you want to apply the settings. If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. Click the Rootkit Disposition show/hide bar.
4. Select each option you want.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

Rootkit Disposition	
Option	**Description**
Disposition	**Note**: To access these options, you must first select the Rootkit Detection option in the Sweep Settings panel. Select how you want Webroot AntiSpyware to handle any found rootkits: • Log only, don't quarantine • Quarantine, delete after 2 days • Quarantine, delete after 7 days • Quarantine, delete after 30 days • Quarantine, delete after 365 days • Do not quarantine, delete right away
Whitelisted Rootkit Files	You can create a whitelist of legitimate program files that use rootkits. You can also add hidden files, folders, or partitions that Webroot Clients will detect as rootkits. Webroot Clients will ignore the files in the whitelist. To add a file to the whitelist: 1. Click **Add** ✚. 2. In the dialog box, enter the full path to the file. 3. Click **OK**. This field opens the list of files that you do not want Webroot Clients to identify as rootkits. To change or delete a file, select it and click **Edit** ✎ or **Delete** ✖. For information about gathering what you need for the whitelist, see "Gather Information for Whitelists" on page 57.

To configure Quarantine Control:

1. From the function tree, select **Administration > Configuration > Detection Settings**.
2. From the group tree, select the group for which you want to apply the settings. If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. Click the Quarantine Control show/hide bar. (You must run a sweep before any items will appear in the Detected Items list.)
4. Select each option you want.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

Quarantine Control	
Option	**Description**
Always Keep/Restore from Quarantine	**Note**: Before items appear in the list, you must first run a sweep. Lists the items you want sweeps to ignore and not quarantine. Once selected, these items will always be kept in the list and ignored in future sweeps for the selected group. Use the arrows to move items between the Always Keep/Restore From Quarantine list and the Detected Items list.
Detected Items	Lists the items detected during the sweep. For any items you want to restore from the Quarantine, select them and click the left arrow to move them to the Always Keep/Restore From Quarantine list. Any already quarantined instances will be restored within five minutes of the next poll.
Item Description	Shows more information about a detected item. Select an item in the Detected Items list and read more about it. For additional information, click **Details**.

To configure Exclusions:

1. From the function tree, select **Administration** > **Configuration** > **Detection Settings**.
2. From the group tree, select the group for which you want to apply the settings. If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. Click the Exclusions show/hide bar.
4. Select each option you want.
5. When you are finished changing all settings, click **Apply** ✓ at the top right.

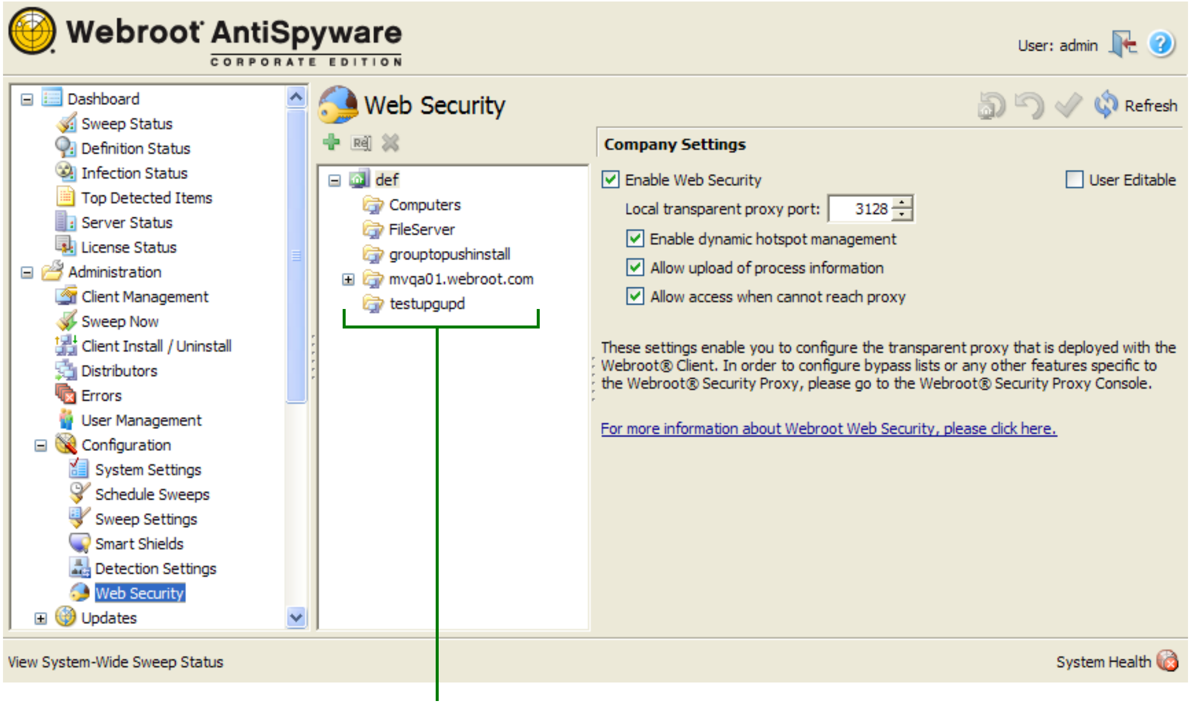
Exclusions

Option	Description
Enable Global Exclusions	Click to enter a list of files you would like skipped during sweeps and shield detection.
Exclude Files, Folders, & Types	Exclude items from the sweep detection as follows: 1. Click **Add** ✚. 2. In the dialog box, enter a file name, folder, or file extensions (for example, “.ext”). **Note:** If desired, you can include environment variables in a directory or file path by using a % sign on either side: for example, enter `%SystemRoot%` as a variable for the system root. Within the string, there can be only one environment variable and it must be placed first (for example, `%SystemRoot%\Windows`). If you do enter a second environment variable or a variable in another position, the system will treat it as a fully qualified directory name instead of a variable. 3. Click **OK**. To change or delete an excluded item, select it and click **Edit** ✎ or **Delete** ✖. Do not exclude .dll, .exe, or .com file types; spyware typically hides in these types of files.

Web Security

You can configure a proxy connection between your Webroot Clients and the Webroot Web Security SaaS (Software as a Service). Web Security SaaS is a hosted Web filtering service that offers an alternative to on-premise hardware and software solutions at a much greater value. The filtering service routes Internet traffic through Webroot data centers, where malicious Web threats and unwanted content are blocked before reaching your network.

During Webroot Client installation, a transparent Desktop Web Proxy is deployed to the client workstations. You can configure the proxy connection in the Web Security panel, as shown in the example below.



Company Settings

☑ Enable Web Security

□ User Editable

Local transparent proxy port: 3128

☑ Enable dynamic hotspot management

☑ Allow upload of process information

☑ Allow access when cannot reach proxy

These settings enable you to configure the transparent proxy that is deployed with the Webroot® Client. In order to configure bypass lists or any other features specific to the Webroot® Security Proxy, please go to the Webroot® Security Proxy Console.

For more information about Webroot Web Security, please click here.

Group tree

To configure the proxy settings:

1. From the function tree, select **Administration** > **Configuration** > **Web Security**.
2. From the group tree, select the group for which you want to apply the settings. If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. Select **Enable Web Security**.
4. If necessary, change the port number for the local transparent proxy port. Otherwise, leave the port number at the default, “3128.”
5. If desired, de-select other options (described in the following table).
6. If you want end users to be able to change settings, select the User Editable checkbox.
7. When you are finished changing all settings, click **Apply** ✓ at the top right.

Web Security Options	
Option	**Description**
Enable dynamic hotspot management	Enables roaming users to temporarily access the Internet when outside their normal IP range (for example, when attempting to access the Internet from a hotel or Internet café). This option establishes a connection with a third-party proxy, so that Web traffic routes through the filtering service.
Allow upload of process information	Allows the Web filtering service to upload information from the Webroot Clients. You can view Webroot Client information from Webroot Security's Admin Portal, if the full logging option is enabled.
Allow access when cannot reach proxy	Allows the Webroot Clients to connect directly to the Internet, without filtering, if the proxy connection cannot be reached.

Gather Information for Whitelists

If you plan to turn on detection options for ActiveX, Browser Helper Objects (BHOs), or rootkits, you must first define whitelists for any programs end users may need that use these technologies. For the whitelists, you need either the class ID or full path to the file. Once you know what programs your end users need, use the following procedure to gather the information needed for the whitelists. The steps use the Google Toolbar and the BHO shield and whitelist as an example.

To define whitelists for the ActiveX, BHO, and rootkits:

1. From the Admin Console, turn on the detection options you want.
2. On a clean computer that does not have any of the ActiveX, BHO, or rootkit programs installed, install the Webroot Client.

   We recommend using the default Tray Icon setting (Stay Minimized), so that you can open the Webroot Client interface on the workstation. You need to view the session log there.
3. From the Admin Console, poll the client workstation to make sure that it has the options turned on that you want. See "Poll Now" on page 20.
4. From the clean computer, try to install the first program that uses ActiveX, BHO, or rootkit technology.

   The Webroot Client will block the installation and the installation will display a message saying that it failed.
5. From the clean computer, double-click the Webroot Client icon in the system tray and select **Reports > Session Log**.
6. Review the session log for information about the attempted installation.

The following example shows what the log contains when you attempt to install the Google Toolbar with the BHO shield turned on:

```
2:40 PM: Browser Helper Object (BHO) Shield is On

2:42 PM: Browser Helper Object (BHO) Removed: c:\program
files\google\googletoolbar1.dll [{2318C2B1-4965-11d4-9B18-009027A5CD4F}]
```

7. In the session log, copy the ID of the .dll file, including the curly brackets.

   For example: {2318C2B1-4965-11d4-9B18-009027A5CD4F}

8. From the Admin Console function tree, select **Administration** > **Configuration** > **Smart Shields**.
9. Click the **Browser Helper Objects (BHO) Shield** show/hide bar.
10. Below the BHO Whitelist, click **Add**.
11. Enter the product or company name to identify the product (informational purposes only).
12. Paste the class ID that you copied from the session log.
13. Click **OK**.

Updates

Using the Updates panel, you can assign automatic or manual updates to client workstations. You can make these assignments to individual client groups and can specify that these groups receive one or more of the following types of updates:

- Bug fixes. Assign clients to receive software bug fixes, when available.
- Major update. Assign clients to receive major software updates, when available.
- Minor update. Assign clients to receive minor software updates, when available.
- Spyware definitions. Assign clients to receive updated spyware definitions, which Webroot AntiSpyware uses as a basis for detecting suspicious items during sweeps. Webroot frequently updates these definitions.
- Virus definitions. Assign clients to receive updated virus definitions, which Webroot AntiSpyware uses as a basis for detecting viruses during sweeps. Webroot frequently updates these definitions.

The Update Service installed on your company server regularly checks the Webroot Update Server for new software and threat definitions. This Update Service runs automatically on a scheduled basis; it can be changed in the System Settings panel, Webroot Server Polling Interval field.

Updates for threat definitions and Webroot Client software are copied to the Download Folder whenever the Update Service contacts the Webroot Update Server. Once the updates are in the folder, you must either manually install them (see Manual Install) or you must configure automatic installation (see Auto Install).

The Updates Panel provides the following options related to updating client workstations:

- Update History. View a history of all updates that were downloaded.
- Auto Install. Configure Webroot AntiSpyware to automatically install updates on client workstations when your company server receives them from Webroot. This is recommended for updating spyware and threat definitions, which can change daily.

- Manual Install. Perform updates on client workstations whenever you receive notification (see "Update Notifications" on page 65). This is recommended for updating bug fixes and major and minor software updates.

Update History

You can view a history of when updates for the Webroot Server and Webroot Clients were downloaded from the Webroot Update Server.

To view the update history:

1. From the Admin Console function tree, select **Administration > Updates > Update History**.

   The Update History panel opens with a list of all of the updates downloaded to date.

2. To see if updates are available, click **Check for Updates**.

Auto Install

You can configure Webroot AntiSpyware to automatically install updates on clients when your company server receives them from the Webroot Update Server. This Auto Install method is ideal for updating threat definitions, so you can keep threat protection as current as possible and ensure that all users have the most recent definitions.

Before installing updates, be aware that:

- If you received any updates before you configured automatic installation, you must manually install them. Automatic installations will only apply to updates received after configuration.
- For Webroot Clients versions 3.0 or later, most definition updates are incremental updates, rather than full updates.
- Previous releases of the Webroot Client may use different formats for threat definitions. When updating threat definitions for a client workstation, be sure to match the definition version with the version installed on the client workstation.
- If the push to the Webroot Client fails, information about the failure appears in the local client's installation log (\windows\temp\ClientInstall.*currentdate*.log).

To configure automatic updates on local client workstations:

1. From the Admin Console function tree, select **Administration > Updates > Auto Install**.

   The Auto Install panel opens. It shows the client groups and the types of updates. You can set up automatic update installation by group or for the whole company. We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

2. Drag an update type to a group in the group tree.
3. If you need to remove an update type from a group, select it and click select **Unassign Update** at the top of the panel.

   The next time each client workstation contacts the company server (based on the polling schedule), it will install any update that you set to "auto install."

To configure mobile clients to automatically receive threat definition updates:

1. From the Admin Console function tree, select **Administration** > **Configuration** > **Sweep Settings**.

   The Sweep Settings panel opens with the sweep settings and group tree.

2. Click the **Other Settings** show/hide bar.

3. In the group tree (middle panel), select the group where you want to change the mobile update setting.

   If you want these settings to apply to the whole company, select the company at the top of the group tree.

4. Select the checkbox, “Enable automatic mobile client definition updates.”

   This option lets mobile-client users receive spyware and virus definition updates directly and automatically from Webroot when they are connected to the Internet (and the company server is not accessible).

   Note

   To download spyware and virus definitions, mobile clients must authenticate themselves by connecting to the Admin Console at least once to retrieve credentials before the downloads will be allowed.

5. Click **Apply** ✓ at the top right.

Note

The Tray Icon Setting must be set to Stay Minimized (recommended) or Pop Up on Scan; otherwise, end users will not be able to display the Webroot Client main window.

Manual Install

You can install updates manually whenever you receive notification (see “Update Notifications” on page 65). This method is ideal for updating bug fixes, and major and minor software updates. It allows you to install updates on a test group to see how they work before deploying them to the entire company.

Before installing updates, be aware that:

- Previous releases of the Webroot Client may use different formats for threat definitions. When updating threat definitions for a client workstation, be sure to match the definition version with the version installed on the client workstation.
- If the push to the Webroot Client fails, information about the failure appears in the local client’s installation log (\windows\temp\ClientInstall.*currentdate*.log).

To install updates manually:

1. From the Admin Console function tree, select **Administration > Updates > Manual Install**.

   The Manual Install panel opens. It shows the current client groups and the available updates. You can manually install updates by group or for the whole company. We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

2. Drag an update to a group in the group tree. To install the update on all client workstations in the company, drag the update to the company name at the top of the group tree.

3. If you need to remove an update type from a group, select it and click select **Unassign Update** at the top of the panel.

   The next time each client workstation contacts the company server (based on the polling schedule), it will install the update.

To configure mobile clients to receive threat definition updates, which the user can install manually:

1. From the Admin Console function tree, select **Administration > Configuration > Sweep Settings**.

   The Sweep Settings panel opens with the sweep settings and group tree.

2. Click the **Other Settings** show/hide bar.

3. In the group tree (middle panel), select the group where you want to change the mobile update setting.

   If you want these settings to apply to the whole company, select the company at the top of the group tree.

4. Select the checkbox: “Enable manual mobile client definition updates.”

5. Click **Apply** ✓ at the top right.

   The next time the mobile client contacts the company server for an update, an **Update Definitions** button displays on the Webroot Client main window so the user can retrieve definition updates when connected to the Internet. (The button is not available if a user downloaded updated threat definitions within the last six hours.)

Note

The Tray Icon Setting must be set to Stay Minimized (recommended) or Pop Up on Scan; otherwise, end users will not be able to display the Webroot Client main window.

Notification Management

The Notification Management panel allows you to define the following:

- E-Mail Notification Formats
- E-Mail Addresses
- Alert Notifications
- Error Notifications
- Update Notifications

E-Mail Notification Formats

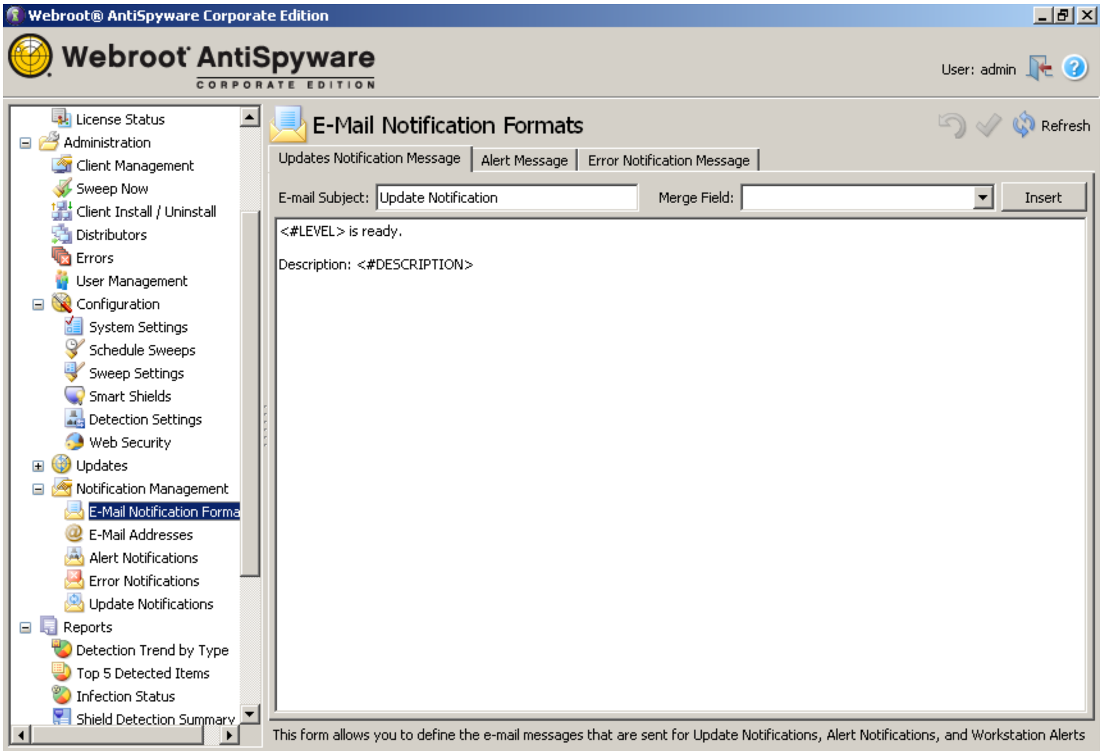
You can configure the format of e-mail messages that the Webroot Server sends for the following types of events:

- Availability of updates or threat definitions to the Webroot Server or the Webroot Client
- Detected spyware and viruses
- Errors that occur on client workstations

To configure the notification format for e-mail messages:

1. From the Admin Console function tree, select **Administration** > **Notification Management** > **E-mail Notification Formats**.

   The E-Mail Notification Formats panel opens.



E-mail Subject: Update Notification

<#LEVEL> is ready.

Description: <#DESCRIPTION>

This form allows you to define the e-mail messages that are sent for Update Notifications, Alert Notifications, and Workstation Alerts

2. Click the tab for the type of message you want to configure:
    - Update Notification Message for software and definition updates from the Webroot Server
    - Alert Message for detected items, such as spyware and virus detections
    - Error Notification Message for errors that occur on workstations
3. In the E-mail Subject field, enter the subject text you want to use for this type of message.

    The field is already populated with example text that you can keep or edit.
4. Enter the message text you want for this type of message.

    The field is already populated with example text that you can keep or edit.

    For information that will vary, select an option from the Merge Field drop down list and click **Insert**. Each event will contain information to fill in these merge fields (variables) with content appropriate to the event.
5. Click **Apply** ✓ at the top right.

E-Mail Addresses

You can define e-mail addresses that will receive Webroot Server notifications of various events, such as the availability of product updates.

To define the e-mail addresses that receive notifications:

1. From the Admin Console function tree, select **Administration** > **Notification Management** > **E-mail Addresses**.

    The E-mail Addresses panel opens.
2. Click the **Add E-mail Address** ✚ icon to add a new address.

    The New E-Mail Address panel opens.
3. Enter the First Name, Last Name, and E-mail Address.
4. Click **OK**.

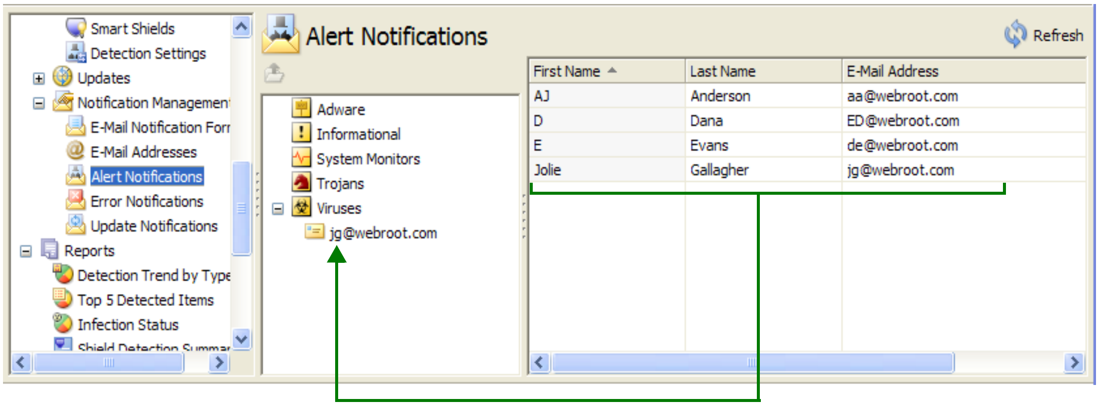
Alert Notifications

You can define an e-mail list of end users who should receive certain types of alert notifications coming from client workstations. These alert types include adware, informational items, system monitors, Trojan horses, and viruses.

To define alert notifications:

1. From the Admin Console function tree, select **Administration** > **Notification Management** > **Alert Notifications**.

    The Alert Notifications panel opens with the alert categories displayed in the middle and a list of all available e-mail addresses (see "E-Mail Addresses" on page 63).
2. Drag a name from the list on the right to an alert category in the middle.



First Name	Last Name	E-Mail Address
AJ	Anderson	aa@webroot.com
D	Dana	ED@webroot.com
E	Evans	de@webroot.com
Jolie	Gallagher	jg@webroot.com

Drag a name to an alert
category in the middle

The e-mail address for that recipient appears under the category. To move a recipient from one category to another, drag it from the current category and drop it onto another category. To remove a recipient from an alert category, select it and click **Unassign E-mail Address**.

Error Notifications

You can define an e-mail list of end users who should receive certain types of error notifications coming from client workstations. These notification types include errors only or errors and warnings.

To define error notifications:

1. From the Admin Console function tree, select **Administration** > **Notification Management** > **Error Notifications**.

   The Error Notifications panel opens with the error categories displayed in the middle and a list of all available e-mail addresses (see "E-Mail Addresses" on page 63).

2. Drag a name from the list to an error category.

   The e-mail address for that recipient appears under the category. To move a recipient from one category to another, drag it from the current category and drop it onto another category. To remove a recipient from a category, select it and click **Unassign E-Mail Address**.

Update Notifications

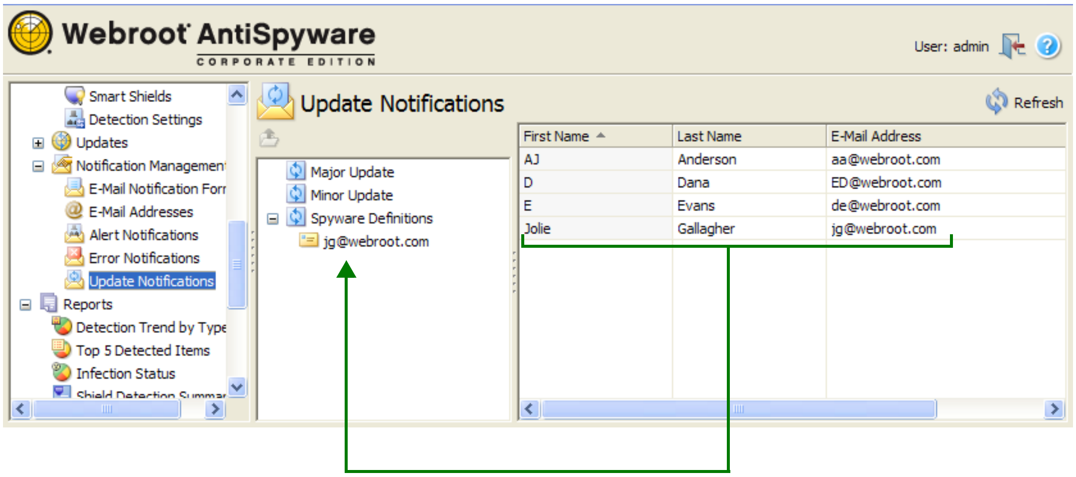
You can configure e-mail notifications for updates that arrive from the Webroot Update Server. These types of notifications include bug fixes, major and minor updates, spyware definitions, and virus definitions.

To configure notifications for Webroot updates:

1. From the Admin Console function tree, select **Administration** > **Notification Management** > **Update Notifications**.

   The Update Notifications panel opens with a list of update types displayed in the middle and a list of all available e-mail addresses (see “E-Mail Addresses” on page 63).

2. Drag the name of an e-mail recipient to the update category.



First Name	Last Name	E-Mail Address
AJ	Anderson	aa@webroot.com
D	Dana	ED@webroot.com
E	Evans	de@webroot.com
Jolie	Gallagher	jg@webroot.com

Drag a name to an update category in the middle

The e-mail address for that recipient appears under the category. To move a recipient to a different update type, drag it from the current location to the new update type. To remove a recipient from an update type, select it and click **Unassign E-Mail Address**.

▲

4: Reports

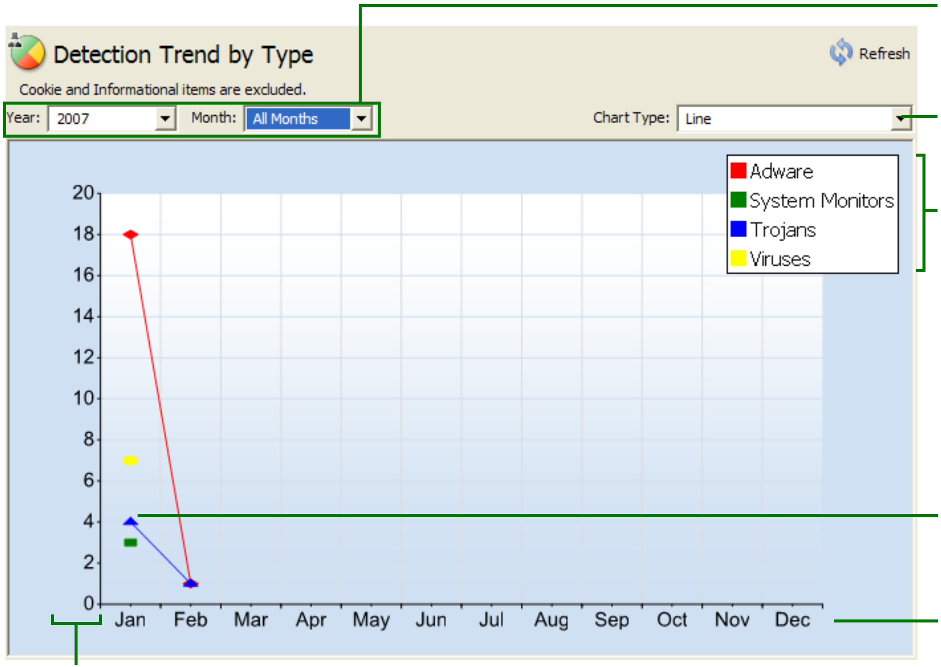
The Admin Console includes extensive reporting features that provide graphical executive summaries, threat reports, and status updates. You can customize reports to provide detailed analysis of the threats by workstation, group, and threat type.

You can generate the following reports:

- Detection Trend by Type Report. A chart format that shows trends in the types of threats found in your network (excluding tracking cookies and informational items) over a selected time frame. The report data includes items found during sweeps and items blocked by shields.
- Top 5 Detected Items Report. A chart format that shows the five most prevalent threats found in your network (excluding tracking cookies and informational items). The report data includes items found during sweeps and items blocked by shields.
- Infection Status Report. A chart format that shows the status of all client workstations: either infected (excluding tracking cookies and informational items), clean, or never swept. The report data includes items found during sweeps, but not items blocked by shields.
- Shield Detection Summary Report. A tabular format that shows a summary of blocked items by shield type.
- Shield Detection Trend Report. A tabular format that shows trends of blocked and allowed items within a specified time range.
- Top Detected Items Report. A tabular format that shows the prevalent threats for your entire company or for each group or workstation. The report data includes items found during sweeps and items blocked by shields.
- Infected Machine Summary Report. A tabular format that shows a summary about any infected client workstations. The report data includes items found during sweeps and items blocked by shields.
- Detection History Report. A tabular format that shows a history about any detected threats. The report data includes items found during sweeps and items blocked by shields.
- Version History Report. A tabular format that shows a history of Webroot Client versions installed on workstations and the threat definition versions.
- Error Report. A tabular format that shows a summary about errors that occurred on client workstations.
- Detection Report. A tabular format that shows a summary of quarantined items on client workstations.
- Single Detected Item Report. A tabular format that shows where a specific type of threat has been detected across all client workstations.

Detection Trend by Type Report

To see trends in the types of potential threats found in your network, you can generate the Detection Trend by Type report. This report shows all item types found during sweeps and blocked by shields (except cookies and informational items) over a single month or year. You can quickly view data in a line graph to see upward and downward trends or in a bar chart to compare overall numbers or percentages of detected threat types.



Detection Trend by Type

Cookie and Informational items are excluded.

Year: 2007 Month: All Months

Chart Type: Line

Select the date range.

Select the chart type.

Color key to item types.

Click a node (or bar) for more details.

Date range.

Number or percentage of items, depending on the selected chart type.

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Detection Trend by Type**.

   The report panel opens at the right.

2. In the Year and Month fields, select the desired time frame.

3. In the Chart Type field, select how you want the information to appear:

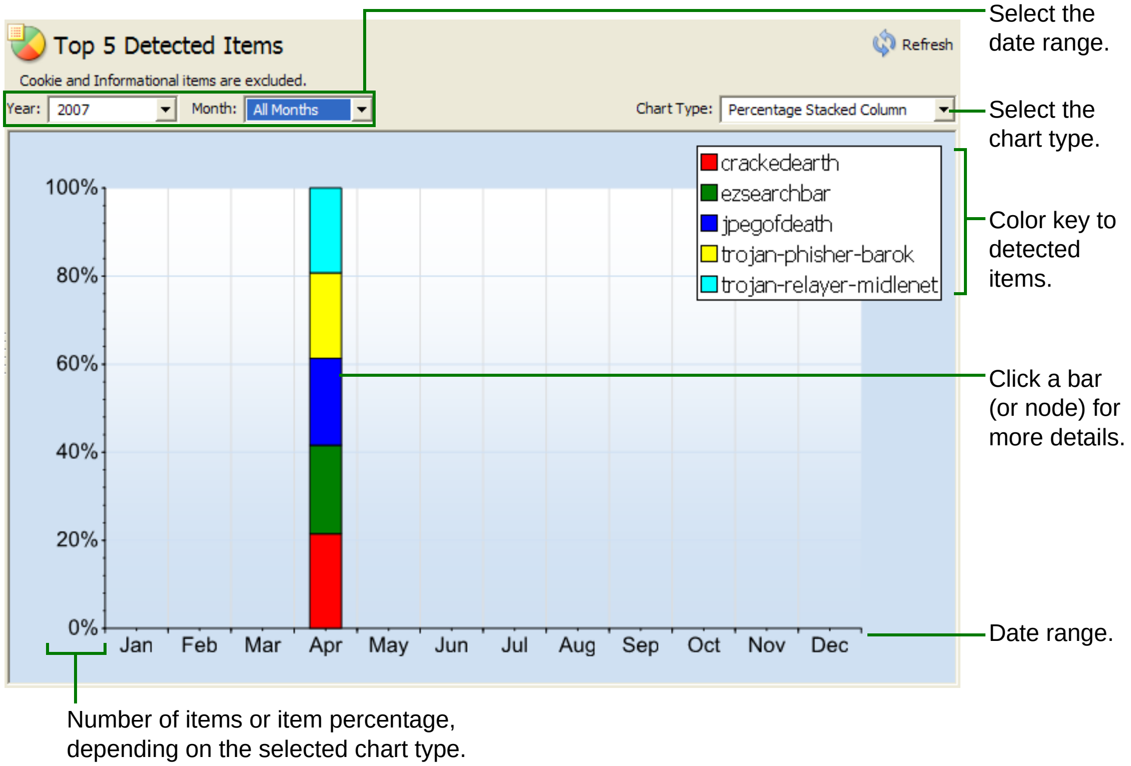
   - **Line chart**. Graphed data over the selected time frame.
   - **Column**. Side-by-side bars for the number of items per type.
   - **Stacked Column**. Stacked bars for the number of items per type.
   - **Percentage Stacked Column**. Stacked bars for the percentage of item types.

4. When the chart opens, click on a node or bar for details about a detected item type:

   - **Series**. Name of the detection type.
   - **Category**. Month or day.
   - **Value**. Total detection count for the type.

Top 5 Detected Items Report

To see the five most prevalent threats found in your network, you can generate the Top 5 Detected Items report. This report shows all items found during sweeps or blocked by shields (except cookies and informational items) over a single month or year. You can quickly view data in a line graph to see upward and downward trends or in a bar chart to compare overall numbers or percentages of detected threats.



Top 5 Detected Items

Cookie and Informational items are excluded.

Year: 2007 Month: All Months

Chart Type: Percentage Stacked Column

Select the date range.

Select the chart type.

Color key to detected items.

Click a bar (or node) for more details.

Date range.

Number of items or item percentage, depending on the selected chart type.

To generate this report:

1. From the Admin Console function tree, select **Reports > Top 5 Detected Items**.

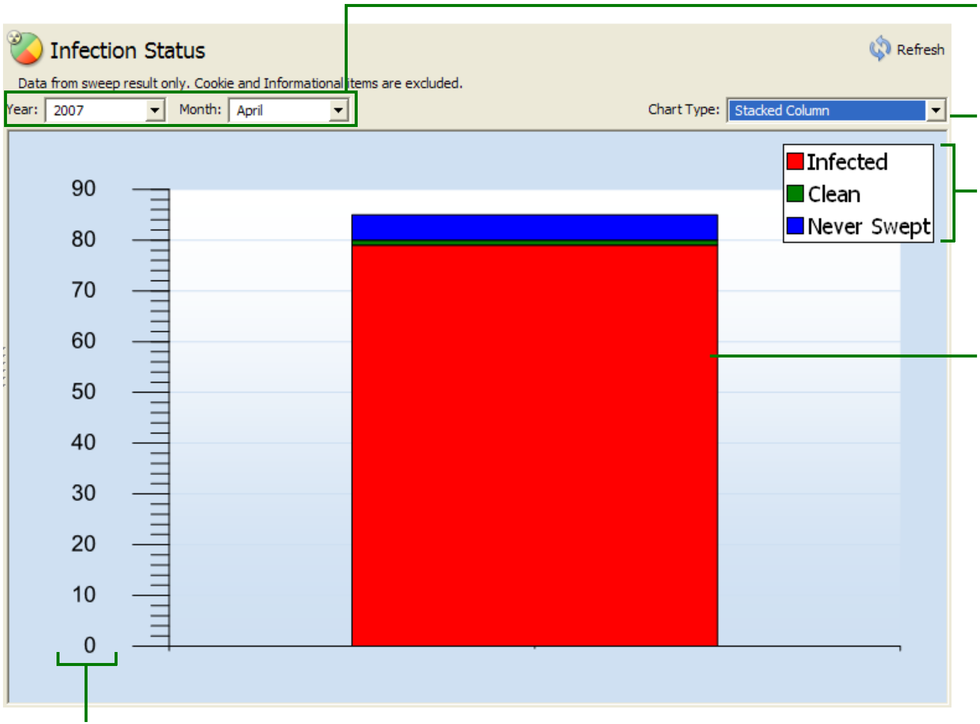
   The report panel opens at the right.

2. In the Chart Type field, select how you want the information to appear:
   - **Line chart**. Graphed data over the selected time frame.
   - **Column**. Side-by-side bars for the number of detections per item.
   - **Stacked Column**. Stacked bars for the number of detections per item.
   - **Percentage Stacked Column**. Stacked bars for the percentage of item detections.

3. When the chart opens, click on a node or bar for details about a detected item:
   - **Series**. Name of the detected item.
   - **Category**. Month or day.
   - **Value**. Total detection count for the item.

Infection Status Report

To view client workstation status gathered from the sweep results, you can generate the Infection Status report. This report shows the number of clients with items detected during a sweep (infected), with no items detected (clean), or never swept. The report does not include data for cookies or informational items. You can quickly view data in a pie chart or in a bar chart to compare overall numbers or percentages of client status.



Infection Status

Data from sweep result only. Cookie and Informational items are excluded.

Year: 2007 Month: April Chart Type: Stacked Column

Select the date range.

Select the chart type.

Shows color key to client status

Click an area for more details.

Shows number of items or item percentage, depending on the selected chart type.

To generate this report:

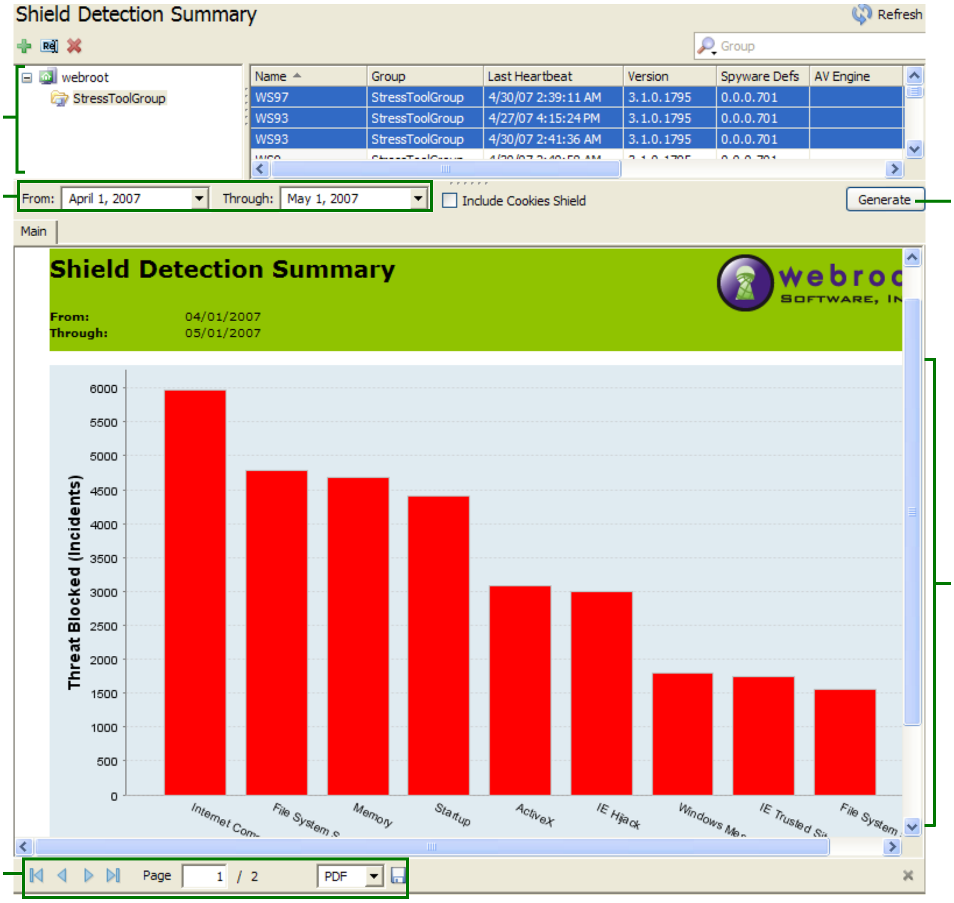
1. From the Admin Console function tree, select **Reports > Infection Status**.

   The report panel opens at the right.

2. In the Year and Month fields, select the desired time frame.
3. In the Chart Type field, select how you want the information to appear:
   - **Pie**. Pie chart showing the client status.
   - **Column**. Side-by-side bars for the number of clients.
   - **Stacked Column**. Stacked bars for the number of clients.
   - **Percentage Stacked Column**. Stacked bars for the percentage of clients.
4. When the chart opens, click on a graph area for details:
   - **Series**. Infected, clean, or never swept.
   - **Value**. Total number of clients.

Shield Detection Summary Report

To view a history of items that shields have detected and blocked on client workstations, you can generate the Shield Detection Summary report. This report displays each type of blocked threat for workstation clients over a selected time period.



Shield Detection Summary

Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine
WS97	StressToolGroup	4/30/07 2:39:11 AM	3.1.0.1795	0.0.0.701	
WS93	StressToolGroup	4/27/07 4:15:24 PM	3.1.0.1795	0.0.0.701	
WS93	StressToolGroup	4/30/07 2:41:36 AM	3.1.0.1795	0.0.0.701	

From: April 1, 2007 Through: May 1, 2007

□ Include Cookies Shield

Shield Detection Summary

From: 04/01/2007
Through: 05/01/2007

Select a group or individual clients.

Select the date range.

Click to generate report.

No. of threats blocked by type.

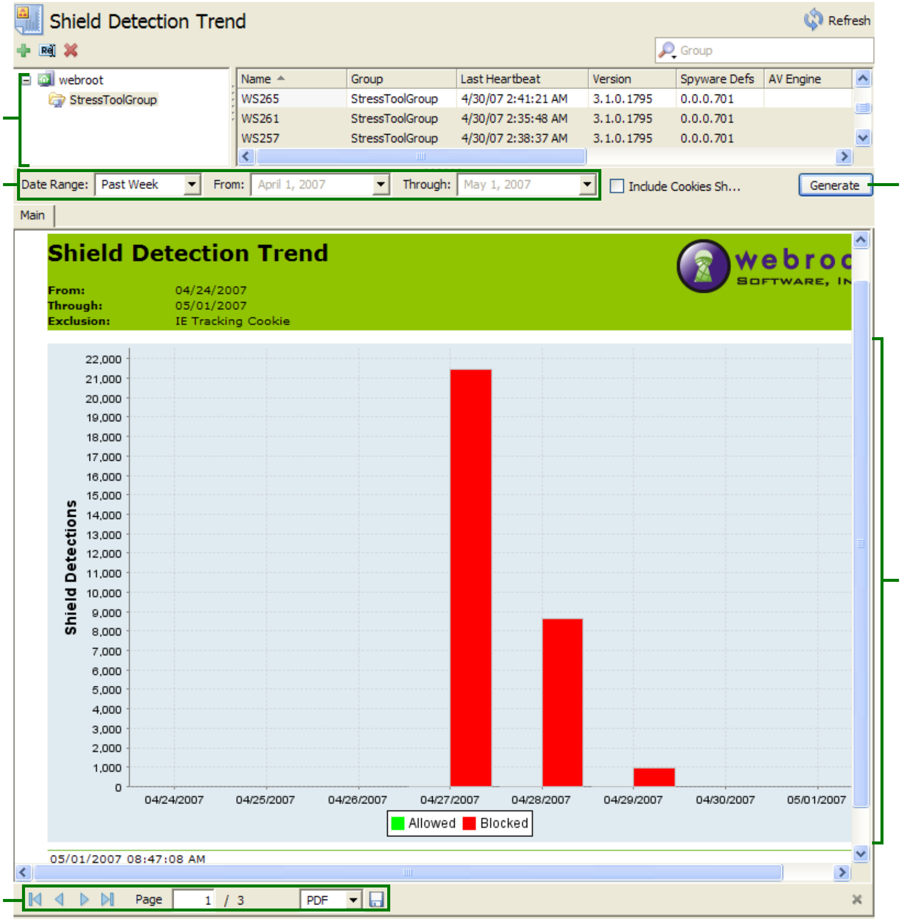
Use navigation buttons or save to a file.

To generate this report:

1. From the Admin Console function tree, select **Reports > Shield Detection Summary**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see "Filter Field" on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, select "Include Cookies Shield" to include data for tracking cookies.
5. Click **Generate**.
6. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF or RTF. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Shield Detection Trend Report

To view shield detection trends found in your network, you can generate the Shield Detection Trend report. This report shows allowed and blocked threats for clients over a selected time period.



Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine
WS265	StressToolGroup	4/30/07 2:41:21 AM	3.1.0.1795	0.0.0.701	
WS261	StressToolGroup	4/30/07 2:35:48 AM	3.1.0.1795	0.0.0.701	
WS257	StressToolGroup	4/30/07 2:38:37 AM	3.1.0.1795	0.0.0.701	

Date Range: Past Week From: April 1, 2007 Through: May 1, 2007 ☐ Include Cookies Sh... Generate

Shield Detection Trend

From: 04/24/2007
Through: 05/01/2007
Exclusion: IE Tracking Cookie

05/01/2007 08:47:08 AM

Page 1 / 3 PDF

Select a group or individual clients.

Select the date range.

Click to generate report.

No. of threats allowed or blocked.

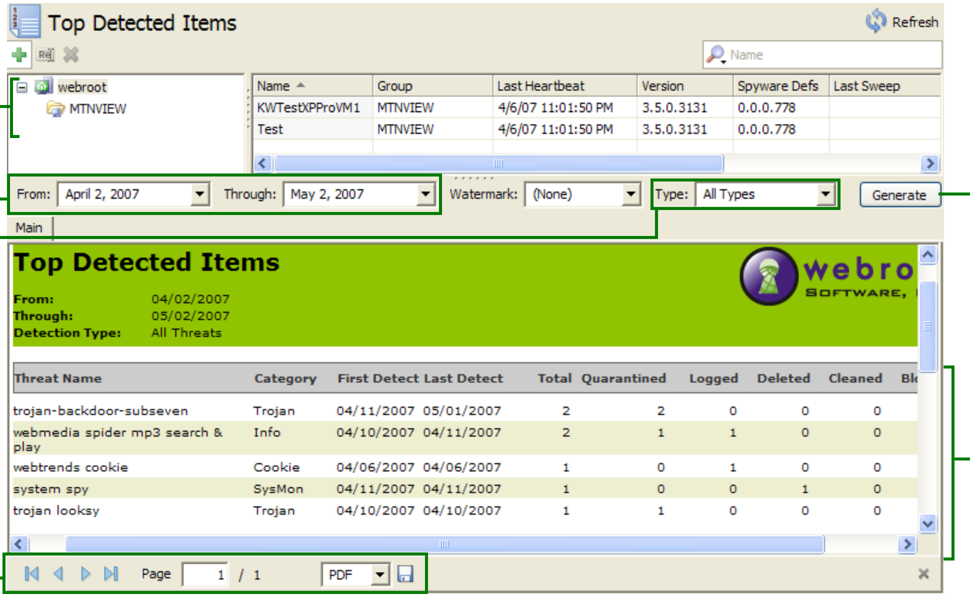
Use navigation buttons or save to a file.

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Shield Detection Trend**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see “Filter Field” on page 8).
3. In the Date Range field, select the time frame for the report data (past week, past month, past 3 months, past 6 months, or past year). If you select Specific Date, enter the date range in the From and Through fields. The maximum range for a specific date is 30 days.
4. Optionally, select “Include Cookies Shield” to include data for tracking cookies.
5. Click **Generate**.
6. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF or RTF. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Top Detected Items Report

To view the most prevalent items found on the client workstations during sweeps and blocked by shields, you can generate the Top Detected Items report. This report shows details about each potential threat, sorted by the item detected most frequently to the item found least frequently. You can include all item types in the report data or individual types.



Select a group or individual clients.

Select the date range.

Select type.

Use navigation buttons or save to a file.

Click to generate report.

Threat details.

Top Detected Items

Name	Group	Last Heartbeat	Version	Spyware Defs	Last Sweep
KWTestXPProVM1	MTNVIEW	4/6/07 11:01:50 PM	3.5.0.3131	0.0.0.778	
Test	MTNVIEW	4/6/07 11:01:50 PM	3.5.0.3131	0.0.0.778	

From: April 2, 2007 Through: May 2, 2007 Watermark: (None) Type: All Types

Top Detected Items

From: 04/02/2007
Through: 05/02/2007
Detection Type: All Threats

Threat Name	Category	First Detect	Last Detect	Total	Quarantined	Logged	Deleted	Cleaned	Bl
trojan-backdoor-subseven	Trojan	04/11/2007	05/01/2007	2	2	0	0	0	
webmedia spider mp3 search & play	Info	04/10/2007	04/11/2007	2	1	1	0	0	
webtrends cookie	Cookie	04/06/2007	04/06/2007	1	0	1	0	0	
system spy	SysMon	04/11/2007	04/11/2007	1	0	0	1	0	
trojan looksy	Trojan	04/10/2007	04/10/2007	1	1	0	0	0	

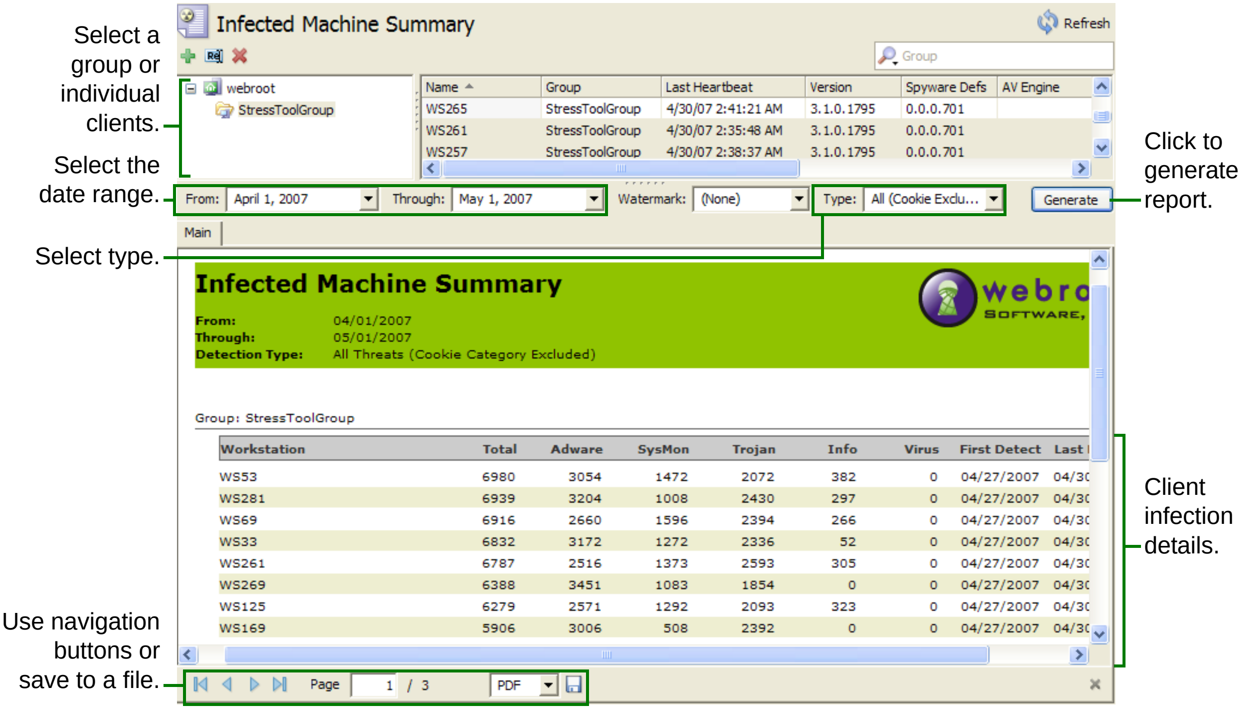
Page 1 / 1 PDF

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Top Detected Items**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see “Filter Field” on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, you can select a watermark (such as “Classified) in the Watermark field.
5. In the Type field, leave the field at “All Types” so the report includes all detected items or select individual types: adware, system monitors, Trojan horses, informational items, and viruses.
6. Click **Generate**.
7. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Infected Machine Summary Report

To view the client workstations in your network that have been infected with potential threats, you can generate the Infected Machine Summary report. This report shows details for each client, sorted by the client with the most infections to the client with the least infections. You can include all infection types in the report data (excluding cookies) or individual types.



Select a group or individual clients.

Select the date range.

Select type.

Use navigation buttons or save to a file.

Click to generate report.

Client infection details.

Infected Machine Summary

Refresh

Group

- webroot
  - StressToolGroup

Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine
WS265	StressToolGroup	4/30/07 2:41:21 AM	3.1.0.1795	0.0.0.701	
WS261	StressToolGroup	4/30/07 2:35:48 AM	3.1.0.1795	0.0.0.701	
WS257	StressToolGroup	4/30/07 2:38:37 AM	3.1.0.1795	0.0.0.701	

From: April 1, 2007 Through: May 1, 2007 Watermark: (None) Type: All (Cookie Exclu... Generate

Main

Infected Machine Summary

From: 04/01/2007
Through: 05/01/2007
Detection Type: All Threats (Cookie Category Excluded)

Group: StressToolGroup

Workstation	Total	Adware	SysMon	Trojan	Info	Virus	First Detect	Last
WS53	6980	3054	1472	2072	382	0	04/27/2007	04/30
WS281	6939	3204	1008	2430	297	0	04/27/2007	04/30
WS69	6916	2660	1596	2394	266	0	04/27/2007	04/30
WS33	6832	3172	1272	2336	52	0	04/27/2007	04/30
WS261	6787	2516	1373	2593	305	0	04/27/2007	04/30
WS269	6388	3451	1083	1854	0	0	04/27/2007	04/30
WS125	6279	2571	1292	2093	323	0	04/27/2007	04/30
WS169	5906	3006	508	2392	0	0	04/27/2007	04/30

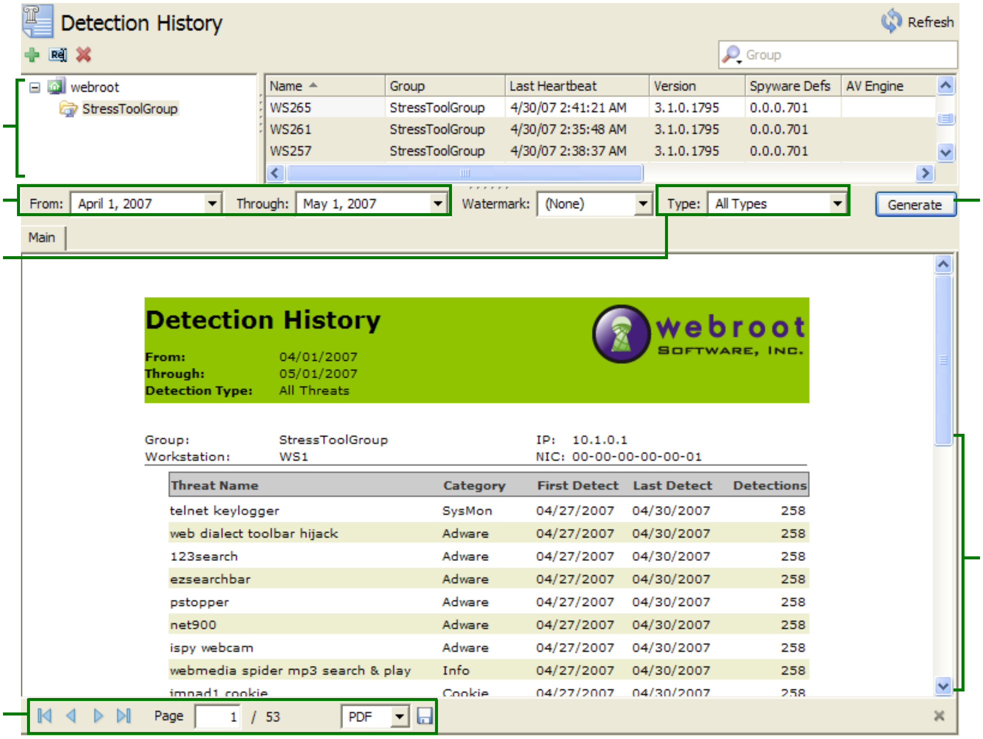
Page 1 / 3 PDF

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Infected Machine Summary**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see “Filter Field” on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, you can select a watermark (such as “Classified) in the Watermark field.
5. In the Type field, leave the field at “All (Cookie Excluded)” so the report includes all detected items except cookies, or select individual threat types: adware, system monitors, Trojan horses, informational items, and viruses.
6. Click **Generate**.
7. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Detection History Report

To view a history of potential threats found on the client workstations in your network, you can generate the Detection History report. This report shows what items have been found on each client. Data is sorted by the client with the most detections to the client with the least detections. You can include all item types in the report data or individual types.



Select a group or individual clients.
Select the date range.
Select type.
Use navigation buttons or save to a file.
Click to generate report.
Threat details by client.
Detection History
Refresh
Group
webroot
StressToolGroup
Main

Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine
WS265	StressToolGroup	4/30/07 2:41:21 AM	3.1.0.1795	0.0.0.701	
WS261	StressToolGroup	4/30/07 2:35:48 AM	3.1.0.1795	0.0.0.701	
WS257	StressToolGroup	4/30/07 2:38:37 AM	3.1.0.1795	0.0.0.701	

From: April 1, 2007 Through: May 1, 2007 Watermark: (None) Type: All Types Generate

Detection History

From: 04/01/2007
Through: 05/01/2007
Detection Type: All Threats

Group: StressToolGroup IP: 10.1.0.1
Workstation: WS1 NIC: 00-00-00-00-00-01

Threat Name	Category	First Detect	Last Detect	Detections
telnet keylogger	SysMon	04/27/2007	04/30/2007	258
web dialect toolbar hijack	Adware	04/27/2007	04/30/2007	258
123search	Adware	04/27/2007	04/30/2007	258
ezsearchbar	Adware	04/27/2007	04/30/2007	258
pstopper	Adware	04/27/2007	04/30/2007	258
net900	Adware	04/27/2007	04/30/2007	258
ispy webcam	Adware	04/27/2007	04/30/2007	258
webmedia spider mp3 search & play	Info	04/27/2007	04/30/2007	258
imnad1 cookie	Cookie	04/27/2007	04/30/2007	258

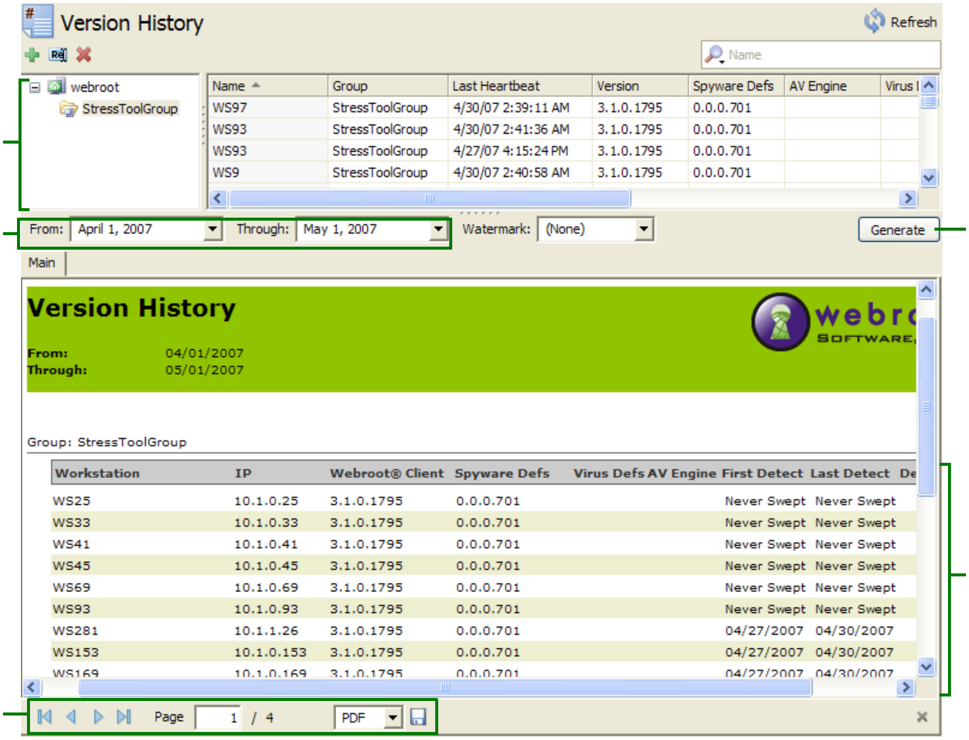
Page 1 / 53 PDF

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Detection History**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see "Filter Field" on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, you can select a watermark (such as "Classified) in the Watermark field.
5. In the Type field, you can leave the field at "All Types" so the report includes all detected items or you can select individual threat types: adware, system monitors, Trojan horses, informational items, and viruses.
6. Click **Generate**.
7. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Version History Report

To view Webroot Client versions and threat definition versions for each workstation, you can generate the Version History report. This report displays versions by client workstation over a selected time period. For the Webroot AntiSpyware with AntiVirus edition, the report also includes the antivirus version information and virus definition version.



Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine	Virus I
WS97	StressToolGroup	4/30/07 2:39:11 AM	3.1.0.1795	0.0.0.701		
WS93	StressToolGroup	4/30/07 2:41:36 AM	3.1.0.1795	0.0.0.701		
WS93	StressToolGroup	4/27/07 4:15:24 PM	3.1.0.1795	0.0.0.701		
WS9	StressToolGroup	4/30/07 2:40:58 AM	3.1.0.1795	0.0.0.701		

From: April 1, 2007 Through: May 1, 2007 Watermark: (None)

Version History

From: 04/01/2007
Through: 05/01/2007

Group: StressToolGroup

Workstation	IP	Webroot® Client	Spyware Defs	Virus Defs	AV Engine	First Detect	Last Detect	De
WS25	10.1.0.25	3.1.0.1795	0.0.0.701			Never Swept	Never Swept	
WS33	10.1.0.33	3.1.0.1795	0.0.0.701			Never Swept	Never Swept	
WS41	10.1.0.41	3.1.0.1795	0.0.0.701			Never Swept	Never Swept	
WS45	10.1.0.45	3.1.0.1795	0.0.0.701			Never Swept	Never Swept	
WS69	10.1.0.69	3.1.0.1795	0.0.0.701			Never Swept	Never Swept	
WS93	10.1.0.93	3.1.0.1795	0.0.0.701			Never Swept	Never Swept	
WS281	10.1.1.26	3.1.0.1795	0.0.0.701			04/27/2007	04/30/2007	
WS153	10.1.0.153	3.1.0.1795	0.0.0.701			04/27/2007	04/30/2007	
WS169	10.1.0.169	3.1.0.1795	0.0.0.701			04/27/2007	04/30/2007	

Select a group or individual clients.

Select the date range.

Use navigation buttons or save to a file.

Click to generate report.

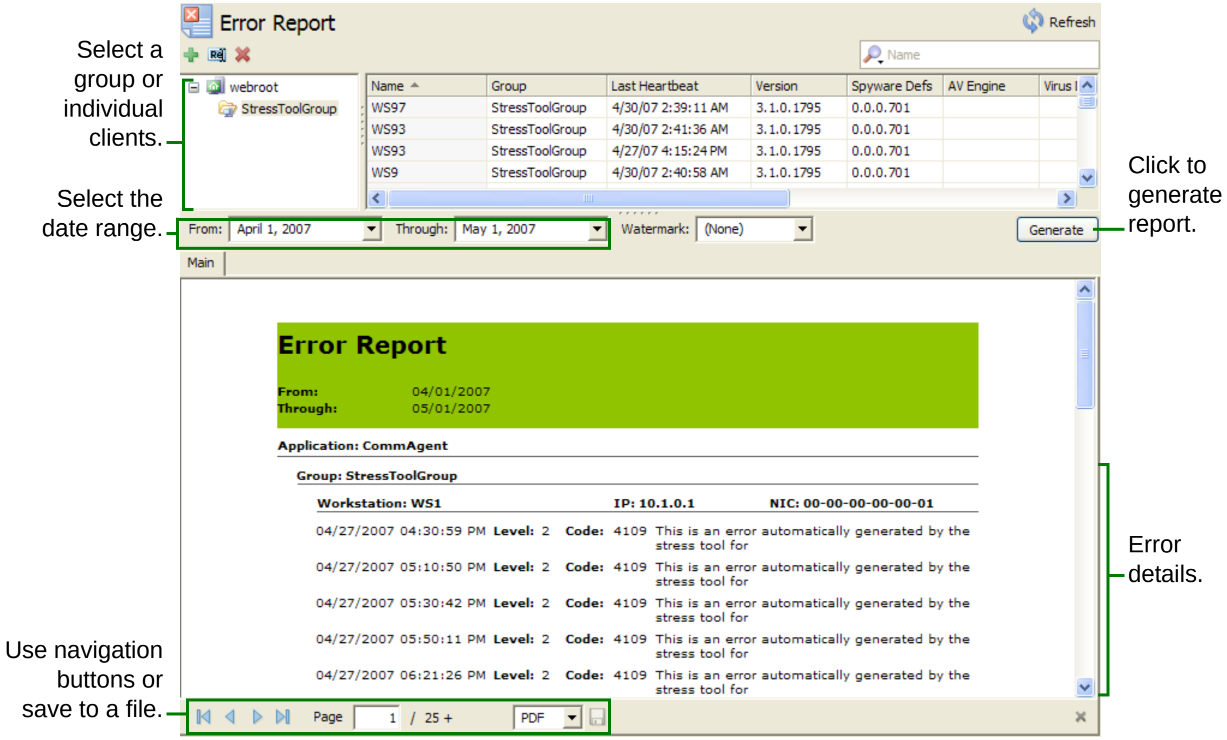
Version details.

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Version History**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see “Filter Field” on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, you can select a watermark (such as “Classified) in the Watermark field.
5. Click **Generate**.
6. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Error Report

To view Webroot Client errors that have occurred on workstations, you can generate the Error report. This report displays errors by clients or groups over a selected time period.



Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine	Virus I
WS97	StressToolGroup	4/30/07 2:39:11 AM	3.1.0.1795	0.0.0.701		
WS93	StressToolGroup	4/30/07 2:41:36 AM	3.1.0.1795	0.0.0.701		
WS93	StressToolGroup	4/27/07 4:15:24 PM	3.1.0.1795	0.0.0.701		
WS9	StressToolGroup	4/30/07 2:40:58 AM	3.1.0.1795	0.0.0.701		

From: April 1, 2007 Through: May 1, 2007 Watermark: (None)

Error Report

From: 04/01/2007
Through: 05/01/2007

Application: CommAgent

Group: StressToolGroup

Workstation: WS1 **IP: 10.1.0.1** **NIC: 00-00-00-00-00-01**

```
04/27/2007 04:30:59 PM Level: 2  Code: 4109 This is an error automatically generated by the
                                            stress tool for
04/27/2007 05:10:50 PM Level: 2  Code: 4109 This is an error automatically generated by the
                                            stress tool for
04/27/2007 05:30:42 PM Level: 2  Code: 4109 This is an error automatically generated by the
                                            stress tool for
04/27/2007 05:50:11 PM Level: 2  Code: 4109 This is an error automatically generated by the
                                            stress tool for
04/27/2007 06:21:26 PM Level: 2  Code: 4109 This is an error automatically generated by the
                                            stress tool for
```

Page 1 / 25 +

Select a group or individual clients.

Select the date range.

Use navigation buttons or save to a file.

Click to generate report.

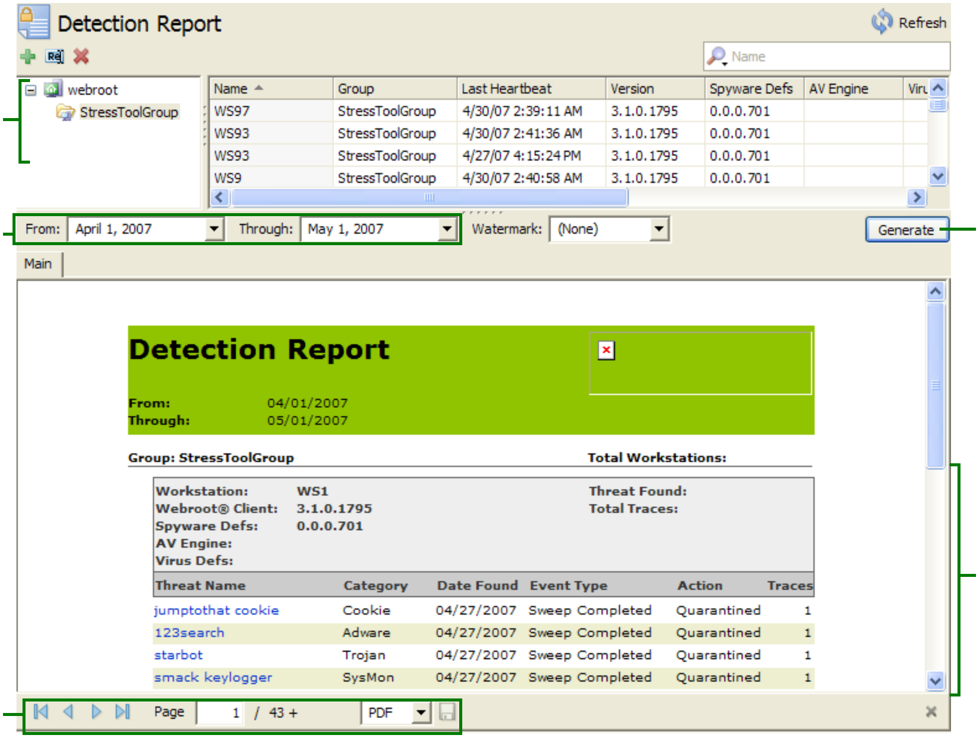
Error details.

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Error Report**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see “Filter Field” on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, you can select a watermark (such as “Classified) in the Watermark field.
5. Click **Generate**.
6. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)

Detection Report

To view details about potential threats that have been found and quarantined on client workstations, you can generate the Detection report. This report shows all the detected items found on each workstation for a selected time frame.



Name	Group	Last Heartbeat	Version	Spyware Defs	AV Engine	Viru
WS97	StressToolGroup	4/30/07 2:39:11 AM	3.1.0.1795	0.0.0.701		
WS93	StressToolGroup	4/30/07 2:41:36 AM	3.1.0.1795	0.0.0.701		
WS93	StressToolGroup	4/27/07 4:15:24 PM	3.1.0.1795	0.0.0.701		
WS9	StressToolGroup	4/30/07 2:40:58 AM	3.1.0.1795	0.0.0.701		

From: April 1, 2007 Through: May 1, 2007 Watermark: (None) Generate

Detection Report

From: 04/01/2007
Through: 05/01/2007

Group: StressToolGroup **Total Workstations:**

Workstation: WS1
Webroot® Client: 3.1.0.1795
Spyware Defs: 0.0.0.701
AV Engine:
Virus Defs:
Threat Found:
Total Traces:

Threat Name	Category	Date Found	Event Type	Action	Traces
jumptothat cookie	Cookie	04/27/2007	Sweep Completed	Quarantined	1
123search	Adware	04/27/2007	Sweep Completed	Quarantined	1
starbot	Trojan	04/27/2007	Sweep Completed	Quarantined	1
smack keylogger	SysMon	04/27/2007	Sweep Completed	Quarantined	1

Page 1 / 43 + PDF

Select a group or individual clients.

Select the date range.

Use navigation buttons or save to a file.

Click to generate report.

Detection details.

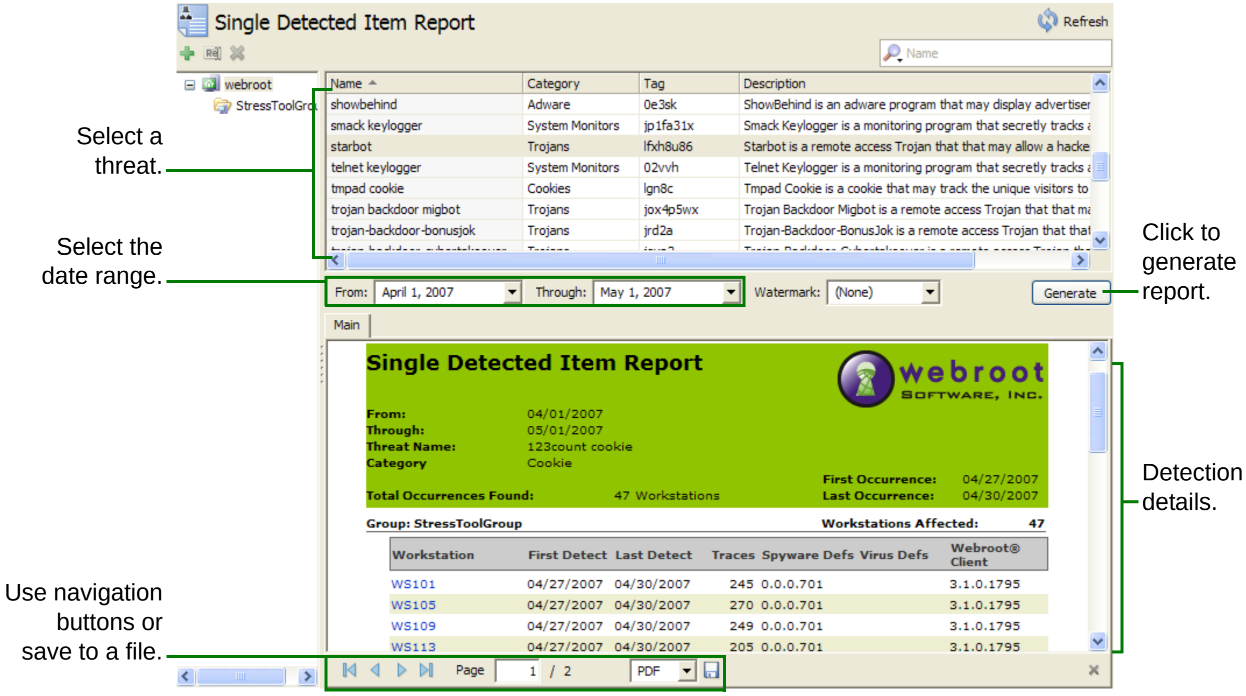
To generate this report:

1. From the Admin Console function tree, select **Reports** > **Detection Report**.
2. Select the clients for the data: either the entire company (select the company name at the top of the group tree), an individual group, or individual clients. To select specific clients, you can use **Ctrl** or **Shift** with your mouse or the filter field (see “Filter Field” on page 8).
3. In the From and Through fields, select the desired date range for the report to include.
4. Optionally, you can select a watermark (such as “Classified) in the Watermark field.
5. Click **Generate**.
6. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)
7. To view more information about a detected item, click on its threat name.

   A Trace Detail report opens in a separate tab for the selected item. This report shows the number of traces found for the threat and the directory and file name where the traces were found. Only Webroot Client versions 3.5 and above can report trace information; legacy client data is not included. The message “include legacy traces not shown” appears next to a trace count when the total trace count is greater than the actual file trace count.

Single Detected Item Report

To view where a specific type of threat has been detected on client workstations, you can generate the Single Detected Item Report. This report shows where a particular item has been found across all workstations for a selected time frame.



Single Detected Item Report

Refresh

Name

webroot

StressToolGro

Name	Category	Tag	Description
showbehind	Adware	0e3sk	ShowBehind is an adware program that may display advertiser
smack keylogger	System Monitors	jp1fa31x	Smack Keylogger is a monitoring program that secretly tracks a
starbot	Trojans	lfxh8u86	Starbot is a remote access Trojan that that may allow a hacke
telnet keylogger	System Monitors	02vvh	Telnet Keylogger is a monitoring program that secretly tracks a
tmpad cookie	Cookies	lgn8c	Tmpad Cookie is a cookie that may track the unique visitors to
trojan backdoor migbot	Trojans	jox4p5wx	Trojan Backdoor Migbot is a remote access Trojan that that ma
trojan-backdoor-bonusjok	Trojans	jrd2a	Trojan-Backdoor-BonusJok is a remote access Trojan that that

From: April 1, 2007 Through: May 1, 2007 Watermark: (None) Generate

Main

Single Detected Item Report

webroot SOFTWARE, INC.

From: 04/01/2007
Through: 05/01/2007
Threat Name: 123count cookie
Category Cookie
First Occurrence: 04/27/2007
Total Occurrences Found: 47 Workstations **Last Occurrence:** 04/30/2007

Group: StressToolGroup **Workstations Affected:** **47**

Workstation	First Detect	Last Detect	Traces	Spyware Defs	Virus Defs	Webroot® Client
WS101	04/27/2007	04/30/2007	245	0.0.0.701		3.1.0.1795
WS105	04/27/2007	04/30/2007	270	0.0.0.701		3.1.0.1795
WS109	04/27/2007	04/30/2007	249	0.0.0.701		3.1.0.1795
WS113	04/27/2007	04/30/2007	205	0.0.0.701		3.1.0.1795

Page 1 / 2 PDF

Select a threat.

Select the date range.

Click to generate report.

Detection details.

Use navigation buttons or save to a file.

To generate this report:

1. From the Admin Console function tree, select **Reports** > **Single Detected Item Report**.
2. Select the company name from the navigation tree.
3. Select a threat from the table. You can use the Filter field to narrow the items in the table (see “Filter Field” on page 8).
4. In the From and Through fields, select the desired date range for the report to include.
5. Optionally, you can select a watermark (such as “Classified) in the Watermark field.
6. Click **Generate**.
7. When the report opens, use the navigation buttons at the bottom of the pane to view additional pages or save the report to one of the following formats: PDF, XLS, RTF, or CSV. (To open a report exported to RTF, you must use MS Word 6.0, 2003, or XP.)
8. To view more information about the item found on a workstation client, click on the workstation name.

   A Trace Detail report opens in a separate tab for the selected workstation. This report shows the number of traces found for the selected item on a workstation and the directory and file name where the traces were found. Only Webroot Client versions 3.5 and above can report trace information; legacy client data is not included. The message “include legacy traces not shown” appears next to a trace count when the total trace count is greater than the actual file trace count.

▲

A: Webroot News and Support

This appendix describes additional information available from Webroot:

- Technical Support
- News and Docs
- Knowledge Base Articles

Technical Support

Technical support is available by phone and e-mail:

- Call 800-870-8102
- Send your questions to: esupport@webroot.com.
  We will respond within one business day.

News and Docs

Webroot maintains a news page that contains information about current version numbers and threat research. It also contains links to notes about updates. To view news, select **News and Docs** from the navigation pane.

Knowledge Base Articles

The Webroot Knowledge Base contains many articles that describe common issues and resolutions for Webroot AntiSpyware operations. These articles are constantly updated, expanded, and refined by Webroot support professionals to ensure that you have access to the very latest information.

To read these articles, visit the Enterprise Knowledge Base available from:
support.webroot.com.

Note

If clicking the link above does not open your browser and take you to the Support Center, copy the text of the link and paste it into your browser.

▲

B: Local Client Access

This section describes how to access the Webroot Client locally and perform tasks from there. See the following topics:

- Unlocking Functions at a Client Workstation
- Accessing the Client from a Command Line
- Running a Sweep in Safe Mode
- Uninstalling Webroot Clients Locally

Unlocking Functions at a Client Workstation

You can unlock functions at a client workstation and customize the Webroot Client settings for an end user. Unlocking functions requires a password that you set in the Admin Console. By default, there is no password defined. You must define the password before you can unlock functions at an end user's client workstation. For information about setting the password, see the Client Password option on page 42.

After you define the password and the client workstation has polled, you can go to an end user's workstation and unlock functions.

Note

If the Tray Icon Setting in the Admin Console is set to Stay Invisible, you can only access the Webroot Client interface using a command line from a client workstation. For information about changing this setting, see "Accessing the Client from a Command Line" on page 84.

To unlock functions at a client workstation:

1. At a client workstation, double-click the Webroot Client icon in the system tray.

   The main window opens.

2. Press **Ctrl+Alt+p**.

   The Admin Password window opens.

3. Enter the password you defined in the Admin Console.
4. Click **OK**.

   Now all functions that are not normally available to end users are available. These include the Quarantine panel for restoring and deleting detected items, as well as other functions that are not configured as user editable in the Admin Console. Refer to the Webroot Client online help for more information about using these functions.

5. After you customize the settings as needed, press **Ctrl+Alt+p** to lock the functions again.

Accessing the Client from a Command Line

If the Tray Icon Setting in the Admin Console is set to Stay Invisible, you can access the Webroot Client interface using a command line from a client workstation.

You must use a password to access the interface. For information about setting the password, see the Client Password option on page 42.

To access functions using a command line:

1. From a Command Prompt window, change directories to the folder where the Webroot Client is installed.

   By default, the folder is C:\Program Files\Webroot\Client.

2. Enter:
   ```
   SpySweeperUI /p <password>
   ```
   The password value is the admin password specified in the Admin Console; there is a space between the **p** and the password.

   You can hide the Webroot Client user interface again by using the **Ctrl+Alt+p** key combination.

To run a sweep from a command line:

1. From a Command Prompt window, change directories to the folder where the Webroot Client is installed.

   By default, the folder is C:\Program Files\Webroot\Client.

2. Enter:
   ```
   SpySweeperUI /s
   ```
   You can hide the Webroot Client user interface again by using the **Ctrl+Alt+p** key combination.

Running a Sweep in Safe Mode

If a client workstation is severely infected with unwanted software, such as spyware or adware, you can run a sweep in safe mode. Running a sweep in safe mode gives Webroot Clients a better chance of removing them. You may want to run a sweep in safe mode if Webroot Clients find the same programs repeatedly.

To run a sweep in safe mode, you must use two batch files that set and remove the following registry keys to enable Webroot AntiSpyware to run in safe mode:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\
WebrootSpySweeperService ]@="Service"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\
WebrootSpySweeperService ]@="Service"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\
WebrootComAgentService]@="Service"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\
WebrootComAgentService]@="Service"
```

To run a sweep in safe mode:

1. Make sure you have set a client password, so you can set sweep options from the client workstation. For more information, see the Client Password option on page 42.
2. From the client workstation, run the batch file SetSafeModeKeys.bat from the client workstation.

   The batch file is on your company server in the installation folder. Typically, the file is in the C:\Program Files\Webroot\Server\SafeModeRemovalTool folder of the system where you installed Webroot Server.
3. Restart the client workstation in safe mode.
4. Display the Webroot Client in one of the following ways:
   - Using Windows Explorer, go to C:\Program Files\Webroot\Client and double-click the SPYSWEEPER.EXE file, then press **Ctrl+Alt+p**, enter the password you defined in the Admin Console, and click **OK**.
   - From a Command Prompt window, change directories to the folder where the Webroot Client is installed (by default, the folder is C:\Program Files\Webroot\Client), then enter:

     ```
     SpySweeperUI /p <password>
     ```

   All functions that are not normally available to end users will now be available. These include the Quarantine panel for restoring and deleting found items, as well as other functions that are not configured as user editable in the Admin Console. Refer to the Webroot Client online help for more information about using these functions.
5. In the Webroot Client interface, select **Configuration** > **Settings**.

   The Settings panel opens.
6. Select the following options to ensure that a thorough sweep is performed:
   - Sweep All Folders on Selected Drives (select all drives listed)
   - Sweep Memory
   - Sweep Registry
7. Select **Sweep System** > **Sweep Now**.

   The Sweep Now panel opens.
8. Click **Start**.
9. After the sweep finishes, restart the computer normally.
10. Run the RemoveSafeModeKeys.bat from the client workstation.

    The batch file is on your company server in the installation folder. Typically, the file is in the C:\Program Files\Webroot\Server\SafeModeRemovalTool folder of the system where you installed Webroot Server.

Uninstalling Webroot Clients Locally

You can remove a Webroot Client locally from a workstation.

Note

The uninstallation process permanently deletes any detected items, such as viruses and spyware, that were quarantined on the client workstation.

To remove a Webroot Client from the local workstation:

1. Browse to the folder containing the WebrootClientSetup.msi file on your network.
2. Double-click WebrootClientSetup.msi and select **Remove**.

Note

You cannot uninstall the Webroot Clients using the Windows Add/Remove Programs feature.

To remove a Webroot Client using the SSECleanup tool:

1. Locate the SSECleanup.exe in the \Server\Client folder.
2. Run the tool from the command line or by double-clicking the file.

   This tool will uninstall any prior versions of the Webroot Clients.

   The tool takes two optional command line parameters, which force the tool either to leave some traces in the registry or to completely clean up the registry:

   - –LeaveCfg: (Default.) Leaves the GUID registry key on the client workstation. Use this option when you plan to reinstall on the client workstation in the future. If you do not use this option, the reinstallation will create a new GUID. It will also create a duplicate entry in the Admin Console. This is the default option and is how the tool is run when you double-click the executable.
   - –Remove: Removes all registry traces completely. Use this option when you are completely uninstalling the Webroot Clients. This will remove all registry traces.

C: Command Line Utilities

Webroot AntiSpyware includes command line utilities that allow you to perform a variety of data tasks against your Webroot database. For example, you can use the utilities to roll up data and generate reports from multiple installations of the Admin Console. These utilities work with your SQL Server installations. You can run them on an ad-hoc basis or at specific predefined intervals as batch processes that you can set up within your own environment.

The following utilities are included in this release:

- SSE Reaper Utility
- SSE Coalesce Utility
- SSE Warehouse Reaper Utility
- SSE Reporter Utility
- SSE Password Encrypt Utility

Because these are standalone utilities, there is no path required for where they must reside on your server.

SSE Reaper Utility

The SSE Reaper utility extracts data from your Webroot production database and produces a flat text file (pipe separated), which contains the following data points.

Data point	Description
`DataDomain`	A unique tag, specified in the SSEReaper.ini settings file, that can designate the hierarchical location of the data in an implementation that has multiple Admin Console installations. This field is also used for creating the output file name of the SSE Reaper utility.
`Company`	A unique tag, specified in the SSEReaper.ini settings file, that can designate company name or another unique identifier that you want to use.
`GroupName`	Group name that a particular workstation is a member of.
`Workstation`	The workstation name of an infected workstation.
`IP`	The IP address of a particular infected workstation.
`MAC`	The MAC address of a particular infected workstation.
`SSVersion`	The version of the Webroot Client running on a particular infected workstation.
`DefVersion`	The current definition version of a particular infected workstation.
`SweepDate`	The sweep date for a single record for a particular workstation.
`SpyID`	The Spy ID for a particular piece of spyware that was found.

Data point	Description
`SpyCategory`	The category of spy that was found.
`SpyName`	The name of a particular spy found during a sweep.
`Traces`	The number of traces for a particular spy found during a sweep.
`ActionTaken`	The action taken for a particular spy that was found during a sweep.

SSEReaper.ini Settings

You should modify the default SSEReaper.ini file (shown below) to match your particular environment.

```
[Settings]
LogFilename=
OutputDir=
DataDomain=
Company=
```

SSEReaper.ini setting	Description
`LogFilename=`	Name and location of the log file to be created. If no file is specified, then logging information is written to the screen. File name and location should be of the form: C:\Program Files\Webroot\Server\ReportingTools\SSEReaper.log. The default setting specifies no log file.
`OutputDir=`	Location (folder) of the output file that will be created.
`DataDomain=`	A unique tag that will designate the hierarchical location of the data in an implementation that has multiple Admin Console installations. This field is also used for creating the output file name as described above. DataDomain values *cannot* contain backslashes.
`Company=`	A simple string that is used in reports. This is any value that you choose for informational or identification purposes only.

Running SSEReaper.exe

By default, SSEReaper extracts data from your production environment from the previous day. This utility is intended for running on a daily basis either manually or as a batch process.

To run SSEReaper, navigate to the folder where the executables are saved on your server (typically this location should be: C:\Program Files\Webroot\Server\ReportingTools\) and enter one of the following commands from a command line:

- `SSEReaper.exe` (extracts records from yesterday’s date)
- `SSEReaper.exe ALL` (extracts all records from the database)
- `SSEReaper.exe YYYYDDMM` (extracts all records on the given date)
- `SSEReaper.exe YYYYDDMM` (extracts all records within the given date range)

You can set parameters in the SSEReaper.ini file the log file name and location, as well as the output folder of where to save the text file that is created.

SSEReaper Output Files

The output file from SSEReaper will be named in one of three ways, based on which parameters were used to run the program. The three file names are described below.

Output file name	**File Format Description**
`DataDomain_YYYYDDMM=`	Created when SSEReaper is run with no parameters or when a single data parameter is passed in. **`DataDomain`** is taken from the value specified in the SSEReaper.ini file. **`YYYYDDMM`** is the previous day's date from when the program is run.
`DataDomain_upto_YYYYDDMM=`	Created when SSEReaper is run with the `ALL` parameter to extract all data. **`DataDomain`** is taken from the value specified in the SSEReaper.ini file. **`_upto_`** is a text string denoting that the output file is a complete extract (all dates up to the current date) from your production system. **`YYYYDDMM`** is the previous day's date from when the program is run.
`DataDomain_YYYYDDMM_to_YYYYDDMM=`	Created when SSEReaper is run with the date range parameters. **`DataDomain`** is taken from the value specified in the SSEReaper.ini file. **`_to_`** is a text string denoting that the output file is a complete extract (all dates up to the current date) from your production system. **`YYYYDDMM`** values are the starting and ending dates specified as parameters.

SSE Coalesce Utility

The SSECoalesce utility will import spyware detection records into a data warehouse table. The source of these records is the text file generated from either SSEReaper.exe (detailed in the previous section) or SSEWarehouseReaper.exe (detailed in the following section). Parameters for SSECoalesce are set in the included .INI file (SSECoalesce.ini), which contains default values that you can customize for your particular environment.

SSECoalesce.ini Settings

You should modify the default SSECoalesce.ini file (shown below) to match your particular environment.

```
[Settings]
DataDomain=
Provider=
Password=
Persist Security Info=1
User ID=
Initial Catalog=
Data Source=
```

SSECoalesce.ini setting	Description
`DataDomain=`	A unique identifier that denotes the hierarchical positioning within your environment. This value will be pre-pended to the DataDomain column of each record in the data warehouse table.
`Provider=`	Your SQL Server "provider" name, typically set to: SQLOLEDB.1.
`Password=`	Your SQL Server password.
`Persist Security Info=`	1=True. 0=False.
`User ID=`	SQL Server user ID.
`Initial Catalog=`	SQL Server "SQL database name."
`Data Source=`	SQL Server "local default instance server name or named instance."

Creating SQL Database Table

To run SSECoalesce with SQL Server, you must first create the proper table within SQL Server. You can use the following SQL statement to create the table.

```
CREATE TABLE "SpyDetection"
(
"ID" INTEGER IDENTITY PRIMARY KEY,
"DataDomain" VARCHAR(255),
"Company" VARCHAR(50),
"GroupName" VARCHAR(50),
"Workstation" VARCHAR(50),
"IP" VARCHAR(15),
"MAC" CHAR(17),
"SSVersion" VARCHAR(15),
"DefVersion" VARCHAR(10),
"SweepDate" DATETIME,
"SpyID" VARCHAR(40),
"SpyCategory" VARCHAR(20),
"SpyName" VARCHAR(50),
"Traces" INTEGER,
"ActionTaken" CHAR(50),
);
```

Running SSECoalesce.exe

To run SSECoalesce, navigate to the folder where the executables are saved on your server (by default they are in C:\Program Files\Webroot\Server\ReportingTools\). Enter the following from a command line:

```
SSECoalesce.exe <filename-to-import>
```

Where `<filename-to-import>` is the output file you created from SSEReaper.exe or SSEWarehouseReaper.exe.

Every warehouse will add its own DataDomain token to the very first field before passing it to the warehouse at a higher level. This enables you to maintain your organizational structure dynamically. The individual Admin Consoles do not have to know about the organizational structure.

The original file from SSEReaper will contain lines like this:

```
AdminConsole1|Webroot Software, Inc.|WESTCHESTER|TN3977|10.16.211.165 |00-
06-5B-7B-5C-DD|1.5.1.3698 |437|12/22/2004|mmrst|Adware|Gator (GAIN)|1|Q
```

The next warehouse upstream will modify strings like this by adding its own tag to a Windows folder-like structure:

```
Warehouse1\AdminConsole1|Webroot Software, Inc.|WESTCHESTER
|TN3977|10.16.211.165|00-06-5B-7B-5C-DD|1.5.1.3698|437|12/22/
2004|mmrst|Adware|Gator (GAIN)|1|Q
```

The next warehouse upstream will modify strings like this:

```
Warehouse-West\Warehouse1\AdminConsole1|Webroot Software, Inc.|
WESTCHESTER|TN3977|10.16.211.165|00-06-5B-7B-5C-DD|1.5.1.3698|437|12/22/
2004|mmrst|Adware|Gator (GAIN)|1|Q
```

SSE Warehouse Reaper Utility

SSEWarehouseReaper is designed to extract all spy detection records from a data warehouse table (this table is populated from the SSECoalesce utility). This utility uses an .INI file (SSEWarehouseReaper.ini) to identify the source database warehouse and the folder location for the exported records.

SSEWarehouseReaper.ini Settings

You should modify the default SSEWarehouseReaper.ini file (shown below) to match your particular environment.

```
[Settings]
OutputDir= C:\Program Files\Webroot\Server\ReportingTools
Provider=
Password=
Persist Security Info=1
User ID=
Initial Catalog=
Data Source=
```

SSEWarehouseReaper.ini setting	Description
`OutputDir=`	The location of the output file that will be created.
`Provider=`	Your SQL Server “provider” name, typically set to: SQLOLEDB.1.
`Password=`	Your SQL Server password.
`Persist Security Info=`	1 = True. 0 = False.
`User ID=`	SQL Server user ID.
`Initial Catalog=`	SQL Server “SQL database name.”
`Data Source=`	SQL Server “local default instance server name or named instance.”

Running SSEWarehouseReaper.exe

To run SSEWarehouseReaper, navigate to the folder where the executables are saved on your server (typically this location is: C:\Program Files\Webroot\Server\ReportingTools\). Enter one of the following commands from a command line:

- `SSEWarehouseReaper` (extracts records from yesterday’s date)
- `SSEWarehouseReaper ALL` (extracts all records from warehouse database)
- `SSEWarehouseReaper MM/DD/YYYY` (extracts all records on the given date)
- `SSEWarehouseReaper MM/DD/YYYY MM/DD/YYYY` (extracts all records within the given date range)

SSEWarehouseReaper Output Files

The output file from SSEWarehouseReaper is a text file that is named based on the last exported spyware record, as detailed below.

Output file	Description
`DataDomain_YYYYMMDD.txt=`	**`DataDomain`** and **`YYYYDDMM`** are both taken from the last exported spyware record.

SSE Reporter Utility

SSEReporter is a command-line utility for generating reports. You can use it to generate reports on spyware activity for a single workstation or for an arbitrary higher-level grouping of workstations. All information needed to generate the requested report is passed in as command-line parameters or read from the corresponding .INI file (SSEReporter.ini).

SSEReporter.ini Settings

You should modify the default SSEReporter.ini file (shown below) to match your particular environment.

```
[Settings]
Provider=
Password=
Persist Security Info=1
User ID=
Initial Catalog=
Data Source=
```

SSEReporter.ini setting	Description
`Provider=`	Your SQL Server “provider” name, typically set to: SQLOLEDB.1.
`Password=`	Your SQL Server password.
`Persist Security Info=`	1 = True. 0 = False.
`User ID=`	SQL Server user ID.
`Initial Catalog=`	SQL Server “SQL database name.”
`Data Source=`	SQL Server “local default instance server name or named instance.”

Running SSEReporter.exe

Usage:
```
SSEReporter [-r reporttype][-m domainfilter][-w workstation]
        [-s startdate][-e enddate][-o outputoption]
         [-f filename][-b watermark]
```

Parameter details:

Parameter	Description
`-r <reporttype>`	Type of report. Options are: • summary—Summary of all infected workstations. • detail—Detailed spy information for all workstations. • historyspy—Spy history for a single workstation. • historystatus—Version information from workstation scans. • threats—Summary of top threats found.
`-m <domainfilter>`	Domain selection filter for the report. Regular expression search tokens are used.
`-w <workstation>`	Name of a particular workstation used for workstation history reports. Regular expression search tokens are used. You must use quotes around any workstation name that includes a white-space character.
`-s <startdate>`	Starting date for report (format **`YYYYDDMM`**).
`-e <enddate>`	Ending date for report (format **`YYYYDDMM`**).
`-o <outputoption>`	Output type. Options are: text, printer, pdf.
`-b <watermark>`	Enables a background watermark on the report. This option is valid for printer output only. Options are: topsecret, secret, classified, and unknown. Examples are at the end of this document.
`-f <filename>`	Fully qualified path and file name for the output file. This option is only necessary if the -o option is set to text or pdf (Adobe Portable Document Format). You must use quotes around any file name or path element that contains white-space characters.

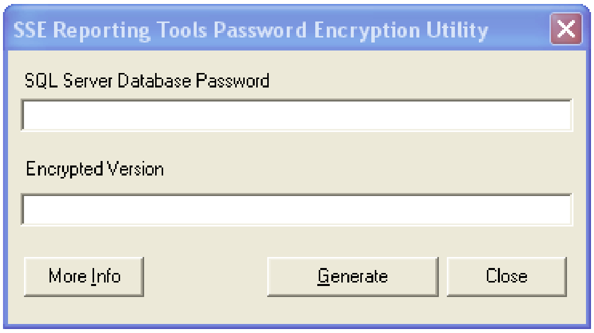
Examples:

```
SSEReporter.exe -r detail -s 20070220 -e 20070505 -m "%Top%" -o text -f
"C:\Results Dir\output.txt"

SSEReporter.exe -r summary -s 20070220 -e 20070505 -m "%Top%" -o text -f
C:\tempoutput.txt

SSEReporter.exe -r historyspy -s 20070220 -e 20070505 -m
"%Topdatafield,middatafield%" -w "WW-6042FHGZN437" -o printer -b classified
```

SSE Password Encrypt Utility

The SSE Password Encrypt utility lets you encrypt your SQL database password to avoid using a clear text password in the INI files for the SSECoalesce, SSEReporter, or SSEWarehouseReaper utilities.

To run SSEPasswordEncrypt, navigate to the folder where the executables are saved on your server (typically this location is: C:\Program Files\Webroot\Server\ReportingTools\) and double-click the SSEPasswordEncrypt.exe file. The following dialog box opens:


SSE Reporting Tools Password Encryption Utility
SQL Server Database Password
Encrypted Version
More Info
Generate
Close

In the top field, enter your SQL database password and click the **Generate** button. The encrypted password will display in the bottom field.

Copy the encrypted password and add `Password Encrypted=1` to the SSECoalesce, SSEReporter, or SSEWarehouseReaper INI files. A “1” means that the password is encrypted and “0” means that it is not.

Glossary

Active Directory

An advanced, hierarchical directory service that comes with Windows 2000 servers. It is LDAP-compliant and built on the Internet's Domain Naming System (DNS). Workgroups are given domain names, just like Web sites, and any LDAP-compliant client (Windows, Mac, Unix, etc.) can gain access to it.

ActiveX

ActiveX technology is a group of functions developed by Microsoft that let programs share information. Many legitimate programs use ActiveX, but some spyware also uses ActiveX to install itself.

adware

Adware is a type of software that may display advertisements on your system. Some adware may also hijack Web searches, meaning it may reroute your Web searches through its own Web page. It may change your default home page to a specific Web site. Adware generally propagates itself using dialog boxes, various social engineering methods, or through scripting errors. Adware and BHOs are often bundled with various free software programs, such as clocks, messengers, alerts, and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Removing adware bundled with free software programs may cause the software to stop operating. These adware programs may also cause slowing of your Web browser and system performance issues.

Alternate Data Stream (ADS)

An Alternate Data Stream is a highly technical way to hide images, data, or code in a file and can be used to hide malicious code. The hidden content is impossible to detect using regularly-available tools, such as Windows Explorer.

Browser Helper Objects (BHOs)

Browser Helper Objects are add-on programs that work with your browser. Some programs add BHOs without your knowledge.

definitions

A definition is a set of fingerprints that characterize a potentially unwanted program, such as spyware or adware, or that identifies types of viruses. Webroot Client Security regularly updates these definitions to provide better protection against the latest versions of spyware and viruses.

dialer

Dialers may disconnect your computer from your Internet Service Provider (ISP) and reconnect you to the Internet using an expensive toll or international phone number. Dialers can accrue significant phone charges and can run in the background, hiding their presence. They generally propagates itself using dialog boxes, various social engineering methods, through scripting errors, or may be delivered with a Trojan horse. The Federal Trade

Commission recommends that you dispute the charges with your telephone company and report the incident.

fingerprints

Fingerprints are the unique patterns of files, cookies, and registry entries that spyware installs. Webroot Client Security compares these patterns to its internal database so it can detect potentially unwanted programs on your computer.

informational items

Applications in the Informational category do not meet Webroot’s definition for any of the other categories, but are detected as part of the Informational category based on requests of customers. The default setting for the Informational category is Log Only, Do Not Quarantine. We strongly recommend that you maintain this setting for the Informational category.

LDAP

Lightweight Directory Access Protocol. A protocol used to access a directory listing. LDAP support is implemented in Web browsers and e-mail programs, which can query an LDAP-compliant directory.

potentially unwanted program

A potentially unwanted program is a program that may change the security or privacy state of your computer and online activities. These programs can (but do not necessarily) collect information about your online activities and send it to a third party without your knowledge or consent. A potentially unwanted program may arrive bundled with freeware or shareware, various social engineering methods, or by someone with access to your computer. Users may decide to remove these programs by using a desktop security product.

rootkits

Rootkits use file-obfuscation techniques to allow spyware and other malicious software to avoid detection and removal. Rootkits typically hide in logins, processes, files and logs, and may include software to capture information from desktops or a network. A rootkit's abilities to hide the presence of an intruder and the intruder’s actions explain the increase in use of this method.

Because rootkits can hook into operating system APIs and effectively hide themselves, Webroot Client Security searches for them by scanning disks directly at the device level, rather than relying on the Operating System APIs to indicate what’s there. Webroot Client Security flags any files or directories that look suspicious and then performs a second round of validations against the spyware definitions. If a detected item matches a definition, Webroot Client Security will flag it as a “rootkit.” If it does not match a definition, Webroot Client Security will flag it as a “rootkit masked file.” Some rootkit masked files can be legitimate files or directories, such as for newer hardware that contains hidden partitions with system restore information. Webroot Client Security allows you to keep a whitelist of legitimate rootkit masked files that will be ignored during sweeps.

spyware

Spyware is a program that may either monitor a user’s online activities or possibly install programs without a user’s consent. Information about online activities may be subsequently sent to a third party for malicious purposes without your knowledge or consent. Spyware may arrive bundled with freeware or shareware, through e-mail or instant messenger, may propagate itself using dialog boxes, various social engineering methods, scripting errors, or by someone with access to your computer. Spyware is difficult to detect, and difficult (if not impossible) for the average user to remove without the use of a top-quality anti-spyware program.

system monitors

System monitors, typically non-commercial, may monitor and capture your computer activity, including recording all keystrokes, e-mails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, and programs run. This program may be capable of taking screen shots of your desktop at scheduled intervals, storing the information on your computer in an encrypted log file for later retrieval. These log files may be e-mailed to a pre-defined e-mail address. This program can run in the background, hiding its presence. These programs typically install via other threats, such as music downloads, and Trojan downloaders. These system monitors may allow an unauthorized, third party to view potentially sensitive information, such as passwords, e-mail, and chat room conversation.

traces

Traces are the individual elements that make up the definition database. The more traces found and put into the definitions the more complete the removal of the potential threats.

tracking cookies

Cookies are pieces of information that are generated by a Web server and stored on your computer for future access. When visiting some Web sites, a cookie may be placed on your system to track your personal preferences and Web surfing habits through uniquely identifiable information (browsing habits, usernames and passwords, areas of interest, etc.), and simultaneously share the information with other Web sites.

Trojan horses

A Trojan horse may manage files on your computer, including creating, deleting, renaming, viewing, or transferring files to or from your computer. It can utilize a program manager that allows a hacker to install, execute, open, or close programs. The hacker can gain remote control of your cursor and keyboard and can even send mass e-mails from your infected computer. It can run in the background, hiding its presence. A Trojan is usually disguised as a harmless software program and may also be distributed as an e-mail attachment. Opening the program or attachment may cause an auto-installation process that loads the downloader onto your computer and download third party programs on your computer, resulting in the installation of unwanted programs without your knowledge or consent, jeopardizing your privacy if it downloads another Trojan or a system monitor. Trojans may open a port on your computer that may enable a hacker to gain remote control of your computer.

viruses

A virus is a self-replicating program that can infest computer code, documents, or applications. While some viruses are purposefully malignant, others are more of a nuisance, replicating uncontrollably and inhibiting system performance.

▲

Index