WEBROOT®

What's New
LabTech plugin V2.5

For LabTech Version 10.5 and above
Document Version 2.0.2

Table of Contents

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.
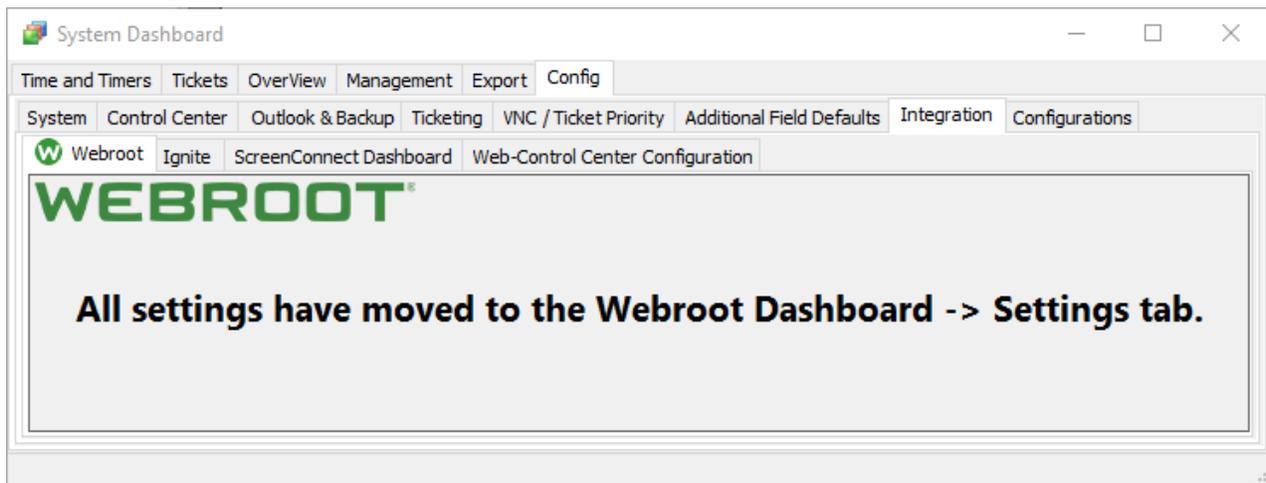
New Enhanced Settings Dashboard

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.
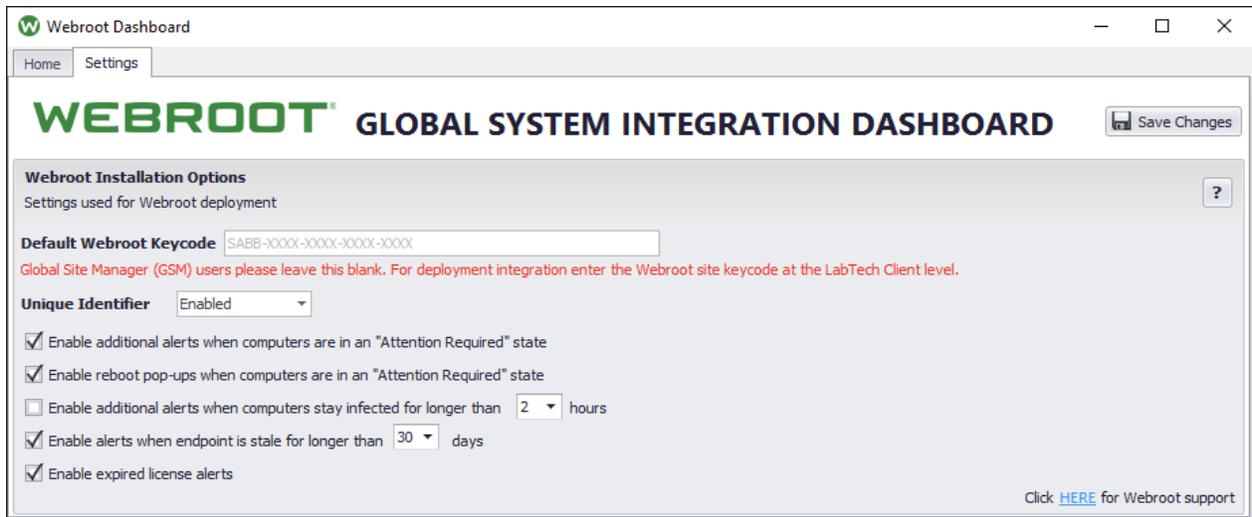
Default Webroot Keycode

This keycode entry is only for Webroot customers who use the <u>same</u> Webroot Site key for <u>all</u> 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.

If issues are detected, selected fields will change to red.
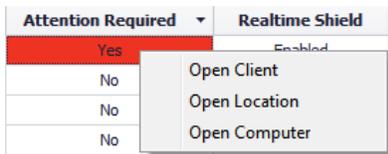
Each cell is interactive and can take you to Client, Location or PC level for ease of management.

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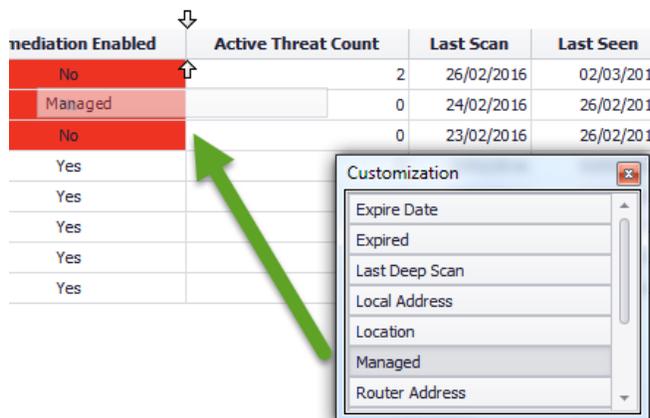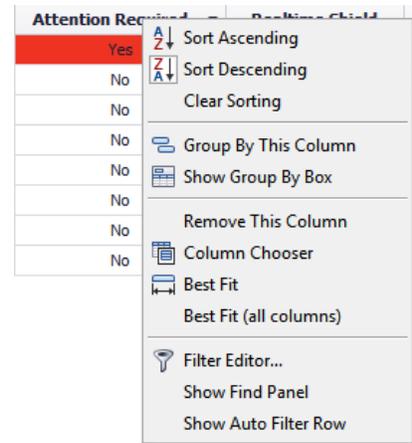
Additional columns can be added from the **Column Chooser** menu – right click to activate.

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.

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.

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.

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.
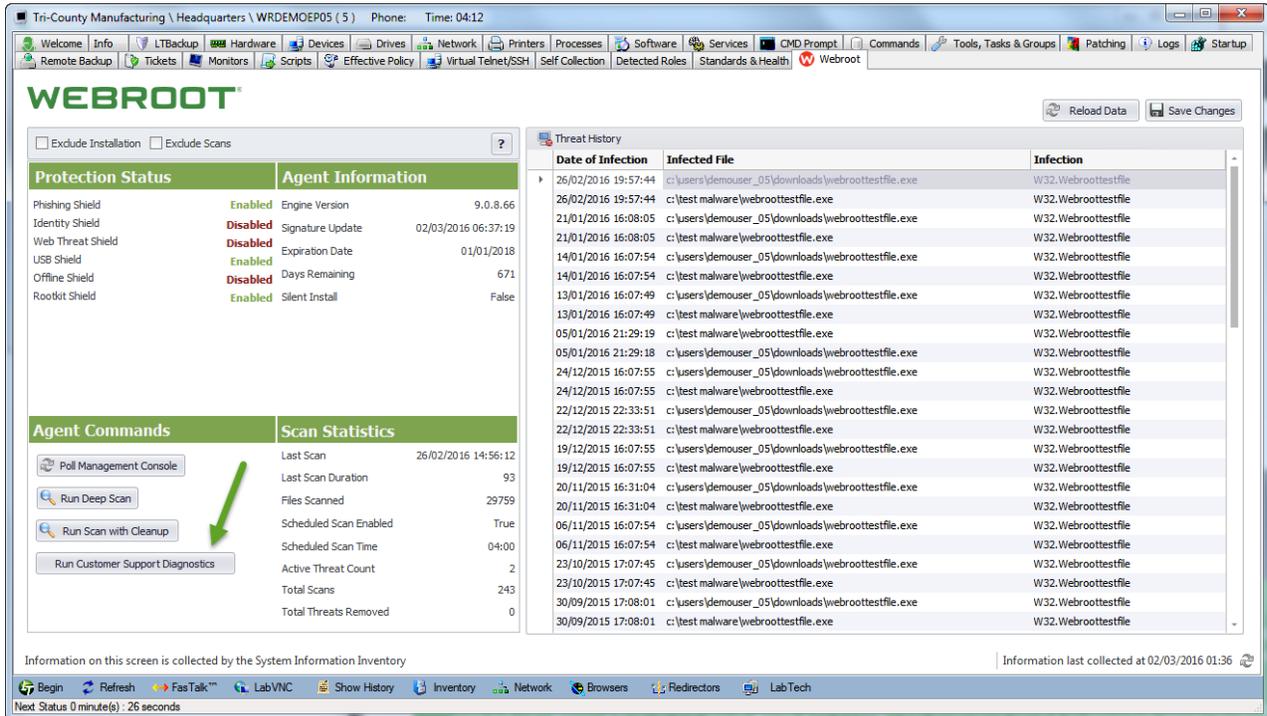
Other Miscellaneous Changes

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.
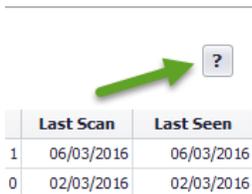
LabTech Health Reports and AV Dashboard Integration

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.

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.

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 ☐ Overview Hide
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 ☐ Invert Check
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.
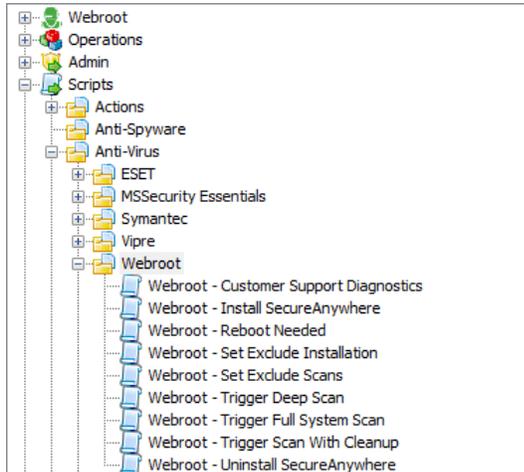
Omissions

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.