

WEBROOT®

*LabTech
Deployment Instructions
Plugin version 2.5*

For LabTech Versions 10.5 & above


Doc Version 1.0.3



Table of Contents

Overview	2
Requirements.....	2
Webroot Activation.....	3
Plugin Installation	5
Global Site Manager Integration	6
Installation Exclusions	7
To exclude a location from auto deployment	7
To exclude a computer from installation via LabTech	7
Enhanced Settings Dashboard	8
Webroot Global System Dashboard.....	10
Information by Computer/Device.....	11
Webroot Integration at Client Level	13
Client Settings	13
Detail View	14
My Webroot Anywhere	14
Webroot Computer Level Integration	15
Help Buttons at Every Level.....	15
LabTech Health Reports and AV Dashboard Integration	16
Reference	17
Monitors	17
Scripts	17
Troubleshooting.....	19
Omissions.....	19

Overview

With LabTech plugin version 2.5, customisability of the UI has been greatly enhanced to make day-to-day tasks easier. With new monitors to provide time saving out the box options for Webroot customers and usability enhancements throughout. Each tab now features **help** content, accessible by the question mark  symbol and pop-up tool tips have been added wherever it makes sense. For more information and user instructions with new monitors click on [What's New with v2.5](#).

The fundamental benefit of the integration is to provide a single point of interaction, which is the LabTech Control Center, for managing all Webroot related information, including monitoring protection status, threat counts, check-in times, and program versions. The custom dashboard has been built to show Client, Location, and Device-specific information.

Requirements

Webroot plugin version 2.5 is optimised for LabTech version 10.5 and above.

Deploying Webroot plugin version 2.5 to LabTech Control Center version 10.0 or lower may cause unpredictable results.

Please use **Webroot Plugin version 2.0 for LabTech version 10.0 and below**. For version 2.0 plugin please click here:

http://download.webroot.com/RMM/LabTech/Webroot-Deploy-Solution_v2-0.zip

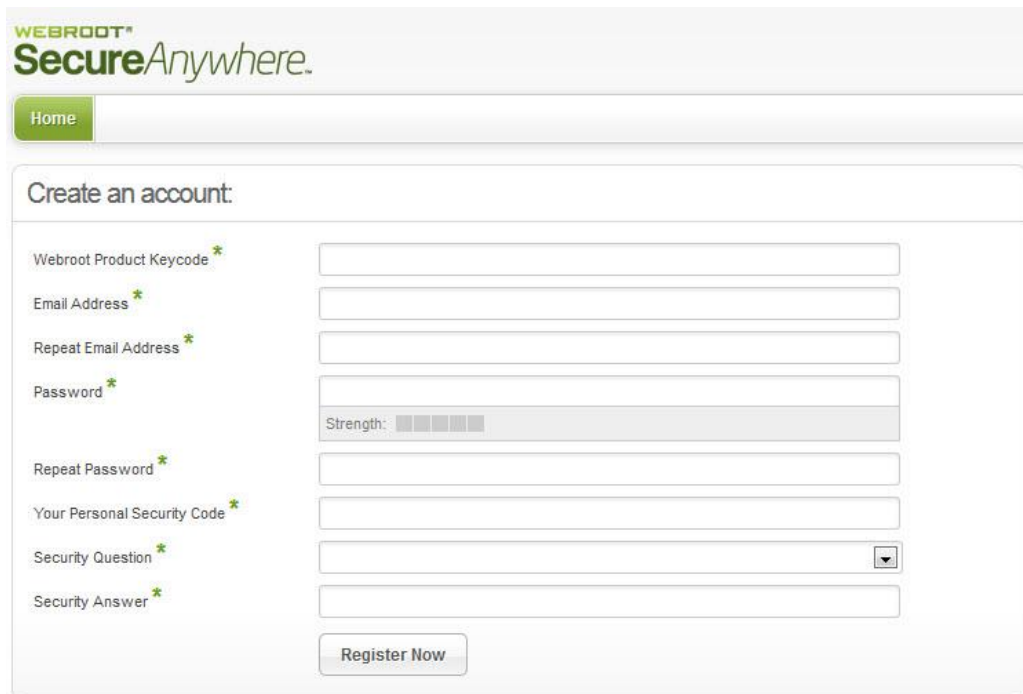
Webroot Activation

In order to seamlessly integrate Webroot with the LabTech Control Center, you first need to activate the Webroot Global Site Manager (GSM) console.

To activate your Webroot cloud management console:

1. In a web browser, enter the following URL:
<https://my.webrootanywhere.com/registration.aspx>

The system displays the Webroot SecureAnywhere Create an account window.

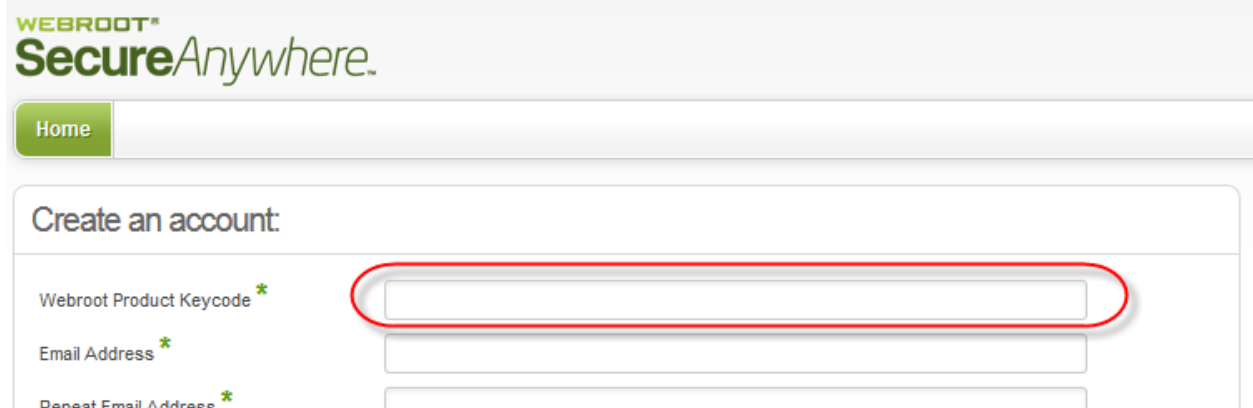


The screenshot shows the Webroot SecureAnywhere registration page. At the top, the Webroot logo and 'SecureAnywhere.' are displayed. Below the logo is a 'Home' button. The main section is titled 'Create an account:' and contains several input fields with asterisks indicating required fields:

- Webroot Product Keycode *
- Email Address *
- Repeat Email Address *
- Password * (includes a strength indicator bar)
- Repeat Password *
- Your Personal Security Code *
- Security Question * (dropdown menu)
- Security Answer *

A 'Register Now' button is located at the bottom of the form.

2. In the Webroot Product Keycode field, enter the 20-digit Webroot keycode.



WEBROOT®
SecureAnywhere.

Home

Create an account:

Webroot Product Keycode *

Email Address *

Repeat Email Address *

Webroot sends you a confirmation email.

3. In the confirmation email, click on the link to validate your email address.
4. Log in to your account and follow the steps in the Setup Wizard to create your endpoint security environment.

Once you have activated your Webroot keycode, you have full access to the management console. There is no server to set up and no definition distribution to worry about. Definitions are stored in the cloud and endpoint agents will access them as needed, performing determination actions when scans or real-time shield activity requires it.

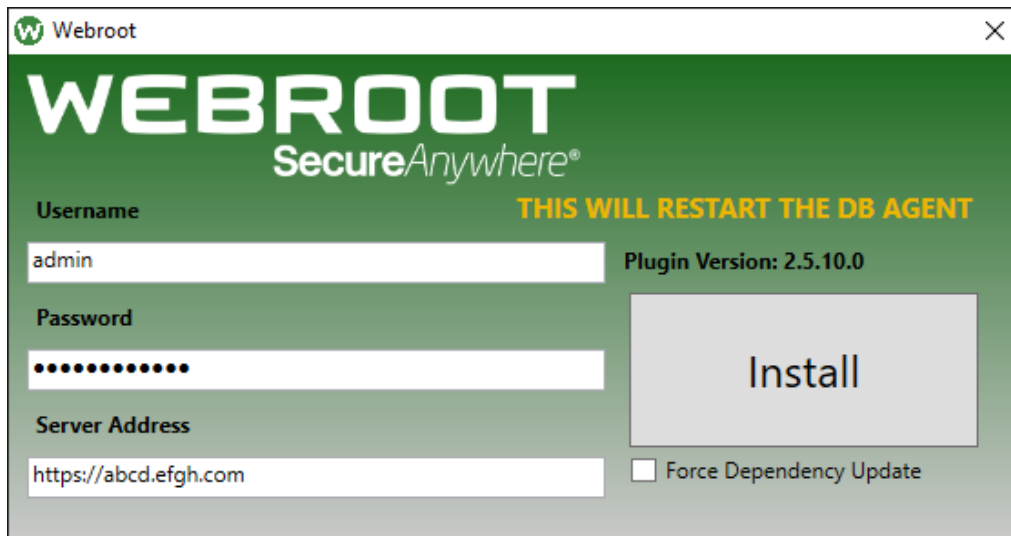
Plugin Installation

You must be a **super admin** to be able to install the program.

To install the plugin:

1. Download **Webroot_LabTech_2.5_Installer.exe** from the following location:
http://download.webroot.com/RMM/LabTech/Webroot-Deploy-Solution_v2-5.zip
2. Double-click the installer package **or If UAC is enabled, run as admin**
3. Enter your **LabTech** admin **Username** and **Password**
4. Leave "Force Dependency Update" checkbox **blank** (used for diagnostics purposes to update all existing plugin dependencies)
5. Click the **Install** button

When updates to the plugin become available, repeat this procedure to update the program.



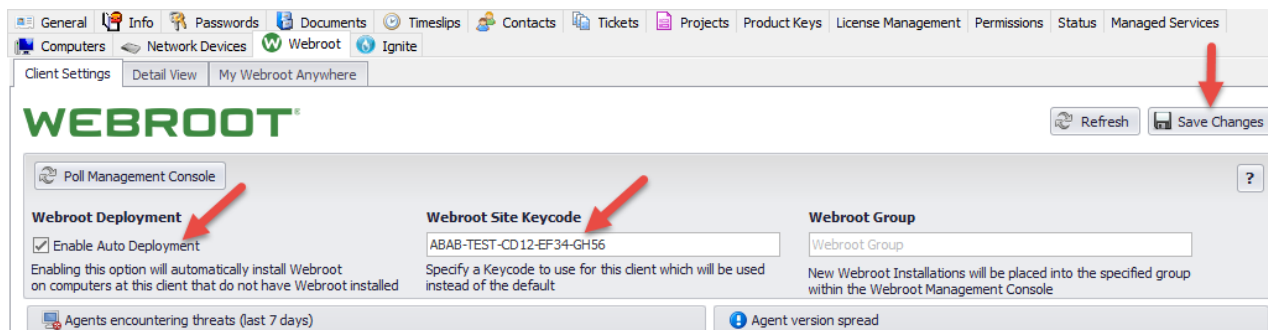
The screenshot shows the Webroot SecureAnywhere LabTech plugin installation window. The window has a green header with the Webroot logo and the text "SecureAnywhere®". Below the header, there are three input fields: "Username" (containing "admin"), "Password" (containing masked characters), and "Server Address" (containing "https://abcd.efgh.com"). To the right of the "Username" field, there is a yellow warning message: "THIS WILL RESTART THE DB AGENT". Below the "Password" field, there is a "Plugin Version: 2.5.10.0" label. To the right of the input fields, there is a large "Install" button. Below the "Install" button, there is a checkbox labeled "Force Dependency Update" which is currently unchecked.

Global Site Manager Integration

The configuration of the Webroot Global Site Manager integration with LabTech is straight-forward and consists of the following steps.

1. From the LabTech Control Center, double-click the desired client.
2. Click the **Webroot** tab.
3. In the **Webroot Keycode** field, enter the site keycode.

Important Note: Always use a site keycode to install WSA agents. Never use the GSM parent keycode.



4. Specifying a **Webroot Group** is optional. Agents will otherwise install to their site Default Group. This is recommended.
5. Agent installation can be automated by clicking **Enable Auto Deployment**. Set [exclusions](#) before enabling auto deployment.

Hint: Agents can be installed individually by right-clicking on each computer and selecting **Scripts > Anti-Virus > Webroot > Install SecureAnywhere**.

6. Click the **Save Changes** button.

Installation Exclusions

Set computer and location exclusions **before enabling auto deployment**.

To exclude a location from auto deployment

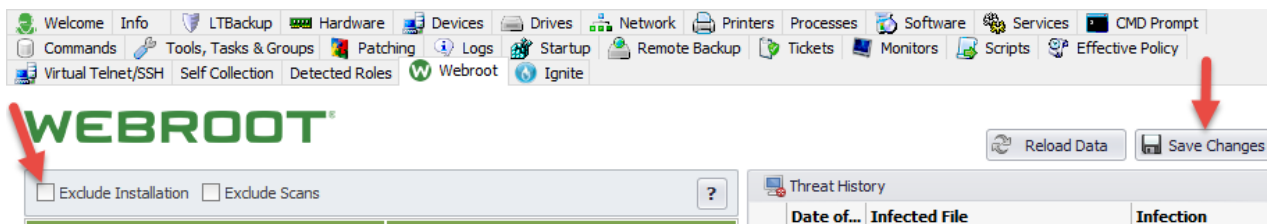
1. Open the location in LabTech.
2. Select the **Exclude Auto Deployment** checkbox.



3. Click **Save Changes**.

To exclude a computer from installation via LabTech

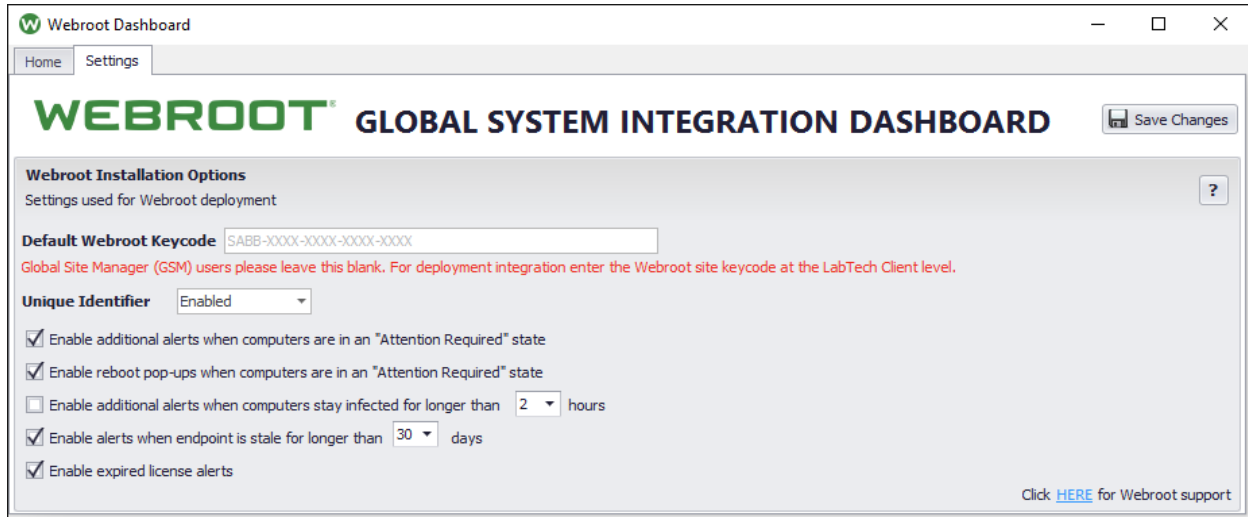
1. Open the computer in LabTech.
2. Select the **Exclude Installation** checkbox.



3. Click **Save Changes**.

Enhanced Settings Dashboard

We recommend you keep the Settings Dashboard at default when first setting up (only Unique Identifier enabled). Once you are familiar with Webroot, you can set up additional alerts to ease day-to-day automation.



The screenshot shows the Webroot Dashboard with the 'Settings' tab selected. The main heading is 'WEBROOT® GLOBAL SYSTEM INTEGRATION DASHBOARD'. Below this is the 'Webroot Installation Options' section, which includes a 'Default Webroot Keycode' field with the value 'SABB-XXXX-XXXX-XXXX-XXXX'. A red note states: 'Global Site Manager (GSM) users please leave this blank. For deployment integration enter the Webroot site keycode at the LabTech Client level.' The 'Unique Identifier' is set to 'Enabled'. There are five checkboxes for additional alerts: 'Enable additional alerts when computers are in an "Attention Required" state' (checked), 'Enable reboot pop-ups when computers are in an "Attention Required" state' (checked), 'Enable additional alerts when computers stay infected for longer than 2 hours' (unchecked), 'Enable alerts when endpoint is stale for longer than 30 days' (checked), and 'Enable expired license alerts' (checked). A 'Save Changes' button is in the top right, and a link to 'Click HERE for Webroot support' is in the bottom right.

Default Webroot Keycode

This keycode entry is only for Webroot customers who use the same Webroot Site key for all LabTech Clients. If you are creating new sites within the Webroot Global Site Manager, site keycodes must be entered at LabTech Client level.

Unique Identifier

When enabled will add a unique string of characters after the computer name in the Webroot web console to help avoid duplicate computer names.

Enable additional alerts when computers are in an "Attention Required" state

When the Webroot agent detects a threat, it will block the threat. Most threats, such as real-time or inactive threats are removed in under 1 minute. Some threats require a clean scan before the endpoint is declared malware free. Sometimes, threats are too deeply embedded in the system to be removed immediately and WSA will require a reboot to clean the infection. After the usual daily scan and reboot, most infections are automatically and safely removed without any intervention.

To keep the malware reporting noise down to a minimum, we have created a new "Attention Required" flag specifically designed for MSP environments. This flag is raised if an endpoint remains infected after 2 contiguous 12 hour checks. If the endpoint is rebooted or performs a scan at the point during any of the checks, the counter will be reset for another 12 hours. In practice, the "Attention Required" flag will be true (1) if the endpoint remains infected after about 36 hours. This ensures the endpoint has gone through at least 1 reboot/scan cycle before raising the "Attention Required" flag. You can choose to take either manual or automatic action if you wish, such as initiating another scan or to inform the end user to reboot. Some actions such as running a cleaning scan, or user reboot request may be automated.

Important Note: The "Attention Required" flag is distinctly different than the "Needs Attention" state in the Webroot Console, which is set as soon as an infection is detected. Each indicator works independently.

Enable reboot pop-ups when computers are in an “Attention Required” state

In some cases for the Webroot agent to fully remediate a persistent threat, or to declare an endpoint free of malware, one or more reboot cycles may be needed. If users do not shutdown their PCs overnight then it could remain infected. Enabling the “reboot pop-up alert” after the “Attention Required” flag is set will ensure a pop-up alert is sent to the end users device at midday, informing the user to reboot.

Enable additional alerts when computers stay infected for longer than xx hours

When a Webroot agent stays infected for longer than the amount of hours defined (2, 8, 12, 24) an additional alert will be triggered via the “Webroot - Active Infection” Internal Monitor. This alert is useful for customers who need to be informed of persistent infections as quickly as possible.

Enable alerts when endpoint is stale for longer than xx days

If a Webroot agent fails to successfully check-in to the Webroot cloud for longer than the days defined (7, 15, 30, 60, 90) an alert will be triggered via the “Webroot - Stale Agents” Internal Monitor.

Enable expired license alerts

When a Webroot agent’s license expires it will trigger an alert via the “Webroot - License Expired” Internal Monitor.

Webroot Global System Dashboard

The integration provides a custom Webroot dashboard that presents computer information from all clients and locations in one screen. This information is based on registry values on these machines and is updated once every 60 minutes. The information can also be updated on demand by selecting **Resend System Info** from the computer's Inventory menu.

The screenshot shows the Webroot Global System Integration Dashboard. It features a table with columns: Client, Computer, Agent Version, Attention Required, Realtime Shield, Infected, Remediation Enabled, Active Threat Count, Last Scan, and Last Seen. The 'Attention Required' column has a dropdown menu. The 'Infected' and 'Remediation Enabled' columns are highlighted in red for rows where the status is 'Yes' or 'No' respectively. The 'Active Threat Count' column shows values like 2, 0, 0, 0, 0, 0, 0, 0. The 'Last Scan' and 'Last Seen' columns show dates. At the bottom, there is a 'Total Displayed : 0' and buttons for 'Export for Excel' and 'Refresh'.

Client	Computer	Agent Version	Attention Required	Realtime Shield	Infected	Remediation Enabled	Active Threat Count	Last Scan	Last Seen
Tri-County Manufacturing	WRDEMOEP05	9.0.8.66	Yes	Enabled	Yes	No	2	26/02/2016	02/03/2016
Test Customer	WR-VM-WINDOWS7	9.0.8.66	No	Enabled	Yes	No	0	24/02/2016	26/02/2016
Test Customer	WR-VM-WINDOWS10	9.0.8.66	No	Enabled	Yes	No	0	23/02/2016	26/02/2016
Tri-County Manufacturing	WRDEMOSVR01	9.0.8.66	No	Enabled	No	Yes	0	18/02/2016	02/03/2016
Tri-County Manufacturing	WRDEMOC01	9.0.8.66	No	Enabled	No	Yes	0	18/02/2016	02/03/2016
Tri-County Manufacturing	WRDEMOEP04	9.0.8.66	No	Enabled	No	Yes	0	18/02/2016	01/03/2016
Tri-County Manufacturing	WRDEMOEP03	9.0.8.66	No	Enabled	No	Yes	0	18/02/2016	02/03/2016
Tri-County Manufacturing	WRDEMOEP01	9.0.7.46	No	Enabled	No	Yes	0	24/02/2016	02/03/2016

If issues are detected, selected fields will change to red.

The screenshot shows the 'Attention Required' dropdown menu. It has a header 'Attention Required' and a sub-header 'Realtime Shield'. The menu is open, showing options: 'Yes', 'No', 'No', 'No'. A context menu is visible over the 'No' options, with options: 'Open Client', 'Open Location', 'Open Computer'.

Attention Required	Realtime Shield
Yes	Enabled
No	
No	
No	

Each cell is interactive and can take you to Client, Location or PC level for ease of management.

Columns are fully customizable and you can select just the columns you need to run your day to day operations. Each change is saved and if the application or the window is closed all settings will remain as saved (except sorting).

The screenshot shows the 'Column Chooser' menu. It has a header 'Attention Required' and a sub-header 'Realtime Shield'. The menu is open, showing options: 'Sort Ascending', 'Sort Descending', 'Clear Sorting', 'Group By This Column', 'Show Group By Box', 'Remove This Column', 'Column Chooser', 'Best Fit', 'Best Fit (all columns)', 'Filter Editor...', 'Show Find Panel', 'Show Auto Filter Row'.

Attention Required	Realtime Shield
Yes	Enabled
No	
No	
No	
No	
No	
No	
No	

The screenshot shows the 'Customization' dialog box. It has a title bar 'Customization' and a list of fields: 'Expire Date', 'Expired', 'Last Deep Scan', 'Local Address', 'Location', 'Managed', 'Router Address'. A green arrow points from the 'Managed' field in the table below to the 'Managed' field in the dialog box.

mediation Enabled	Active Threat Count	Last Scan	Last Seen
No	2	26/02/2016	02/03/2016
Managed	0	24/02/2016	26/02/2016
No	0	23/02/2016	26/02/2016
Yes			
Yes			
Yes			
Yes			

Additional columns can be added from the **Column Chooser** menu – right click to activate.

The fields in the screenshots below represent the default view; you remove and add fields by right-clicking on the column header and clicking on **Column Chooser**.

Information by Computer/Device

The screenshot shows the Webroot Dashboard with a table of client information. The table has columns for Client, Location, Computer, Version, Attention Required, Realtime Shield, Infected, Managed, Remediation Enabled, Active Threat Count, Total Threats Removed, Last Scan, Last Seen, Signature Up, Expire Date, Scheduled Scan, Scheduled Scan Date, Secondary Address, Local Address, and Router Address. The table contains two rows of data for 'Test Client #1'.

Client	Location	Computer	Version	Attention Req.	Realtime S.	Infected	Managed	Remediation En.	Active Threat	Total Threats Re.	Last Scan	Last Seen	Signature Up	Expire D.	Scheduled	Scheduled Scan	Secondary	Local Add.	Router Addr.
Test Client #1		Test	8.0.4...	No	Enabled	No	Yes	Yes	0	0	5/19/2014 1...	5/19/2014 11:0...	5/19/2014 11:0...	No	6/10/2014	Enabled	10:00	None	192.168.12...
Test ...		Test	8.0.4...	No	Enabled	No	No	Yes	0	1	5/5/2014 10:...	5/16/2014 11:5...	5/19/2014 11:5...	No	9/27/2014	Enabled	10:00	None	192.168.15...

Data	Description
Client	Name of client associated with the agent/device.
Location	Name of the location with the agent/device.
Computer	Name of device where agent is installed.
Version	Version of Webroot SecureAnywhere that is installed on that device.
Attention Required	<p>To keep the malware reporting noise down to a minimum, we have created a new "Attention Required" flag specifically designed for MSP environments. This flag is raised if an endpoint remains infected after 2 contiguous 12 hour checks. If the endpoint is rebooted or performs a scan at the point during any of the checks, the counter will be reset for another 12 hours. In practice, the "Attention Required" flag will be true (1) if the endpoint remains infected after about 36 hours. This ensures the endpoint has gone through at least 1 reboot/scan cycle before raising the Attention Required flag.</p> <p>Important Note: The Attention Required flag is distinctly different than the "Needs Attention" state in the Webroot Console, which is set as soon as an infection is detected. Each indicator works independently.</p>
Realtime Shield	<p>Status of realtime shield:</p> <ul style="list-style-type: none"> Enabled Disabled
Infected	<p>Identifies whether the remote system has an active infection.</p> <p>Note: Infectins are blocked once detected</p>
Managed	Identifies whether the remote agent is managed via a Webroot policy.
Remediation Enabled	Identifies whether auto remediation is enabled on the remote agent.
Active Threat Count	Number of active threats detected, blocked but not yet remediated on the device.
Total threats Removed	Total number of threats that have been removed from the remote agent via Webroot.
Last Scan	Last scan date of the device.
Last Seen	Last time the Webroot agent reported into the cloud.

Data	Description
Signature Updated	Webroot does not use definition signatures. This value instead represents the date/time the agent last requested threat determination data.
Expired	Identifies whether the remote agent's Webroot license has expired.
Expire Date	Based on licensing information, the date when coverage will expire unless licenses are updated/renewed.
Scheduled Scan	Identifies whether any scans are scheduled via the Webroot console.
Scheduled Scan Time	Displays the time the next scheduled scan will be performed.
Secondary AV	Identifies whether there is another anti virus program, other than Webroot, installed on the remote system.
Local Address	Internal IP of remote system.
Router Address	External IP of remote system.

Webroot Integration at Client Level

Client level integration have 3 separate tabs.

- 1- **Client Settings** – Client level settings
- 2- **Detailed View** – Computer information from all clients in one screen
- 3- **My Webroot Anywhere** – Integrated access to Webroot Consoles

Client Settings

The Webroot Client settings allows you to set up a tight integration between Webroot Sites and LabTech Clients.

(ClientID: 1)

General Info Passwords Documents Timeslips Contacts Tickets Projects Product Keys License Management Permissions Status

Managed Services Computers Network Devices Webroot Ignite Standards & Health

Client Settings Detail View My Webroot Anywhere

WEBROOT® Refresh Save Changes

Poll Management Console

Webroot Deployment

☒ Enable Auto Deployment

Enabling this option will automatically install Webroot on computers at this client that do not have Webroot installed

Webroot Site Keycode

Specify a Keycode to use for this client which will be used instead of the default

Webroot Group

New Webroot Installations will be placed into the specified group

Webroot Group

This field is case-sensitive, be sure that the value is identical to the Group Name you created in the Webroot Management Console.

* This field cannot contain spaces.

Agents encountering threats (last 7 days)

10 9 8 7 6 5 4 3 2 1 0

26 February 27 February 28 February 29 February 01 March 02 March 03 March

1 1

Agent version sp

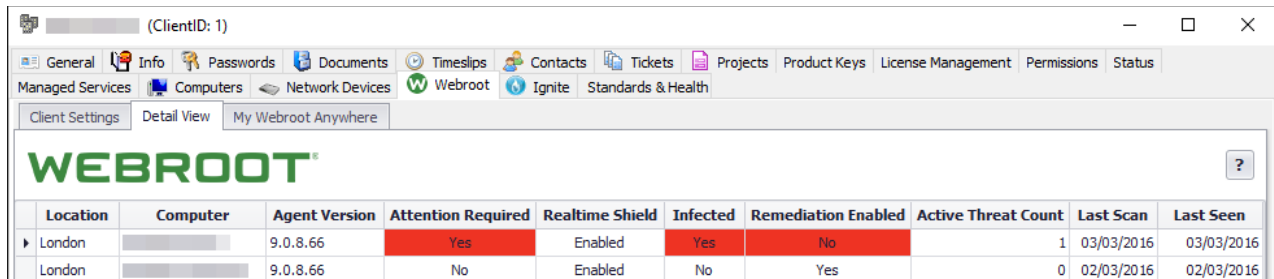
100% (5)

9.0.8.66

Print Client Report Refresh Cancel Save

Detail View

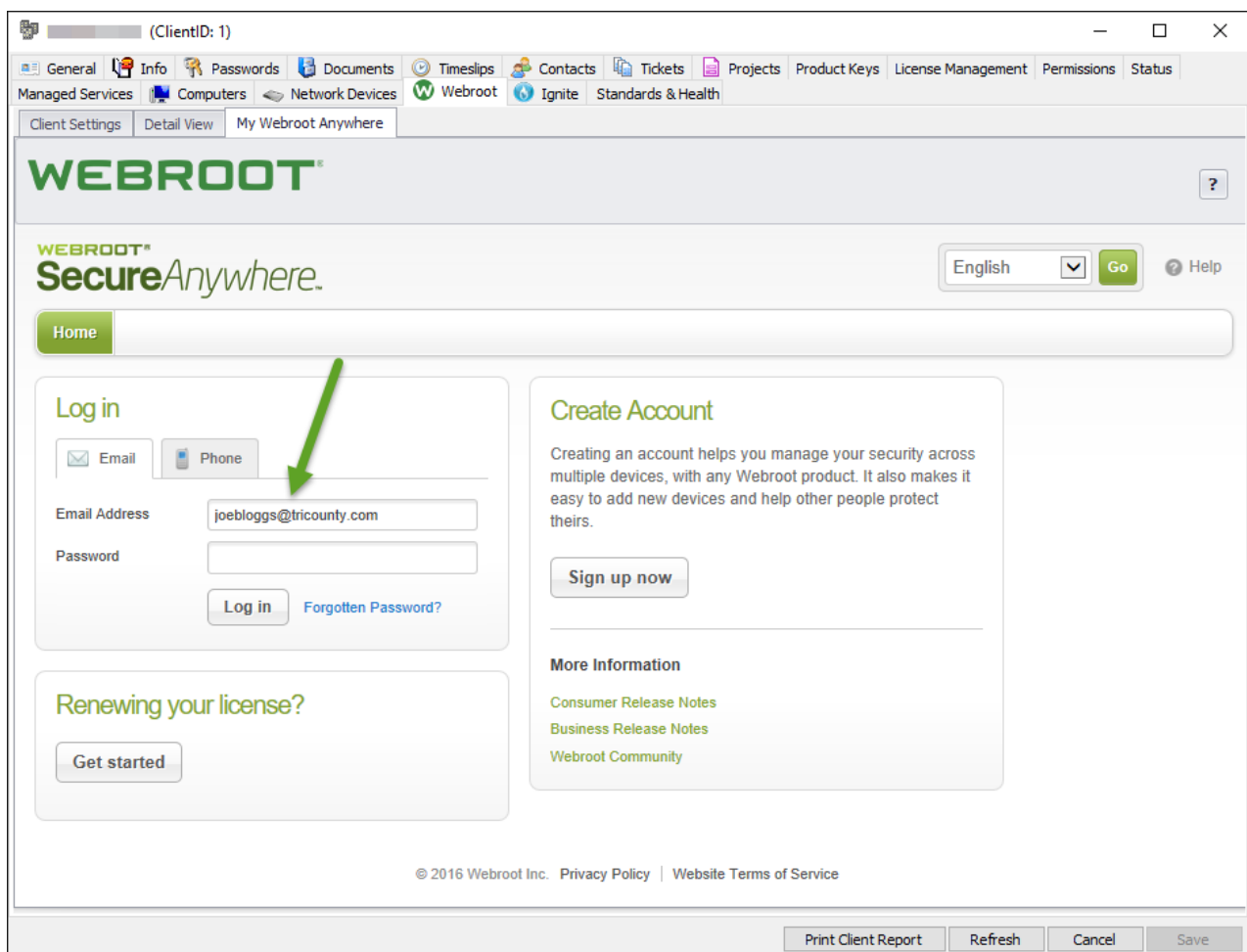
The Detail View site level allows Computer information from all clients in one screen. The Columbus and fields are fully customisable, allowing you to set all the data columns your own way and the set up can be saved.



Location	Computer	Agent Version	Attention Required	Realtime Shield	Infected	Remediation Enabled	Active Threat Count	Last Scan	Last Seen
London		9.0.8.66	Yes	Enabled	Yes	No	1	03/03/2016	03/03/2016
London		9.0.8.66	No	Enabled	No	Yes	0	02/03/2016	02/03/2016

My Webroot Anywhere

The Webroot Console is easy to access then before. The email address of the logged-in LabTech user is automatically passed to the integrated Webroot Console viewer.



© 2016 Webroot Inc. [Privacy Policy](#) | [Website Terms of Service](#)

Webroot Computer Level Integration

The Webroot Computer Level integration provides computer specific settings, Webroot Agent Commands and Threat History. You can see if the computer is infected by the color of the Webroot icon. Actions can be taken manually. With version 2.5 we have added a new "Run Customer Support Diagnostics" button, which downloads wsablogs.exe at the endpoint and automatically sends detailed computer logs to Webroot for further analysis.

The screenshot shows the Webroot interface with the following sections:

- Protection Status:**
 - Phishing Shield: Enabled
 - Identity Shield: Disabled
 - Web Threat Shield: Disabled
 - USB Shield: Enabled
 - Offline Shield: Disabled
 - Rootkit Shield: Enabled
- Agent Information:**
 - Engine Version: 9.0.8.66
 - Signature Update: 02/03/2016 06:37:19
 - Expiration Date: 01/01/2018
 - Days Remaining: 671
 - Silent Install: False
- Agent Commands:**
 - Run Customer Support Diagnostics (highlighted with a green arrow)
- Scan Statistics:**
 - Last Scan: 26/02/2016 14:56:12
 - Last Scan Duration: 93
 - Files Scanned: 29759
 - Scheduled Scan Enabled: True
 - Scheduled Scan Time: 04:00
 - Active Threat Count: 2
 - Total Scans: 243
 - Total Threats Removed: 0
- Threat History:**

Date of Infection	Infected File	Infection
26/02/2016 19:57:44	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
26/02/2016 19:57:44	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
21/01/2016 16:08:05	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
21/01/2016 16:08:05	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
14/01/2016 16:07:54	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
14/01/2016 16:07:54	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
13/01/2016 16:07:49	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
13/01/2016 16:07:49	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
05/01/2016 21:29:19	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
05/01/2016 21:29:18	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
24/12/2015 16:07:55	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
24/12/2015 16:07:55	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
22/12/2015 22:33:51	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
22/12/2015 22:33:51	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
19/12/2015 16:07:55	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
19/12/2015 16:07:55	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
20/11/2015 16:31:04	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
06/11/2015 16:07:54	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
06/11/2015 16:07:54	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
23/10/2015 17:07:45	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
23/10/2015 17:07:45	c:\test\malware\webroottestfile.exe	W32.Webroottestfile
30/09/2015 17:08:01	c:\users\demouser_05\downloads\webroottestfile.exe	W32.Webroottestfile
30/09/2015 17:08:01	c:\test\malware\webroottestfile.exe	W32.Webroottestfile

Help Buttons at Every Level

We have added help buttons at every tab that explains each function at every level. Just click on the question mark icon to open up the help content.

The close-up shows the following help buttons:

- A green arrow points to a question mark icon in the top right corner of the "Last Scan" and "Last Seen" table.
- A green arrow points to a question mark icon in the top right corner of the "Protection Status" and "Agent Information" section.
- A green arrow points to a question mark icon in the top right corner of the "Threat History" section.

LabTech Health Reports and AV Dashboard Integration

We have integrated the total number of scans performed in the LabTech Health reports. Each of the scan scripts have had the script stat "VirusScanRunStat" record in each run.

Service Statistics	
Alerts Issued:	0
Scripted Services	
Total Antivirus Scans:	1,055
Total Spyware Scans:	0
Disk Cleanup Performed:	0
Backup Success/Fail:	0 / 0
System Activities	
Remote Sessions:	0
Tunneled Sessions:	1
Files Transferred:	1,201
Executables Ran:	0
Other Commands:	6,374
Total Commands:	7,576

NOTE: Only the scans run by the LT based scripts are counted. Normal WSAB daily scans are not included.

In addition, we have integrated "Last Threat Found" and "Action Taken" results in the LabTech AV Dashboard. Stats are recorded to the inherent "virus tables" in LabTech.

This is additional to recording the stats on the Webroot custom plugin tables.

Antivirus Dashboard						
Icon	Virus Scanner	Computer Name	Scanner Status	Virus Definitions	Last Threat Found	Action Taken
	Webroot SecureAnywhere 64bit		Running	03/03/2016	c:\windows\leicar.com	Processed By Plugin
	Webroot SecureAnywhere 64bit		Running	03/03/2016	None Found	None Found
	None Found		Not Running	None Found	None Found	None Found

Reference

The following is a list of relevant monitors and scripts that have been developed for the integration and their description/intended purpose.

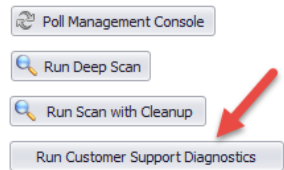
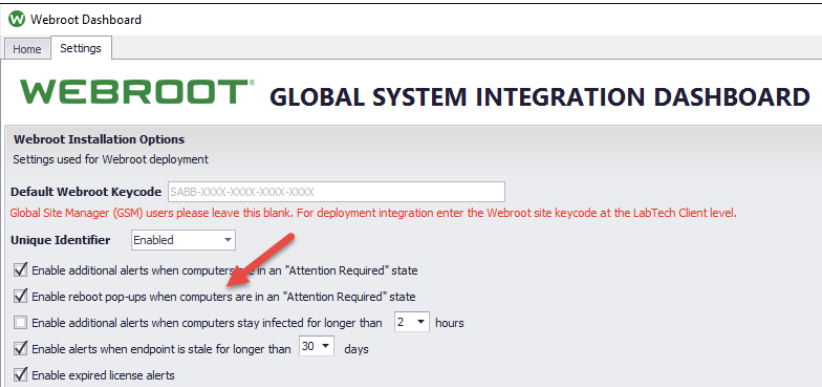
Monitors

There are 6 customizable monitors to ease day-to-day automation:

- 1- **Active Treats** - Checks the registry value for active threat status and alerts if there is an active threat. There are 32 and 64 bit versions of this monitor
- 2- **Attention Required** - Checks the registry value for attention required status and alerts if attention is required (see [Enhanced Settings Dashboard](#) for further information)
- 3- **Reboot Needed** - Checks the registry value for attention required status and triggers a reboot needed alert at the customers computer (see [Enhanced Settings Dashboard](#) for further information)
- 4- **Active Infection** - Checks the registry value for active threat status and alerts if the infection has been active for a certain number of hours (see [Enhanced Settings Dashboard](#) for further information)
- 5- **Stale Agents** - Checks the registry value for update time status and alerts if the agent has not checked into the Webroot for a certain number of days (see [Enhanced Settings Dashboard](#) for further information)
- 6- **License Expired** - Checks the registry value for Is Expired status and alerts if the agent license has expired (see [Enhanced Settings Dashboard](#) for further information)

Scripts

Script	Description
Webroot – Trigger Deep Scan	Triggers a deep scan once the agent polls the registry for updates.
Webroot – Trigger Full Scan	Triggers a full scan once the agent polls the registry for updates.
Webroot – Trigger Scan with Cleanup	Triggers a scan with cleanup by setting the RunCleanupNow registry key. The next time the agent checks in, scan/cleanup will commence.

Script	Description
Install Webroot SecureAnywhere	<p>Installs the Webroot agent on a machine.</p> <ul style="list-style-type: none"> If the Webroot Group client has been populated by the user and saved, the agent installs under that group in the Webroot, rather than the LabTech, group structure. If the EDF is blank, SecureAnywhere installs under the default group. <p>Note: The group name must be typed in exactly as it appears in the Webroot groups and cannot contain any spaces or certain special characters. You can also enter the Group ID which can be found in the Webroot Site Console.</p>
Uninstall Webroot SecureAnywhere	Uninstalls the Webroot Agent.
Customer Support Diagnostics	<p>Designed to run in conjunction with the Run Customer Support Diagnostics button at computer level. <u>Do not run on its own!</u></p> <div> <p>Agent Commands</p>  </div>
Reboot Needed	<p>Designed to run in conjunction with the new "Enable reboot pop-ups when computers are in an "Attention Required" state.</p> <div>  </div>

Troubleshooting

For a previous Webroot agent deployment prior to installing LabTech, the Webroot agents should be picked up automatically. If they are not, update their status using the following steps.

To troubleshoot:

1. Use the right-click menu from client, location, or computer hierarchies.
2. For affected endpoints, do both of the following.
 - Select **Commands > LabTech**, then click **Update Plugins**.
 - Select **Commands > Inventory**, then click **Resend System Info**.

Omissions

We have taken every care to keep the information within this document as accurate as possible, however omissions or inaccuracies can occur. If you spot any, please report it to your Webroot representative.
