

Webroot Enterprise System Administrator Guide



Webroot Software, Inc.
PO Box 19816
Boulder, CO 80308
www.webroot.com

Draft August 15, 2005

Webroot Enterprise version 2.5 System Administrator Guide

© 2004–2005 Webroot Software, Inc. All rights reserved. Webroot, Spy Sweeper, and the Webroot and Spy Sweeper icons are registered trademarks or trademarks of Webroot Software, Inc. All other trademarks are properties of their respective owners.

Contents

1: Planning Your Installation	1
About This Guide	1
Conventions	1
Technical Support	2
System Requirements	2
Understanding Webroot Enterprise	3
Planning for Webroot Enterprise Deployment	5
How Webroot Enterprise Updates Work	8
Key Steps to Installing and Setting Up Webroot Enterprise	8
2: Installing Webroot Enterprise	11
Setting up a SQL Server Database	11
Installing Webroot Enterprise Server on Your Company Server	13
Configuring Log On Properties for Webroot Administration Console Service	23
Installing Webroot Enterprise Server on Windows Server 2003 Service Pack 1	27
Setting Up Client Workstations	28
Accessing the Admin Console	28
Setting Up Client Workstations from the Admin Console	29
Alternate Client Workstation Setup Methods	30
Client Installation Options	31
Example Logon Script	32
Uninstalling Spy Sweeper from Client Workstations	33
Installing and Assigning Distributor Servers	33
Installing Distributor Servers	33
Assigning Distributor Servers	34
Changing the Distributor Server Port	35
3: Setting Up the Webroot Enterprise Server	37
Viewing News	37
Editing the Server Settings	37
Changing the Distributor Service Port on the Company Server	41
Setting Up Notification	42
Setting Up Notification E-mail Addresses	42
Setting Up Notification Messages	42
Setting Up Error Notification	43
Managing Clients	43
Managing Groups	44
Creating and Exporting Client Reports	45
Polling Client Workstations Now	46
Deleting Client Workstations	46
Managing Admin Console Users	47
4: Managing Spy Sweeper	49
Managing Spyware	49

Setting Up Automatic Spyware Handling	49
Setting Up Continuous Monitoring: Smart Shields	51
Configuring Sweeps	54
Configuring Sweep Settings	54
Setting Up Sweep Alerts	56
Running Sweeps	56
Running a Sweep Now	57
Scheduling Sweeps	57
Running a Sweep in Safe Mode	58
Viewing and Stopping Sweeps	60
Updating Spy Sweeper	60
Installing Updates Manually	61
Installing Updates Automatically	61
Setting Up Update Notification	62
Setting Up Updating for Mobile End Users	63
Unlocking Functions at a Client Workstation	63
5: Monitoring Status	65
Reviewing the Webroot Enterprise Dashboard	65
Viewing the Sweep Status	66
Viewing the Definition Status	67
Viewing the Infection Status	67
Viewing the Top Spyware Threats	68
Viewing the Server Status	69
Viewing License Status	69
Viewing Update History and Installed Versions	70
Viewing Update History	70
Viewing Applications Installed by Workstation	70
Viewing Client Status	71
Viewing Errors	71
Generating Reports	72
Generating Charts	72
Generating Tabular by Group and Workstation	72
A: Webroot Enterprise Port Requirements	75
B: Migrating an Existing Installation from DBISAM to SQL Server	77
C: Automated Group Mapping and Assignment Utility	79
Rules File Format	79
Rules File Syntax	79
IP and Name Examples	80
Active Directory Rule Format	80
Active Directory Rule Example	81
Parameter Delimiter	81
Processing the Rules File	82
Running GroupAssignPass.exe	82
Running GroupAssign.exe	82
D: Data Extraction and Reporting Utilities	85
SSE Reaper Utility	85
SSEReaper.ini Settings	86
Running SSEReaper.exe	86

SSEReaper Output Files87
SSE Coalesce Utility87
SSECoalesce.ini Settings88
Creating SQL Database Table88
Running SSECoalesce.exe89
SSE Warehouse Reaper Utility89
SSEWarehouseReaper.ini Settings90
Running SSEWarehouseReaper.exe90
SSEWarehouseReaper Output Files91
SSE Reporter Utility91
SSEReporter.ini Settings91
Running SSEReporter.exe92
Sample Reports94
Summary Report94
Detail Report95
Spy History Report96
Workstation Version History96
Top Threats97

Index

99

1: Planning Your Installation

Webroot Enterprise™ lets you install and manage Webroot® products throughout your company. You can set up groups with different settings, install updates automatically or manually, view the status of all products, and much more.

Webroot Enterprise gives you companywide management and control to ensure that your company's computer resources are protected from a variety of threats.




About This Guide

This *Guide* tells you how to set up and use Webroot Enterprise to install and manage Webroot products throughout the company. It assumes that you have detailed knowledge of the Windows operating systems in use in your company and your network.

The information in this *Guide* is also available from the help button.

Conventions

This *Guide* uses several typographical conventions to help explain how to use Webroot Enterprise.

Convention	Definition
Bold	Words in bold show items to select or click, such as menu items or buttons.
Tree navigation	The Guide uses parent node > child node notation for tree navigation. For example, Admin Tasks > Settings . This means to expand to the Admin Tasks node in the tree and select the Settings node.
 Note	This symbol means the following information is a note that gives you important information that may affect how you use Webroot Enterprise.
 Caution	This symbol means the following information is a caution that warns you about actions that may affect your ability to use some programs on your computer.
	This symbol means that the following information is a procedure.

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.

System Requirements

Following are the system requirements for Webroot Enterprise.

Table 1: Company server system requirements

Operating system	Windows NT 4.0 SP5 or higher, Windows 2000, Windows XP (see note below), Windows Server 2003
CPU	200 MHz minimum; 350 MHz or better recommended
Memory	512 MB recommended
Disk space	140 MB free space for operation. Additional free space needed for database growth. We recommend 1 GB of free space.

Table 2: Distributor server system requirements

Operating system	Windows NT 4.0 SP5 or higher, Windows 2000 SP4 or higher, Windows XP (see note below), Windows Server 2003
CPU	200 MHz minimum; 350 MHz or better recommended
Memory	512 MB recommended
Disk space	60 MB free space for operation.

Table 3: Client workstation system requirements

Operating system	Windows 98SE, ME, NT 4.0, 2000, or XP
CPU	300 MHz or better recommended
Memory	128 MB RAM minimum; 256 MB RAM or better recommended
Disk space	15 MB free space
Internet Explorer	Version 6.0 with Service Pack 1 required for Windows 98, 98SE, and ME



Note

Due to modifications that Microsoft made in Service Pack 2 for Windows XP that limit simultaneous TCP/IP connections, we do not recommend using the Poll Now or Sweep Now functions for more than five client workstations at a time. If you do, you may see temporary system lag and an Event ID error 4226 entry in your Windows system log. If you are managing large numbers of clients with frequent polling intervals from a server with Windows XP and SP2, you may also see the 4226 error when more than five clients poll in simultaneously.

Understanding Webroot Enterprise

Webroot Enterprise offers a total enterprise solution for your companywide spyware management using a client/server architecture. [Figure 1](#) shows a base configuration and how Webroot Enterprise works.

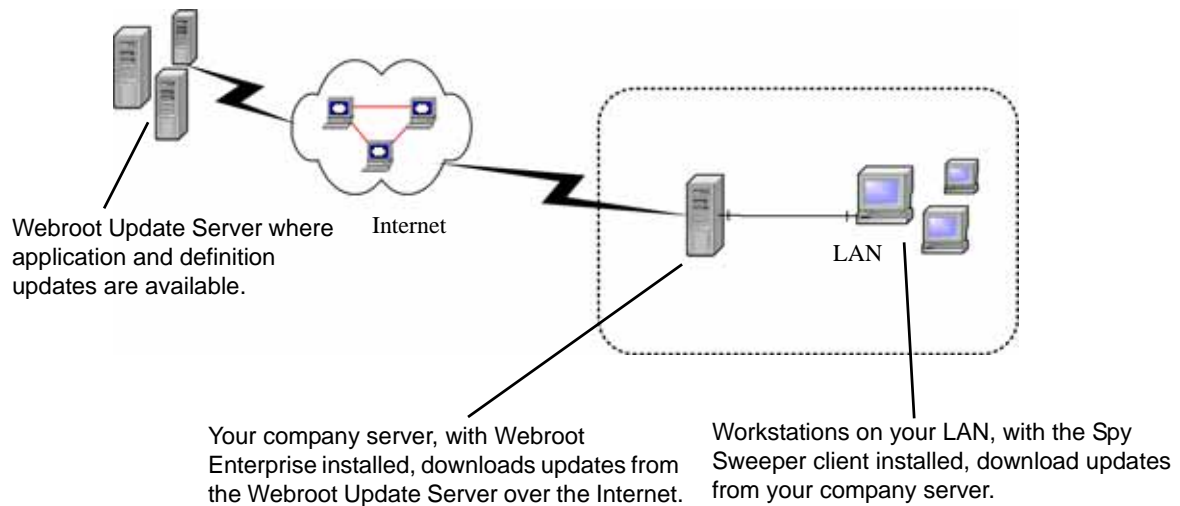


Figure 1: Webroot Enterprise base architecture

The Webroot Enterprise product includes three types of components that you install on your computers:

- On a company server, you install Webroot Enterprise Server™, which is described in [Table 4](#).
 - If you want to use more than one company server, consider using additional distributor servers, as described in “[Planning for Webroot Enterprise Deployment](#)” on page 5, or contact technical support for assistance.
- On each end user’s computer, you install the client workstation components, which are described in [Table 5](#).
- On each distributor server, you install the distributor service, which is described in [Table 6](#).

If you have a complex internal network, run firewall programs at the desktop or server level, or use proxy servers internally, you should review “[Appendix A, Webroot Enterprise Port Requirements](#)” on page 75.

Table 4: Webroot Enterprise Server components

Component	File name	Description	Installation/Network Access Requirement
Client Service™	WebrootClientService.exe	Controls the communication between the client workstations and your company server.	<ul style="list-style-type: none"> Installed during the installation of Webroot Enterprise Server. Requires local network access.
Update Service™	WebrootUpdateService.exe	Controls the updates from the Webroot Update Server™ to your company server.	<ul style="list-style-type: none"> Installed during the installation of Webroot Enterprise Server. Requires local network and Internet access. Requires use of port 443 on your server.
Admin Console™	WebrootAdminConsole.exe	Provides a browser-based graphical user interface (GUI) to let you set up and manage the Webroot applications across the company. Most of this <i>Guide</i> describes how to use this component.	<ul style="list-style-type: none"> Installed during the installation of Webroot Enterprise Server. Requires local network access. Requires use of port 50003 on your server, by default. The distributor service on your server uses the same port. For Secure Sockets Layer (SSL) access, requires use of port 50023.

Table 5: Webroot Enterprise client workstation components

Component	File name	Description	Installation/Network Access Requirement
Communication Agent (CommAgent™)	ComAgent.exe	<ul style="list-style-type: none"> Communicates periodically with the Client Service on your company server to see if any new or updated applications are available. Runs as a system service on each client workstation. 	<ul style="list-style-type: none"> Installed when you set up client workstations. Requires local network access. Requires use of ports 50001 and 50002 on the client workstation.

Table 5: Webroot Enterprise client workstation components

Component	File name	Description	Installation/Network Access Requirement
Spy Sweeper	SpySweeper.exe	<ul style="list-style-type: none"> Detects spyware and provides access to options for workstations users. Runs as a process on each client workstation. 	<ul style="list-style-type: none"> Installed when you set up client workstations.
Spy Sweeper Engine	wrsssdk.exe	<ul style="list-style-type: none"> Provides the core functions for Webroot Spy Sweeper Enterprise. Runs as a system service on each client workstation. 	<ul style="list-style-type: none"> Installed when you set up client workstations. Requires local network or Internet access, depending on which is needed to access the company server.

Table 6: Webroot Enterprise distributor server components

Component	File name	Description	Installation/Network Access Requirement
Distributor service	WebrootUpdateDistributor.exe	<ul style="list-style-type: none"> Communicates periodically with the Client Service on your company server to receive updates and with CommAgents to distribute updates. Runs as a system service on the server. 	<ul style="list-style-type: none"> Installed when you set up distributor servers. Requires local network access. Requires use of port 50003 on your server. The Admin Console service on your company server uses the same port.

Planning for Webroot Enterprise Deployment

If you plan to deploy Webroot Enterprise to 500 or fewer client workstations, you can use the base configuration shown in [Figure 1](#). If you are deploying to more than 500 client workstations, you should review the information in this section to determine the best configuration and settings to use.

[Table 7](#) provides general configuration and database recommendations based on the number of client workstations.

Table 7: Configuration and database recommendations

Number of client workstations	Company server specifications	Database	Number of distributor servers	Poll no more frequently than
Up to 500	Single 350 MHz processor with 512 MB RAM	DBISAM	0	One hour
500 to 10,000	Single 1 GHz processor, 512 MB RAM	DBISAM	0 to 2	Two hours

Table 7: Configuration and database recommendations

Number of client workstations	Company server specifications	Database	Number of distributor servers	Poll no more frequently than
10,000 to 40,000	Single 1 GHz processor, 1 GB RAM	MS SQL Server	2 to 3	Four hours
40,000 to 75,000	Dual 1 GHz processors, 2 GB RAM	MS SQL Server	3 to 6	Four hours
Over 75,000	Deploy multiple company servers Contact technical support for assistance	Base on number of client workstations each server handles	Base on number of client workstations each server handles	Base on number of client workstations each server handles

You may want to install additional distributor servers or company servers for two reasons:

- You have multiple sites and want to minimize bandwidth usage on WAN segments between the sites. The normal communication between the client and the server is only about 1 KB. Spy definition updates are typically about 900 KB. A new Spy Sweeper client update can be as large as 7.5 MB.
- You have a large number of clients relative to your server capabilities. Many things can affect the performance of the server.

Deploying distributor servers reduces WAN bandwidth consumed when spy definitions or software updates are delivered. Distributor servers receive copies of Spy Sweeper client and definitions updates. For more information about how updates work, see [“How Webroot Enterprise Updates Work”](#) on page 8.

In a configuration that uses distributor servers, the client workstations poll the company server. If updates are available, the company server sends a randomized list of distributor servers to each client workstation. The client workstation requests updates from the first distributor server on the list. The distributor server sends the updates to the client workstation. If the distributor server is not available, the client workstation sends its request to the next distributor server on the list. The company server is always the last server on the list and will send the updates if no distributor server is able to do so.

The figures that follow show some recommended configurations for typical deployments.

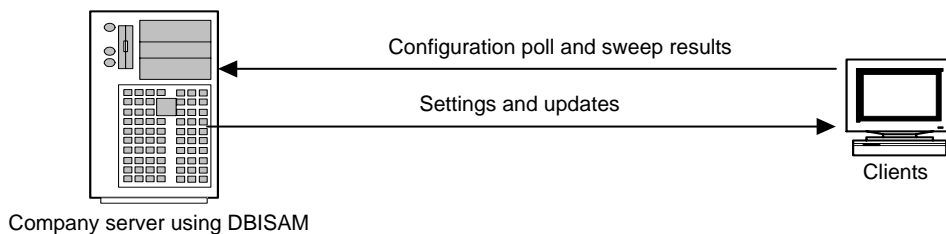


Figure 2: Single site with 500 clients

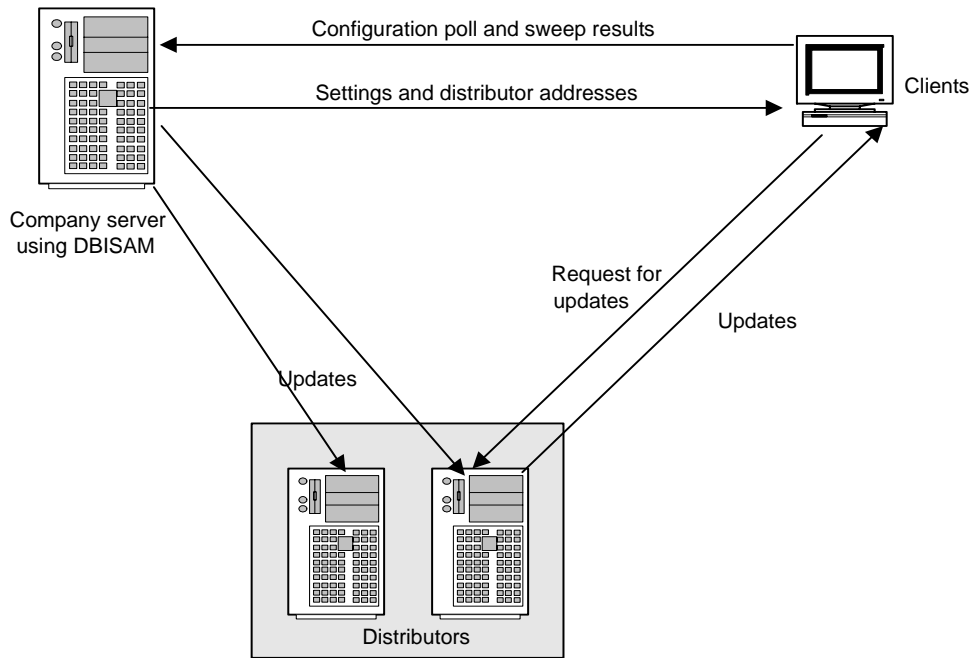


Figure 3: Single site with 10,000 clients

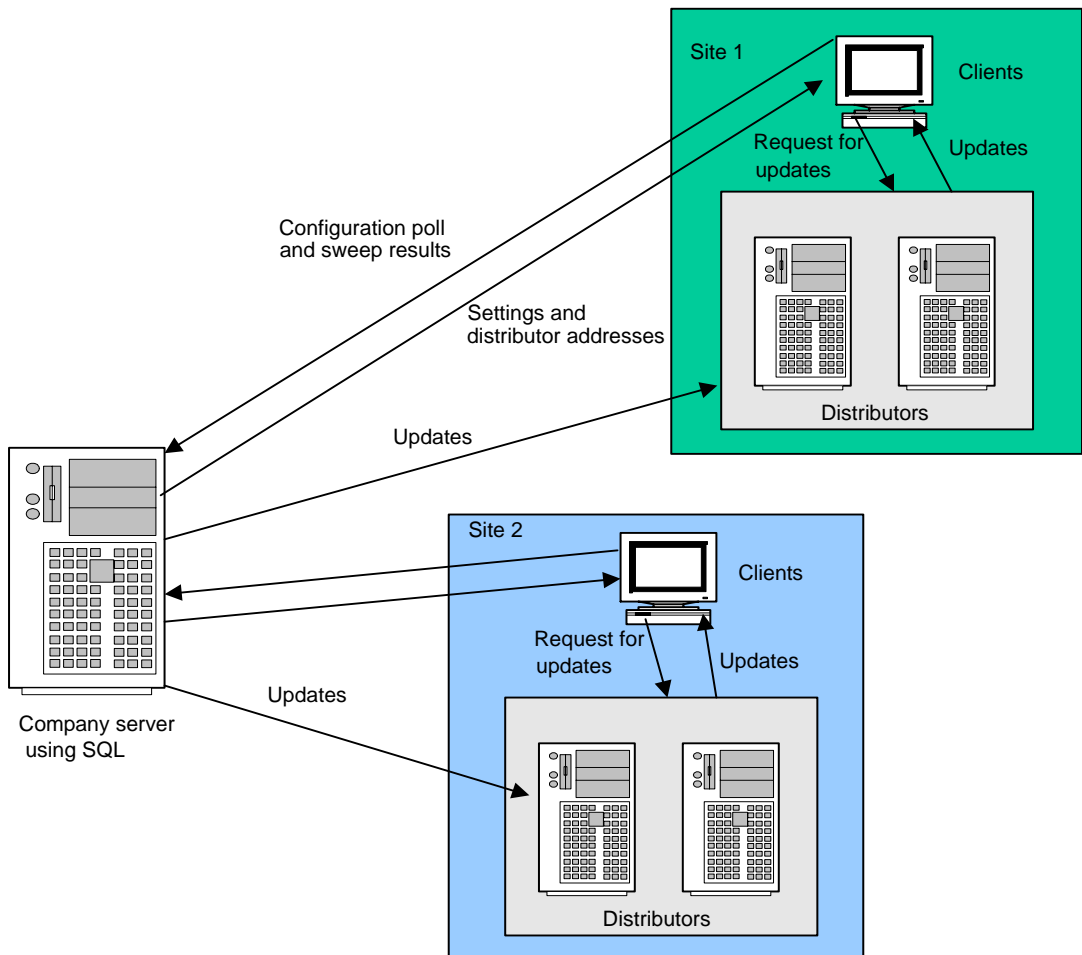


Figure 4: Multiple sites with more than 10,000 total clients

How Webroot Enterprise Updates Work

Most Webroot Enterprise updates are completely automatic after initial installation and setup. The whole update process works like this:

1. Your company server automatically moves updates to all assigned distributors once they are downloaded from the Webroot Update Server. Your distributor servers synchronize with your company server every minute.
2. The client workstations poll the company server.
3. If updates are available, the company server sends a randomized list of distributor servers containing the update to the client workstation.
 - For client workstations to receive updates, you must assign updates to specific groups or to the company as a whole. From the Admin Console, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper** and go to either **Manual Install** or **Auto Install**. If you set up automatic installation on *after* an update has downloaded, the automatic installation does not apply to that update. For more information, see [“Updating Spy Sweeper”](#) on page 60.
4. The client workstation requests updates from the first distributor server on the list.
5. The distributor server sends the updates to the client workstation.
6. If the distributor server is not available, then the client workstation sends its request to the next distributor server on the list. The company server is always the last server on the list, and it will send the updates if no other distributor server is able to do so.

This process spreads the load across all distributor servers to ensure that the servers are not overwhelmed with update requests.

Key Steps to Installing and Setting Up Webroot Enterprise


Once you have determined how you will deploy Webroot Spy Sweeper Enterprise in your environment, you are ready to begin the installation and setup. The six major steps in getting started are:

1. Gather information for server installation.
 - For more information, see [Table 8](#) on page 13.
2. Install Webroot Enterprise Server.
 - For more information, see [“Installing Webroot Enterprise Server on Your Company Server”](#) on page 13.
3. Check for latest news and updates.
 - For more information, see [“Viewing News”](#) on page 37 and [“Installing Updates Manually”](#) on page 61.
4. Deploy initial clients.
 - For more information, see [“Setting Up Client Workstations”](#) on page 28.

5. Set up sweep settings and initial sweeps.
 - For more information, see [“Managing Spyware”](#) on page 49, [“Configuring Sweeps”](#) on page 54, and [“Running Sweeps”](#) on page 56.
6. Broader deployment.



2: Installing Webroot Enterprise

 You must perform the following tasks to install Webroot Enterprise:

1. If you are using Microsoft SQL Server for your database, set up the SQL database. (See [page 11.](#))
 - For information about determining what database to use, see “[Planning for Webroot Enterprise Deployment](#)” on page 5.
2. Install Webroot Enterprise Server on your company server. (See [page 13.](#))
3. Set up one or more client workstations. (See [page 28.](#))
4. If you are using distributor servers, install one or more distributors. (See [page 33.](#))

Setting up a SQL Server Database

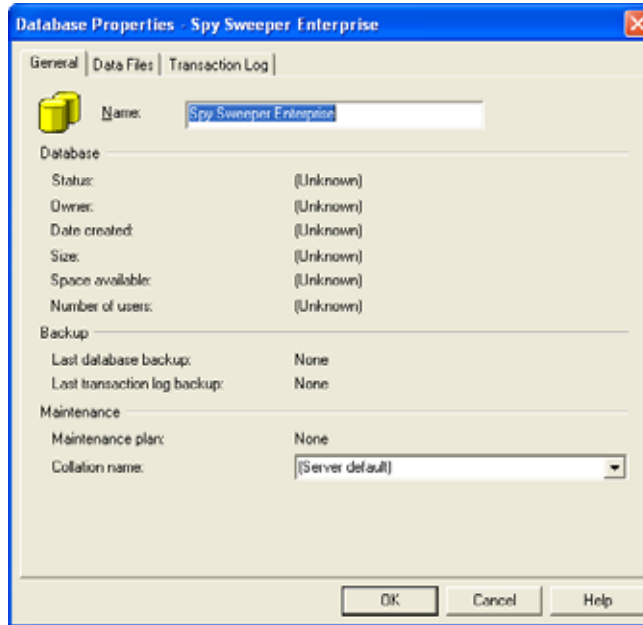
If you determined that you will use Microsoft SQL Server for your installation, you must create the database and a system DSN before starting the installation process. You must also have the user name and password available.

For information about determining whether to use SQL Server, see “[Planning for Webroot Enterprise Deployment](#)” on page 5. If you have an existing Webroot Enterprise installation and need to migrate the database from DBISAM to SQL Server, see “[Appendix B, Migrating an Existing Installation from DBISAM to SQL Server](#)” on page 77.

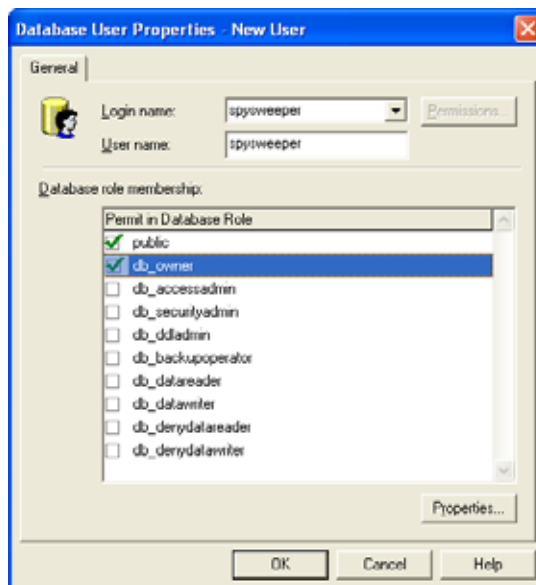
 To set up the SQL Server database:

1. Open the SQL Enterprise Manager.
2. Browse to the Databases folder.
3. Right-click and select **New Database**.

4. Give the new database a unique name.



5. Browse to the Users pane of the new database.
6. Right-click and select **New Database User**.
7. Create a new user and select the db_owner role in the Database Role Membership section.



8. Configure your SQL server for SQL Server and Windows authentication and use a SQL user account instead of a Windows account to access a SQL database with Webroot Enterprise.
9. When you install Webroot Enterprise Server, select SQL Server 2000 in the Database Settings window.
 - The Select the SQL Server 2000 drop-down list takes a moment to populate with the list of SQL servers in your environment.
10. Select the SQL server where you just set up the database.

- If the server name of your SQL Server does not appear in the drop-down list, you can manually enter the name into the field.
11. Enter the name and login information for the database created above.
- The installer program attempts to log in to the SQL database with the credentials provided and displays a message if it cannot connect to the database.

**Note**

SQL Server databases must use Case Insensitive collation to function correctly with Webroot Enterprise Server.

Installing Webroot Enterprise Server on Your Company Server

The Webroot Enterprise Server installation process installs all of the executables described in [Table 4](#) on page 4. You must install Webroot Enterprise Server while logged in with Administrative rights.

The WebrootClientService.exe and WebrootUpdateService.exe run as Windows services and should always be started. This permits your company server to download updates from the Webroot Update Server and client workstations to download updates and configuration changes from your company server.

If you are installing on Windows Server 2003 Service Pack 1, and receive errors during installation, see [“Installing Webroot Enterprise Server on Windows Server 2003 Service Pack 1”](#) on page 27.

During the installation, you must enter all of the information requested to continue the process. You should be prepared with the information listed in [Table 8](#).

Table 8: Information required for Webroot Enterprise Server installation

Field	Description
Download Folder	Path to the folder where your company server stores the updates it downloads from the Webroot Update Server. For best performance, use a folder on the same server. It can also be a folder on any drive your company server can access.
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. Be sure to include the brackets.
E-mail Host	Fully qualified domain name for your e-mail server used for outgoing mail (SMTP server).
From Address	E-mail address that notification messages will come from. Must be a real e-mail address in the format: tom@webroot.com.
Client Service Port	Port on your company server that the Client Service will use to communicate with your client workstations. The default port is 50000. Be sure that the port you use is not used to by another process.

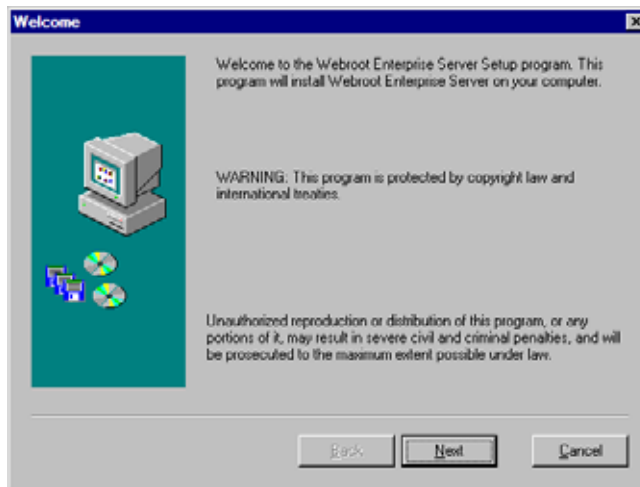
Table 8: Information required for Webroot Enterprise Server installation (Continued)

Field	Description
Proxy Server	<p>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:</p> <ul style="list-style-type: none"> • server_name.company.com:80 • 10.0.0.1:80 <p>If you do not use a proxy server, leave the field blank.</p>
Proxy User Name	If you use a proxy server that requires authentication, enter your proxy server user name.
Proxy Password	If you use a proxy server that requires authentication, enter your proxy server password.
Client Service IP	Enter the IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, select the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, enter the fully qualified domain name of your server (requires a properly configured DNS environment).

To install Webroot Enterprise Server:

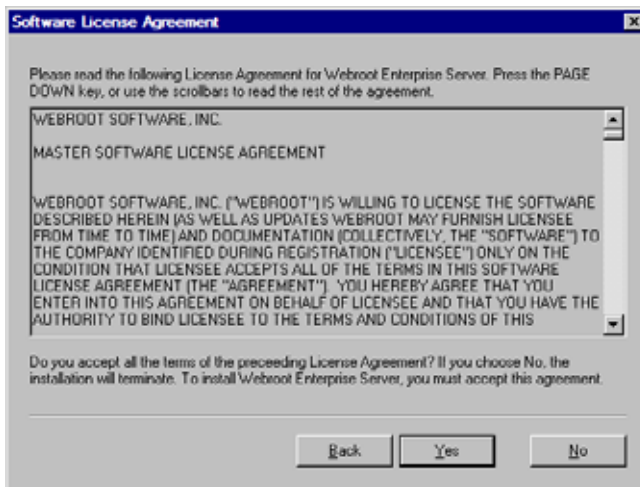
1. Close all other Windows programs that you have open on your computer.
2. Start the installation program.

To install from a CD	To install from a downloaded file
<ol style="list-style-type: none"> 1. Insert the CD into your CD drive. <ul style="list-style-type: none"> • The installation options should display automatically. If they do not, use Windows Explorer to navigate to your CD drive. Then double-click WebrootEnterpriseServerSetup.exe to start the installation. 2. Click Install Webroot Enterprise to start the installation. <ul style="list-style-type: none"> • The Welcome window displays. 	<ol style="list-style-type: none"> 1. Follow the instructions on the Web site to download the WebrootEnterpriseServerSetup.exe file. 2. Go to where you downloaded the file. <ul style="list-style-type: none"> • If you downloaded the file to your Windows Desktop, close all open programs, and you will see an icon on your desktop for the file you downloaded. • If you downloaded the file to a different location, use Windows Explorer to navigate to the file. 3. Double-click WebrootEnterpriseServerSetup.exe. <ul style="list-style-type: none"> • The Welcome window displays.



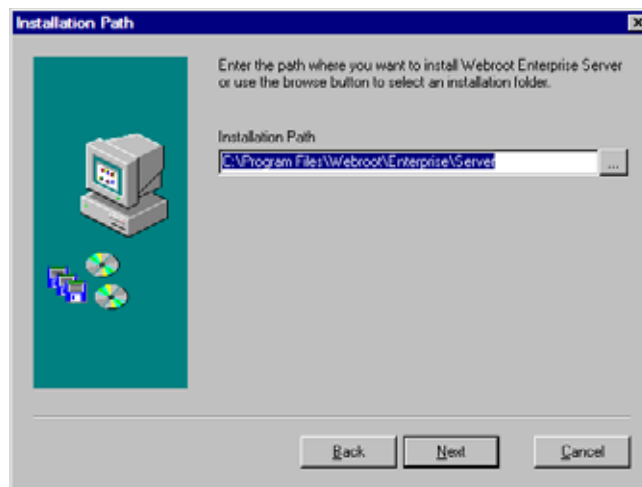
3. Click **Next**.

- The Software License Agreement window displays.



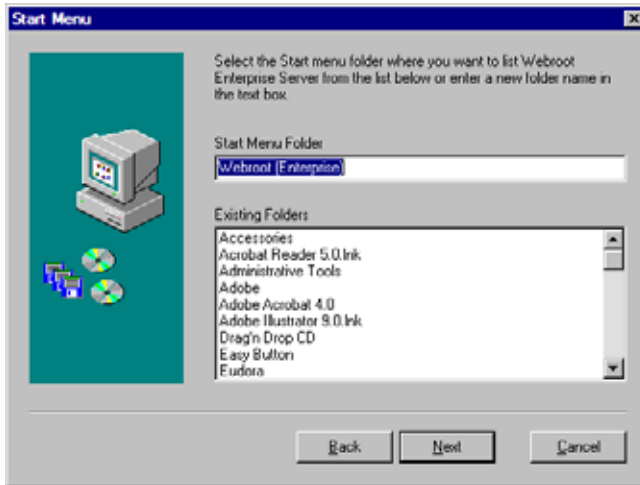
4. Read the license agreement and click **Yes** if you agree with the content.

- The Installation Path window displays showing you the default installation location.



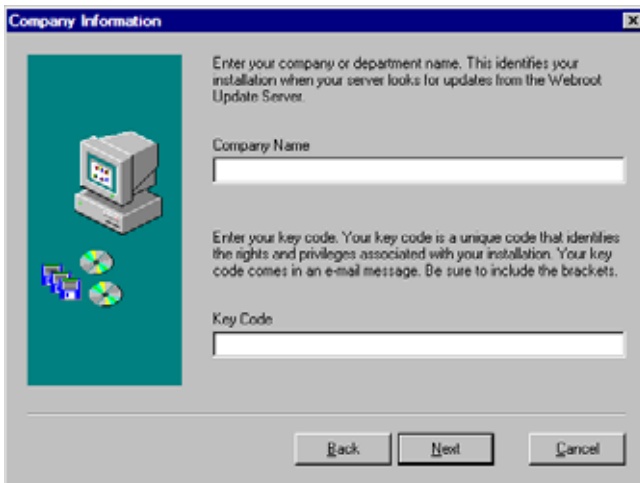
5. Click **Next**.

- If you want to install to a different location, click browse and navigate to the new location.
- The Start Menu window displays showing the default Start menu folder.



6. Click **Next**.

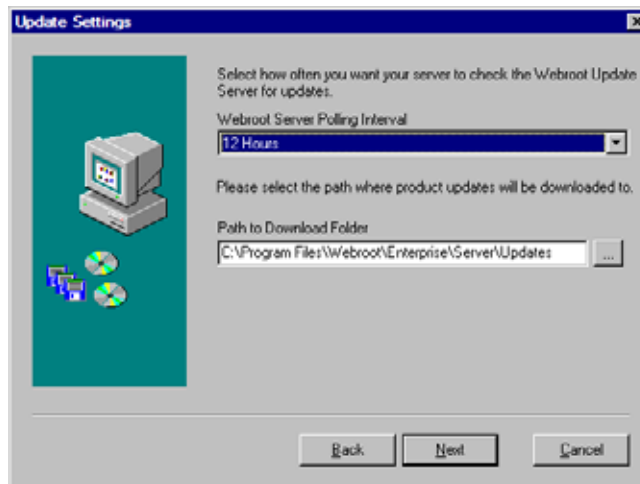
- If you want to use a different Start menu folder, enter a new name or select an existing group.
- The Company Information window displays.



7. Enter the information and click **Next**.

Company Name	Name of your company. This identifies your Webroot Enterprise product when your company server looks for updates from the Webroot Update Server.
Key Code	<p>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.</p> <p>If you purchased Webroot Enterprise through a sales representative or online, you received your key code in an e-mail message. You can copy the key code from the message and paste it in. If you purchased Webroot Enterprise from a store or received it already installed on your computer, the key code is on the product packaging.</p> <p>Be sure to include the braces.</p>

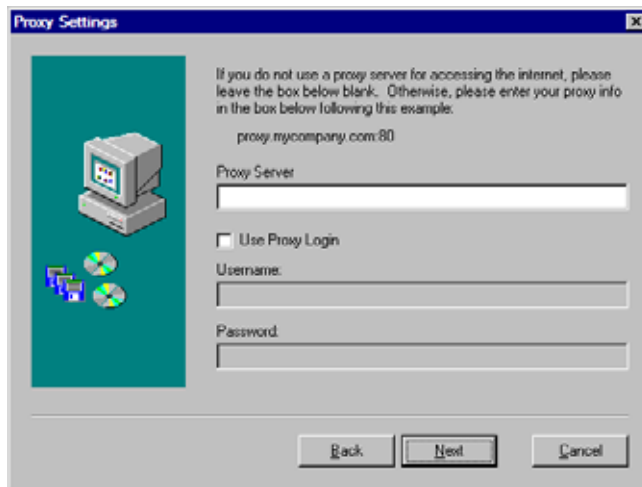
- The Update Settings window displays.



8. Enter or select the information and click **Next**.

Webroot Server Polling Interval	Select how often you want your server to check the Webroot Update Server for updates.
Path to Download Folder	Path to the folder where your company server stores the updates it downloads from the Webroot Update Server. For best performance, use a folder on the same server. It can also be a folder on any drive your company server can access.

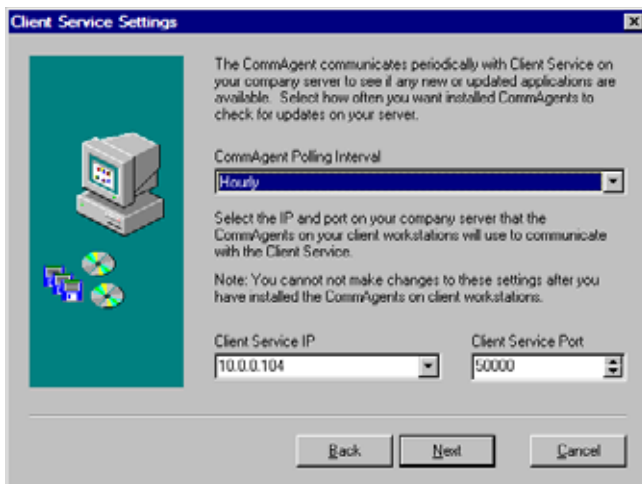
- The Proxy Settings window displays.



9. Enter or select the information and click **Next**.

Proxy Server	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: <ul style="list-style-type: none"> • server_name.company.com:80 • 10.0.0.1:80 If you do not use a proxy server, leave the field blank.
Use Proxy Login	If you use a proxy server that requires authentication, select this option.
Proxy User Name	If you use a proxy server that requires authentication, enter your proxy server user name.
Proxy Password	If you use a proxy server that requires authentication, enter your proxy server password.

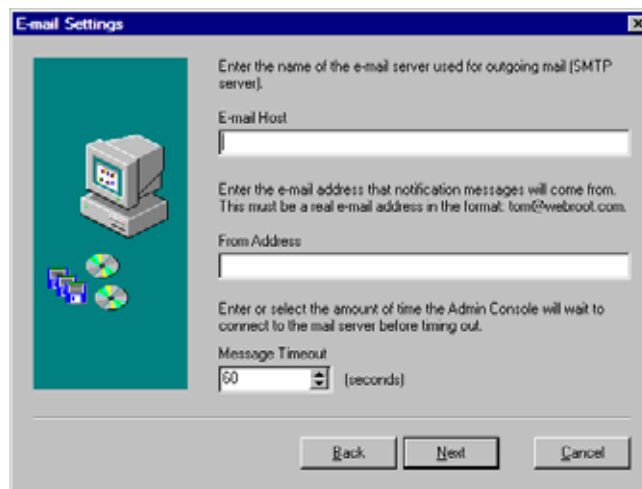
- The Client Service Settings window displays.



10. Enter or select the information and click **Next**.

CommAgent Polling Interval	How often you want installed CommAgents on each client workstation to check for updates and for schedule and configuration changes from your server.
Client Service IP	Enter the IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, select the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, enter the fully qualified domain name of your server (requires a properly configured DNS environment).
Client Service Port	Port on your company server that the Client Service will use to communicate with your client workstations. The default port is 50000. Be sure that the port you use is not used to communicate with another system.

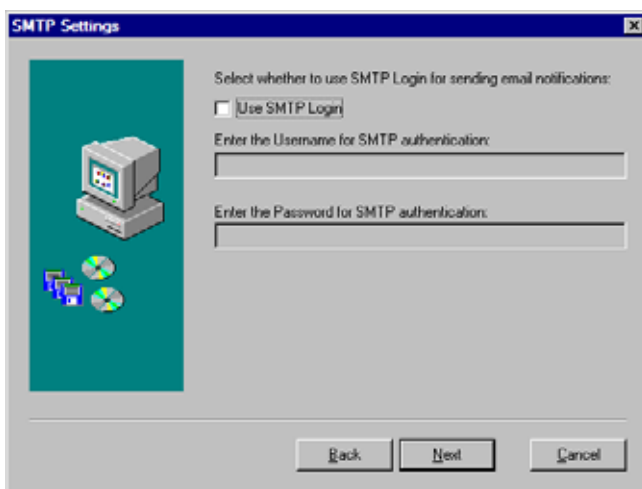
- The E-mail Settings window displays.



11. Enter or select the information and click **Next**.

E-mail Host	Fully qualified domain name for your e-mail server used for outgoing mail (SMTP server). If you do not have this information, enter NA and edit the information from the Admin Console.
From Address	E-mail address that notification messages will come from. 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.

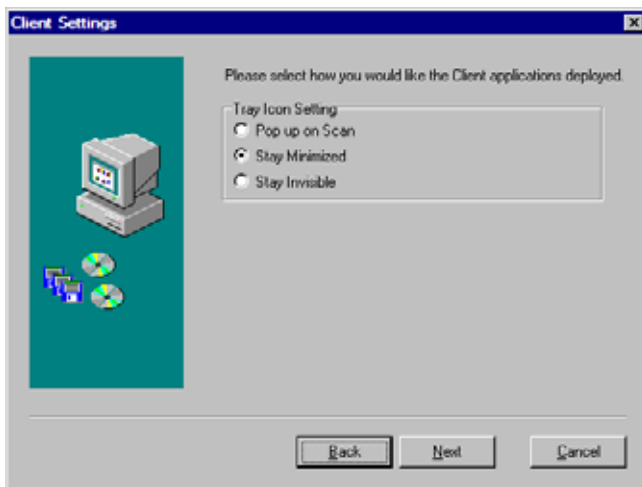
- The SMTP Settings window displays.



12. Enter or select the information and click **Next**.

Use SMTP Login	If you use a secure SMTP e-mail server, select this option and enter the user name and password below.
User Name for SMTP	Name needed to log in to a secure SMTP server.
Password for SMTP	Password needed to log in to a secure SMTP server.

- The Client Settings window displays.

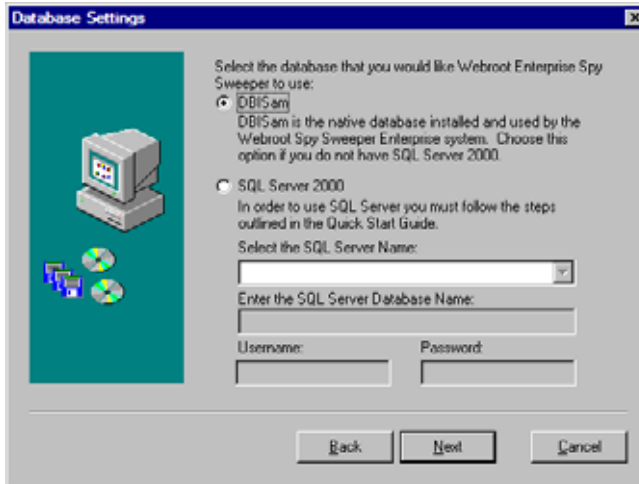


13. Enter or select the information and click **Next**.

Tray Icon Setting	Select how you want Spy Sweeper to appear on client workstations. You can change this setting from the Admin Console by selecting Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings .
Pop up on Scan	Displays a system tray icon that end users can double-click to display the Spy Sweeper 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 Spy Sweeper window, but does <i>not</i> 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 Spy Sweeper 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 <i>no</i> access to the Spy Sweeper window to use options that are set as editable in the Admin Console.

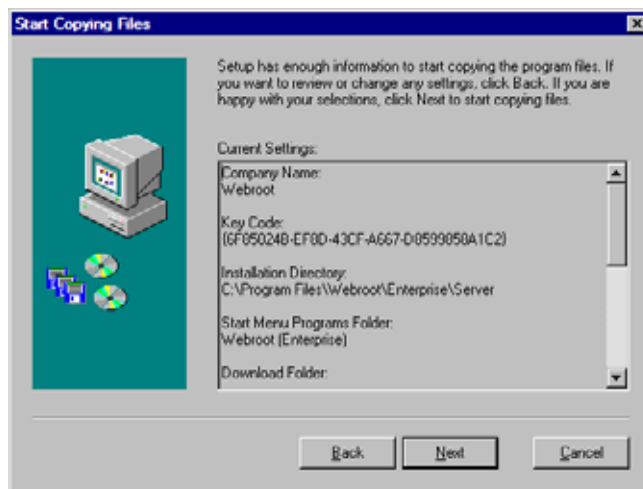
- The Database Settings window displays.



14. Enter or select the information and click **Next**.

DBISam	Select this option only if you have fewer than 10,000 client workstations.
SQL Server 2000	Select this option only if you have SQL Server 2000 and you have over 10,000 client workstations. The Select the SQL Server 2000 drop-down list takes a moment to populate with the list of SQL servers in your environment. Select the SQL server where you set up the database.
SQL Server Database Name field	Enter the name of your SQL Server database. You must already have the database and a system DSN set up.
User Name and Password fields	Enter the user name and password for your SQL Server.

- The Start Copying window displays showing you the current settings.



15. Click **Next**.

- Webroot Enterprise Server installs and automatically starts the Client Service and Update Service.
- A message displays telling you to set up your client workstations.

16. Click **Finish**.

- Webroot Enterprise Server updates automatically when necessary.

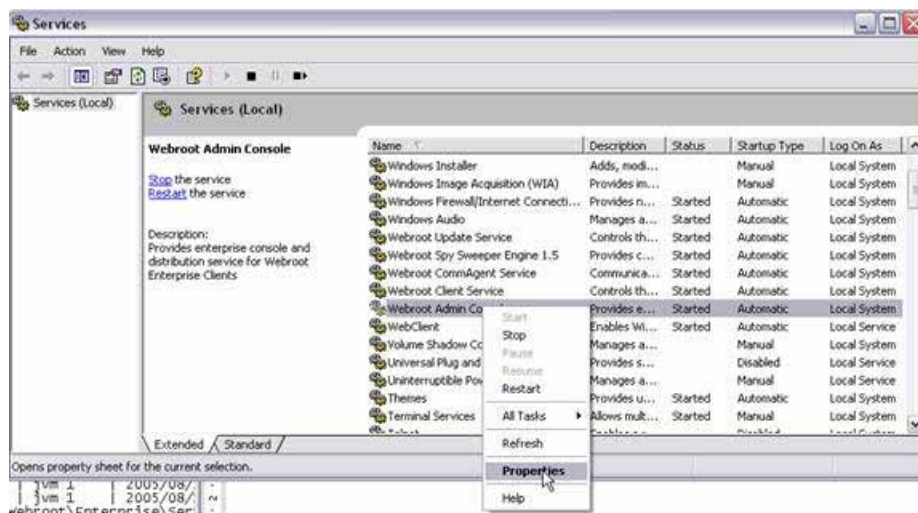
You are now ready to set up one or more client workstations and distributor servers (if needed). For more information, see [“Setting Up Client Workstations”](#) on page 28 and [“Installing and Assigning Distributor Servers”](#) on page 33.

Configuring Log On Properties for Webroot Administration Console Service

To use the Client Deployment feature of the Administration Console to remotely install/uninstall the Spy Sweeper Client, you must first properly credential the Webroot Admin Console Service. This is done from within the Services control panel in Windows. The user account that you specify must have administrative privileges in the Domain(s) that you wish to remotely install/uninstall the client software on.

To open the Services control panel in Windows:

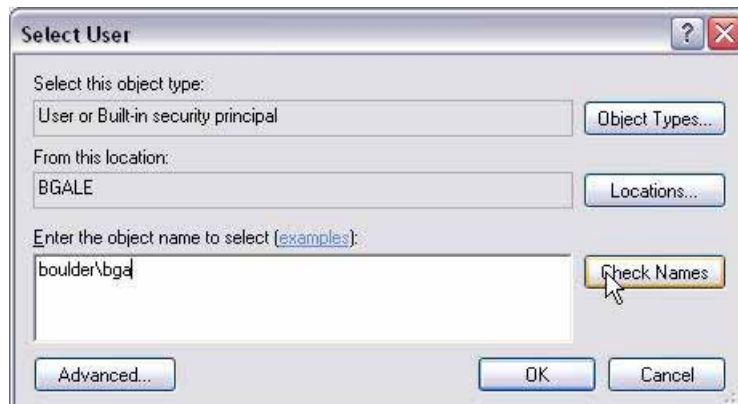
1. From the Start menu, click **Control Panel**
2. Select **Administrative Tools**
3. Select **Services**
4. Highlight the Webroot Admin Console Service, right-click and select **Properties**.



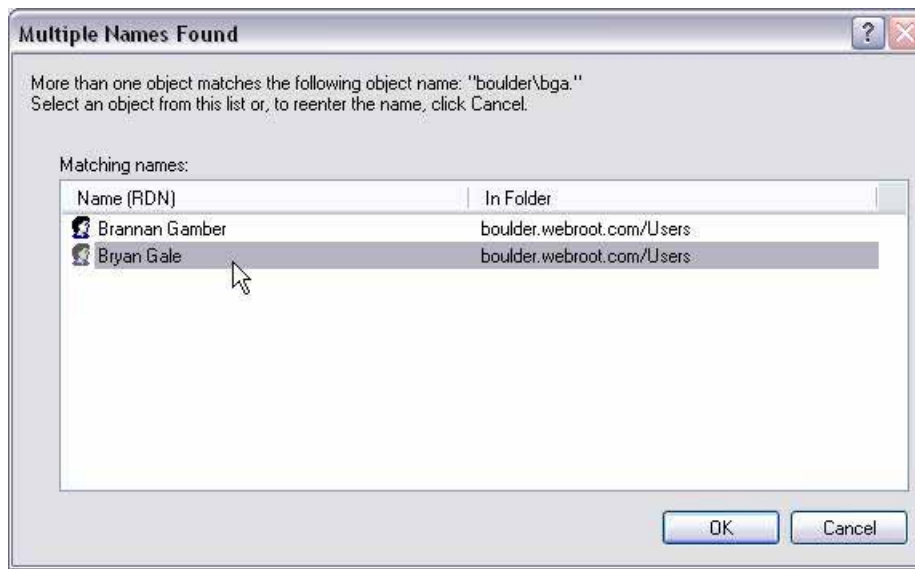
5. Click the **Log On** tab
6. Select **This account**
7. Click **Browse**



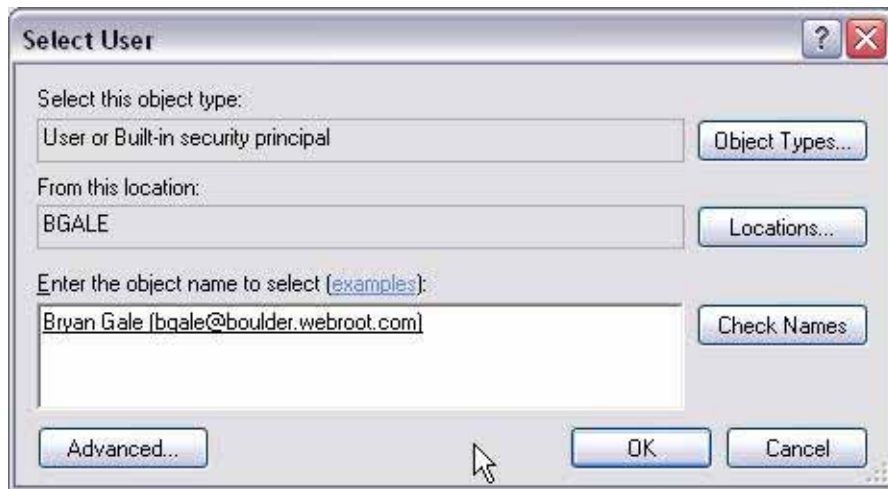
8. Enter domainname\partialusername.
 9. Click **Check Names**
- The User that you select must be a Domain Administrator



10. Highlight the correct user then click **OK**.



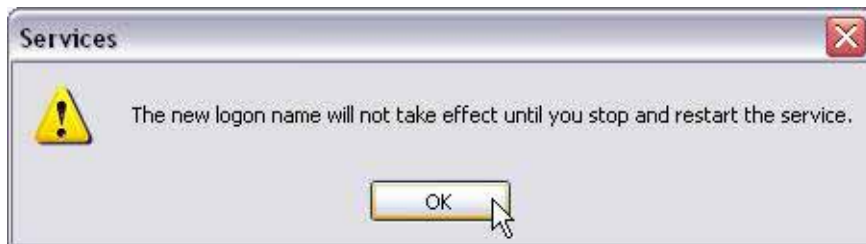
11. Click on OK again



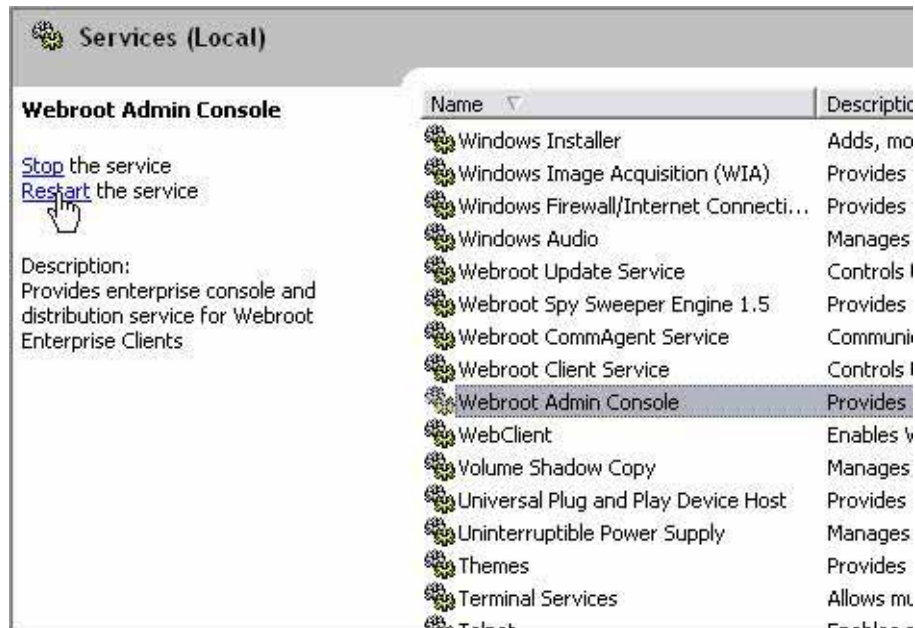
12. Highlight the password and field and enter the correct password for the user in both the Password and Confirm Password fields.
13. Click **Apply**
14. Click **OK**



15. Click **OK**.



16. Restart the Service



Installing Webroot Enterprise Server on Windows Server 2003 Service Pack 1

When installing Webroot Enterprise Server on Windows Server 2003 Service Pack 1, you may receive various errors, and the installation may fail. Following the steps below will often resolve installation problems that occur. This procedure changes your server's Data Execution Prevention (DEP) setting. For information about DEP, refer to Microsoft's Web site at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/memory/base/data_execution_prevention.asp



Note

You must restart your computer after changing the DEP setting.

To change the DEP setting:

1. Open all ports that Webroot Enterprise uses in the Windows firewall.
 - Select **Start > Control Panel > Windows Firewall** and open the following ports: 443, 50000, 50001, 50002, and 50003.
2. Set the Windows DEP setting to "Essential Windows programs and services only."
 - Right-click My Computer and select **Properties**. Click the **Advanced** tab, then click **Settings** under Performance. Click the **Data Execution Prevention** tab and select the "Essential Windows programs and services only" option.
3. Restart your computer.
4. Install Webroot Enterprise Server as described in "[Installing Webroot Enterprise Server on Your Company Server](#)" on page 13.

Setting Up Client Workstations

After you install the Webroot Enterprise Server, you must set up one or more client workstations. This setup installs two components on each client workstation:

- CommAgent—communicates periodically with your company server to see if any configuration changes, new or updated applications, or definitions are available. The CommAgent also updates its settings based on the current server settings in the Admin Console each time it communicates with the company server.
- Spy Sweeper—protects your computers from spyware.

You can install and update these components from the Admin Console. If you prefer to use other installation methods, see [“Alternate Client Workstation Setup Methods”](#) on page 30.

Accessing the Admin Console

You can use the Admin Console to set up client workstations, to install and assign distributors, and to configure all other settings for Webroot Enterprise. The Admin Console is a browser-based interface that supports Internet Explorer 6.0 and later.

You can also access the Admin Console using an HTML Application (HTA) that installs when you install the Webroot Enterprise Server.

You must enter a user name and password to access the Admin Console. The defaults are:

- User Name—admin
- Password—admin

You can log in to the Admin Console only once with a user name. If you try to log in from another location using the same user name, the Admin Console will tell you that you must log out of the existing session before starting a new session.

 To access the Admin Console:

1. Start Internet Explorer and enter one of the following in the Address bar:
 - If you are working from the computer where the Webroot Enterprise Server is installed, enter: `http://localhost:50003/Admin/UI`
 - If you are working from another computer on your network, enter: `http://[Enterprise_server_computer_name]:50003/Admin`
 - If you want to access the HTA version, select **Start > All Programs > Webroot (Enterprise) > Admin Console**.
 - The Welcome to Spy Sweeper Enterprise window displays.
2. Enter your user name and password.
3. Click **Log In**.
 - A progress bar displays showing the status of the resources loading, then the Admin Console displays in your browser.



Note

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

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



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

Setting Up Client Workstations from the Admin Console

You can install and update client workstation components from the Admin Console. You can also see what version each client workstation has installed and the last heartbeat.



Note

Installing the client components from the Admin Console requires Windows networking and access to the admin share (c\$).

To install and update client workstations from the Admin Console:

1. Access the Admin Console.
 - For more information, see “[Accessing the Admin Console](#)” on page 28.
2. From the Admin Console function tree, select **Admin Tasks > Client Deployment**.
 - The Client Deployment panel displays, with a list of the domains or workgroups that exist on your network..
3. Select the domain or workgroup whose workstations you want to see.
4. Select the client workstations where you want to install the client components.
 - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
 - If you are updating an existing installation, you do *not* need to uninstall the client components first.
5. Click **Deploy Client**.
 - If you do not have access to the admin share (c\$) of a workstation, the workstation asks for a user name and password that has admin share access.
 - If you need to uninstall the client components, select the workstation and click **Uninstall Client**.
6. Click **Refresh** or go to the Client Management panel to see the status of the installation.

Alternate Client Workstation Setup Methods

You can also install these components using any of the following methods:

- Going to each individual workstation and executing one of the following:
 - Execute the SpySweeperSetup.msi file.
 - Make sure that all seven of the client installation files (instmsi.exe, instmsiw.exe, SpySweeperSetup.exe, SpySweeperSetup.ini, SpySweeperSetup.msi, SseCleanup.exe, and SSEStart.exe) are in the same folder whenever SpySweeperSetup.msi executes. Typically, these files are in the C:\Program Files\Webroot\Enterprise\Server\Client folder of the system where you installed Webroot Enterprise Server.
 - The SpySweeperSetup.ini file contains the IP address and port of your company server and is needed for the client to install successfully.
 - For unpatched Windows 98, 98SE, ME, or NT execute the SpySweeper.exe file.
 - This file installs Windows Installer 2.0, which is required for the client workstation installation, then installs the client components.
 - Make sure that all seven of the client installation files (instmsi.exe, instmsiw.exe, SpySweeperSetup.exe, SpySweeperSetup.ini, SpySweeperSetup.msi,

SseCleanup.exe, and SSEStart.exe) are in the same folder whenever SpySweeper.exe executes. Typically, these files are in the C:\Program Files\Webroot\Enterprise\Server\Client folder of the system where you installed Webroot Enterprise Server.

- Using a logon script to execute one of the above files. Webroot has provided some example logon scripts that you can change to meet your needs. See “[Example Logon Script](#)” on page 32.
- Using Group Policies, if you use Active Directory. For more information, refer to <http://support.microsoft.com/default.aspx?kbid=314934> and <http://support.microsoft.com/?kbid=302430>.
- Including the Spy Sweeper client as part of an image installed on workstations.
 - Install Spy Sweeper on the target system you are intending to image. If you will be implementing multiple Admin Consoles, you need to create a separate image for clients managed under each console.
 - Stop the Webroot CommAgent service.
 - Remove the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\guid
 - Create your image.

The SpySweeperSetup.msi client installation program defaults to visible installation where you see a progress bar and receive feedback when the installation is complete. For information about using different installation options, see “[Client Installation Options](#)” on page 31.

The CommAgents contact the Client Service on your company server, as displayed in the Client Service Settings in the Admin Console (**Admin Tasks > Settings**, Network section), to look for product updates and configuration changes. If updates are available, the CommAgents access the updates from the distributors assigned on the Assign Distributors panel in the Admin Console. If no other distributors are assigned, the company server (the default distributor) passes updates to the client workstations.

Client workstations poll the company server at random intervals within 20 seconds of installation. During the first contact, the CommAgent also provides the name and MAC address of the client workstation and automatically adds the client to a default group. For more information, see “[Managing Groups](#)” on page 44.

Once you set up the client workstations and they have polled the company server, you can change the groups, if needed. You can also schedule sweeps and change sweep settings based on groups. For more information, see “[Chapter 3, Setting Up the Webroot Enterprise Server](#)” on page 37.

Client Installation Options

You can use the following options in your logon script when you set up client workstations:

- If you would like to use a silent installation, add the /q switch in the line that executes SpySweeperSetup.msi. The installation program defaults to visible installation where you see a progress bar and receive feedback when the installation is complete. The syntax is:
 - `SpySweeperSetup.msi /q`

- You can specify the server IP address and port in the command line instead of relying on the .ini file. The syntax is:

```
- SpySweeperSetup.msi SERVERIP=10.10.10.10 SERVERPORT=50000
```

For a silent installation:

```
- SpySweeperSetup.msi /q SERVERIP=10.10.10.10 SERVERPORT=50000
```

- You can also pass the client deployment setting. This setting should go after the /q switch if you are using that:

```
- Pop up on scan—RUN_CLIENT_AS=0
```

```
- Stay minimized—RUN_CLIENT_AS=1
```

```
- Stay invisible—RUN_CLIENT_AS=2
```

The syntax is:

```
- SpySweeperSetup.msi /q RUN_CLIENT_AS=1 SERVERIP=10.10.10.10  
SERVERPORT=50000
```

- You can apply any of these command line arguments to the SpySweeperSetup.exe installer (which is used for installing on systems lacking the 2.0 version of Windows Installer). The syntax is:

```
- SpySweeperSetup.exe /q RUN_CLIENT_AS=1 SERVERIP=10.10.10.10  
SERVERPORT=50000
```

Example Logon Script

Below is an example logon script. You have to adjust it for your setup and network environment.

You have to put the script on your domain controllers or logon servers, then assign it so that it executes when a workstation logs in to your network. This script assumes that you have a shared drive on your network that contains the SpySweeperSetup.msi and SpySweeperSetup.ini files.

Typically, these files are in the C:\Program Files\Webroot\Enterprise\Server\Client folder of the system where the Webroot Enterprise Server has been installed. Copy the client files to the network share of your choice, then adjust the script to meet your share path. Also be sure to give all workstations read and execute access to the share.

```
@echo off  
REM Check to see if clients are installed on the local machine, if they  
are then display a confirmation  
REM message otherwise install the client package and display a message  
REM Check to see if the Enterprise CommAgent is installed, if not go to  
install otherwise go to check  
if exist "C:\Program Files\Webroot\Enterprise\Spy  
Sweeper\SpySweeper.exe"  
goto check if not exist "C:\Program Files\Webroot\Enterprise\Spy  
Sweeper\SpySweeper.exe"  
goto install  
REM Check to see if Enterprise Spy Sweeper is installed, if not go to  
install otherwise go to loaded  
:check if exist "C:\Program Files\Webroot\Enterprise\Spy  
Sweeper\SpySweeperTray.exe"  
goto loaded if not exist "C:\Program Files\Webroot\Enterprise\Spy  
Sweeper\SpySweeperTray.exe"  
goto install
```

```
REM Display an install message, execute the client setup package from a
shared network drive and then go to end
:install echo Loading Webroot Enterprise Clients...
"C:\Program Files\Webroot\Enterprise\Server\Client\SpySweeperSetup.msi"
goto end
REM If the clients are already installed then display the following
message
:loaded echo Webroot Enterprise Clients are already Installed
:end
```

Uninstalling Spy Sweeper from Client Workstations

You can uninstall client workstation components using the Admin Console from the Client Deployment panel (**Admin Tasks > Client Deployment**). Select the client workstation and click **Uninstall Client**. You can most easily uninstall clients that were deployed from the Client Deployment panel using this method. If you need to uninstall one of these clients manually, you need to browse to a folder containing the SpySweeperSetup.msi file on your network.

Double-click SpySweeperSetup.msi and select **Uninstall**. You cannot uninstall the client using Windows Add/Remove programs feature.



Note


The uninstallation process permanently deletes all spyware that was quarantined on the client workstation.

Installing and Assigning Distributor Servers

By default, the Distributor service is installed with Webroot Enterprise Server on your company server. This acts as a single distributor server.

If you need to add distributor servers, you can install the distributor server software on one or more of your servers. For information about determining whether you need additional distributor servers, see [“Planning for Webroot Enterprise Deployment”](#) on page 5.

Installations with 500 or fewer client workstations typically do not need to install additional distributor servers.

 You must complete the following tasks to install and use distributor servers:

1. Install the distributor server software. (See [page 33](#).)
2. Assign distributor servers. (See [page 34](#).)

Installing Distributor Servers

The distributor server installation installs and starts the Distributor service (WebrootUpdateDistributor.exe).

 To install distributor servers:

1. Execute the WebrootDistributorSetup.exe file on the server you want to be a distributor server.
 - The file is typically in the C:\Program Files\Webroot\Enterprise\Server\Distributor folder of the system where you installed Webroot Enterprise Server.
2. Follow the on-screen instructions.
 - You can now assign distributor servers.

Assigning Distributor Servers

After you install the distributor server on your servers, you must assign those servers to groups.

You can assign a distributor server to one or more groups or to the whole company. For example, if you set up four distributor servers and assign them all to the whole company, the system randomly selects the order of distributors it sends back to the client workstations.

For a complete description of the how the update process works, see [“How Webroot Enterprise Updates Work”](#) on page 8.

This process spreads the load across the servers to ensure that the servers are not overwhelmed with update requests. Distributor servers also can control bandwidth use over a WAN by localizing the client definition and update downloads.



To assign a distributor server:

1. Access the Admin Console.
 - For more information, see [“Accessing the Admin Console”](#) on page 28.
2. From the Admin Console function tree, select **Admin Tasks > Assign Distributors**.
 - The Assign Distributors panel displays, with a list of all existing groups on the left side.
3. Click **Add Distributor**.
 - The Add Distributor window displays.
4. 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.
5. If necessary, enter the IP address of the server.
6. Click **OK**.
 - The server name now displays in the list on the right side of the panel.

7. 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 and click **Unassign Distributor**.
 - To update the status of the distributors, click **Refresh**.
 - To remove the selected distributors from their assignments and from the list of distributors, click **Delete Distributors**.
 - Your company server will automatically send copies of all updates to all distributors. You still need to assign updates manually (from **Spy Sweeper >Update Spy Sweeper >Manual Install**) or set automatic installation rules (from **Spy Sweeper >Update Spy Sweeper >Auto Install**) to determine which updates should be applied to which groups.

Changing the Distributor Server Port

By default, a distributor server listens to port 50003.



Note

If you need to change a distributor server to listen on a different port, you can do so. However, the port on each distributor server must be the same as the port used on the company server for the Distributor Service. For information on changing the local distributor port on the company server, see [“Changing the Distributor Service Port on the Company Server”](#) on page 41. The Admin Console service on your company server also uses the same port.

To change the distributor server port:

1. On the distributor server, create a backup copy of the following file:
C:\Program Files\Webroot\Enterprise\Server\WebServer\etc\jetty.xml
2. Edit the original jetty.xml file with Notepad or another text editor.
3. Change the jetty.port attribute inside the addListener block from the default port of 50003 to the new port.
4. Open regedit and browse to:
HKEY_LOCAL_MACHINE\Software\Webroot\Enterprise\Server\.
5. Enter a new string Value named: DistributorPort.
 - Be sure to capitalize the letters D and P.
6. As a value, enter a new listening port.
 - Be sure to leave out all trailing and leading spaces.
7. Restart the Webroot Update Distributor service.
 - To restart the Webroot Update Distributor service, select **Start > Control Panel > Administrative Tools > Services**. Select the Webroot Update Distributor service and click the **Restart the service** link in the upper-left corner of the window.



3: Setting Up the Webroot Enterprise Server

You can perform the following tasks to complete the setup of the Webroot Enterprise Server:

- View news (see [page 37](#))
- Edit the server settings (see [page 37](#))
- Set up notification (see [page 42](#))
- Manage client workstations (see [page 43](#))
- Assign distributor servers (see [page 34](#))
- Manage Admin Console users (see [page 43](#))

Viewing News

The Admin Console is where you set up, manage, and monitor Webroot Enterprise updates and applications.

Webroot maintains a Webroot Spy Sweeper Enterprise news page that contains information about current version numbers and general spyware news. It also contains links to notes about updates and current documentation.

To access the Admin Console and view news:

1. Access the Admin Console.
 - For more information, see [“Accessing the Admin Console”](#) on page 28.
2. Select **Admin Tasks > News**.
3. Click **Refresh**.

Editing the Server Settings

You entered your server settings during the installation process. These settings provide information to each Spy Sweeper client about the frequency and address for contacting your company server.

Below are important notes about the server settings:

- Client workstations will only get updates and setting changes when the CommAgent polls your company server. Any updates you make here (or elsewhere) will be applied after the polling interval has passed. For example, if your polling interval is every hour and your last client heartbeat was 30 minutes ago, changes you make will be applied 30 minutes from now.

- If you need to be sure that all clients 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.
- Updates for the Webroot Enterprise Server, including the Admin Console, download and install automatically whenever your company server contacts the Webroot Update Server.
- Updates for the Spy Sweeper program and definitions download whenever your company server contacts the Webroot Update Server, but they do *not* install automatically. You must either manually install them (see “[Installing Updates Manually](#)” on page 61) or set up automatic installation (see “[Installing Updates Automatically](#)” on page 61).

To edit the server settings:

1. From the Admin Console function tree, select **Admin Tasks > Settings**.
 - The Settings panel displays, with several sections of settings you can view and edit.
2. Enter information into each field.
 - Click the show/hide bar that separates each section of the panel to see each section’s options.

Field	Description
Basic section	
Company Name	Name of your company. This identifies your Webroot Enterprise product when your server looks for updates from the Webroot Update Server.
Download Folder	Path to the folder where your company server stores the updates it downloads from the Webroot Update Server. Typically, this is a folder on your company server. It can also be a folder on any drive your company server can access.
Polling Intervals: Webroot Server	How often you want your server to check for updates on the Webroot Update Server. If you select Manual Only, you must manually check for updates from Status > Update History , then click Check for Updates .
Polling Intervals: Client	How often you want installed CommAgents on each client workstation to check for updates and configuration changes on your server. If you change this, each CommAgent will retrieve the new setting the next time it contacts the server.
Key Code	<p>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.</p> <p>If you purchased Webroot Enterprise online, you received your key code in an e-mail message. You can copy the key code from the message and paste it in. If you purchased Webroot Enterprise from a store or received it already installed on your computer, the key code is on the product packaging.</p> <p>Be sure to include the braces.</p>

Field	Description
Automatically Install Server Updates	Select this option to have Webroot Enterprise automatically update your Webroot Enterprise Server, including the Admin Console, whenever updates are available.
E-mail section	
From Address	E-mail address that notification messages will come from. 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. Reduces the number of e-mail messages recipients receive.
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 below.
User Name	Name needed to log in to a secure SMTP server.
Password	Password needed to log in to a secure SMTP server.
Send Test E-mail	Select an e-mail address from the drop-down list and click Send Test E-mail . All e-mail addresses entered into Admin Tasks > E-mail Addresses are listed in the drop-down list. You can also enter an e-mail address to test it before adding it.
Advanced section	
Server	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: <ul style="list-style-type: none"> • server_name.company.com:80 • 10.0.0.1:80 If you do not use a proxy server, leave the field blank.
User Name	If you use a proxy server that requires authentication, enter your proxy server user name.
Password	If you use a proxy server that requires authentication, enter your proxy server password.
Initial Interval Min	Minimum 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.
Initial Interval Max	Maximum time a rejected client workstation should wait before trying to connect again. The actual retry time will be between the minimum and maximum, as described above.
Maximum Interval	Amount of time between retries after the client has been rejected several times. The rejected client continues to retry to connect at this interval until it is successful.

Field	Description
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 Admin Tasks > E-mail Addresses are listed in the drop-down list.
Network section	
IP/Host Name	Enter the IP address or host name that the client workstations uses to communicate with your company server. For IP resolution, select the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, enter the fully qualified domain name of your server (requires a properly configured DNS environment).
Ports: No SSL and SSL (Client Service Settings)	<p>Port on your company server that the Client Service uses to communicate with your client workstations. The default port is 50000. Be sure that the port you use is not used to communicate with another system.</p> <p>Fill in one or both fields with the port you want to use. If you want to use SSL, you must also select the Use SSL option at the bottom of the Network section.</p> <hr/> <p>Note: If you change the IP/Host Name or Port here, you must manually change the HKEY_LOCAL_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\su key on every client workstation.</p> <hr/>
Ports: No SSL and SSL (Admin Server/ Local Distributor Settings)	<p>Port on your company server that the Distributor Service uses to distribute updates to distributor servers and client workstations. The default port is 50003. Be sure that the port you use is not used to communicate with another system. The Admin Console service on your company server also uses the port you configure here.</p> <p>Fill in one or both fields with the port you want to use. If you want to use SSL, you must also select the Use SSL option at the bottom of the Network section.</p> <hr/> <p>Note: If you need to change this port, you must also complete the procedure described in “Changing the Distributor Service Port on the Company Server” on page 41. The port on <i>each</i> distributor server must be the same as the port here. For information on changing the port on the distributor servers, see “Changing the Distributor Server Port” on page 35.</p> <hr/>
Sweep Now Ports: No SSL and SSL (Client Settings)	<p>Port on your company server used to start a Spy Sweeper sweep of the selected client workstations from the Admin Console. The default port is 50001. Be sure that the port you use is not used to communicate with another system.</p> <p>Fill in one or both fields with the port you want to use. If you want to use SSL, you must also select the Use SSL option at the bottom of the Network section.</p>

Field	Description
Poll Now Ports: No SSL and SSL (Client Settings)	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. Be sure that the port you use is not used to communicate with another system. Fill in one or both fields with the port you want to use. If you want to use SSL, you must also select the Use SSL option at the bottom of the Network section.
Use SSL	If you want to use SSL connections for the ports listed above, select this option. Note: Selecting this option means that <i>all</i> of the ports with the SSL field will use SSL. Be sure to fill in the SSL field for each port above.
Database section	
Server Type	You cannot change the type of database after installation. The information in this section is read-only.

3. Click **Apply**.

Changing the Distributor Service Port on the Company Server

The Distributor Service on your company server uses port 50003 by default to distribute updates to your distributor servers and client workstations.



Note

If you need to change this port, you must complete the procedure below. However, the port on each distributor server must be the same as the Distributor Service port on the company server. For information on changing the port on the distributor servers, see [“Changing the Distributor Server Port”](#) on page 35.

Be sure that the port you use is not used to communicate with another system. The Admin Console service on your company server also uses the same port.

To change the Distributor Service port on the company server:

1. From the Admin Console function tree, select **Admin Tasks > Settings**.
 - The Settings panel displays, with several sections of settings you can view and edit.
2. Click the **Network** show/hide bar.
3. Change the port under Local Distributor Settings.
4. Click **Apply**.
5. Log out of the Admin Console.
6. On the company server, create a backup copy of the following file:
C:\Program Files\Webroot\Enterprise\Server\WebServer\etc\jetty.xml
7. Edit the original jetty.xml file with Notepad or another text editor.

8. Change the `jetty.port` attribute inside the `addListener` block from the default port of 50003 to the new port.
9. Restart the Webroot Admin Console Service.
10. Access the Admin Console using the new port number.
11. From the Admin Console function tree, select **Webroot Enterprise Dashboard > Server Status**.
 - The Server Status panel displays.
12. Check that the Update Distributor port is open.


Setting Up Notification

You can set up the following for the messages that the Webroot Enterprise Server sends to notify you of various events such as the availability of product updates:

- E-mail addresses to use for notification (see [page 42](#))
- E-mail message content (see [page 42](#))
- Error notification (see [page 43](#))
- Update notification (see [page 62](#))

Setting Up Notification E-mail Addresses

You can set up e-mail addresses that the Webroot Enterprise Server uses to notify you of various events such as the availability of product updates.

 To set up notification e-mail addresses:

1. From the Admin Console function tree, select **Admin Tasks > E-mail Addresses**.
 - The E-mail Addresses panel displays.
2. Click **Add E-mail Address** to add a new address.
3. Enter the First Name, Last Name, and E-mail Address.
4. Click **OK**.

Setting Up Notification Messages

You can set up the messages that Webroot Enterprise Server sends for the following types of events:

- Availability of updates or definitions to the Webroot Enterprise Server or client workstation components
- Detected spyware
- Errors that occur on client workstations

 To set up notification e-mail messages:

1. From the Admin Console function tree, select **Admin Tasks > Configure E-mail Notifications**.
 - The Configure E-mail Notifications panel displays.
2. Click the tab for the type of message you want to set up.
3. Enter the E-mail Subject 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**.

Setting Up Error Notification

You can configure who receives notification of different types of errors that come from your client workstations.



To set up error notification:

1. From the Admin Console function tree, select **Admin Tasks > Error Notifications**.
 - The Error Notifications panel displays with a list of all e-mail addresses you have entered for notification and the alert categories of increasing scope.
2. Drag a name from the list to an alert 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**.
 - To receive all error messages, move the e-mail address to the Errors, Warnings & Info category.

Managing Clients

You can manage client workstations and perform the following functions from the Admin Console:

- Manage groups (see [page 44](#))
- Create and export client reports (see [page 45](#))
- Poll client workstations now (see [page 46](#))
- Delete client workstations (see [page 46](#))


Managing Groups

You can set up groups to help administer the Webroot product updates, sweep scheduling, and sweep settings. Every workstation where you have installed the Spy Sweeper client must belong to a group. By default, each client workstation is added to a default group named after the domain or workgroup the client workstation is in.

You can administer the following by group:

- Which applications to install on client workstations
- Which updates to install on client workstations
- Specific settings for each application

You can change the group organization and assignments to meet your needs. You might use groups to distinguish between different types of users. For example, you could have a group that includes all system administrators and use this group to test new products and product updates before distributing them throughout the company. You can also use groups to distinguish between departments, geographic locations, or any other category you choose.



To set up groups:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
 - The Client Management panel displays, with a list of all existing groups on the left side.
 - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Click **Add Group**.
 - You can also right-click anywhere in the group tree and select **Add Group**.
 - The New Group window displays.
3. Enter a group name.

4. Click **OK**.
 - The group name now displays in the group tree on the left side of the panel.
5. Drag a workstation from the list to a group in the group tree.
 - To move a workstation from one group to another, drag it from the current group and drop it onto another group.
 - To delete a group, move all workstations in the group to another group, then select the group you want to delete, and click **Delete Group**.
 - To delete a workstation from a group, select the group, then select the workstation and click **Delete Workstations**. If the deleted workstation contacts the company server, the workstation is added to a default group named after the domain or workgroup the client workstation is in.

Creating and Exporting Client Reports

Using the Client Management panel, you can create various reports. For example, you can sort based on the Last Heartbeat, Version, or Definitions column. If you want to save a report as file, you can export it as a comma separated (CSV) file.



To create and export client reports:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
 - The Client Management panel displays with a list of all existing groups on the left side.
 - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Click the group that includes the workstation you want to report on.
3. Select the workstations you want to include in the report.
 - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
4. Click **Export Workstations**.
 - You can also right-click the selected workstations and select **Export Workstations**.
 - The Save Workstations to File window displays.
5. Select where you want to save the file and enter a file name.
6. Click **Save**.

Polling Client Workstations Now

You can poll one or more client workstations from the Client Management panel. You can use this function if you have changed some settings, such as assigning program or definition updates, and you want client workstations to receive those updates immediately.



Note

Use this option selectively to ensure that you do not overwhelm your network and servers with a large number of client workstations requesting updates at the same time.

To poll client workstations now:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
 - The Client Management panel displays with a list of all existing groups on the left side.
 - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Click the group that includes the client workstation you want to poll.
3. Select the client workstation you want to poll.
 - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
4. Click **Poll Now**.
 - You can also right-click the selected workstations and select **Poll Now**.
 - The poll starts on the selected client workstations. A confirmation message displays, with the number of workstations the system sent the polling message to.
 - To check the status of the polling, click **Refresh** and sort on the Last Heartbeat column to see that client workstations have updated.

Deleting Client Workstations

If you find that a client workstation has not had a heartbeat for a long time or you know that the workstation no longer exists, you can delete the workstation from the database. If the client workstation reconnects to the network and contacts your company server, the system creates a new database entry, and the client workstation is added to a default group named after the domain or workgroup the client workstation is in.

To delete client workstations:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
 - The Client Management panel displays with a list of all existing groups on the left side.
 - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Click the group that includes the client workstation you want to delete.

3. Select the client workstation you want to delete.
 - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
4. Click **Delete Workstations**.
 - You can also right-click the selected workstations and select **Delete Workstations**.
 - The system deletes the workstation from its database.

Managing Admin Console Users

You must enter a user name and password to access the Admin Console. The defaults are:

- User Name—admin
- Password—admin

You can edit the default user name and add new users as needed.

You can also view a daily audit log that lists the actions taken by each Admin Console user. The logs are stored in your Webroot Enterprise Server installation folder. The default location is: C:\Program Files\Webroot\Enterprise\Server\WebServer\logs. The log file names start with Webroot_Enterprise_Audit_ and have the date at the end, for example, Webroot_Enterprise_Audit_20050621.log.

You set how long to retain the daily audit logs in **Admin Tasks > Settings**, Advanced section.



To add new users:

1. From the Admin Console function tree, select **Admin Tasks > User Management**.
 - The User Management panel displays with a list of all existing user names.
2. Click **Add User**.
 - The Add Admin Console User window displays.
3. Enter the user information.
 - The following fields are required: User Name, Password, First Name, Last Name, and E-mail Address..
 - You can use up to 20 characters for user names and passwords.
4. Click **OK**.
 - To edit an existing user, select the row and click **Edit User**.
 - To delete an existing user, select the row and click **Delete User**.

4: Managing Spy Sweeper

Spy Sweeper lets you protect your end users' privacy and your company's computers from a variety of spyware including those that monitor all computer activities (system monitors) and those that can steal or destroy data (Trojan horses). It also detects spyware that pops up ads on your computer (adware) and cookies that may contain personal information (tracking cookies).

You can set up and perform the following Spy Sweeper functions from the Admin Console:

- Manage spyware (see [page 49](#))
- Configure sweeps (see [page 54](#))
- Run sweeps (see [page 56](#))
- Update Spy Sweeper (see [page 60](#))
- View a summary of detected spyware (see [page 63](#))

As a system administrator, you can also unlock functions at a client workstation and customize the Spy Sweeper settings for an end user. For more information see [“Unlocking Functions at a Client Workstation”](#) on page 63.

Managing Spyware

You can manage spyware for client workstations in the following ways:

- Set up automatic handling of spyware found (see [page 49](#))
- Set up continuous monitoring of certain spyware activities (see [page 51](#))

Setting Up Automatic Spyware Handling

By default, Spy Sweeper quarantines detected spyware for 30 days. You can change this default behavior for client workstations in the following ways:

- By setting up exceptions for spyware by type
 - You can set up Spy Sweeper to automatically handle detected spyware based on the spyware type. Spy Sweeper can automatically do one of the following for each spyware type:
 - Log only, don't quarantine (default)
 - Quarantine, delete after 2 days
 - Quarantine, delete after 7 days
 - Quarantine, delete after 30 days
 - Quarantine, delete after 365 days
 - Don't quarantine, delete right away

- By setting up exceptions for specific spyware to keep or to restore already quarantined spyware
 - To override the default spyware handling for each spyware type, you can set specific spyware to keep. You may want to use this option if your end users have specific spyware on their computers that they need to keep to make another program run properly.
 - Spy Sweeper must detect the spyware on at least one client workstation before you can set Spy Sweeper to keep it.
 - Setting a specific spyware to keep also restores that spyware from quarantine, when the client workstation next polls, if it has already been detected and quarantined.



Note


The settings here override the settings for each spyware type.

You can set up automatic spyware handling by group or for the whole company.



Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

 To set up automatic spyware handling:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Manage Spyware > Detected Spyware**.
 - The Detected Spyware panel displays with a list of each spyware type.
2. From the group tree, select the group you want to set up.
 - If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. For each spyware type, select how you want Spy Sweeper to handle it.
4. For any spyware you want to always keep, move the spyware from the Found Spy List to the Always Keep/Restore from Quarantine list.
 - The Found Spy List includes each spyware instance that Spy Sweeper has found on a workstation in the company.
 - To see more information about a specific spyware item, select it in the Found Spy List and click **More**.
 - Moving spyware to the Always Keep/Restore from Quarantine list restores any already quarantined instances of the spyware on the next sweep.

5. Click **Apply**.

- Spy Sweeper will now automatically handle each spyware type based on your selections. It will also always keep the spyware in the Always Keep/Restore from Quarantine list for the selected group when it runs sweeps.
- 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 Company Settings**.

Setting Up Continuous Monitoring: Smart Shields

You can set up Spy Sweeper to continuously monitor several common spyware-related activities. We call these settings “Smart Shields.” You can set up continuous monitoring options by group or for the whole company.



Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

To set up continuous monitoring:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Manage Spyware > Smart Shields**.
 - The Smart Shields panel displays with the continuous monitoring (Smart Shields) options.
2. From the group tree, select the group you want to set up.
 - If you want these settings to apply to the whole company, select the company at the top of the group tree.
 - The sections in the Smart Shields panel show the current settings for the selected group or for the company.
3. Select each option you want.
 - Click the show/hide bar that separates each section of the panel to see each section’s options.

Option	Description
Windows System section	
Memory Shield On	Sweeps memory once per minute looking for spyware.
Messenger Shield On	(Applies only to Windows NT, 2000, and XP.) This option 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.

Option	Description
Messenger Service Startup Type	If you turn the Messenger Shield off, after having turned it on, this option controls the state of the Messenger Service Startup Type when the Messenger Shield is off.
Leave the Messenger Service Running when Messenger Shield Is Turned Off	If you turn the Messenger Shield off, after having turned it on, this option controls the status of the Messenger Service when the Messenger Shield is off.
Alternate Data Stream (ADS) Shield	(Applies only to Windows NT, 2000, and XP.) This option 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.
Internet Explorer section	
Tracking Cookie Shield On	Actively watches for tracking cookies as you visit Web sites and removes them. Tracking cookies are cookies that can track your Web activities. These <i>may</i> include cookies that contain user names, passwords, or similar information that you enter on some Web sites.
IE Hijack Shield On	Actively protects various Internet Explorer functions, such as the home page, search page, error pages, and other default pages that Internet Explorer displays. Some spyware changes (“hijacks”) these pages without letting you know. Whenever spyware tries to change these pages, Spy Sweeper blocks the change.
Protected Home Page	Enter the Web 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 home page 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 >Internet Explorer panel in Spy Sweeper. If the Tray Icon Setting (Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings) is set to Stay Invisible, end users will not be able to change their home page.
Hosts File Shield On	This option actively prevents changes to the Hosts file. Some spyware will add or change the IP address for a Web site in the Hosts file. When you try to go to the added or changed Web site, you will really go to a different Web site, such as an advertising site. This shield ensures that spyware does 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	If you turn the Hosts File Shield off, after having turned it on, this option controls the state of the Hosts file when the Hosts File Shield is off.
IE Favorites Shield	This actively protects Internet Explorer favorites. Whenever a Web site tries to change favorites, Spy Sweeper stops the Web site from making the change. Some Web sites add entries to IE favorites without letting the user know. Users can still add to favorites in the normal way in IE.
Startup section	

Option	Description
Startup Shield On	Actively watches startup items for any changes. Some spyware will add startup items, so that the spyware will always start. This shield ensures that spyware does not add something to the startup items, but also effectively prevents end users from installing software. Be sure that your users do not need to install new software before selecting this shield or set this shield to user editable and instruct users to disable the shield before installing software.
Enter/Edit Application Not to Block	You can set up a whitelist of applications that your users need to install and startup with Windows. Spy Sweeper will not block the applications in the whitelist. To add an application to the whitelist, enter the .exe file name in this field and click Add . You can also enter the entire run key that will be added to the registry for the application.
Startup Shield Whitelist	Displays the list of applications that Spy Sweeper will not block from installing and adding to the Windows startup list. To change or delete an application, select it and click Modify or Delete .
Common Ad Sites section	
Blocked Websites Shield On	Adds a list of known advertising sites to your Hosts file and sets the IP address for those 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 Webroot Spyware Definitions	Uses the list of known advertising sites that comes as part of the Spy Sweeper definitions to block banner and other advertising from the sites on the list.
Use Custom List	Uses the list of sites that you added below to block banner and other advertising from the sites on the list.
Enter/Edit Website to Block	You can add to the list of blocked sites. To add a site, enter the site address in this field and click Add .
Common Ad Websites	Displays the of Web sites you have added. To change or delete a site, select it and click Modify or Delete .
Spy Installation section	
Spy Installation Shield On	Actively watches for known spyware that tries to install itself on your computer. Whenever known spyware tries to install itself, Spy Sweeper stops the installation.
Enter/Edit Application to Block	You can add executable file names to the list, and this shield will stop the file from executing on the client computer 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 an application, enter the file name in the text box and click Add .
Additional Blocked Applications	Displays the of blocked applications you have added. To change or delete an application, select it and click Modify or Delete .

4. If you want end users to be able to change a setting, select the User Editable option.
5. Click **Apply**.
 - Spy Sweeper will now actively shield the settings you selected.
 - 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 Company Settings**.

Configuring Sweeps

You can configure the following settings related to spyware sweeps:

- Sweep settings (what to sweep) (see [page 54](#))
- Alerts related to found spyware (see [page 56](#))

Configuring Sweep Settings

You can configure settings that control how Spy Sweeper sweeps client workstations looking for spyware. You can also set up a password to unlock functions at a client workstation. For more information, see “[Unlocking Functions at a Client Workstation](#)” on page 63.

You can configure sweep settings by group or for the whole company.



Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.



To configure sweep settings:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings**.
 - The Sweep Settings panel displays with available sweep options.
2. From the group tree, select the group you want to set up.
 - If you want these settings to apply to the whole company, select the company at the top of the group tree.
 - The settings in the Sweep Settings panel show the current settings for the selected group or for the company.
3. Select each option you want.

Option	Description
Sweep Drives	Select the drives you want Spy Sweeper to sweep. Typically, most spyware installs on the C: drive, but you should sweep all hard drives periodically.
Sweep Folders	

Option	Description
Only Known Spyware Folders	Select this option to make the sweep run faster. When you use this option, Spy Sweeper only looks in the folders where spyware files are typically found. Using this option performs a less thorough sweep. You should periodically sweep all folders.
All Folders on Selected Drives	Select this option to have Spy Sweeper look in all folders on the drives you select to sweep. This type of sweep will take longer to run. Using this option performs a more thorough sweep.
Memory	Select this option to have Spy Sweeper sweep your computer's memory for spyware. Typically, you want to sweep memory each time you run a sweep. Spyware commonly loads into memory.
Registry	Select this option to have Spy Sweeper sweep your computer's registry for spyware. Typically, you want to sweep the registry each time you run a sweep. Spyware commonly creates entries in your computer's registry.
Tray Icon	Select how you want Spy Sweeper to appear on client workstations.
Pop up on Scan	Displays a system tray icon that end users can double-click to display the Spy Sweeper window and automatically pops up the window whenever a sweep starts, whether scheduled or using Sweep Now. Also places an item on the Start menu of the client workstation.
Stay Minimized	Default and recommended setting. Displays a system tray icon that end users can double-click to display the Spy Sweeper window, but does <i>not</i> 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 Spy Sweeper is sweeping their system. Also places an item on the Start menu of the client workstation.
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 Spy Sweeper window to use options that are set as editable in the Admin Console.
Allow Users to Cancel Sweeps	Select this option to permit end users to stop a sweep, regardless of how the sweep was started.
Close Internet Explorer after Sweeps	Defaults to selected, which closes Internet Explorer after a sweep if the sweep found spyware or other threats that Spy Sweeper could not delete with Internet Explorer open. If you have users who work in Internet Explorer regularly, <i>deselect</i> this option. Deselecting the option leaves Internet Explorer open after a sweep and deletes any found spyware and threats that Spy Sweeper could not delete with Internet Explorer open when the user closes Internet Explorer.
Close Windows Explorer after Sweeps	Defaults to selected, which closes Windows Explorer after a sweep if the sweep found spyware or other threats that Spy Sweeper could not delete with Windows Explorer running.
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 Spy Sweeper definition updates directly from Webroot automatically when they are connected to the Internet. For more information, see " Setting Up Updating for Mobile End Users " on page 63.

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 Spy Sweeper definition updates directly from Webroot by clicking a button when they are connected to the Internet. For more information, see “Setting Up Updating for Mobile End Users” on page 63.
Client Password	Enter a password that lets system administrators access and change Spy Sweeper settings when you are working at a client workstation. For more information, see “Unlocking Functions at a Client Workstation” on page 63.

4. If you want end users to be able to change a setting, select the User Editable option.
5. Click **Apply**.
 - Spy Sweeper will use these options when running sweeps.
 - 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 Company Settings**.

Setting Up Sweep Alerts

You set Spy Sweeper to send e-mail alerts to specific people when it detects different types of spyware. Before you can set up e-mail alerts, you must enter one or more notification recipients. For more information, see [“Setting Up Notification E-mail Addresses”](#) on page 42.

To set up sweep alerts:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Alert Notifications**.
 - The Alert Notifications panel displays with the available alert types and notification recipients.
2. Drag the name of a notification recipient to the alert tree.
 - To remove a recipient from an alert type, select it and click **Unassign E-mail Address**.
 - Spy Sweeper will use these settings to send alerts when it detects spyware.

Running Sweeps

You can run sweeps the following ways:

- Run a sweep now (see [page 57](#))
- Schedule sweeps (see [page 57](#))
- Run a sweep in safe mode (see [page 58](#))

You can also view and stop sweeps that are running. For more information, see [“Viewing and Stopping Sweeps”](#) on page 60.

Running a Sweep Now

You can run a sweep on one or more client workstations when you learn about a critical spyware threat. The sweep will use the current sweep settings. If you want to change the settings, make the changes first and wait for the next polling interval to ensure that client workstations receive the new settings. You can also use the Poll Now function to tell all client workstations to poll and get the new settings immediately. For information about changing sweep settings, see “[Configuring Sweep Settings](#)” on page 54. For information about polling now, see “[Polling Client Workstations Now](#)” on page 46.

The Sweep Now function uses port 50001 to communicate with client workstations. You cannot edit this setting.



Note

Running a sweep during business hours may slow performance for each affected client workstation, though sweeps in version 2.5 and later run approximately five times faster than in previous versions.

You can start a sweep now from either the Sweep Now panel or the Client Management panel.

To run a sweep now:

From the Sweep Now panel	From the Client Management panel
<ol style="list-style-type: none"> From the Admin Console function tree, select Manage Desktop Applications > Spy Sweeper > Manage Spyware > Sweep Now. <ul style="list-style-type: none"> The Sweep Now panel displays. Select the group or client workstation where you want to run the sweep. <ul style="list-style-type: none"> If you want to run the sweep on all client workstations in the company, select the company at the top of the group tree. Click Sweep Now. <ul style="list-style-type: none"> To cancel a sweep that is running, select the group or client workstation where you want to stop the sweep and click Cancel Sweep. 	<ol style="list-style-type: none"> From the Admin Console function tree, select Admin Tasks > Client Management. <ul style="list-style-type: none"> The Client Management panel displays with a list of all existing groups on the left side. Select the group or client workstation where you want to run the sweep. <ul style="list-style-type: none"> You can select more than one client workstation by using Ctrl or Shift as you select workstations. If you want to run the sweep on all client workstations in the company, select the company at the top of the group tree. Right-click the client workstations you want and select Sweep Now. <ul style="list-style-type: none"> The sweep starts on the selected client workstations. To check the status of the sweeps, go to Manage Desktop Applications > Manage Spyware > Sweep Now and click the group that the workstations belong to.

Scheduling Sweeps

You can schedule sweeps to run on one or more specific days at a specific time.

You can schedule sweeps by group or for the whole company. Below are some things to consider when setting up scheduled sweeps:

- Avoid scheduling sweeps at the same time as anti-virus scans.

- Schedule different groups to sweep at different times to reduce load on the company server when clients report their results.
- You can schedule Windows NT, 2000, XP, and 2003 clients to sweep during off-hours as long as the system remains powered on (even with the user logged out). For Windows 98, 98SE, and ME systems, the user will need to be logged in to execute a scheduled sweep. You need to let users know when their sweep is scheduled to make sure they leave their computer in the proper state for the sweep to run.

To schedule sweeps:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Run Sweeps > Schedule Sweeps**.
 - The Schedule Sweeps panel displays.
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 settings in the Schedule Sweeps panel show the current settings for the selected group or for the company.
3. If you want end users to be able to change these settings, select the User Editable option.



Note

We do not recommend making the schedule options user editable.

4. Select the day of the week and the time you want to run the sweep.
 - The schedule uses the 24-hour clock.
5. If you want to sweep only known spyware folders at Windows startup, select the Sweep Known Spyware Folders on Startup option.
 - This option only scans known spyware folders, so the sweep runs quickly. Using this option helps to ensure that sweeps are run periodically, even if the computer is turned off when regular sweeps are scheduled.
 - If you want the startup sweep to do an in-depth memory sweep, select the Enable In Depth Memory Scan option. This option may delay Windows startup for a few minutes.
6. Click **Apply**.
 - 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 Company Settings**.

Running a Sweep in Safe Mode

If a client workstation is severely infected with spyware, adware, or other unwanted software, you can run a sweep in safe mode. Running a sweep in safe mode gives Spy Sweeper a better chance of removing spyware. You may want to do this if a client workstation finds the same spyware repeatedly.

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

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

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

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

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



Note

If the Tray Icon Setting in the Admin Console is set to Stay Invisible, you cannot access the Spy Sweeper interface at all from a client workstation. For information about changing this setting, see the Tray Icon Setting option in step 3 of “[Configuring Sweep Settings](#)” on page 54.

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 “[Unlocking Functions at a Client Workstation](#)” on page 63.
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\Enterprise\Server\SafeModeRemovalTool folder of the system where you installed Webroot Enterprise Server.
3. Restart the client workstation in safe mode.
4. Double-click the Spy Sweeper icon in the system tray.
5. Press **Ctrl+Alt+p**.
 - The Admin Password window displays.
6. Enter the password you set up in the Admin Console.
7. Click **OK**.
 - Now all functions that are not normally available to end users are available. These include Always Keep and Always Remove, as well as other functions that are not set up as user editable in the Admin Console. Refer to the Spy Sweeper online help for more information about using these functions.
8. Select **Options > Configure**.
 - The Configure panel displays.
9. Select the following options to ensure that the sweep is thorough:
 - Sweep All Folders on Selected Drives
 - Select all drives listed
 - Sweep Memory
 - Sweep Registry

10. Select **Sweep System > Sweep Now**.
 - The Sweep Now panel displays.
11. Click **Start**.
12. After the sweep finishes, restart the computer normally.
13. 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\Enterprise\Server\SafeModeRemovalTool folder of the system where you installed Webroot Enterprise Server.

Viewing and Stopping Sweeps

You can view sweeps that are running. You can also stop sweeps, regardless of how you or an end user started the sweep.



To view and stop sweeps:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Manage Spyware > Sweep Now**.
 - The Sweep Now panel displays, with information about sweeps that are running.
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 client workstation where you want to stop the sweep and click **Cancel Sweep**.

Updating Spy Sweeper

Your company server checks with the Webroot Update Server for any available server updates, client program updates, and definition updates. You configure the frequency of this check using the Webroot Server Polling Interval field, which is on the Basic section of the Settings panel (**Admin Tasks > Settings**).

If you want server component updates to install automatically as soon as they are downloaded, select the Automatically Install Server Updates option in the Basic section. If this option is not selected, you must manually install server updates by executing the setup batch file contained in each server update folder.

Updates for the client Spy Sweeper program and definitions download whenever your company server contacts the Webroot Update Server, but they do *not* install automatically. You must either manually install them or set up automatic installation rules at the company or group level.

You can set up and do the following related to the distribution of Spy Sweeper updates:

- Install updates manually (see [page 61](#))
- Install updates automatically (see [page 61](#))
- Set up notification (see [page 62](#))
- Set up updating for mobile end users (see [page 63](#))

Installing Updates Manually

You can install updates manually whenever you receive notification of an update. For information about setting up notification, see “[Setting Up Update Notification](#)” on page 62.

You may want to use manual updates for major and minor updates as well as bug fixes and new products. This gives you the chance to install these updates on a few client workstations to see how they work before deploying them to many users.



Note

Release 2.5 includes a change to the format of the spy definitions. Until you upgrade all of your client desktops to the 2.5 release, you must apply the release 2.1 definition format to older client desktops and the release 2.5 definition format to upgraded client desktops.

You can manually install updates by group or for the whole company.



Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

To install updates manually:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper > Manual Install**.
 - The Manual Install panel displays with the available updates and group tree.
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. Repeat step 2 for each update and group you want to install.
 - The next time each client workstation contacts the company server, it will install the update.

Installing Updates Automatically

You can setup Spy Sweeper to automatically install updates when your company receives them from the Webroot Update Server. The automatic settings only apply to updates received *after* you change these settings. You must manually install any updates that you received before you set up the automatic installation.

We suggest that definitions be set to automatically install. You want to keep your definitions as up to date as possible and automatically installing them assures that all users will have the most recent definitions.



Note

Release 2.5 includes a change to the format of the spy definitions. Until you upgrade all of your client desktops to the 2.5 release, you must apply the release 2.1 definition format to older client desktops and the release 2.5 definition format to upgraded client desktops.



Note

We recommend setting *only* definitions to install automatically. Install other update types manually.

You can set up automatic update installation by group or for the whole company.



Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.



To install updates automatically:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper > Auto Install**.
 - The Auto Install panel displays with the types updates and group tree.
2. Drag an update type to a group in the group tree.
 - To set the update type to automatically install on all client workstations in the company, drag the update type to the company name at the top of the group tree.
 - To remove an update type from a group, select it and click **Unassign Update**.
3. Repeat step 2 for each update type and group.
 - The next time each client workstation contacts the company server (based on the polling interval), it will install any available updates set to install automatically.

Setting Up Update Notification

You can set up e-mail notification for Spy Sweeper updates. Whenever an update arrives from the Webroot Update Server, the Admin Console can send an e-mail message to one or more people. Before you can set up notification, you must enter one or more notification recipients. For more information, see [“Setting Up Notification E-mail Addresses”](#) on page 42.



To set up notification for Spy Sweeper updates:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper > Update Notifications**.
 - The Update Notifications panel displays with a list of the types of updates and available e-mail notification recipients.
2. Drag the name of an e-mail recipient to the update tree.
 - 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**.

Setting Up Updating for Mobile End Users

If you have end users who use laptops and travel a lot, you can let them receive Spy Sweeper definition updates directly from Webroot.



Note

Be sure that the Tray Icon Setting is set to Stay Minimized (recommended) or Pop Up on Scan, or end users will not be able to display the Spy Sweeper main window.

To set up updating for mobile end users:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings**.
 - The Sweep Settings panel displays with the types updates and group tree.
2. Select the group or client workstation 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.
3. Select the Enable Manual Mobile Client Definition Updates option.
4. Click **Apply**.
 - The next time each client workstation contacts the company server, it will update Spy Sweeper and make visible the **Update Spy Definitions** button on the Spy Sweeper main window. Whenever end users have an Internet connect, they can use the button to retrieve definition updates. The button is not available for use if a user downloaded updated definitions within the last six hours.
 - If you want mobile end users to receive updated definitions automatically anytime they are connected to the Internet, select the Enable Automatic Mobile Client Definition Updates option.

Unlocking Functions at a Client Workstation


As a system administrator, you can unlock functions at a client workstation and customize the Spy Sweeper settings for an end user. Unlocking functions requires a password that you set in the Admin Console. By default, there is no password set up. You must set up the password before you can unlock functions at an end user's client workstation. For information about setting the password, see the Password option in step 3 of "[Configuring Sweep Settings](#)" on page 54.

After you set up 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 cannot access the Spy Sweeper interface at all from a client workstation. For information about changing this setting, see the Tray Icon Setting option in step 3 of "[Configuring Sweep Settings](#)" on page 54.



To unlock functions at a client workstation:

1. At a client workstation, double-click the Spy Sweeper icon in the system tray.
 - The Spy Sweeper window displays.
2. Press **Ctrl+Alt+p**.
 - The Admin Password window displays.
3. Enter the password you set up in the Admin Console.
4. Click **OK**.
 - Now all functions that are not normally available to end users are available. These include *Always Keep* and *Always Remove*, as well as other functions that are not set up as user editable in the Admin Console. Refer to the Spy Sweeper 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.



5: Monitoring Status

You can monitor the status of Webroot Enterprise in the following ways:

- Review the Webroot Enterprise Dashboard (see [page 65](#))
- View update history and installed applications (see [page 70](#))
- View client status (see [page 71](#))
- View errors (see [page 71](#))
- Generate reports (see [page 72](#))

Reviewing the Webroot Enterprise Dashboard

The Webroot Enterprise Dashboard shows you an overview of your overall system health. The main Dashboard panel lets you see at a glance whether you have any issues that require your attention in the following categories:

- Sweep Status—Shows whether client workstations have completed a full sweep within the last week. (See [page 66](#).)
- Definition Status—Shows whether client workstations have the current definitions installed. (See [page 67](#).)
- Infection Status—Shows whether threats have been found on client workstations. (See [page 67](#).)
- Top Spyware Threats—Shows whether moderate or critical threats have been found on client workstation in the last 48 hours. (See [page 68](#).)
- Server Status—Shows the last downloaded software versions, port status, and Webroot Enterprise services status. (See [page 69](#).)
- License Status—Shows the expiration status of your licenses. (See [page 69](#).)

Each category in the Dashboard can have one of the following statuses:




-  Good (green)—All items in the category are good.
-  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.
 - See the details about each category for more information about what the status icons specifically mean for the category.

Figure 5 shows the main Dashboard panel.

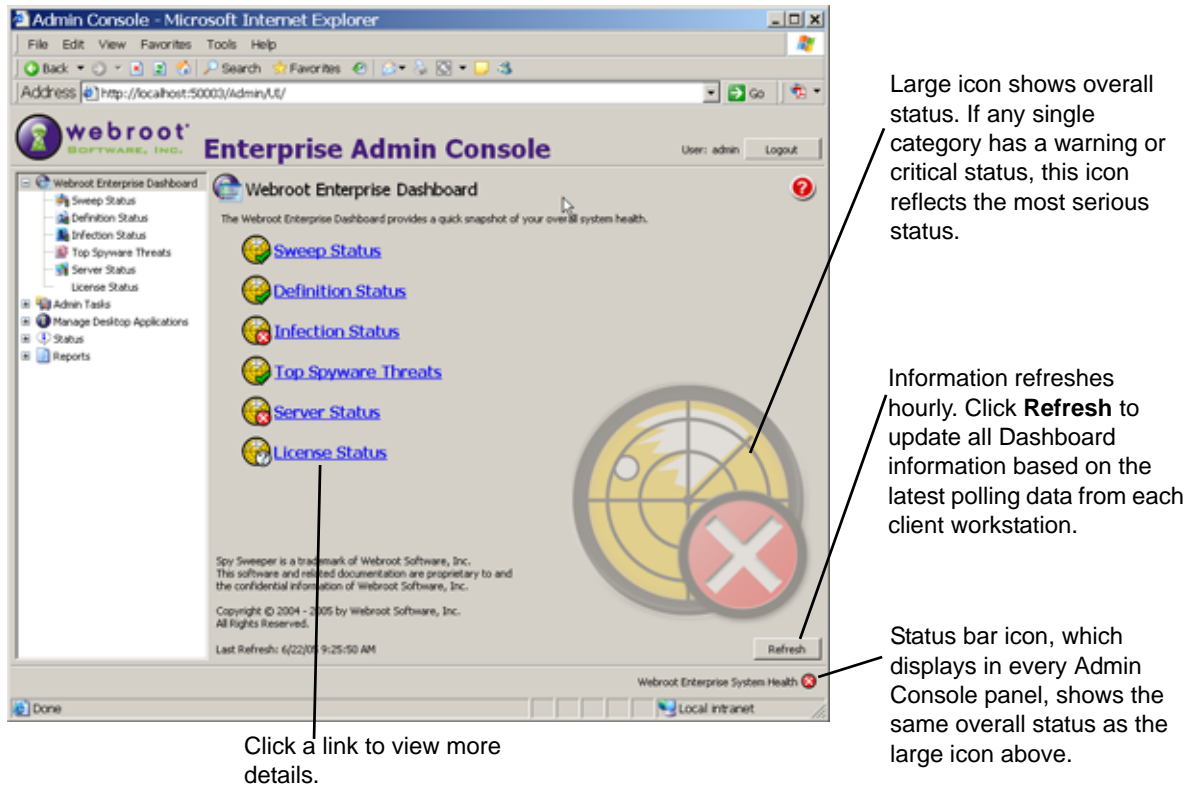




Figure 5: Webroot Enterprise Dashboard main panel

Viewing the Sweep Status

The Dashboard Sweep Status panel lists client workstations that have one of the following statuses:

-  Critical (red)—These client workstations have not completed a full sweep in the last 30 days or more.
-  Warning (yellow)—These client workstations have not completed a full sweep in the last 7 to 29 days.

A full sweep is any sweep that uses the Sweep All Folders on Selected Drives option (**Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings**).



To view the Sweep Status:

1. From the Admin Console function tree, select **Webroot Enterprise Dashboard > Sweep Status**.
 - The Sweep Status panel displays.

2. Click **Refresh** to update the status based on the latest polling data from each client workstation.
 - To export the data from either list of client workstations, click **Export All** or select the workstations you want to include and click **Export to Excel**. You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
 - If you want to change any sweep or other Admin Console settings for one or more client workstations in either list, select the workstations and click **Poll Now** to tell the client workstations to poll and get the new settings immediately.
 - If you want to sweep one or more client workstation in either list, select the workstations and click **Sweep Now**.

Viewing the Definition Status

The Dashboard Definition Status panel lists client workstations that have one of the following statuses:


-  Critical (red)—These client workstations have a definition version number that is five or more below the highest downloaded definition version.
-  Moderate risk (yellow)—These client workstations have a definition version number that is between one and four below the highest downloaded definition version.

To view the Definition Status:

1. From the Admin Console function tree, select **Webroot Enterprise Dashboard > Definition Status**.
 - The Definitions Status panel displays.
2. Click **Refresh** to update the status based on the latest polling data from each client workstation.
 - To export the data from either list of client workstations, click **Export All** or select the workstations you want to include and click **Export to Excel**. You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
 - If you want to change any sweep or other Admin Console settings for one or more client workstations in either list, select the workstations and click **Poll Now** to tell the client workstations to poll and get the new settings immediately.
 - If you want to sweep one or more client workstation in either list, select the workstations and click **Sweep Now**.

Viewing the Infection Status

Dashboard Infection Status panel lists client workstations that have one of the following statuses:

-  Critical (red)—Spy Sweeper found threats on these client workstations that totalled 5 points or more.


-  Moderate risk (yellow)—Spy Sweeper found threats on these client workstations that totalled between 1 and 4 points.

Table 9 shows the points Spy Sweeper assigns to found threats

Table 9: Points assigned to found threats

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

Client workstations remain listed on this panel until the workstation has a clean sweep and the date changes to the next calendar day.



To view the Infection Status:

1. From the Admin Console function tree, select **Webroot Enterprise Dashboard > Infection Status**.
 - The Infection Status panel displays.
2. Click **Refresh** to update the status based on the latest polling data from each client workstation.
 - To export the data from either list of client workstations, click **Export All** or select the workstations you want to include and click **Export to Excel**. You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
 - If you want to change any sweep or other Admin Console settings for one or more client workstations in either list, select the workstations and click **Poll Now** to tell the client workstations to poll and get the new settings immediately.
 - If you want to sweep one or more client workstation in either list, select the workstations and click **Sweep Now**.

Viewing the Top Spyware Threats

The Dashboard Top Spyware Threats panel lists the top spyware threats found in the last 48 hours and includes an overall threat status:



-  Critical (red)—Spy Sweeper found threats on client workstations that totalled 5 points or more.
-  Moderate risk (yellow)—Spy Sweeper found threats on client workstations that totalled between 1 and 4 points.

Table 10 shows the points Spy Sweeper assigns to found threats

Table 10: Points assigned to found threats

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

To view the Top Spyware Threats:

1. From the Admin Console function tree, select **Webroot Enterprise Dashboard > Top Spyware Threats**.
 - The Top Spyware Threats panel displays.
2. Click **Refresh** to update the status based on the latest polling data from each client workstation.
 - To see more information about a specific spyware item, select it in the list and click **Details**.
 - To export the data from either list of client workstations, click **Export All** or select the workstations you want to include and click **Export to Excel**. You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
 - If you want to change any sweep or other Admin Console settings for one or more client workstations in either list, select the workstations and click **Poll Now** to tell the client workstations to poll and get the new settings immediately.
 - If you want to sweep one or more client workstation in either list, select the workstations and click **Sweep Now**.

Viewing the Server Status



The Dashboard Server Status panel lists the latest downloaded software and definition versions, the current port settings, and the Webroot services status for the company server.

To view the Server Status:

1. From the Admin Console function tree, select **Webroot Enterprise Dashboard > Server Status**.
 - The Server Status panel displays.
2. 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 one is not, check your firewall and proxy settings.

Viewing License Status

The Dashboard License Status panel lists your license expiration date and shows your license status:

-  Critical (red)—One or more licenses has expired or will expire within 30 days.
-  Moderate risk (yellow)—One or more licenses will expire within 60 days.

To view the License Status:

1. From the Admin Console function tree, select **Webroot Enterprise Dashboard > License Status**.
 - The License Status panel displays.
2. Click **Refresh** to update the status.

Viewing Update History and Installed Versions

You can view the following information about updates and installed applications:

- Update history—List of updates downloaded from the Webroot Update Server. (See [page 70](#).)
- Installed applications—List of versions installed by client workstation. (See [page 70](#).)

Viewing Update History

You can view a history of when Webroot Enterprise Server and Spy Sweeper client updates were downloaded from the Webroot Update Server.

To view the update history:

- From the Admin Console function tree, select **Status > Update History**.
 - The Update History panel displays with a list of all of the updates downloaded to date.

Viewing Applications Installed by Workstation

You can view information about the applications installed and the version for each client workstation.

To view applications installed:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
 - The Client Management panel displays with a list of all existing groups on the left side.
 - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Sort by the Version column.

Viewing Client Status

You can view a list of each client workstation that has the Spy Sweeper client installed on it and when it last contacted the company server. The information also includes when Spy Sweeper last ran a sweep on the client workstation.



To view the client status:

- From the Admin Console function tree, select **Admin Tasks > Client Management**.
- The Client Management panel displays with a list when each client workstation last contacted the company server.

Viewing Errors

You can view any errors that an application generates on a client workstation. You can then report the error to Webroot.

You should review the error list periodically to determine if any applications have caused errors.



To view errors:

1. From the Admin Console function tree, select **Status > Errors**.
 - The Errors panel displays with a list errors.
2. Contact Webroot Enterprise Support for assistance with the resolving the error.

Generating Reports

You can generate the following major types of reports:

- Charts—Lets you create charts that summarize threats.
- Tabular data by group and workstation—Lets you create tables by group and workstation that show threats, threat history, and version history.

Generating Charts

You can generate the following types of charts:

- Spyware Trend by Type
- Top 5 Spies
- Infection Status

To generate charts:

1. From the Admin Console function tree, select **Reports** and one of the chart types.
2. Select the Year and Month you want.
3. Select the Chart Type.
 - The chart displays in the panel.

Generating Tabular by Group and Workstation

You can generate the following types of tabular reports:

- Top Threats
- Spyware Detail
- Infection Summary
- Spyware History
- Version History
- Error

To generate tabular reports:

1. From the Admin Console function tree, select **Reports** and one of the tabular reports.
2. From the group tree, select the group you want.
 - If you want the report to include the whole company, select the company name at the top of the group tree.
3. Select the From and Through date range you want the report to include.
4. Select the Watermark you want to use.
5. Click **Generate** to view the report.

- To save the report to any of several file formats, click **Print**, then select the Print to File option, Type, and Where to save the file.



A: Webroot Enterprise Port Requirements

A number of communication ports must be opened for proper communications between all network components within the Webroot Enterprise architecture. [Table 11](#) describes the port requirements for a Webroot Enterprise installation.

The aim of this information is not to document how to open all of these ports for a particular firewall, but rather to describe what ports must be open and on what systems within your Webroot Enterprise architecture.

Table 11: Webroot Enterprise communications ports

Port	Component	Description	Installation/network access requirement
443	WebrootUpdateService.exe Required on Distributor Servers	<ul style="list-style-type: none"> • HTTP protocol over SSL. • Communicates periodically with Webroot to retrieve updates and move them to distributor servers. • Runs as a system service on the server. 	<ul style="list-style-type: none"> • Installed when you set up distributor servers. • Requires local network access.
50003	<ul style="list-style-type: none"> • WebrootUpdateDistributor.exe; required on Distributor Servers. • WebrootAdminConsole.exe; required on company server 	<ul style="list-style-type: none"> • HTTP. • Distributor service—Responds to CommAgent on client workstations to distribute updates • WebrootAdminConsole.exe—Provides the browser-based Admin Console interface. • Both run as system services on the server. 	<ul style="list-style-type: none"> • Distributor service—Installed when you set up distributor servers. • WebrootAdminConsole.exe—Installed when you install Webroot Enterprise Server. • Requires local network access.
50000	WebrootClientService.exe Required on company server and client workstations	Controls the communication between the client workstations and your company server.	<ul style="list-style-type: none"> • Installed during the installation of Webroot Enterprise Server. • Requires local network access.
50001	Sweep Now function Required on company server and client workstations	Function initiated from the Admin Console that initiates a Spy Sweeper sweep of the selected client workstations.	<ul style="list-style-type: none"> • Not an installed component, but a function called from within the Admin Console. • Requires local network access.

Table 11: Webroot Enterprise communications ports (Continued)

Port	Component	Description	Installation/network access requirement
50002	Poll Now function Required on company server and client workstations	Function initiated from the Admin Console that initiates a poll of the selected client workstations to update their heartbeat and status to the server.	<ul style="list-style-type: none"> • Not an installed component, but a function called from within the Admin Console. • Requires local network access.
50023	<ul style="list-style-type: none"> • WebrootAdminConsole.exe if using SSL to access the Admin Console. 	Provides the SSL access to the browser-based Admin Console interface.	<ul style="list-style-type: none"> • Installed when you install Webroot Enterprise Server. • Requires local network access.



B: Migrating an Existing Installation from DBISAM to SQL Server

If you have an existing Webroot Enterprise installation and need to migrate the database from DBISAM to SQL Server, you can do so. The migration tool only changes a DBISAM database to a SQL Server database for the same version of Webroot Enterprise.



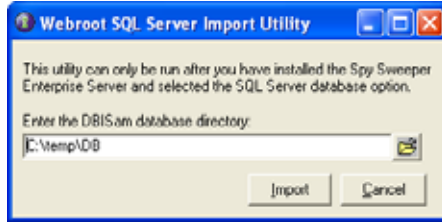
Note

You only need to migrate to SQL Server if you expect to install more than 10,000 clients.

To migrate from DBISAM to SQL Server:

1. From your Webroot Enterprise company server, start the Admin Console and select **Help > About** to be sure that your installation has updated to version 2.0
 - You can only migrate to SQL Server if you have version 2.0 or later installed.
2. Stop the following Webroot Enterprise services:
 - Webroot Client Service
 - Webroot Update Service
3. Copy the DB folder to a temporary location.
 - If you installed the Webroot Enterprise Server to the default location, the DB folder is in the following location:
 - : C:\Program Files\Webroot\Enterprise\Server\
4. Uninstall the following Webroot Enterprise programs, in this order, using Add/Remove Programs:
 - Webroot Spy Sweeper Enterprise Client, if installed on the company server
 - Webroot Spy Sweeper Enterprise Distribution Server
 - Webroot Enterprise Server
5. Set up the SQL database.
 - For more information, see “[Setting up a SQL Server Database](#)” on page 11.
6. Install a new Webroot Enterprise Server, making sure you select the SQL Server 2000 option during the installation.
 - The full installation file for Webroot Enterprise Server 2.1 is available from the Supplemental Downloads page at: <http://www.webroot.com/entcenter>.
 - For more information, see “[Installing Webroot Enterprise Server on Your Company Server](#)” on page 13.

7. Start the import utility to bring the DBISAM database files into the SQL Server database.



- If you installed the Webroot Enterprise Server to the default location, the import utility is in the following location:
 - C:\Program Files\Webroot\Enterprise\Server\SSEImport.exe
- Depending on the size of the database being imported, the process can take from a few seconds to several minutes.
- On completion of the import, a confirmation message displays.



C: Automated Group Mapping and Assignment Utility

This command line utility reads a text file as input. The text file contains the rules for assigning client workstations to groups.

Assumptions:

- Group mapping is based on Active Directory rules, IP address, subnet or workstation names.
- Input file must be provided that corresponds to Webroot Enterprise API as outlined in this document.

There are two executables for this utility.

- GroupAssign.exe—The main utility that parses your rules file and updates your Admin Console database.
- GroupAssignPass.exe—This utility uses Blowfish encryption so that you can pass in a secure, encrypted password for your Active Directory server into your rules file.

Rules File Format

The rules file must conform to the following structure and rules:

- One rule per line.
- Leading and trailing spaces are ignored.
- By default, the parameters are separated by the comma (,) character. However as commas are allowed in Active Directory rules, if you are using Active Directory rules, use semicolons (;).
- The rules file is processed from the bottom up, therefore the top-most record takes precedence over all other rules.
- Wildcard is the asterisk (*).

Rules File Syntax

GROUPNAME, {IP|NAME|ADS}, Value

Parameter	Description
GROUPNAME	This is either a group that exists in the database or a group you want to create.
IP, NAME, or ADS	Indicates whether an IP/subnet, workstation name, or Active Directory rule is used as the parameter.
Value	Value passed as in the examples below.

IP and Name Examples

Syntax	Description
GROUPNAME, IP, 10.10.10.10	For a single IP address
GROUPNAME, IP, IPLOW-IPHIGH	For a range of IPs 10.70.96.1 - 10.70.99.254
GROUPNAME, IP, 10.*	All workstations with an IP starting with 10.
GROUPNAME, IP, 10.10.*	All workstations with an IP starting with 10.10.
GROUPNAME, IP, 10.10.10.*	All workstations with an IP starting with 10.10.10.
GROUPNAME, IP, 10.10.9*	All workstations with an IP starting with 10.10.9
GROUPNAME, IP, IP/bits	bits = CIDR bits for Classless Inter Domain Routing
GROUPNAME, IP, IP/netmask	netmask = netmask in the form 255.255.252.0
GROUPNAME, NAME, workstationname	workstationname = single workstation name
GROUPNAME, NAME, mktg*	All workstations with names beginning with mktg

Active Directory Rule Format

Supported platforms for Active Directory rules are:

- Windows 2000 Active Directory SP 4 or later
- Windows 2003
- Windows SBS

GROUPNAME;ADS;BIND_DN;User;Pass;Filter;\$RULENAME;RULEPARAM1;RULEPARAM(n)

Parameter	Description
GROUPNAME or \$RULE=	This is the name of the group that will be created for workstations matching this rule. There are two valid formats for this parameter: <ul style="list-style-type: none"> • GROUPNAME—Simply the name of the group that you want to add workstations to. • \$RULE—The literal string \$RULE which denotes that the group name is created as the result of an Active Directory rule that is specified by \$RULENAME (below). This is the name of an organizational unit within Active Directory.
ADS=	Indicates that this is an Active Directory rule.
Bind_DN=	The Lightweight Directory Access Protocol (LDAP) URL defining the base DN to bind the filter search to as defined in RFC2255.
User=	The name of the user account to access the ADS.
Pass=	The encrypted password for the user, as plain text, created by GroupAssignmentPass.exe. The format is: OBF: 12A79DF36EE.
Filter=	The LDAP filter to filter workstations that this group might be a member of, as defined in RFC2254.

Parameter	Description
\$RULENAME=	The name of the rule to be applied. Supported \$RULENAMES are: TOP_OU or BOTTOM_OU.
\$RULEPARAM1=	The parameter to pass into the rule that is provided by \$RULENAME. Supported \$RULEPARAM1 for TOP_OU or BOTTOM_OU. The CN of the top or bottom DN to use as group automatic name generation (for example, OU, L, G).

Active Directory Rule Example

```
[Groupname or $RULE];ADS;LDAP://servername/DC=EnterpriseLab,DC=local;
elab\joeshmoe;OBF:12A79DF36EED12F; (&(objectclass=computer)(CN=FP*));BOTT
OM_OU;DC
```

Processing this rule:

1. When the tool is run and this rule is encountered, this rule will be applied to each workstation in the Webroot Spy Sweeper Enterprise (SSE) database that meet the rule criteria.
2. The workstation is looked up by hostname of the ADS and the Computer object returned (using user,pass).
3. The DN is inspected for the highest (Top) or lowest (Bottom) OU that is found specified by the rule.
4. This DN is converted in to an SSE “safe” group name (contains only characters allowed in group names).
5. This group is created if it does not exist but only if the -G switch is set.
6. If the group does not exist and the -G switch is not set, the software reports this condition and continues processing the next rule.
7. The workstation record is updated to reflect this new group, if it is not already set properly.
8. A log of all actions is created.

Parameter Delimiter

You can specify the parameter delimiter on any single line in the rules file to specify the delimiter for the next rule or rules processed. For Active Directory rules, you should use the; character, as commas are valid characters in LDAP filters. You can use any delimiter character that you choose by specifying the variable SEPCHAR as shown below:

Example delimiters:

```
SEPCHAR= ,
SEPCHAR= |
```

If you are combining IP rules and Active Directory rules in a single file, you can use multiple delimiters within the same rules file by specifying the character to use before each rule:

```
$RULE | ...
SEPCHAR= |
$RULE ; ...
SEPCHAR= ;
GROUPNAME , ...
```

SEPCHAR= ,

Processing the Rules File

Rules at the top of the input file take precedence. So if a client workstation matched two rules that were for different groups, the workstation would be placed in the group from the first rule listed. Rules are followed one by one for every workstation in the workstations table in the SSE database. When a match is found, the workstation is moved from its current group to the specified group in the SSE database.

Once the input file is processed, you will see a new command prompt.

If any rule cannot be executed, a message similar to the following displays:

```
Executing rule: "85 court st, NAME,TN6* " ...  
Error: Invalid Rule "85 court st, NAME,TN6*"
```

Each time the utility is run, you can specify a new log file name (that is, with time/date stamp.)

Running GroupAssignPass.exe

This utility uses standard Blowfish encryption to generate an encrypted version of your Active Directory server password. This lets you use the password in your rules file and run the GroupAssign utility from a batch process.

Navigate to the folder where the executable is saved and type the following from a command line (typically this location should be C:\Program Files\Webroot\Enterprise\Server\GroupAssignTool):

```
GroupAssignPass.exe <password to encrypt>
```

Running GroupAssign.exe

Navigate to the folder where the executable is saved and type one of the following options from a command line (typically this location should be C:\Program Files\Webroot\Enterprise\Server\GroupAssignTool):

```
GroupAssign.exe <RulesFilename> [-V] [-P] [-G]  
GroupAssign.exe <RulesFilename> [<LogFilename>]  
GroupAssign.exe -R <RulesFilename> [-L <LogFilename>]  
GroupAssign.exe [-L <LogFilename>] -R <RulesFilename>
```

[]—indicate optional switches which are:

- -V—Operate in verbose mode.
- -P—Operate in preview mode.
- -G—Create groups in the SSE database that are specified in your rules file if those groups do not already exist in your database.
- -R—Specify the rules file to read as input.
- -L—Specify the log file to be created.

If the <LogFilename> parameter is missing, the log will be written to the screen.

If <RulesFilename> parameter is missing, the default is set to GroupAssignmentRules.txt in the same folder as GroupAssign.exe.

If a filename contains spaces it must be enclosed in double quotes.

If a command line option for a different log file name and location is specified, then the log file should be created there. If the location is invalid, or the file cannot be created for any other reason, then an error message will display that states:

"Log file cannot be created. Please check the path specified and ensure that you have write access. Optionally you may run without specifying a log file in which case errors will be displayed to standard output."

If no input file is specified, or if the input file cannot be found or read for any reason, then the following error message will display: "Error opening input file. Please check the path specified and ensure that the file exists."

If the input file resides in the folder of the executable GroupAssign.exe, then using the filename (input.txt) will work. However, you must use the full path name or a relative path name at the command line if the input file is located in some other location than the executable.



Note

If you delete a group to which you have assigned workstations using the Admin Console, the workstations will display in your default group at the top of the group tree when they poll back into the Admin Console.



D: Data Extraction and Reporting Utilities

This set of command line utilities allows you to perform a variety of data extraction and reporting tasks against your Webroot Enterprise database. These utilities let you roll up data and generate reports from multiple installations of the Admin Console.

These utilities work with either your DBISAM or SQL Server installations. As these are command line utilities, you can run them on an ad-hoc basis or at specific pre-defined intervals as batch processes that you can set up within your own environment.

There are four utilities included in this release:

- SSE Reaper (SSEReaper.exe)
- SSE Coalesce (SSECoalesce.exe)
- SSE Warehouse Reaper (SSEWarehouseReaper.exe)
- SSE Reporter (SSEReporter.exe)

Details for each utility are in the following sections.

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

SSE Reaper Utility

The SSE Reaper utility is a data extraction utility that extracts data from your Webroot Spy Sweeper Enterprise production database and produces a flat text file (pipe separated) that contains the following data points.

Data point	Description
DataDomain	Specified in the SSEReaper.ini settings file, this is a unique tag that designate the hierarchical location of the data in a Spy Sweeper implementation that has multiple Admin Console installations. This field is also used for creating the output file name of the SSE Reaper utility.
Company	Specified in the SSEReaper.ini settings file, this is a unique tag 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 Spy Sweeper Client running on a particular infected workstation.
DefVersion	The current definition version of a particular infected workstation.

Data point	Description
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.
SpyCategory	The category of spy that was found. Options are: Trojan, System Monitor, Adware, and Other.
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=	Specify the 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\Enterprise\Reporting\SSEReaper.log. Default setting specifies no log file.
OutputDir=	Specify the location (folder) of the output file that will be created.
DataDomain=	This is a unique tag that will designate the hierarchical location of the data in a Spy Sweeper 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 prior day and is meant to be run 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\Enterprise\Server\ReportingTools\)) and type 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 MM/DD/YYYY
Extracts all records on the given date.
```

SSEReaper.exe MM/DD/YYYY MM/DD/YYYY

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 any of three different ways, based on which parameters were used to run the program. The three file names are described below.

Output file name	Description
DataDomain_YYYYDDMM=	<p>This file name format is created when SSEReaper is run with no parameters or when a single data parameter is passed in.</p> <p>DataDomain is taken from the value specified in the SSEReaper.ini file.</p> <p>YYYYDDMM is the previous day's date from when the program is run.</p>
DataDomain_upto_YYYYDDMM=	<p>This file name format is created when SSEReaper is run with the ALL parameter to extract all data.</p> <p>DataDomain is taken from the value specified in the SSEReaper.ini file.</p> <p>_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.</p>
DataDomain_YYYYDDMM_to_YYYYDDMM=	<p>This file name format is created when SSEReaper is run with the date range parameters.</p> <p>DataDomain is taken from the value specified in the SSEReaper.ini file.</p> <p>_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.</p> <p>YYYYDDMM values are the starting and ending dates specified as parameters.</p>

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 as described in the next section.

SSECoalesce.ini Settings

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

```
[Settings]
DataDomain=
OutputToSQLServer=0
OutputToDBISAMDatabase=1
[DBISAM Settings]
DBPath=C:\Program Files\Webroot\Enterprise\Server\ReportingTools\DB
[SQL Server Settings]
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.
OutputToSQLServer=	Flag to use SQL Server database. 1=Turn SQL Server output on. 0=Turn SQL Server output off. * If you use SQL Server, then the value for DBISAM should be set to 0.
OutputToDBISAMDatabase=	Flag to use DBISAM database table. 1=Turn DBISAM output on. 0=Turn DBISAM output off. * If you use DBISAM, then the value for SQL Server should be set to 0.
DBPath=	DBISAM setting only. By default it points to C:\Program Files\Webroot\Enterprise\Server\ReportingTools\DB.
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=	Set to the SQL Server "SQL database name."
Data Source=	Set to the 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. This is not an issue if you are using DBISAM as your database, as we ship the SpyDetection table with this utility.

```
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(10),  
"SpyCategory" VARCHAR(20),  
"SpyName" VARCHAR(50),  
"Traces" INTEGER,  
"ActionTaken" CHAR(1),  
);
```

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\Enterprise\Server\ReportingTools\) and type 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|mnrst|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|mnrst|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|mnrst|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 (either DBISAM or MS SQL Server) and what folder to output the exported records file to.

SSEWarehouseReaper.ini Settings

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

```
[Settings]
UseSQLServer=0
UseDBISAMDatabase=1
OutputDir= C:\Program Files\Webroot\Enterprise\Server\ReportingTools
[DBISAM Settings]
DBISAMInputDir= C:\Program
Files\Webroot\Enterprise\Server\ReportingTools\DB
[SQL Server Settings]
Provider=
Password=
Persist Security Info=1
User ID=
Initial Catalog=
Data Source=
```

SSEWarehouseReaper.ini setting	Description
UseSQLServer=	Flag to use SQL Server database. 1=Turn SQL Server output on. 0=Turn SQL Server output off. * If you use SQL Server, then the value for DBISAM should be set to 0.
UseDBISAMDatabase=	Flag to use DBISAM database table. 1=Turn DBISAM output on. 0=Turn DBISAM output off. * If you use DBISAM, then the value for SQL Server should be set to 0.
OutputDir=	Specify the location of the output file that will be created.
DBISAMInputDir=	DBISAM setting only. The standard location on your Admin Console server is: C:\Program Files\Webroot\Enterprise\Server\ReportingTools\DB.
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=	Set to the SQL Server "SQL database name."
Data Source=	Set to the 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\Enterprise\Server\ReportingTools\) and type 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). The program supports both SQL Server and DBISAM databases.

SSEReporter.ini Settings

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

```
[Settings]
UseSQLServer=0
UseDBISAMDatabase=1
[DBISAM Settings]
DBPath= C:\Program Files\Webroot\Enterprise\Server\ReportingTools\DB
[SQL Server Settings]
Provider=
Password=
Persist Security Info=1
User ID=
Initial Catalog=
Data Source=
```

SSEReporter.ini setting	Description
UseSQLServer=	Flag to use SQL Server database. 1=Turn SQL Server output on. 0=Turn SQL Server output off. * If you use SQL Server, then the value for DBISAM should be set to 0.
UseDBISAMDatabase=	Flag to use DBISAM database table. 1=Turn DBISAM output on. 0=Turn DBISAM output off. * If you use DBISAM, then the value for SQL Server should be set to 0.
DBPath=	DBISAM Setting only. The standard location on your Admin Console server is: C:\Program Files\Webroot\Enterprise\Server\ReportingTools\DB
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=	Set to the SQL Server “SQL database name.”
Data Source=	Set to the 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: <ul style="list-style-type: none"> 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 mm/dd/yyyy).
-e <enddate>	Ending date for report (format mm/dd/yyyy).
-o <outputoption>	Output type. Options are: text, printer, pdf.

Parameter	Description
-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 2/20/2004 -e 5/05/2005 -m "%Top%" -o text -f "C:\Results Dir\output.txt"
```

```
SSEReporter.exe -r summary -s 2/20/2004 -e 5/05/2005 -m "%Top%" -o text -f C:\tempoutput.txt
```

```
SSEReporter.exe -r historyspy -s 2/20/2004 -e 5/05/2005 -m "%Topdatafield,middatafield%" -w "WW-6042FHGZN437" -o printer -b classified
```

Sample Reports

Summary Report



Infected Machines Summary
12/30/1899 through 5/18/2005
Domain Filter: %

<u>Domain</u>	<u>Group</u>	<u>Workstation</u>	<u>Tot Spies</u>	<u>Adware</u>	<u>SMon</u>	<u>Trojans</u>	<u>Other</u>	<u>1st Detect</u>	<u>Lst Detect</u>
\Boulder.AC	Boulder	\Workstation 1	5	2	1	1	1	5/5/2005	5/5/2005
\Boulder.AC	Boulder	\Workstation 2	5	2	1	1	1	5/5/2005	5/5/2005
\Boulder.AC	Boulder	\Workstation 3	5	2	1	1	1	5/5/2005	5/5/2005
\Boulder.AC	Boulder	\Workstation 4	5	2	1	1	1	5/5/2005	5/5/2005
\Boulder.AC	Boulder	\Workstation 5	5	2	1	1	1	5/5/2005	5/5/2005
\London.AC	London	\Workstation 6	5	2	1	1	1	5/5/2005	5/5/2005
\London.AC	London	\Workstation 7	5	2	1	1	1	5/5/2005	5/5/2005
\London.AC	London	\Workstation 8	5	2	1	1	1	5/5/2005	5/5/2005
\London.AC	London	\Workstation 9	5	2	1	1	1	5/5/2005	5/5/2005
\London.AC	London	\Workstation 10	5	2	1	1	1	5/5/2005	5/5/2005
\Paris.AC	Paris	\Workstation 11	5	2	1	1	1	5/5/2005	5/5/2005
\Paris.AC	Paris	\Workstation 12	5	2	1	1	1	5/5/2005	5/5/2005
\Paris.AC	Paris	\Workstation 13	5	2	1	1	1	5/5/2005	5/5/2005
\Paris.AC	Paris	\Workstation 14	5	2	1	1	1	5/5/2005	5/5/2005
\Paris.AC	Paris	\Workstation 15	5	2	1	1	1	5/5/2005	5/5/2005
\Tokyo.AC	Tokyo	\Workstation 16	5	2	1	1	1	5/5/2005	5/5/2005
\Tokyo.AC	Tokyo	\Workstation 17	5	2	1	1	1	5/5/2005	5/5/2005
\Tokyo.AC	Tokyo	\Workstation 18	5	2	1	1	1	5/5/2005	5/5/2005
\Tokyo.AC	Tokyo	\Workstation 19	5	2	1	1	1	5/5/2005	5/5/2005
\Tokyo.AC	Tokyo	\Workstation 20	5	2	1	1	1	5/5/2005	5/5/2005

Detail Report

<u>SpyName</u>	<u>SpyID</u>	<u>SpyCategory</u>	<u>Traces</u>	<u>Sweep Date</u>
SaveNow - WhenUSave	sos9s	Adware	218	5/5/2005
Some Keylogger	023ht	System Monitor	4	5/5/2005
Troy Trojan	980ka	Trojans	3	5/5/2005
Something Else	893hh	Other	456	5/5/2005
Gain	99sh2	Adware	977	5/5/2005

Company:	Webroot Software Inc.	Domain:	\Boulder AC
Group:	Boulder	IP:	127.0.0.2
Workstation:	Workstation 2	MAC:	00-00-00-00-00-02

<u>SpyName</u>	<u>SpyID</u>	<u>SpyCategory</u>	<u>Traces</u>	<u>Sweep Date</u>
SaveNow - WhenUSave	sos9s	Adware	218	5/5/2005
Some Keylogger	sos9s	System Monitor	4	5/5/2005
Troy Trojan	sos9s	Trojans	3	5/5/2005
Something Else	sos9s	Other	456	5/5/2005
Gain	sos9s	Adware	977	5/5/2005

Company:	Webroot Software Inc.	Domain:	\Boulder AC
Group:	Boulder	IP:	127.0.0.3
Workstation:	Workstation 3	MAC:	00-00-00-00-00-03

<u>SpyName</u>	<u>SpyID</u>	<u>SpyCategory</u>	<u>Traces</u>	<u>Sweep Date</u>
SaveNow - WhenUSave	sos9s	Adware	218	5/5/2005
Some Keylogger	sos9s	System Monitor	4	5/5/2005
Troy Trojan	sos9s	Trojans	3	5/5/2005
Something Else	sos9s	Other	456	5/5/2005
Gain	sos9s	Adware	977	5/5/2005

Spy History Report

<u>Spy Name</u>	<u>Spy Category</u>	<u>First Detect</u>	<u>Last Detect</u>	<u>Detections</u>
SaveNow - WhenUSave	Adware	5/5/2005	5/5/2005	1
Some Keylogger	System Monitor	5/5/2005	5/5/2005	1
Troy Trojan	Trojans	5/5/2005	5/5/2005	1
Something Else	Other	5/5/2005	5/5/2005	1
Gain	Adware	5/5/2005	5/5/2005	1

SECRET

Workstation Version History

<u>Spy Sweeper Version</u>	<u>Definitions Version</u>	<u>First Sweep</u>	<u>Last Sweep</u>	<u>Count</u>
2.1.0.3835	0.0.0.469	5/5/2005	5/5/2005	5

UNKNOWN

Top Threats



Threats Found Detail

12/30/1899 through 5/18/2005

Domain Filter: %

<u>Spy Name</u>	<u>First Sweep</u>	<u>Last Sweep</u>	<u>Detections</u>	<u>Quarantined</u>	<u>Logged</u>	<u>Deleted</u>
SaveNow - WhenUSave	5/5/2005	5/5/2005	20	84		
Some Keylogger	5/5/2005	5/5/2005	16	84		
Troy Trojan	5/5/2005	5/5/2005	16	84		
Something Else	5/5/2005	5/5/2005	16	84		
Gain	5/5/2005	5/5/2005	16	84		
Some Keylogger	5/5/2005	5/5/2005	4	4		
Troy Trojan	5/5/2005	5/5/2005	4	4		
Something Else	5/5/2005	5/5/2005	4	4		
Gain	5/5/2005	5/5/2005	4	4		



Index

A

- Add Group button 44
- Add User button 47
- Additional Blocked Applications list 53
- Admin Console
 - configuring server settings 37
 - defined 4
 - installing 4
 - managing users of 47
 - understanding 3
 - understanding the main window 29
 - updating 38
 - viewing user audit logs 47
- Advanced section 39
- alerts, setting up for sweeps 56
- All Folders on Selected Drives option 55
- Allow Users to Cancel Sweeps option 55
- Alternate Data Stream Shield (ADS) option 52
- Always Keep list 50
- applications
 - viewing errors from client workstations 71
 - viewing installed by group 70
 - viewing update history of 70
- assigning distributor servers 33, 34
- audit logs for Admin Console users 47
- Automatically Install Server Updates 39

B

- Basic section 38
- Blocked Websites Shield On option 53

C

- canceling sweeps 60
- changing
 - the port for distributors servers 35
- Check for Updates button 38
- client components
 - example logon script 32
 - installation options 31
- client components, installing 28, 29, 30
- Client Password field 56
- Client Service
 - defined 4
 - installing 4
- Client Service IP field 14, 19
- Client Service Port field 13, 19
- client workstations

- adding to groups 44
- creating reports about 45
- deleting 46
- example logon script 32
- managing 43
- options for setting up 31
- polling now 46
- removing from groups 44
- setting up 28, 29, 30
- uninstalling Spy Sweeper from 33
- unlocking Spy Sweeper functions at 63
- viewing application errors from 71

- Close Internet Explorer after Sweeps option 55
- Close Windows Explorer after Sweeps option 55
- CommAgent Polling Interval field 19
- CommAgents
 - defined 4
 - installation options 31
 - installing 4, 28, 29, 30
 - viewing heartbeat status of 71
 - viewing update history of 70
- Common Ad Websites list 53
- Company Name field 17, 38
- company server status, monitoring 69
- configuration examples 6
- configuring sweeps 54
- Consolidate Alerts field 39
- continuous monitoring, setting up 51
- conventions, typographic 1
- creating
 - reports about client workstations 45
- customer support 2

D

- Dashboard
 - Definition Status panel 67
 - icons defined 65
 - Infection Status panel 67
 - License Status panel 69
 - Refresh button 65
 - reviewing 65
 - Server Status panel 69
 - status bar 65
 - Sweep Status panel 66
 - Top Spyware Threats panel 68
- database
 - migrating from DBISAM to SQL 77

- setting up SQL 11
- Database section 41
- database, recommendations about selecting type 5
- DBISam option 21
- DBISAM, migrating from 77
- Definition Status panel
 - defined 67
 - icons in 67
- definition status, monitoring 67
- definitions
 - updating 60
 - updating automatically 61
 - updating for mobile end users 63
 - updating manually 61
- Delete Group button 45
- Delete Workstations button 45, 47
- deleting
 - client workstations 46
- Deploy Client button 30
- distributor servers
 - assigning 33, 34
 - changing the default port for 35
 - how they work 6
 - installing 33
 - recommendations about number to use 5
 - removing 34
 - unassigning 34
 - updating process 8
- distributors
 - defined 5
 - installing 5
- Download Folder field 13, 38

E

- E-mail Host field 13, 19
- E-mail Recipient field 40
- E-mail section 39
- Enable Automatic Mobile Client Definition Updates 55
- Enable Automatic Mobile Client Definition Updates option 63
- Enable In Depth Memory Scan option 58
- Enable Manual Mobile Client Definition Updates option 56, 63
- Enter/Edit Application Not to Block field 53
- Enter/Edit Application to Block field 53
- Enter/Edit Website to Block field 53
- errors
 - viewing for applications on client workstations 71
- example logon script 32
- Export Workstations button 45
- exporting reports about client workstations 45

F

- file, saving reports to 72

- firewalls
 - configuring ports required for Webroot Enterprise 75
- From Address field 13, 19, 39

G

- generating reports 72
- groups
 - deleting 44
 - renaming 44
 - setting up 44
 - viewing applications installed 70

H

- handling
 - spyware 49
 - spyware automatically 49
 - spyware automatically by type 49
- heartbeat status, viewing for CommAgents 71
- Hosts File Shield On options 52

I

- icons
 - defined for the main Dashboard panel 65
- IE Favorites Shield option 52
- IE Hijack Shield On option 52
- Infection Status panel
 - defined 67
 - icons in 67
- infection status, monitoring 67
- Initial Interval Max field 39
- Initial Interval Min field 39
- installing
 - client components 28, 29, 30
 - CommAgents 28, 29, 30
 - distributor servers 33
 - example logon script 32
 - key steps for 8
 - options for client components 31
 - options for CommAgents 31
 - options for Spy Sweeper 31
 - Spy Sweeper 28, 29, 30
 - Webroot Enterprise 11
 - Webroot Enterprise Server 13
- IP/Host Name field 40

K

- Keep Hosts File Read-only option 52
- keeping spyware 50
- Key Code field 13, 17, 38

L

- Leave the Messenger Service Running when Messenger Shield Is Turned Off 52
- License Status panel

- defined 69
- icons in 69
- license status, monitoring 69
- logins, managing for the Admin Console 47
- logon script example 32
- Logs Expire After field 40
- logs, viewing for Admin Console users 47

M

- managing
 - Admin Console users 47
 - client workstations 43
 - Spy Sweeper 49
 - spyware 49
 - spyware automatically 49
 - spyware automatically by type 49
- Maximum Interval field 39
- Memory option 55
- Memory Shield On option 51
- Message Timeout field 19, 39
- messages for notification, setting up 42
- Messenger Service Startup Type option 52
- Messenger Shield On option 51
- migrating
 - from DBISAM to SQL 77
- monitoring
 - definition status 67
 - infection status 67
 - licence status 69
 - server status 69
 - status 65
 - sweep status 66
 - top spyware threats 68

N

- Network section 40
- News, viewing 37

notification

- setting up 42
- setting up e-mail addresses for 42
- setting up for errors 43
- setting up for Spy Sweeper updates 62
- setting up messages for 42

O

- Only Known Spyware Folders option 55

P

- Password field 39
- Password for SMTP field 20
- passwords
 - managing for the Admin Console 47
- Path to Download Folder field 17
- planning for Webroot Enterprise deployment 5

- Poll Now button 46
- polling
 - client workstations now 46
 - recommendations about setting frequency 5
- Polling Intervals
 - Client field 38
 - Webroot Server field 38
- Pop up on Scan option 20, 55
- Port field 40, 41

ports

- changing for distributor servers 35
- Webroot Enterprise requirements for 75
- Protected Home Page field 52
- Proxy Password field 14, 18
- Proxy Server field 14, 18
- Proxy User Name field 14, 18

Q

- quarantine period, setting up 49
- quarantined spyware, what happens during uninstallation 33

R

- Refresh button 46
- Registry option 55
- removing distributor servers 34
- reports
 - creating related to client workstations 45
 - saving to a file 72
- reports, generating 72
- restoring spyware 50
- running
 - a sweep now 57
 - sweeps 56
 - sweeps in safe mode 58
 - sweeps on a schedule 57

S

- safe mode, running sweeps in 58
- saving reports to a file 72
- scheduling sweeps 57
- Send Test E-mail button 39
- Server field 39
- server settings, configuring in the Admin Console 37
- Server Status panel
 - defined 69
 - icons in 69
- server status, monitoring 69
- Server Type 41
- setting
 - a SQL database 11
- setting sweep settings 54
- setting up
 - client workstations 28, 29, 30

- continuous monitoring 51
 - error notification 43
 - groups 44
 - key steps for 8
 - notification 42
 - notification e-mail addresses 42
 - notification messages 42
 - options for client workstations 31
 - sweep alerts 56
 - shields, setting up 51
 - Smart Shields, setting up 51
 - Spy Installation Shield On option 53
 - Spy Sweeper
 - defined 5
 - example logon script 32
 - installation options 31
 - installing 5, 28, 29, 30
 - managing 49
 - setting up notification about updates 62
 - unlocking functions at a client workstation 63
 - updating 60
 - updating automatically 61
 - updating definitions for mobile end users 63
 - updating manually 61
 - viewing date of last sweep 71
 - Spy Sweeper Engine
 - defined 5
 - installing 5
 - spyware
 - handling automatically by type 49
 - managing 49
 - managing automatically 49
 - restoring 50
 - setting up to always keep 50
 - spyware, monitoring 68
 - SQL
 - migrating to 77
 - setting up database 11
 - SQL Server 2000 option 21
 - SQL Server Database Name field 21
 - Startup Shield On option 53
 - Startup Shield Whitelist 53
 - status
 - monitoring 65
 - Stay Invisible option 21, 55
 - Stay Minimized option 21, 55
 - stopping sweeps 60
 - support 2
 - Sweep Drives drop-down list 54
 - Sweep Folders 54
 - Sweep Known Spyware Folders on Startup option 58
 - Sweep Now button 57
 - Sweep Status panel
 - defined 66
 - icons in 66
 - sweep status, monitoring 66
 - sweeps
 - configuring 54
 - running 56
 - running in safe mode 58
 - running now 57
 - scheduling 57
 - setting up alerts for 56
 - settings for 54
 - stopping 60
 - viewing those running 60
 - sweeps, viewing last date of 71
 - system health status bar, defined 65
 - system requirements 2
- ## T
- technical support 2
 - threats, monitoring 68
 - Top Spyware Threats panel
 - defined 68
 - icons in 68
 - Tracking Cookie Shield On option 52
 - Tray Icon option 55
 - Tray Icon Setting field 20
 - typographic conventions 1
- ## U
- unassigning distributor servers 34
 - Uninstall Client button 30
 - uninstalling, Spy Sweeper 33
 - unlocking, Spy Sweeper functions at a client workstation 63
 - Update Service
 - defined 4
 - installing 4
 - updates, viewing history of 70
 - updating
 - definitions 60
 - definitions automatically 61
 - definitions for mobile end users 63
 - definitions manually 61
 - overview of for Webroot Enterprise 8
 - Spy Sweeper 60
 - Spy Sweeper automatically 61
 - Spy Sweeper manually 61
 - the Admin Console 38
 - Webroot Enterprise Server 38
 - Use Custom List option 53
 - Use Proxy Login option 18
 - Use SMTP Login option 20, 39
 - Use Webroot Spyware Definitions 53
 - user

- viewing audit logs for Admin Console 47
- User Editable option 54, 56
- User Name and Password fields 21
- User Name field 39
- User Name for STMP field 20
- users
 - managing for the Admin Console 47

V

- viewing
 - applications installed by group 70
 - heartbeat status of CommAgents 71
 - News 37
 - sweeps 60
 - update history 70

W

- Webroot Enterprise
 - architecture 3, 5

- installing 11
- key steps to installing and setting up 8
- planning deployment of 5
- port requirements 75
- understanding 3
- updating process described 8
- Webroot Enterprise Server
 - installing 13
 - updating 38
 - viewing update history of 70
- Webroot Server Polling Interval field 17
- workstations
 - adding to groups 44
 - creating reports about 45
 - deleting 46
 - moving to a different group 44
 - polling now 46
 - removing from groups 44

