

WEBROOT®

What's New LabTech plugin V2.5

For LabTech Version 10.5 and above
Document Version 2.0.2



Table of Contents

Introduction2

Installation & Compatibility2

Relocated Webroot Settings Dashboard2

New Enhanced Settings Dashboard.....3

 Default Webroot Keycode3

 Unique Identifier3

 Enable additional alerts when computers are in an "Attention Required" state3

 Enable reboot pop-ups when computers are in an "Attention Required" state4

 Enable additional alerts when computers stay infected for longer than xx hours4

 Enable alerts when endpoint is stale for longer than xx days4

 Enable expired license alerts.....4

New Enhanced Interactive Home Dashboard5

Webroot Client level changes6

 Client Settings6

 Detail View.....7

 My Webroot Anywhere7

Webroot Computer level changes8

Other Miscellaneous Changes8

 Help Content8


 LabTech Health Reports and AV Dashboard Integration.....9

 Additional Monitors.....10

 Additional Scripts11

Omissions.....11

Introduction

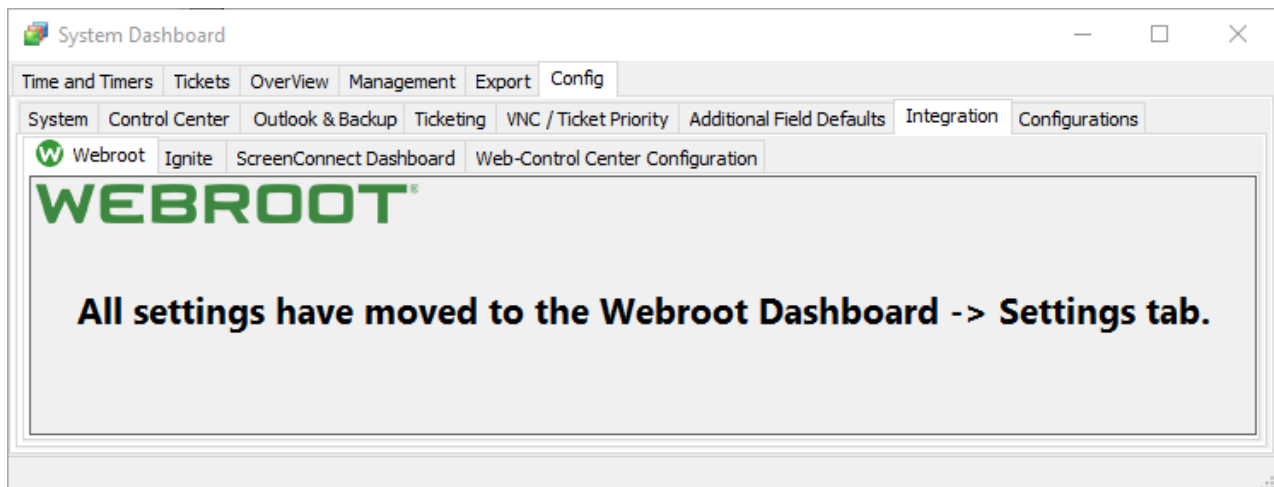
With LabTech plugin version 2.5, customisability of the UI has been greatly enhanced to make day-to-day tasks easier. With new monitors to provide time saving out the box options for our customers and usability enhancements throughout. Each tab now features **help** content, accessible by the question mark  symbol and pop-up tool tips have been added wherever it makes sense.

Installation & Compatibility

Version 2.5 of the plugin is designed for **LabTech Control Centre 10.5 and above**. When upgrading or installing for the first time, please use the installer provided (do not use the DLL). This ensures all the right additional components are loaded to support the enhanced user interface.

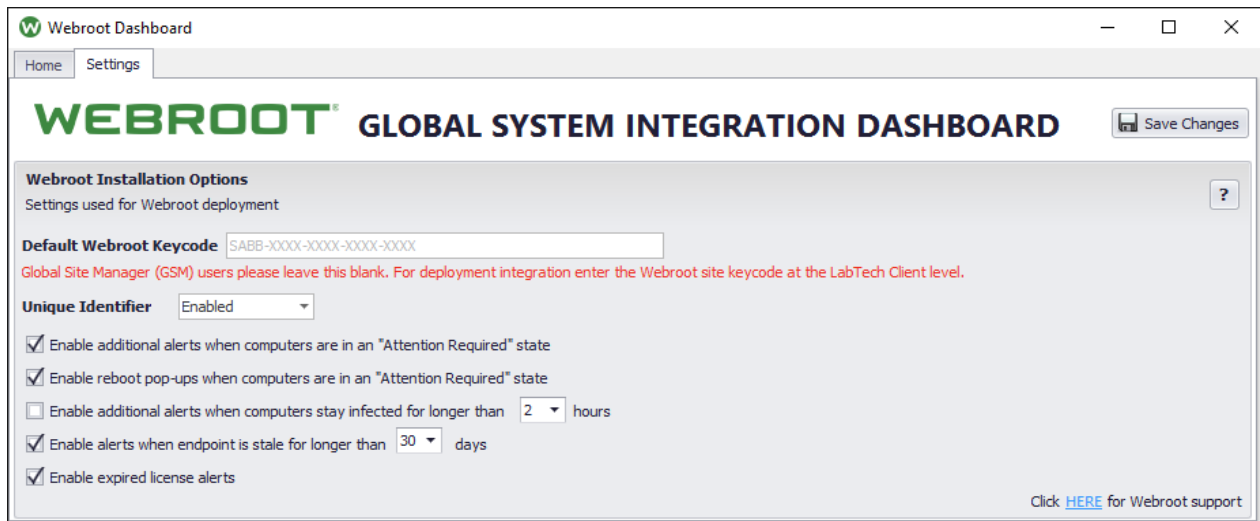
Relocated Webroot Settings Dashboard

To make navigation simpler, we have relocated the Settings Dashboard to a new location inside the Global System Integration Dashboard, easily accessible by clicking on the Webroot icon in the main LabTech navigation bar, located on the top of the main screen.



New Enhanced Settings Dashboard

The new home for the Settings tab! We have added a number of new alerts to help our customers manage and automate their environments right out the box.



The screenshot shows the Webroot Dashboard 'Settings' tab. The title is 'WEBROOT GLOBAL SYSTEM INTEGRATION DASHBOARD'. Below the title is a 'Save Changes' button. The main section is 'Webroot Installation Options' with a subtitle 'Settings used for Webroot deployment'. It includes a 'Default Webroot Keycode' field with the value 'SABB-XXXX-XXXX-XXXX-XXXX' and a red note: 'Global Site Manager (GSM) users please leave this blank. For deployment integration enter the Webroot site keycode at the LabTech Client level.' Below this is a 'Unique Identifier' dropdown set to 'Enabled'. There are five checkboxes: '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' (unchecked, with a dropdown set to '2' hours), 'Enable alerts when endpoint is stale for longer than' (checked, with a dropdown set to '30' days), and 'Enable expired license alerts' (checked). A link at the bottom right says 'Click [HERE](#) for Webroot support'.

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. The MSP can choose to take either manual or automatic action if they 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.

New Enhanced Interactive Home Dashboard

Have it the way you want! The new **Home** dashboard brings in customization of the main display. This is the first of a series of planned enhancements to ease everyday use of the plugin.

Webroot Dashboard

Home Settings

WEBROOT® GLOBAL SYSTEM INTEGRATION DASHBOARD

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	WRDEMODC01	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

Total Displayed : 0

Export for Excel Refresh

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

Attention Required	Realtime Shield
Yes	Enabled
No	
No	
No	

Open Client
Open Location
Open Computer

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).

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

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			
Yes			

Customization

- Expire Date
- Expired
- Last Deep Scan
- Local Address
- Location
- Managed
- Router Address

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

Webroot Client level changes

All client level tabs have been updated, these are listed below.

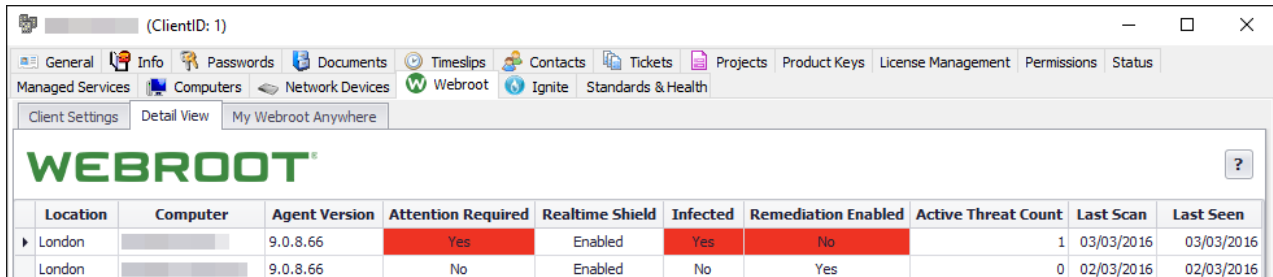
Client Settings

The Webroot Client setting have an updated layout, updated tooltips, new help screen and updated wording for clarity. The Optional Webroot Group setting has been moved off to the right.

The screenshot displays the Webroot Client Settings window for ClientID: 1. The interface includes a top navigation bar with tabs for General, Info, Passwords, Documents, Timeslips, Contacts, Tickets, Projects, Product Keys, License Management, Permissions, and Status. Below this is a sub-navigation bar with Managed Services, Computers, Network Devices, Webroot, Ignite, and Standards & Health. The main content area is titled 'Client Settings' and includes a 'Detail View' tab and a 'My Webroot Anywhere' link. The Webroot logo is prominently displayed at the top left of the main content area, with 'Refresh' and 'Save Changes' buttons to its right. The 'Poll Management Console' section contains three main configuration areas: 'Webroot Deployment' with a checked 'Enable Auto Deployment' option, 'Webroot Site Keycode' with a text input field, and 'Webroot Group' with a dropdown menu. A tooltip for the 'Webroot Group' field explains that the value is case-sensitive and cannot contain spaces. Below these settings are two charts: 'Agents encountering threats (last 7 days)' showing a bar chart with two red bars of height 1 on February 27 and March 3, and 'Agent version sp' showing a donut chart at 100% (5) with a version number of 9.0.8.66. At the bottom of the window are buttons for 'Print Client Report', 'Refresh', 'Cancel', and 'Save'.

Detail View

The new detailed view site level dashboard brings in customization of the main display, allowing you to set all the data columns your own way.



(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

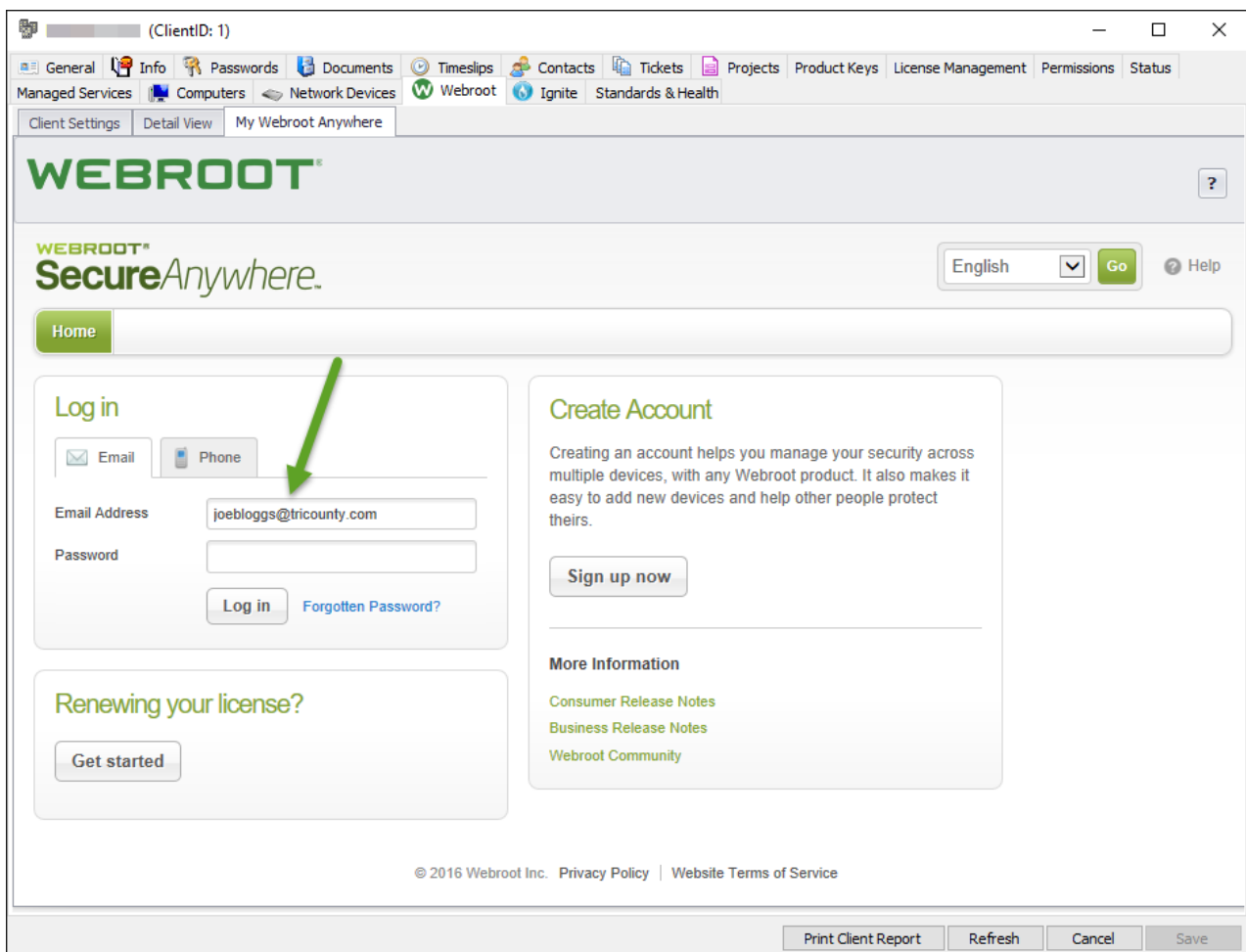
Client Settings Detail View My Webroot Anywhere

WEBROOT®

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



(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®

WEBROOT® SecureAnywhere.

English Go Help

Home

Log in

Email Phone

Email Address:

Password:

Log in Forgotten Password?

Create Account

Creating an account helps you manage your security across multiple devices, with any Webroot product. It also makes it easy to add new devices and help other people protect theirs.

Sign up now

Renewing your license?

Get started

More Information

Consumer Release Notes

Business Release Notes

Webroot Community

© 2016 Webroot Inc. Privacy Policy Website Terms of Service

Print Client Report Refresh Cancel Save

Webroot Computer level changes

We have added a new command button and changed the layout and the wording of the display for ease of use. The new "Run Customer Support Diagnostics" button will run a script against the remote agent, which will download the wsablogs.exe file from Webroot and run it on the remote computer using the logged-in LabTech user's email address as the ID.

The screenshot shows the Webroot interface within a LabTech environment. The 'Run Customer Support Diagnostics' button is highlighted with a green arrow. The interface includes sections for Protection Status, Agent Information, Agent Commands, and Scan Statistics. The Threat History table is also visible.

Protection Status	Agent Information
Phishing Shield: Enabled	Engine Version: 9.0.8.66
Identity Shield: Disabled	Signature Update: 02/03/2016 06:37:19
Web Threat Shield: Disabled	Expiration Date: 01/01/2018
USB Shield: Enabled	Days Remaining: 671
Offline Shield: Disabled	Silent Install: False
Rootkit Shield: Enabled	

Agent Commands	Scan Statistics
Run Customer Support Diagnostics	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

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
20/11/2015 16:31:04	c:\test malware\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

Other Miscellaneous Changes

Help Content

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 screenshot shows the LabTech interface with a green arrow pointing to the question mark icon in the top right corner of the main content area. The interface includes sections for Protection Status, Agent Information, and Threat History.

Last Scan	Last Seen
1 06/03/2016	06/03/2016
0 02/03/2016	02/03/2016

Protection Status	Agent Information
Phishing Shield: Enabled	Engine Version: 9.0.8.72
Identity Shield: Disabled	Signature Update: 02/03/2016 19:45:37

Date of Infection
04/03/2016 19:...
03/03/2016 18:...
21/02/2016 10:...

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:	7,578

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

Additional Monitors

We have added 5 new customizable monitors to ease day-to-day automation:

- 1- Attention Required
- 2- Reboot Needed
- 3- Active Infection
- 4- Stale Agents
- 5- License Expired

Remote Agent Monitors Remote Network Monitors System Monitors Locations Internal Monitors						
No Filter		Search	Clear	Options		
Monitor Name	Monitor Status	Monitor Duration	Monitor Scan Date	Monitor Next Scan	Alert Template Name	Alert Template Comment
Webroot - Stale Agents	No Problems	Every Hour	06/03/2016 19:40:33	06/03/2016 20:40:33	Default - Create LT Ticket	Creates a LabTech Ticket for action
Webroot - Reboot Needed	Detected	Every Hour	06/03/2016 19:40:33	06/03/2016 20:40:33	Webroot - Reboot	
Webroot - Not Installed	No Problems	Every 5 Minutes	06/03/2016 20:32:52	06/03/2016 20:37:52	Webroot - Install Agent	
Webroot - Needs Attention	Detected	Every Hour	06/03/2016 19:40:33	06/03/2016 20:40:33	Default - Create LT Ticket	Creates a LabTech Ticket for action
Webroot - License Expired	No Problems	Every Hour	06/03/2016 19:40:33	06/03/2016 20:40:33	Default - Create LT Ticket	Creates a LabTech Ticket for action
Webroot - Active Infection	No Problems	Every Hour	06/03/2016 19:40:33	06/03/2016 20:40:33	Webroot - Active Threat	

Webroot - Active Infection (61006)

Status

Configuration

Monitor Target

Alerting

Exclusions

History

Query Results

Internal Monitor Information

Monitor Name

Webroot - Active Infection

Interval and Next Run Time

Every Hour

20:40:33

Monitor Mode and Duplicate Alert Frequency

Send Fail After Success

Check Condition

Table to Check

Computers

Field to Check

ComputerID

Check Condition

GreaterThan

Result

0

Identity Field

computers.name

Additional Condition

computers.OS like '%Windows%' AND computers.ComputerID IN (SELECT DISTINCT computerid FROM Computers LEFT JOIN plugin_webroot_threats t USING (computerid) WHERE t.ActiveThreat = 1 AND t.InfectionDate < (SELECT DATE_SUB(NOW(), INTERVAL (SELECT stayinfectedtime FROM plugin_webroot_globalsettings) HOUR))) AND (SELECT stayinfectedenabled FROM plugin_webroot_globalsettings) = '1'

Monitor will send Success Messages when results are no longer detected.

Do not use Date\Time limiting SQL as this will skew results.

Build and View Query

Reset Monitor

Refresh

Export

Save

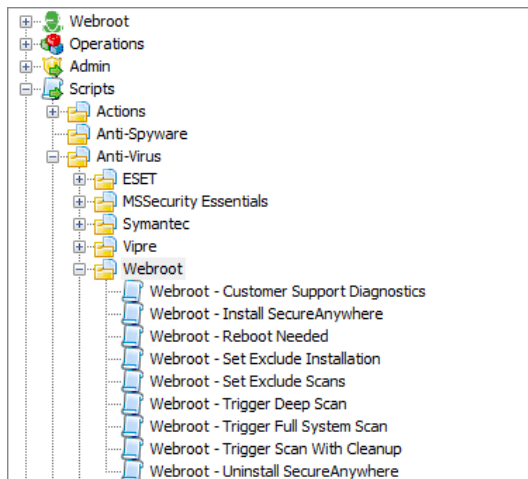
Close

Additional Scripts

We have added 2 new customizable scripts to ease day-to-day automation:

- 1- Customer Support Diagnostics
- 2- Reboot Needed

NOTE: The new monitors are only designed to be used in conjunction with the "Run Customer Support Diagnostics" button and "Reboot Needed" monitor, and not on their own.



Omissions

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