

# Installation Guide

This *Installation Guide* describes how to install and configure version 3.5.1 of Webroot<sup>®</sup> AntiSpyware Corporate Edition or Webroot<sup>®</sup> AntiSpyware Corporate Edition with AntiVirus. (In this guide, "Webroot AntiSpyware" refers to either product version.)

#### Installation checklist

The following table provides a checklist for installing and configuring Webroot AntiSpyware.

Step	See
1. Check system requirements for each Webroot AntiSpyware component.	"Webroot component requirements" on page 3.
2. If you are upgrading from a previous version of Webroot Enterprise or Webroot SME Security, check the upgrade requirements.	"Upgrading from a previous version" on page 7.
3. Install a Microsoft SQL Server 2000, 2005, or 2005 Express, and configure a database.	"Configuring a SQL Server database" on page 7.
4. Install Webroot Server components.	"Installing and configuring the Webroot Server" on page 8.
5. Install Webroot Clients on workstations. (If you are upgrading from a previous version, some older Webroot Clients are still supported by Webroot AntiSpyware. See the table, "Webroot Client compatibility," on page 7.)	"Installing and configuring the Webroot Client" on page 17.
6. If you have workstations located at different sites or over 500 workstations in your network, install Distributors and assign them to client groups.	"Distributor configuration" on page 4 and "Installing and assigning Distributors" on page 26.

#### **Technical Support**

If you need assistance with installation and configuration, Webroot Technical Support is available by phone and e-mail:

- Call 800-870-8102 (press 2 for Technical Support).
- Send your questions to: esupport@webroot.com.

© 2008 Webroot Software, Inc. All rights reserved.

Webroot Software, Webroot, Spy Sweeper, the Webroot icon and the Spy Sweeper icon are registered trademarks of Webroot Software, Inc. All other trademarks are the properties of their respective owners.

## Planning the installation

Before you begin installing Webroot AntiSpyware, read this section to familiarize yourself with the product architecture and to check component requirements.

## Webroot AntiSpyware architecture

Webroot AntiSpyware offers a total enterprise solution for company-wide threat management using a client/server architecture. If you purchased the AntiVirus edition, you can also protect client workstations from virus infiltrations.

The Webroot AntiSpyware architecture includes the following components:

- **SQL Server Database**. Stores information gathered from Webroot AntiSpyware components. You can install it on the same company server with the Webroot Server component or on another server in the network. **This software must be installed before any other Webroot component**.
- Webroot Server. Includes the central services that communicate with Webroot Clients and that receive updates from the Webroot Update Server. The Webroot Server installation also includes an Admin Console, which is the main user interface for Webroot AntiSpyware operations.
- Webroot Client. Includes the functions that detect and quarantine potential threats (such as spyware) on corporate workstations and includes a service for communicating with the Webroot Server.
- Webroot Distributor. Manages a heavy load of client communications or clients located in different geographical areas (only necessary for large environments, as described in "Distributor configuration" on page 4).

The following illustration shows a base configuration for Webroot AntiSpyware.



To receive updates from Webroot, the Webroot AntiSpyware components communicate as follows:

- Webroot provides the most current threat definitions and product updates from its Update Server. You determine how often your Webroot Server will check for updates.
- The Webroot Server, installed on one of your company servers, downloads the updates over the Internet to a download folder.
- The Webroot Clients, installed on workstations on your LAN, poll the Webroot Server based on a polling schedule you determine. If updates are available, the Webroot Clients can automatically download them from your company server, if you have set the "Auto Install" option. Otherwise, updates need to be installed manually.
- The Webroot Clients sweep workstations for potential threats, such as spyware and viruses, using the most current threat definitions that were downloaded. You determine how often to schedule sweeps.

For more information, see the System Administrator Guide.

## Webroot component requirements

Before installing Webroot AntiSpyware, review the requirements for the Webroot Server, Webroot Client, and Webroot Distributors. (If your internal network is complex or uses proxy servers, or if you run firewall programs at the desktop or server level, see also "Port requirements" on page 6.)

Webroot Server requirements		
Operating system:	<ul> <li>Windows 2000 Pro or Server with SP4</li> <li>Windows XP Pro with SP2*, SP3</li> <li>Windows Vista SP1, Premium, Business, or Ultimate</li> <li>Windows 2003 Standard, Enterprise, R2, Small Business Server R2 with SP1</li> <li>VMWare Workstation 5.5 or higher</li> </ul>	
CPU:	1 GHz minimum	
Memory:	1 GB minimum	
Disk space:	1 GB minimum	
Database support:	<ul> <li>Microsoft SQL Server 2005 Express Edition SP2 (English language; free download)</li> <li>Microsoft SQL Server 2000 SP4 or 2005 (for Vista: SQL Server 2005 SP2 is required)</li> </ul>	
Browser:	<ul><li>Internet Explorer 6.0 SP1 or later</li><li>Firefox 2.0.0.1</li></ul>	
Network and port requirements:	The Webroot Server components require the following network access: <b>Client Service</b> (WebrootClientService.exe): requires local network access and use of TCP port 50003 for inbound communication. (Clients prior to version 3.5 use port 50000.) <b>Update Service</b> (WebrootUpdateService.exe): requires local network and Internet access and outbound access for HTTPS requests on port 443 for your company server. <b>Admin Console</b> (WebrootAdminConsole.exe): requires local network access, use of port 50003 on your server, by default. The Distributor Service on your server uses the same port. Secure Sockets Layer (SSL) access requires use of port 50023.	

\* 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.

Webroot Client requirements		
Operating system:	<ul> <li>Windows 2000 Pro or Server</li> <li>Windows XP SP2, SP3, Home, Professional, or Tablet</li> <li>Windows Vista SP1, Home Basic, Premium, Business, or Ultimate</li> <li>Windows 2003 Standard, Enterprise, R2, or Small Business Server R2</li> </ul>	
CPU:	1 GHz minimum	
Memory:	512 MB RAM recommended; 1 GB RAM for Vista Premium	
Disk space:	100 MB free space	
Browser:	<ul><li>Internet Explorer 6.0 SP1 or later</li><li>Firefox 2.0.0.1</li></ul>	
Network and port requirements:	The Webroot Client components require the following network access: <b>CommAgent™</b> (CommAgent.exe): requires local network access and use of ports 50000, 50001, and 50002 on the client workstation. <b>Webroot Client</b> (SpySweeperUI.exe): <i>no network requirements</i> . <b>Spy Sweeper Engine</b> (SPYSWEEPER.exe): requires local network or Internet access.	

Webroot Distributor requirements <sup>*</sup>		
Operating system:	<ul> <li>Windows 2000 Pro or Server with SP4</li> <li>Windows XP Pro with SP2, SP3</li> <li>Windows XP (2014)</li> </ul>	
	<ul> <li>Windows Vista SP1 Home Premium, Business, or Oltimate</li> <li>Windows 2003 Standard, Enterprise, R2, or Small Business Server R2</li> </ul>	
CPU:	1 GHz minimum	
Memory:	1 GB minimum	
Disk space:	1 GB minimum	
Network and port requirements	<b>Distributor Service</b> (WebrootUpdateDistributor.exe): Requires local network access and use of port 50003 on your server. The Admin Console service on your company server uses the same port.	

\* You do not need to install Distributors unless you have workstations at different geographical sites or your network has more than 500 workstations. See the next section, "Distributor configuration."

### **Distributor configuration**

If you will be managing client workstations in different geographical locations or you have over 500 workstations in the network, read this section for Distributor configuration recommendations. If you plan to use a base configuration as shown in the example on page 2, skip this section.

The following illustration shows an example configuration for Webroot AntiSpyware with two Distributors.



#### **Reducing bandwidth**

You may want to configure Distributors to minimize bandwidth on WAN segments between multiple sites. The normal communication between the Webroot Clients and the Webroot Server is only about 1 kilobyte. Spyware and virus definition updates are typically about 3 megabytes, although incremental updates can be as small as 20 kilobytes. A new Webroot Client update can be as large as 10 megabytes. By configuring Distributors, you can reduce WAN bandwidth consumed when spyware and virus definitions or software updates are delivered.

After you configure Distributors, spyware and virus definitions are updated automatically, as follows:

- 1. Your company server (Webroot Server) automatically moves updates to all assigned Distributor servers once they are downloaded from the Webroot Update Server. The Distributor servers synchronize with your company server every 60 minutes and every time new updates are received.
- 2. The Webroot Clients poll the Webroot Server.
- 3. If updates are available, the Webroot Server sends a randomized list of Distributors containing the updates to the Webroot Client workstations.

For workstations to receive updates, you must assign updates to specific groups or to the company as a whole. If you configure automatic installation *after* an update has downloaded, the automatic installation does not apply to that update. (See the *System Administrator Guide* for more information.)

- 4. The Webroot Client requests updates from the first Distributor server on the list.
- 5. If the Distributor server is available, it sends the updates to the Webroot Client. If the Distributor server is not available, it cannot send information and the Webroot Client sends its request to the next Distributor server on the list.

The Webroot Server is always the last server on the list and will send the updates if no 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.

#### Managing a large number of workstations (over 500)

You may also want to configure Distributors if there are a large number of Webroot Clients relative to your company server's capabilities and you want to improve server performance. The following table provides general recommendations for the number of Distributors to use based on the number of client workstations. The following table provides recommendations (based on the number of Distributors) for the Webroot Server, type of database, and Webroot Client polling frequency.

No. of Distributor servers	Company server specifications	Database type	Poll no more frequently than
0 to 2 Distributors	Single 1 GHz processor; 1 GB RAM	MS SQL Server Express Edition	Two hours
2 to 3 Distributors	Single 1 GHz processor; 1 GB RAM	MS SQL Server	Four hours
3 to 6 Distributors	Dual 1 GHz processors; 2 GB RAM	MS SQL Server	Four hours

## **Port requirements**

A number of ports must be opened for proper communications between all Webroot components. Each component requires local network access. The following table describes the port requirements for a Webroot AntiSpyware installation.

Port requirements		
Port	Component	Component description
443	WebrootUpdateService.exe Required on company server and client workstations with mobile client enabled	<ul> <li>Installed on your Admin Console server</li> <li>HTTP protocol over SSL</li> <li>Communicates periodically with Webroot to retrieve updates and move them to Distributor servers</li> <li>Runs as a system service on the server</li> </ul>
50003	WebrootUpdateDistributor.exe; required on Distributor servers WebrootAdminConsole.exe; required on company server WebrootClientService.exe; required on company server and client workstations for version 3.5	<ul> <li>Distributor service: installed when you configure Distributor servers and responds to CommAgent on client workstations to distribute updates</li> <li>WebrootAdminConsole.exe: installed when you install Webroot Server and provides the browser-based Admin Console interface</li> <li>Both run as system services on the server</li> <li>Use HTTP</li> </ul>
50000	WebrootClientService.exe Required on company server and client workstations for versions prior to 3.5.	<ul> <li>Installed during the installation of Webroot Server</li> <li>Controls the communication between the client workstations (CommAgent service) and your company server</li> </ul>
50001	Sweep Now function Required on company server and client workstations	Not an installed component, but a function called from within the Admin Console that initiates a sweep of the selected client workstations
50002	Poll Now function Required on company server and client workstations	Not an installed component, but a function called from within the Admin Console that initiates a poll of the selected client workstations to update their heartbeat and status
50020	WebrootClientService.exe, if using SSL for communication between the client workstations and company server	<ul> <li>Installed when you install Webroot Server</li> <li>Provides the SSL access for communication between the client workstations and your company server</li> </ul>
50021	Sweep Now function, if using SSL for communication between the client workstations and company server	<ul> <li>Not an installed component, but a function called from within the Admin Console</li> <li>Provides the SSL access for the function initiated from the Admin Console that initiates a sweep of the selected client workstations</li> </ul>
50022	Poll Now function, if using SSL for communication between the client workstations and company server	<ul> <li>Not an installed component, but a function called from within the Admin Console</li> <li>Provides the SSL access for the function that initiates a poll of the selected client workstations to update their heartbeat and status</li> </ul>
50023	WebrootAdminConsole.exe, if using SSL to access the Admin Console	<ul> <li>Installed when you install Webroot Server</li> <li>Provides the SSL access to the browser-based Admin Console interface</li> </ul>

## Upgrading from a previous version

If your company is currently running Webroot Spy Sweeper Enterprise or Webroot SME Security, and a supported MS SQL database (2000, 2005, or 2005 Express), you can easily upgrade by following the instructions in this guide to install the Webroot components.

## Webroot Clients

If you want to run previous versions of Webroot Clients, you can keep most versions. See the following table.

Webroot Client compatibility		
If your company is running Follow these steps		
Webroot Spy Sweeper Clients 2.5.1, 3.0, 3.1, or 3.1.5	These previous versions of the Client are supported for older operating systems. You do not need to upgrade these clients unless you want to do so.	
Webroot Spy Sweeper Client 2.1	This version is no longer supported. You must upgrade to the new Webroot Client or to one of the versions listed above.	

## **Desktop Web Proxy**

This latest version of Webroot AntiSpyware (3.5.1) includes a Desktop Web Proxy with the Webroot Client installation. This proxy is a component for Microsoft Windows XP and Vista that intercepts HTTP/HTTPS traffic and reroutes it to the Webroot Web Security SaaS, a hosted Web filtering service.

If your Webroot Client computers already have a standalone installation of the Desktop Web Proxy (DWP), the proxy component bundled with the Webroot Client will not work. You must either uninstall the standalone DWP installation to take advantage of central management in the Admin Console or you must manage the DWP installations manually.

## Configuring a SQL Server database

As a first step, you must install and configure either a SQL Server or SQL Server Express database on a network server.

See the following table for important database installation notes.

Database	Installation notes
Microsoft SQL Server 2000 or 2005 (English version)	If you will use SQL Server 2000 or 2005 for your database, you must create the database before installing the Webroot Server. Make sure you have the user name and password available before installing the Webroot Server. You may also want to create a system data source name (DSN) if you experience problems connecting to the database. Also make certain the "Name Pipes" option is enabled in the SQL Server Configuration Manager.
	When you install the Webroot Server, the installer attempts to enable TCP/IP access and the correct authentication mode (mixed mode). If you have problems with the database configuration, refer to Webroot's Knowledge Base available from: http://webrootenterprise.supportportal.com/Portal/Home.aspx <b>Note:</b> The instance name is typically left blank in SQL Server 2000 or 2005.
Microsoft SQL Server 2005 Express Edition (English version)	<ul> <li>If you will use SQL Server 2005 Express for your database, you can either:</li> <li>Install it in advance</li> <li>Link to it from the Webroot AntiSpyware installer</li> <li>You must first install Microsoft .NET Framework 2.0, which can also be accessed from the Webroot Server installer. During the database installation, make sure you select Mixed Mode for the authentication mode.</li> <li>Note: If you will be configuring a large number of Distributors, do not use the SQL Server Express version.</li> </ul>

## Installing and configuring the Webroot Server

Follow these instructions to install the Webroot Server components:

- Client Service. Controls communications between the Webroot Server and Webroot Clients.
- Update Service. Controls updates from the Webroot Update Server.
- Admin Console. Provides a user interface for administering Webroot AntiSpyware.

#### Note

For Windows Server 2003 Service Pack 1 or 2 only: When installing the Webroot Server on Windows Server 2003 Service Pack 1 or Service Pack 2, the installation might fail. If this happens, you must change your server's Data Execution Prevention (DEP) setting. To change the setting, open all ports that Webroot AntiSpyware uses in the Windows firewall by selecting Start > Control Panel > Windows Firewall and opening the following TCP ports: 443, 50000, 50001, 50002, and 50003. Next, turn on the "essential Windows programs and services only" option in System Properties (right-click "My Computer," select Properties, click the Advanced tab, click Settings under Performance, click the Data Execution Prevention tab, and select the "Turn on DEP for essential Windows programs and services only"). Finally, restart your computer. For information about DEP, refer to the Microsoft Web site at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/memory/base/data\_execution\_prevention.asp)

To install the Webroot Server components:

- 1. Log into the system with Administrative rights.
- 2. Make sure all Windows programs are closed.
- 3. Start the installation program, as described in the following table.

To install from a CD:	To install from a downloaded file:
<ol> <li>Insert the CD into your CD drive.         If the installation options do not open automatically, use Windows Explorer to navigate to your CD drive. Then double-click WebrootServerSetup.exe to start the installation.     </li> <li>Click Install Webroot AntiSpyware to start the installation and open the Welcome window.</li> </ol>	<ol> <li>Follow the instructions on the Web site to download the WebrootServerSetup.exe file.</li> <li>Navigate to the downloaded file location. If you downloaded the file to your Windows Desktop, you will see an icon on your desktop. If you downloaded the file to a different location, use Windows Explorer to navigate to the file.</li> <li>Double-click WebrootServerSetup.exe to start the installation and open the Welcome window.</li> </ol>

4. At the Welcome screen, click Next.

The License Agreement window opens.

- 5. In the License Agreement window, select the "I Accept the License Agreement" option if you agree with the content.
- 6. In the Installation Checklist window, select each item in the checklist and click Next.

7. To specify database information, follow the appropriate instructions in the following table.

Database instructions	
If SQL Server 2000 or 2005 is already installed:	<ul> <li>A Database Connection window opens that shows the following fields:</li> <li>SQL Server Name: Name of the server running MS SQL Server or SQL Server Express.</li> <li>Instance Name: For SQL Server Express, enter the name of the instance that you defined for Webroot AntiSpyware data. For SQL Server, leave this field blank unless you know the SQL Server instance you want to use.</li> <li>Database Name: Name of the database you defined for Webroot AntiSpyware data.</li> <li>SQL User Name: User name you defined for the Webroot AntiSpyware database in SQL Server or SQL Server Express.</li> <li>Password: Password you defined for the Webroot AntiSpyware database in SQL Server or SQL Server Express.</li> <li>Click Next.</li> </ul>
If SQL Server Express is already installed:	The SQL Server Express Settings window opens, indicating that Setup has detected SQL Server Express on your system, but that some settings are incorrect. Select the "Attempt to Fix the Incorrect SQL Server Express Settings" option and click <b>Next</b> . The setup program will then enable the correct settings for TCP/IP and Named Pipes protocols in SQL Express. If you select "Continue" without Repairing the SQL Server Express Installation option, you must change the SQL Server Express settings yourself before Webroot AntiSpyware will work with the database.
If no database is installed and you want to download SQL Server Express:	The Prerequisites window opens with links to download and install SQL Server Express and .NET 2.0. (Installing .NET 2.0 is required only if you are using SQL Server Express.) If you want to install SQL Server Express or .NET 2.0, click the links provided, download the files, and follow the installation wizards. Be sure to remember the database name, user name, and password you set during the SQL Server Express installation. You will need this information when you continue with the installation of the Webroot Server. When you install SQL Server Express, you can accept all the default values during the installation. However, <b>you must select the Mixed</b> <b>Mode option</b> in the Authentication Mode window.

The Company Information window opens.

Webroot® Server - InstallS	hield Wizard	X
Company Infe	ormation	
✓ Installation Checklist	Please enter your user and company name. This name is used to identify your installation when your server looks for updates from the Webroot Update Server.	
Server Settings	Registered User:	
Client Settings	Company Name:	
Summary and Finish	Please enteryour keycode. You received your keycode in an email message at the time of purchas from your sales representative or from the Webroot website. Please copy and paste the entire keycode including the (braces).	ð
Webroot AntiSpyware	KeyCode:	
InstallShield	< Back Next> Cancel	

8. In the Company Information window, enter the registration and Key Code information (include the braces at each end of the code) and click **Next**.

Registered User:	Name of the person who will be the registered user of Webroot AntiSpyware and the Admin Console.
Company Name:	Name of your company.
KeyCode:	Unique code that identifies the rights and privileges associated with your installation, such as the number of licenses you have purchased. If you purchased Webroot AntiSpyware 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 (include the braces). If you purchased Webroot AntiSpyware from a store or received it already installed on your computer, the Key Code is on the product packaging.

The Default Admin Account window opens.

Installation Checklist	Please create a defau O Local User	It administration user or specify an AD user to u	se for administration.
Server	Active Directory and a sector of the sect	thentication	
Settings	User Name:	admin	Brow
Client	Domain:		
Settings	Password:		
Summany and	Verify Password:		
Finish		Allow all users from this Active Directory group	to log in:
	Group:		Bīow
	Domain:	1	

9. In the Default Admin Account window, create an Admin account as described in the table below and click **Next** when you are done.

Local User: <i>or</i> Active Directory authentication:	Select "Local user" to create an Admin account locally on your system. or Select "Active Directory authentication" to create an Admin account from existing users and groups in your Active Directory.
Local User: User Name: Password Verify Password:	If you selected "Local User," enter a login name and password for accessing the Admin Console. The password must be at least 7 characters with one non-alphanumeric character. <b>Be sure to write</b> <b>down the user name and password; you need this information to</b> <b>log into the Admin Console.</b>
Active Directory authentication: User Name: Domain: Password Allow all users from this Active Directory group to log in: Group: Domain:	If you selected "Active Directory authentication," enter the user name and domain name or click <b>Browse</b> to search the Active Directory and select a name and domain from a pop-up window. If you type in the domain name, make sure to use the fully qualified domain name (for example, <i>domain.company.com</i> ). If you want to allow a group to have access to the Admin account, you can select the "Allow all users from this Active Directory" checkbox. Enter a group and domain name or click <b>Browse</b> to search the Active Directory.

The Start Menu Entry window opens and shows the default Start menu folder.

Webroot® Server - InstallShield Wizard			
Start Menu Entry			
✓ Installation Checklist	Please enter the name of the start menu folder where you want to list Webroot® Server. You may also select a start menu location that already exists from the list.		
Server Settings	Program Folder: Webroot (Corporate Edition)	]	
Client Settings	Existing Folders: Accessories Administrative Tools Adobe		
Summary and Finish	Child Safe Cisco Systems VPN Client Del Printers Games Intel PROSet Wrieless Intel PROSet Wrieless Microsoft Office Microsoft Office Perforce PrintMe Internet Printing	2	
Webroot AntiSpyware			
InstallShield	< Back Next > Cancel		

10. If you want to use the default folder, click **Next**. If you want to use a different Start menu folder, enter a new name or select an existing folder.

The Installation Paths window opens and shows you the default locations for installing the components and for product updates and spyware/virus definitions.

Webroot® Server - InstallS	hield Wizard	X		
Installation Paths				
✓ Installation Checklist	Please specify the directory where you want to store the files for the Webrool® Server in the boxes below. NOTE: Directory locations must be local drives on your Webrool® Server.			
Server Settings	Please Select the path where the server files will be stored			
Client Settings	Install Path: [C:\Program Files\Webroot\Server Browse			
Summary and Finish	Please select the path to which definition and product updates will be downloaded.			
	Updates Path: C.\Program Files\Webroot\Server\Updates Browse			
InstallShield	< Back Next > Cancel			

11. If you want to keep the default locations, click **Next**. Otherwise, select or enter new locations. Both paths must refer to local disks that are physically on the server. Network disks are not supported.

Install Path:	If you want to install the Webroot Server to a different folder, enter the path or click <b>Browse</b> to navigate to the folder you want.
Updates Path:	If you want to download Webroot Server updates to a different folder, enter the path or click <b>Browse</b> to navigate to the folder you want. <b>You cannot change this folder after installation.</b>

The Proxy Settings window opens.

Webroot® Server - InstallS	nield Wizard	X
Proxy Setting	s	
✓ Installation Checklist	If you do not use a proxy server for accessing the internet, please leave the box below blank. Otherwise, please enter your proxy information. The server you enter should conform to the following example: proxy.mycompany.com.80	
Server Settings	Proxy Server:	
Client Settings	Praxy Login Settings	
Summary and Finish	🗌 Use Praxy Login	
	User.	
	Password:	
InstallShield	< Back Next > Cancel	

12. If you do not use a proxy server to access the Internet, click **Next** to skip this screen. If you will use a proxy server to access the Internet, enter the information in the fields.

Proxy Server:	Enter the proxy server name or IP address and port number in one of the following formats: <i>server_name.company.com:80</i> or <i>10.0.0.1:80</i> .
Use Proxy Login: User: Password:	If you use a proxy server that requires authentication, select the Use Proxy Login option. Enter your user name and password in the fields.

The Email Settings window opens.

Webroot® Server - InstallS	hield Wizard	X
Email Setting	ļs	
✓ Installation Checklist	Please fill in the settings that the Webroot® Server will use for sending email in the boxes below.	
Server Settings	Please enter the name of the E-mail server used for outgoing (SMTP) mail.	
Client Settings	Please enter the E-mail address that notification messages will come from. This must be a real E-r address in the form user@server.com.	nail
Summary and Finish	From Address: Select whether to use SMTP Login for sending email notifications	
	My SMTP Server requires a login	
Webroot' AntiSpyware	Password	
InstallShield	< Back Next > Cancel	

13. In the Email Settings window, enter or select the information and click **Next**. (You can edit these settings later in the Admin Console.)

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: name@webroot.com.
My SMTP Server Requires a Login User Name: Password for SMTP:	If you use a secure SMTP e-mail server, select this option. Enter the user name and password in the fields. <b>Note:</b> Webroot AntiSpyware only supports Auth-Login.

The Server Settings window opens.

Webroot® Server - InstallSi	nield Wizard			
Server Settings				
✓ Installation Checklist	Periodically, this server needs to communicate with the Webroot update server to download definitions and code updates. What frequency should be used to see if definition, software updates or configuration changes are available?			
Server Settings	Server Polling Intervat Daily			
Client Settings	Enter the IP or host name that you will use to communicate with this server. Select the network interface visible to client workstations or enter the fully qualified name.			
Summary and Finish	This will be the host in the URL you will use to access the administration console remotely.			
	Server IP/Name: 10.10.8.50			
	, on or regard electron			
Webroot' AntiSpyware				
InstallShield	< Back Next > Cancel			

14. In the Server Settings window, verify or enter new information and click **Next**. If desired, you can edit these settings later in the Admin Console.

Server Polling Interval:	Select how often you want the Webroot Server to check the Webroot Update Server for new spyware/virus definitions and software updates.
Client Service IP/Host Name:	Select or enter the IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, use a static IP address of the network interface card (NIC) visible to client workstations. For host name resolution, select or enter the fully qualified domain name of your server (requires a properly configured DNS environment).
Port for legacy clients:	If you plan to run legacy Webroot Clients (below version 3.5), specify the port number these clients use to communicate. The default port is 50000.

The Client Settings window opens.

Webroot® Server - InstallShield Wizard 🛛 🛛 🔀		
Client Settings		
✓ Installation Checklist	Tray Icon Setting C Pop up on Scan	
✓ Server Settings	<ul> <li>Stay Minimized in Tray</li> <li>Stay Invisible</li> </ul>	
Client Settings	Client Polling interval:	1
Summary and Finish	<ul> <li>Install new definitions automatically</li> <li>Install new client updates automatically</li> </ul>	
	Shield and Sweep Settings C Maximum protection	
@ Webroot	Recommended     Contract (Cations configured starting)	
	<ul> <li>Lusson (Secongs configured area installation)</li> </ul>	
InstallShield	< <u>B</u> ack <u>N</u> ext >	Cancel

15. In the Client Settings window, select the desired information and click **Next**. If desired, you can edit these settings later in the Admin Console.

Tray Icon Setting:	<ul> <li>Select how you want the Webroot Client to appear on client workstations.</li> <li>Pop up on Scan: Displays a tray icon that client users can double-click to display the Webroot Client window and automatically pops up the window whenever a sweep starts, whether scheduled or using Sweep Now.</li> <li>Stay Minimized in Tray: Default and recommended setting. Displays a system tray icon that client users can double-click to display the Webroot Client, 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.</li> <li>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 Webroot Client window.</li> </ul>
Client Polling interval:	Select how often you want Webroot Clients to check for updates and for schedule and configuration changes from your server.
Install new definitions automatically	Select to have spyware and virus definitions installed automatically on all client workstations whenever updates are available.
Install new client updates automatically	Select to have Webroot Client program updates installed automatically on all client workstations whenever updates are available.
Shield and Sweep Settings:	<ul> <li>Select the desired settings:</li> <li>Maximum protection: Turns on all shields and schedules a weekly sweep at 12 am Saturday.</li> <li>Recommended: Turns on all Windows System and Internet Explorer shields to protect workstations from unauthorized changes.</li> <li>Custom: No settings will be configured at this time. See the <i>System Administrator Guide</i> for configuration instructions.</li> </ul>

The Service Credentials window opens.

Installation Checklist	In order to deploy clients remo credentials for the service. If have to specify a service user	tely in a Windows Domain environme you are not in a Domain, or you do r	ent, you must use admin not need to deploy, you do noi
Server Settings	Run the Admin Console S	ervice as a specific user.	
Client	User Name:		Biowse
Settings	Password:		
Summary and Finish			
Webroot AntiSpyware			

16. If you want to install the Webroot Clients remotely from the Admin Console, you must select the "Run..." checkbox and enter Admin credentials for running the Webroot Server and Webroot Client services. If you plan to install Webroot Clients locally at each workstation (see "Using alternate methods to install Webroot Clients" on page 24), skip this screen. Click Next.

Run the Admin Console Service as a specific user	Select this checkbox if you want to install Webroot Clients remotely.
User Name	For a local account, enter the user name. For an Active Directory account, enter the Domain and user name (for example, domain/username) or click Browse to select a domain and user name from a pop-up window.
Password	Enter the password.

The Summary window opens and shows the current settings.

17. Verify that the settings are correct and click Next.

The Webroot Server installs and automatically starts the Client Service and Update Service. These services (WebrootClientService.exe and WebrootUpdateService.exe) run as Windows services and should always be running. This permits your company server to download updates from the Webroot Update Server and permits client workstations to download updates and configuration changes from your company server.

18. Click Finish.

You are now ready to configure one or more Webroot Clients, and if needed, one or more Distributors. For more information, see "Installing and configuring the Webroot Client" on page 17 and "Installing and assigning Distributors" on page 26.

## Installing and configuring the Webroot Client

Follow these instructions to install the Webroot Client components:

- **CommAgent**. Communicates periodically with your Webroot Server to check for configuration changes, new or updated applications, or updated threat definitions.
- Webroot Client. Detects spyware and other potential threats. Also provides access to options for workstation users.
- Spy Sweeper Engine. Provides the core functions for Webroot AntiSpyware.



Caution

Do not install the Webroot Client on a file server.

Method	Description
Admin Console	Configure the logon properties for the Webroot Admin Console Service, access the Admin Console, then install the Webroot Clients on workstations from the Admin Console. See the next section, "Using the Admin Console to install Webroot Clients."
MSI file	Go to each workstation and manually execute the installation files. (If you have a third-party deployment tool, such as SMS or Altiris, you can also use that tool to execute the WebrootClientSetup.msi file.) See "Using the MSI file" on page 24.
Logon script	Use the example logon scripts provided by Webroot. See "Using a logon script" on page 25.
Group Policies	If you use Active Directory, you can use Group Policies. See "Using group policies" on page 25.
Image of Webroot Client	Include the Webroot Client as part of an image installed on each workstation. See "Using an image file" on page 25.

Determine the best method for installing the Webroot Client as described in the table:

## Using the Admin Console to install Webroot Clients

You can install and update the Webroot Clients from the Admin Console, which requires that you complete the following tasks:

- Configure the logon properties for the Webroot Admin Console Service.
- Access the Admin Console.
- Install the Webroot Clients.

#### Configuring logon properties for Webroot Admin Console service

To use the client deployment feature of the Admin Console, you must first properly credential the Webroot Admin Console Service from the Services control panel in Windows. The user account that you specify must have administrative privileges in the domains where you want to remotely install and uninstall the Webroot Client.

To configure the logon properties:

- 1. From the Start menu, select Control Panel.
- 2. Select Administrative Tools, then Services.
- 3. Right-click the Webroot Admin Console and select Properties.

Services							Ge	×
File Action View	Help							
+ → 🔟 🚰	3 🖫 😢 🕨 🔳 🗰							
Services (Local)	🍪 Services (Local)							
	Webroot Admin Console	Name 5		Description	Status	Startup Type	Log On As	1
	Bog the service Restart the service Description: Provides enterprise console and distribution service for Webroot Enterprise Clients	Windows Instaler Windows Instaler Windows Frewal/In Windows Audio Webroot Update Ser Webroot Update Ser Webroot Clent Serv Webroot Clent Serv Webroot Clent Serv Webroot Adam Co WebClent Wahme Shadow Cc Wuhmersal Plag and Universal Plag and Universal Plag and Universal Plag and	usition (WIA) ternet Connecti vice er Engine 1.5 k Service ke Stort Stop Plause Resume Restart	Adds, mod Provides im Provides n Manages a Controls th Provides c Controls th Provides e Provides e Provides e Provides e Manages a Provides u	Started Started Started Started Started Started Started Started	Manual Manual Automatic Automatic Automatic Automatic Automatic Automatic Automatic Manual Disabled Manual Automatic	Local System Local System Local System Local System Local System Local System Local System Local System Local System Local Service Local Service Local Service Local Service Local System	-
	Extended (Standard /	Terminal Services	All Tasks	Allows mult	Started	Manual	Local System	
Opens property sheet fo	or the current selection.		Properties					
	005/08/ - 005/08/ ~		Help					

4. Click the Log On tab.

General Log On Red	covery Dependencies	
Log on as:		
Local System acco Allow service to	ount interact with desktop	
This account:		Browse
Password:	•••••	- hè
Confirm password:		_
You can enable or disa Hardware Profile	able this service for the hardwa	re profiles listed below:
You can enable or disa Hardware Profile Profile 1	able this service for the hardwa	re profiles listed below:   Service   Enabled

- 5. Select This account.
- 6. Click Browse.
- 7. Enter the domain name and partial user name using the following format: DomainName\PartialUserName.

The user name must be a domain administrator.

8. Click Check Names.



9. If multiple user names display, select the correct user name and click **OK**.

Multiple Names Found	? 🛛
More than one object matches the followin Select an object from this list or, to reenter i Matching names:	g object name: "boulder\bga." he name, click Cancel.
Name (RDN)	In Folder
🕵 Brannan Gamber	boulder.webroot.com/Users
🔮 Biyan Gale	boulder.webroot.com/Users
L	OK Cancel

10. Click OK again.

Select User			? 🔰
Select this object type:			
User or Built-in security principal			Object Types
From this location:			
BGALE			Locations
Enter the object name to select ( <u>examples</u> ):			
Bryan Gale (bgale@boulder.webroot.com)			Check Names
Advanced	N	OK	Cancel

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

General Log On Rec	covery Dependencies	
Log on as:		
Local System acco Allow service to	unt interact with desktop	
This account:	bgale@boulder.webroot.com	Browse
Password:	•••••	
Confirm password:	•••••	]
You can enable or disa	able this service for the hardware pro	ofiles listed below
You can enable or disa Hardware Profile Profile 1	able this service for the hardware pr	ofiles listed below Service Enabled
You can enable or disa Hardware Profile Profile 1	able this service for the hardware pr	ofiles listed below Service Enabled Disable
You can enable or disa Hardware Profile Profile 1	able this service for the hardware pr	ofiles listed below Service Enabled

14. Click OK.

Services	×
1	The new logon name will not take effect until you stop and restart the service.
	ОК

15. Restart the service.

🏶 Services (Local)		
Webroot Admin Console	Name $\nabla$	Descriptio
Stop the service Restart the service Description: Provides enterprise console and distribution service for Webroot Enterprise Clients	Windows Installer Windows Image Acquisition (WIA) Windows Firewall/Internet Connecti Windows Audio Webroot Update Service Webroot Spy Sweeper Engine 1.5 Webroot CommAgent Service	Adds, mo Provides Provides Manages Controls I Provides Communi-
	Webroot Admin Console	Provides
	🏶 WebClient	Enables V
	🤹 Volume Shadow Copy	Manages
	🏶 Universal Plug and Play Device Host	Provides
	🖏 Uninterruptible Power Supply	Manages
	Themes	Provides
	Terminal Services	Allows mu

#### Accessing the Admin Console

You can access the Admin Console from a server in your network through a browser or from the HTML Application (HTA) that installed on your local server.

To access the Admin Console:

- 1. Do one of the following:
  - If you are working from the computer where the Webroot Server is installed, open your browser and enter:

http://localhost:50003/Admin

- If you are working from another computer on your network, open your browser and enter: http://[server\_computer\_name]:50003/Admin
- If you want to access the HTA version, select **Start > All Programs > Webroot (Corporate Edition) >** Admin Console.

Because all communications from the Admin Console to the Webroot Server are encrypted using SSL (Secure Sockets Layer), a security warning opens the first time you attempt to access the Admin Console, as shown in the example below for the HTA version of the Admin Console (Internet Explorer 7 and FireFox browsers will open different warnings).

Securit	ty Alert 🔀
£	Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
	The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
	The security certificate date is valid.
	The security certificate has a valid name matching the name of the page you are trying to view.
	Do you want to proceed?
	Yes No View Certificate

- 2. You must configure SSL between the Admin Console and the Webroot Server in one of three ways:
  - Accept the self-signed certificate once for the current session. If you choose this option, you can go directly to the Admin Console, but the security warning will open every time you access the Admin Console in the future. This is just a temporary solution; we recommend that you either accept the self-signed certificate permanently or use a trusted certificate authority.
  - Accept the self-signed certificate permanently. If you choose this option, you will not see the warning again. Using the self-signed certificate is convenient and free, but not completely secure because the certificate itself was not generated by a certification authority trusted by your organization.
  - Use a Trusted Certificate Authority. If you choose this option, you will have the highest level of security. It requires that you install your own certificate by a signed certificate authority, which is used by the Webroot Server and is already trusted by workstations running the Admin Console. This certificate authority could be from a third party, such as Thawte or VeriSign, or from within your organization. Depending on the type of certificate, you need to install it so that the Webroot Server, which is based on the Jetty application server, can use it to create SSL connections.

For more detailed instructions on configuring SSL, see "Configuring SSL communications" on page 29.

3. When the Login windows opens (shown below), enter your username and password, which were determined during Webroot Server installation. For domain authentication, you can enter the user account in three different formats: user@domain, domain/user, or domain/user.

<u>()</u>	Webroot AntiSpyware
Username:	
	For domain authentication, enter: domain\username
Password:	
	Login
i Plea buti	ise enter your username and password, then dick the Login ton or press Enter.

4. Click Login.

A progress bar opens and shows the status of the resources loading, then the Admin Console displays in your browser. Use the function tree to navigate in the Admin Console. Do *not* use the **Back** button in your browser.

#### Installing Webroot Clients using the Admin Console

You can install and update the Webroot Clients from the Admin Console. You can also see what Webroot Client version each workstation has installed and the last heartbeat from the workstations.

*If your client workstations are using Windows XP SP2 and the Windows Firewall*, you must configure the firewall to have certain exceptions. For more information, see "Configuring Windows Firewall to permit installation from the Admin Console" on page 23.

Installing the Webroot Client from the Admin Console requires Windows networking, access to the admin share (admin\$), and NetBIOS enabled on your network. (If you use Active Directory for the installation, NetBIOS is not required.)

To install and update Webroot Clients from the Admin Console:

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

The Client Install/Uninstall panel opens.



- 2. Select either the Active Directory View tab or the Network View tab to see a list of the domains or workgroups that exist on your network (middle panel). To view clients in the Active Directory View tab, you must be logged into the Admin Console as a domain user.
- 3. From the middle panel, select a domain or workgroup of workstations.

A list of workstations appears in the far right panel.

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

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

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

- 5. Click Install Client.
- 6. Click Refresh or go to the Client Management panel to see the status of the installation.

#### Configuring Windows Firewall to permit installation from the Admin Console

For client workstations using Windows XP SP2 *and* the Windows Firewall, you must change the settings in the Windows Firewall. Changing the settings is required for the following:

- Installation of the Webroot Client on workstations from the Admin Console.
- Communication between the company server and the client workstation.

You can install the Webroot Client on workstations using another method; however, the Webroot Client will not work properly if it cannot communicate with the company server. The Windows Firewall must be **turned off** completely for the installation to work from the Admin Console.

To configure Windows Firewall:

- 1. At the client workstation, access the Control Panel.
- 2. Double-click Security Center.
- 3. Click Windows Firewall.
- 4. Make sure the Don't Allow Exception option is *not* selected.
- 5. Click the **Exceptions** tab.
- 6. Make sure the File and Printer Sharing option is selected.
- 7. Add the following three ports by clicking Add Port:
  - Webroot Client Service port: Controls the communication between the client workstations and your company server.
    - Name: Enter any name.
    - Port Number: 500003 for version 3.5 or 50000 for previous versions
    - TCP
  - Sweep Now port: Function initiated from the Admin Console that initiates a Webroot Client sweep of the selected client workstations.
    - Name: Enter any name.
    - Port Number: 50001
    - TCP
  - Poll Now Function: Function initiated from the Admin Console that initiates a poll of the selected client workstations to update their heartbeat and status to the server.
    - Name: Enter any name.
    - Port Number: 50002
    - TCP
- 8. From the Admin Console, select Client Management.
- 9. Select the client workstation you just configured.
- 10. Click Poll Now.
- 11. Click Refresh and verify that the Last Heartbeat updates to the current date and time.

## Using alternate methods to install Webroot Clients

In addition to using the Admin Console, you can install the Webroot Client using any of these alternate methods:

- Execute the WebrootClientSetup.msi file from each workstation.
- Use a logon script to execute the WebrootClientSetup.msi file.
- Use Group Policies, if you use Active Directory.
- Include the Webroot Client as part of an image installed on workstations.

#### Using the MSI file

From each workstation, you can execute the WebrootClientSetup.msi file.

i)	Note
----	------

If you have a third-party deployment tool, such as SMS or Altiris, you can use that tool to execute the WebrootClientSetup.msi file.

Make sure that all five of the client installation files are in the same folder whenever WebrootClientSetup.msi executes:

- WebrootClientSetup.exe
- WebrootClientSetup.ini
- WebrootClientSetup.msi
- SSECleanup.exe
- SSEStart.exe

Typically, these files are in the \Program Files\Webroot\Client folder of the system where you installed the Webroot Server. The WebrootClientSetup.ini file contains the IP address and port of your company server and is needed for the Webroot Client to install successfully. The WebrootClientSetup.msi client installation program defaults to a visible installation where you see a progress bar and receive feedback when the installation is complete.

You can use the following client installation options when you configure client workstations:

Client Installation Options			
Performing a silent install:	If you would like to perform a silent installation, add the /q switch in the line that executes WebrootClientSetup.msi. The installation program defaults to a visible installation where you see a progress bar and receive feedback when the installation is complete. The syntax is:		
	WebrootClientSetup.msi /q		
Specifying the server IP address and port:	You can specify the server IP address and port in the command line instead of relying on the .ini file. The syntax is:		
	WebrootClientSetup.msi SERVERIP=10.10.10.10 SERVERPORT= 50000		
	For a silent installation:		
	WebrootClientSetup.msi /q SERVERIP=10.10.10.10 SERVERPORT=50000		
Bypassing client deployment settings:	You can also bypass the client deployment settings, as described in the examples below. (If you are using the /q switch, the setting should go after it.)		
	Pop-up on scan: RUN_CLIENT_AS=0		
	Stay minimized: RUN_CLIENT_AS=1		
	Stay invisible: RUN_CLIENT_AS=2		
	The syntax is:		
	WebrootClientSetup.msi /q RUN_CLIENT_AS=1 SERVERIP= 10.10.10.10 SERVERPORT=50000		

#### Using a logon script

Use a logon script to execute the WebrootClientSetup.msi file (see also the previous table). Webroot has provided some example logon scripts that you can change to meet your needs.

Below is an example logon script. You must adjust it for your setup and network environment. You must 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 WebrootClientSetup.msi and WebrootClientSetup.ini files. Typically, these files are in the \Program Files\Webroot\Client folder of the system where the Webroot Server has been installed. Copy the client files to the network share of your choice, then adjust the script to match your share path. Also be sure to give all workstations read access and execute access to the share.

```
@echo off
if exist "C:\Program Files\Webroot\Client\SPYSWEEPER.EXE" goto check
if not exist "C:\Program Files\Webroot\Client\SPYSWEEPER.EXE" goto install
:check
if exist "C:\Program Files\Webroot\Client\SpySweeperUI.exe" goto loaded
if not exist "C:\Program Files\Webroot\Client\SpySweeperUI.exe" goto install
:install
echo Loading Webroot Enterprise Clients...
"C:\Program Files\Webroot\Server\Client\WebrootClientSetup.msi"
goto end
:loaded
echo Webroot Enterprise Clients are already Installed
:end
```

#### Using group policies

Use 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.

#### Using an image file

To use an image file, include the Webroot Client as part of an image installed on workstations.

- Install the Webroot Client 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.

## Monitoring Webroot Client polling

Webroot Clients poll the company server at random intervals within 20 seconds of installation. During the first contact, the Webroot Client's CommAgent also provides the name and MAC address of the client workstation and automatically adds the client to a default group. To view client information in the Admin Console, go to Administration > Client Management. Once you configured 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 the *System Administrator Guide*.

The CommAgents contact the Client Service on your company server, as assigned in the Client Service Settings in the Admin Console (Administration > Configuration > System 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. See "Assigning Distributor servers" on page 27 for more information.

## Installing and assigning Distributors

By default, a Distributor service is installed with the Webroot Server and acts as a single Distributor server. If your workstations are located in different geographical locations or you have a large number of workstations (over 500), you should install the Distributor Service on one or more of your company servers.

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

- Install the Distributor Service software.
- Assign Distributor servers.
- Change the port number Distributors use.

## Install the Distributor service

Follow these instructions to install and start a Distributor service (WebrootUpdateDistributor.exe) on a company server.

By default, the Distributor listens to port 50003. If you need to change a Distributor 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 port used by Distributors" on page 27. The Admin Console service on your company server also uses the same port.

You can install a Distributor using several methods, as described in the following table.

Distributor Installation Options		
Performing a silent install (or uninstall):	If you would like to perform a silent installation, add the /qn switch in the line that executes WebrootDistributorSetup.msi:	
	WebrootDistributorSetup.msi /qn	
	The installation program defaults to a visible installation where you see a progress bar and receive feedback when the installation is complete.	
	Or, if you are using the WebrootDistributorSetup.exe file, add the following:	
	WebrootDistributorSetup.exe /s /v" /qn"	
	If necessary, you can perform a silent <i>un</i> install by executing one of the following:	
	WebrootDistributorSetup.msi /qn REMOVE="ALL"	
	WebrootDistributorSetup.exe /s /v" /qn" REMOVE=\"ALL\""	
Specifying a folder:	You can specify the folder where you install the Distributor, as follows:	
	WebrootDistributorSetup.msi INSTALLDIR=" <drive>:\<folder>\"</folder></drive>	
	0ľ	
	WebrootDistributorSetup.exe /v"INSTALLDIR=\" <drive>:\<folder>\""</folder></drive>	
Enabling logging:	To enable logging when using the MSI file ("no logging" is the default), use the following syntax:	
	WebrootDistributorSetup.msi /qn INSTALLDIR=" <drive>:\<folder>\" /l*v "<drive>:\<folder>\name.log"</folder></drive></folder></drive>	

To install the Distributor Service:

1. On the system where you installed the Webroot Server, access the following folder: \Program Files\Webroot\Server\Distributor.

This is the default folder where the WebrootDistributorSetup files are installed. If you installed them to a different directory, access that directory instead.

- 2. Copy the files in this folder to the server you want to act as a Distributor.
- 3. Execute the WebrootDistributorSetup.exe file.
- 4. Follow the on-screen instructions.
- 5. Continue with the instructions in the next section for assigning Distributor servers.

## **Assigning Distributor servers**

After you install Distributor services, you must assign their servers to client groups. By default, each client workstation is added to a default group named after the domain or workgroup the client workstation is in. You can assign a Distributor to one or more groups or to the whole company. For example, if you install four Distributors and assign them all to the whole company, the system randomly selects the order of Distributors it sends back to the client workstations. This process spreads the load across the servers to ensure that the servers are not overwhelmed with update requests.

To assign a Distributor server:

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

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

2. Click Add Distributor.

The Add Distributor window opens.

Add Dis	stributor
2	Name: *
$\checkmark$	Resolve
	IP Address: *
	0.0.0.0
	* - Denotes required fields
	OK Cancel

3. Enter a name for the Distributor server.

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

- 4. If necessary, enter the IP address of the server.
- 5. Click OK.

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

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

To remove a server assignment, select the server in the group tree and click **Unassign Distributor**. To remove the selected Distributors from their assignments and from the list of Distributors, click **Delete Distributors**.

To update the status of the Distributors, click Refresh.

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

## Changing the port used by Distributors

The company server (Webroot Server) uses the same port (50003, by default) for both the Distributor service and Admin Console service. The Distributor servers that you configured must use the same port for the Distributor Service.

If you need to change this port, complete the following tasks:

- 1. Change the Distributor Service port on the company server.
- 2. Change the Distributor Service port on each Distributor server.

#### 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. 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 Administration > Configuration > System Settings.

The System Settings panel opens, with several subpanels where you can view and edit settings.

- 2. Click the Network show/hide bar.
- 3. Change the port under Admin Server/Distributor Settings.

😰 Webroot® AntiSpyware Corporat	e Edition	_ 8 ×
Webroot AntiS	pyware	User: admin 🖟 🥝
Dashboard     Sweep Status	System Settings	🗐 🎻 🧔 Refresh
🖓 Definition Status	Basic	×
infection Status	E Mail	~
Top Detected Items	C-Mail	~
Server Status	Advanced	≈
License Status	Network	\$
Client Management	A Warning:	
	Please consult the online help or System Administrator Guide before changing and applying these s	ettings.
🔡 Client Install / Uninstall	Client Service Settings	
si Distributors		
Errors	IP / Host Name: 192.168.247.132	
🚆 User Management	Ports: No SSL: 50000 🗧 SSL: 50020 🐳 (for clients prior to 3.5)	
🖃 😪 Configuration		
System Settings	Admin Server / Distributor Settings	
	Ports: No SSL: 50003 - SSL: 50023 - (for clients 3.5 and above)	
Smart Shields	Client Settings	
Detection Settings	Sweep Now Ports: No SSL: 50001 - SSL: 50021 -	
🥥 Web Security 🚽		
🗉 🎯 Updates	Poll Now Ports: No SSL: 50002 🔂 SSL: 50022 🔂	
🗄 🔄 Notification Management	Use SSL	
🖃 🔙 Reports		
Detection Trend by Type	Database	×

- 4. Click Apply.
- 5. Log out of the Admin Console.
- 6. Restart the Webroot Admin Console Service.
- 7. Access the Admin Console using the new port number.
- 8. From the Admin Console function tree, select **Dashboard > Server Status**.

The Server Status panel opens.

9. Check that the Update Distributor port is open.

#### Changing the Distributor service port on the Distributor server

If you change the Distributor service port on the company server, you must also change it on each Distributor service.

The paths in the following steps assume you have installed the Admin Console and the Update Distributors in the default location: "\Program Files\Webroot." If you have installed any of them to a different directory, substitute the correct root in the specified path.

To change the Distributor service port on the Distributor server:

- 1. On the Distributor server, stop the Webroot Update Distributor service.
- For backup purposes, rename the following file on the Distributor server: "\Program Files\Webroot\Server\WebServer\conf\ WebrootUpdateDistributor.conf"
- 3. From your company server, copy the file "C:\Program Files\Webroot\Server \WebServer \conf\WebrootUpdateDistributor.conf" to the Distributor server.
- 4. Restart the Webroot Update Distributor service.

5. To test that the correct port is open, open a browser and try the following URLs:

http://<distributor\_name>:<non\_ssl\_port>/Distributor/servlet/UpdateReplicator
https://<distributor\_name>:<ssl\_port>/Distributor/servlet/UpdateReplicator
You should get an empty page as a response.

Trying the same URLs with the incorrect port yields a failure to connect to server error, which will be treated in various ways by your browser, such as navigating to a search page.

## **Configuring SSL communications**

Starting with version 3.5, the Admin Console uses HTTPS to communicate with the Webroot Server, which means that all communications from the Admin Console to the Server will be encrypted using SSL (Secure Sockets Layer) and will provide a secure transport of user names, passwords, and administrative information.

To configure SSL communications, you can do one of the following (options are listed from least secure to most secure):

- Temporarily accepting a self-signed certificate
- Permanently accepting a self-signed certificate
- Using a trusted certificate authority

## Temporarily accepting a self-signed certificate

You can quickly proceed to the Admin Console by temporarily accepting a self-signed certificate. However, a security warning will open each time you attempt to access the Admin Console unless you permanently accept a self-signed certificate or use a trusted certificate authority. Follow the appropriate instructions below to temporarily accept a self-signed certificate.

#### For the HTA version and Internet Explorer 6:

- 1. Start the Admin Console, as described in step 1 of "Accessing the Admin Console" on page 21.
- 2. At the security warning screen, click Yes to proceed.

#### For Internet Explorer 7:

- 1. Start the Admin Console, as described in step 1 of "Accessing the Admin Console" on page 21.
- 2. At the security warning screen, select Continue to this web site.

The browser's address bar displays with a red background and shows a "Certificate Error."

#### For FireFox:

- 1. Start the Admin Console, as described in step 1 of "Accessing the Admin Console" on page 21.
- 2. At the security warning screen, select Accept this certificate temporarily for this session and click OK.

The browser's address bar displays with a yellow background.

### Permanently accepting a self-signed certificate

You can create a self-signed certificate, which is a convenient method for stopping the security warning from opening again, but may not be the most secure solution because the certificate is not generated by a certification authority trusted by your organization.

#### ) Note

When you install a self-signed certificate, make sure to install it as a root certificate.

You can accept a self-signed certificate from the security warning screen that opens when you attempt to access the Admin Console or accept it from the **webroot.crt** file.

#### From the Security warning screen

Start the Admin Console, as described in step 1 of "Accessing the Admin Console" on page 21. Then follow the appropriate instructions below:

#### Internet Explorer 6 and the HTA Admin Console:

- 1. At the security warning screen, click View Certificate.
- 2. When the Certificate window opens, click Install Certificate and follow the on-screen instructions.

#### **Internet Explorer 7:**

- 1. At the security warning page, click **Continue to this Web site (not recommended)**, click the **Certificate Error** button immediately to the right of the address bar, then click the **View Certificates** button at the bottom of the dialog.
- 2. When the Certificate window opens, click Install Certificate and follow the on-screen instructions.

#### **FireFox:**

- 1. At the security warning screen, select Accept this certificate permanently.
- 2. Click OK.

#### From the webroot.crt file

1. Click the following file:

\program files\webroot\server\webserver\etc\webroot.crt

2. When the certificate window opens, click Install Certificate and follow the on-screen instructions.

### Using a trusted certificate authority

Using a trusted certificate authority provides the highest level of security. To do this, you must install your own certificate by a signed certificate authority for the Webroot Server to use. This certificate authority could be from a third party, such as Thawte or VeriSign, or from within your organization.

To get a certificate signed and imported to the Webroot keystore:

- Open a command line and switch to the following directory: <installdirectory>\Server\WebServer\etc
- 2. Obtain an unsigned certificate using one of the following methods:
  - a Generate a new certificate, as follows:
    - Make a copy of **webroot\_keystore** so that you can restore it, if needed. Remove the existing **webroot\_keystore** file; the Webroot Admin Console Service can only handle one certificate per keystore.
    - Create the new certificate by entering:

```
..\java\bin\keytool.exe -keystore webroot_keystore -storepass
1@sam1AM1AM -keypass 1@sam1AM1AM -alias <full_host_name> -genkey
-keyalg RSA -validity 1825 -dname "CN=<full_host_name>,OU=Webroot
AntiSpyware Corporate Edition,O=Webroot Software\, Inc.,C=US"
```

Where <*full\_host\_name*> is either the host name of the server (such as *myserver.mydomain.com*) or the IP address used to access the Webroot Server. This name or address must be identical to what is used in the URL to access the Webroot Admin Console service (set during Webroot Server installation) to avoid browser security warnings.

You can use any value for OU, O, or C as desired; the above examples are what the Webroot installation uses.

b Use the self-signed certificate already created and stored in the **webroot\_keystore** by the Server installation. You don't need to do anything else.

3. Generate the CSR, as follows:

```
..\java\bin\keytool.exe -certreq -keystore webroot_keystore -storepass
1@sam1AM1AM -storetype JKS -alias <full_host_name> -keypass 1@sam1AM1AM
-keyalg RSA -sigalg MD5withRSA -file webroot.p10
```

The **webroot.p10** file is the CSR. You may need to open it with Notepad and copy its content or provide the file to the CA for signing.

The content of **webroot.p10** will look similar to the following:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
<several lines of letters and numbers (base-64 encoded)>
-----END NEW CERTIFICATE REQUEST-----
```

4. Copy the PKCS#7 response for the CSR (you may get a file or the response on-screen). For example, if the response is in a file called **webroot.p7b**, the content of **webroot.p7b** will look similar to the following:

```
-----BEGIN CERTIFICATE-----
<many lines of letters and numbers (base-64 encoded)>
-----END CERTIFICATE-----
```

5. Import the CA certificate reply to the key-pair entry (in the webroot\_keystore Java keystore file):

```
..\java\bin\keytool.exe -import -keystore webroot_keystore -storepass
1@sam1AM1AM -storetype JKS -alias <full_host_name> -keypass 1@sam1AM1AM
-file webroot.p7b
```

The **webroot\_keystore** will now contain the signed certificate. It corresponds to the host name, as entered.

6. For the new (unsigned or trusted) certificate to take effect, restart the Webroot Admin Console service.