WEBROOT®

LabTech
Integration Instructions

WEBROOT®

Table of Contents

Overview

Version 2 of Webroot's LabTech integration has been greatly enhanced. Most noticeably, the integration is now a LabTech plugin. It was designed and developed with the base of the v1 integration but has been greatly enhanced via the feedback from LabTech partners.

The plugin includes many features such as a Custom Dashboard, Monitors, Scripts, Searches, Group, an agent-based data collection that alleviates the over utilization of the LabTech server's script engine, and a polished interface.

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

LabTech version must be 2013 or greater.

Webroot Activation

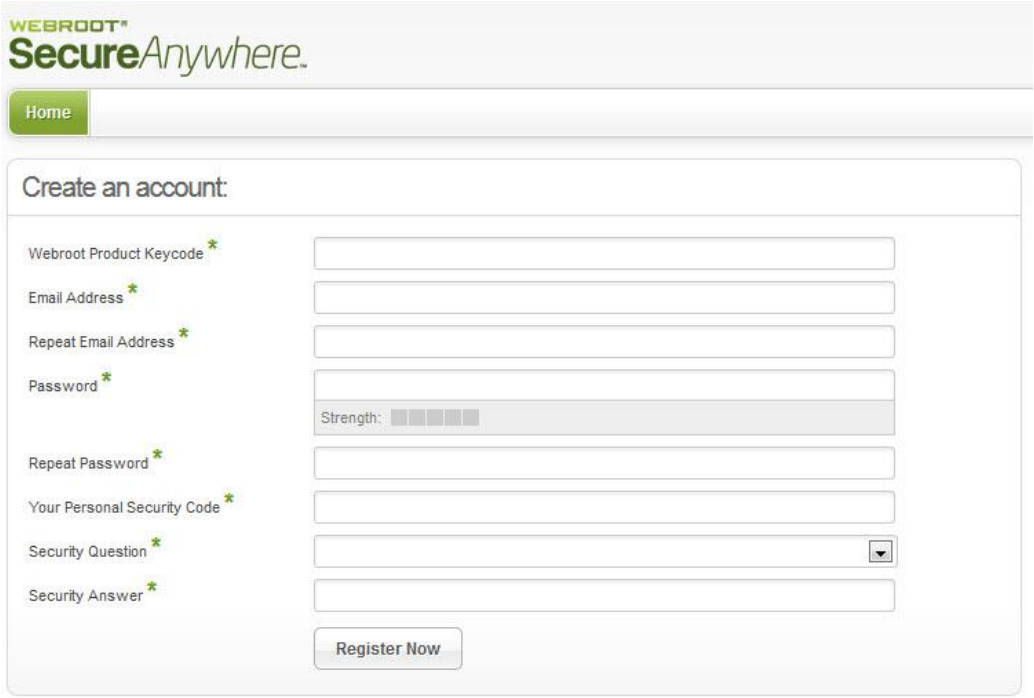
In order to seamlessly integrate Webroot with the LabTech Control Center, you first need to activate the Webroot Global Site Manager (GSM) console.

To activate your Webroot cloud management console:

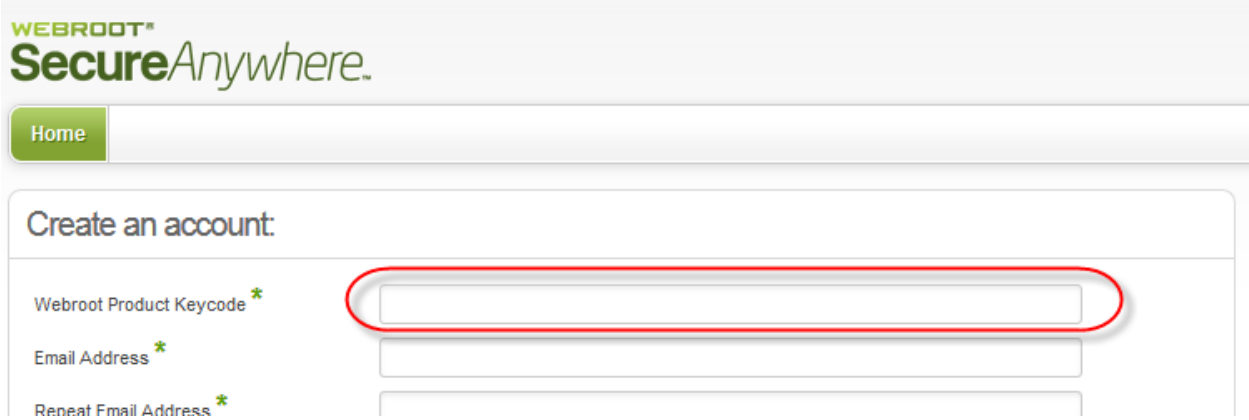
1. In a web browser, enter the following URL:

   https://my.webrootanywhere.com/registration.aspx

   The system displays the Webroot SecureAnywhere Create an account window.



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



   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.

Plug-In Installation

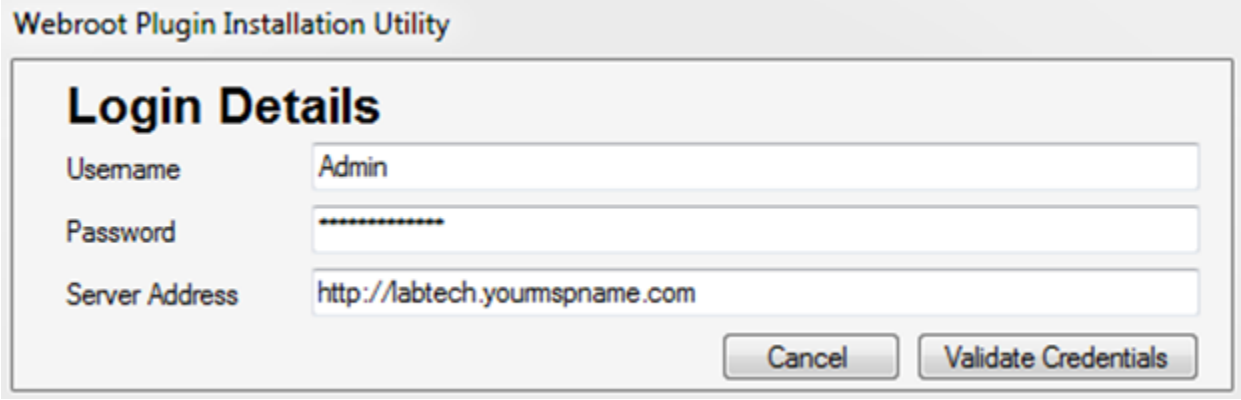
You must be a super admin to be able to install the program.

To install the plug-in:

1. Download **Webroot Plugin Installer.exe** from the following location:

   http://download.webroot.com/RMM/LabTech/Webroot-Deploy-Solution.zip
2. Double-click the installer package.
3. If UAC is enabled, run as admin.
4. Follow the steps provided by the installation wizard.
5. Enter your LabTech admin **Username** and **Password**.
6. Click the **Next** button.
7. Click the **Install** button.

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

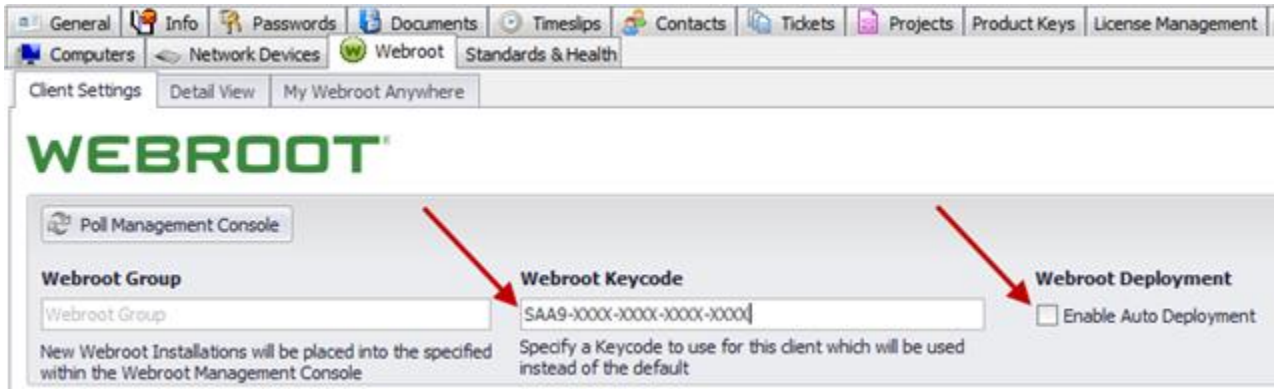


Global Site Manager Integration

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.

   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.**

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

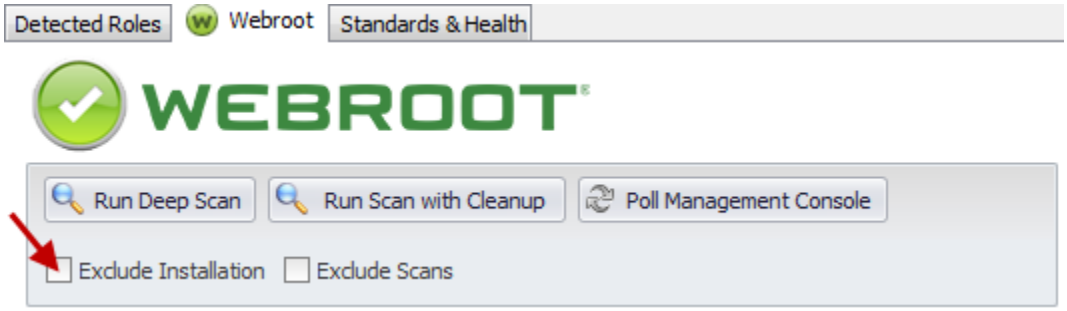
6. Click the **Save Changes** button.

Installation Exclusions

Set computer and location exclusions before enabling auto deployment.

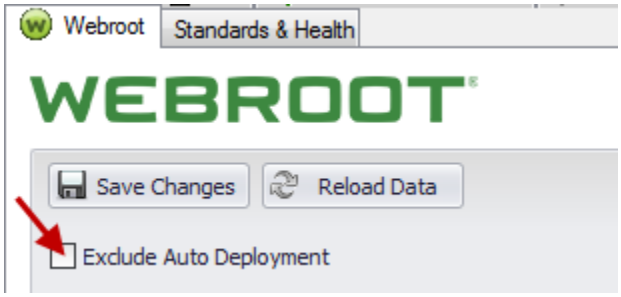
To exclude a computer from installation via LabTech:

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



To exclude a location from auto deployment:

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

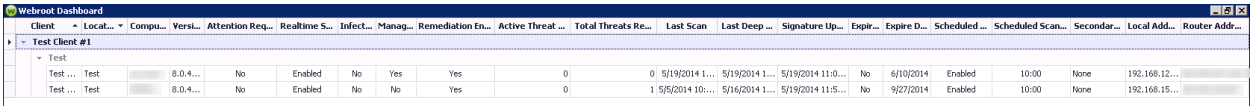


Usage

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 Inventroy menu.

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**.

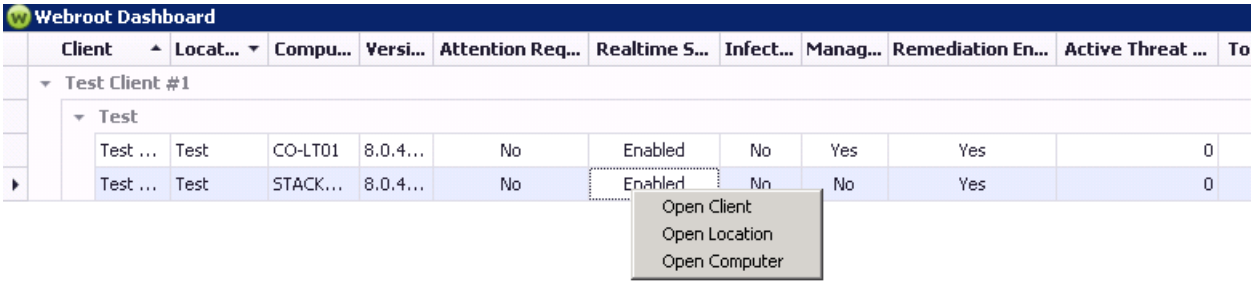
Information by Computer/Device



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	Any shield besides **Realtime** is disabled, such as Offline, Identity, etc.
Realtime Shield	Status of realtime shield: • Enabled • Disabled
Infected	Identifies whether the remote system has an active virus.
Managed	Identifies whether the remotes agent is managed via a Webroot policy.
Remediation Enabled	Identifies whether auto remediation is enabled on the remote agent.

Data	Description
Active Threat Count	Number of active threats, not yet treated, 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 Deep Scan	Last deep scan date of the device.
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.
Schedueld Scan	Identifies whether any scans are schedueld 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.

The following view is designed to allow you easy access to all devices where SecureAnywhere has been deployed. By right-clicking on any device, you can access the computer, location, or client.



Reference

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

Remote Monitors (runs every 5 min)

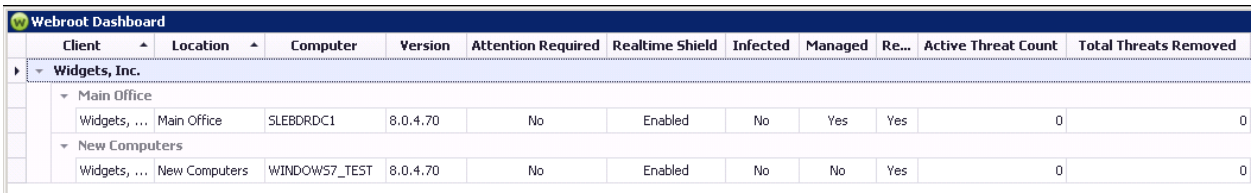
Webroot – Active Threats – There are both 32 and 64 bit versions of this remote monitor. It checks the registry value for active threat status and alerts Webroot if there is an active threat.

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.
Install Webroot SecureAnywhere	Installs the Webroot agent on a machine. • 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. **Note:** The group name must be typed in exactly as it appears in the Webroot groups and cannot contain any spaces.
Uninstall Webroot SecureAnywhere	Uninstalls the Webroot Agent.

Webroot Custom Dashboard

This dashboard displays all of the computers for all clients and location in one view and allows the ability to administer them from one dashboard.



Webroot Dashboard

Client	Location	Computer	Version	Attention Required	Realtime Shield	Infected	Managed	Re...	Active Threat Count	Total Threats Removed
Widgets, Inc.										
Main Office										
Widgets, ...	Main Office	SLEBDRDC1	8.0.4.70	No	Enabled	No	Yes	Yes	0	0
New Computers										
Widgets, ...	New Computers	WINDOWS7_TEST	8.0.4.70	No	Enabled	No	No	Yes	0	0

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**.