

WEBROOT®

an **opentext™** company

Kaseya VSA Cloud Module

Assembly Version 2.0.21053.1 & above

Webroot.vsz file 1.5.20134.2 & above

Getting Started Guide

Document Version 2.0.1



Table of Contents

Overview	2
What's New with Version 2.0	2
New Features	2
Enhancements.....	2
Prerequisites.....	2
Installing Webroot Kaseya VSA Cloud Module	3
Controlling Access to Webroot Settings.....	6
Getting Started and Deployment.....	9
Overview Menu	9
Plugin Version Notification.....	10
Admin Data Sync.....	11
Webroot Business Agent Deployment	12
Configuring and Obtaining a Unique Webroot Site Key	12
Auto Deploy Exclusions.....	17
Adopting Existing Webroot Business Agents.....	19
Deploying Webroot Agents via the Kaseya Module.....	20
Viewing Installation and Dashboard Level Webroot Agent Statuses	21
Indicators in the Deployment & Status Dashboard	22
Red W.....	22
Warning Icon in Kaseya Agent Refresh Column.....	22
Running Webroot Agent Commands	23
Launching Live Connect	24
Detailed Webroot Agent Status & Agent Commands.....	25
Integrated Alarm Parameters with Kaseya Alert Actions	28
Setting Up Kaseya Emails and Ticketing.....	31
Disclaimer	34

Overview

The Webroot Kaseya VSA Cloud Module is designed to increase operational efficiency by tightly integrating Webroot SecureAnywhere Business Endpoint Protection (WSAB) as a module into the Kaseya VSA Cloud Platform, while complementing the advantages available within the Webroot Global Site Manager console (GSM).

The Kaseya VSA Cloud Module offers powerful features including manual & auto-deployment options, auto-discovery, overview dashboards, detailed endpoint statistics for fast troubleshooting, Webroot agent commands, actionable alerts, and threat history.

The Module is designed to be extremely easy to install, requiring only a few clicks. It's intuitive to use, with helpful hints throughout; however, we recommend you read through this guide before deployment. This module is in complete compliance to all third party integration definitions for Kaseya VSA Cloud version 9.5 and up.

If you have any suggestions please contact your Webroot representative, alternatively you can post suggestions or comments in our Kaseya Partner Group community [here](#).

What's New with Version 2.0

New Features

- Fully configurable, granular, GUI-driven auto-deployment management
- Flexible, easy-to-set deployment exclusion management
- Multi-tier Kaseya Organization and Group management

Enhancements

- Improved in-product messaging dashboard
- Increased efficiency and & shorter response times

Prerequisites

- This guide.
- One of the following:
 - A Webroot GSM Super Admin account
 - At least one Webroot SecureAnywhere site key

Note: If you are a first-time Webroot user, please complete your GSM account setup before going any further. For more information, see [Creating Webroot Accounts](#).

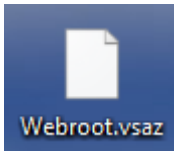
- For MSPs, we recommend setting up **each of your customers** as **different Sites within Webroot GSM**; allocating one Site Key per customer.
- Kaseya VSA Cloud Version 9.5 and up.
- Kaseya administrator account.
- The latest **Webroot.vsaz** installer, is available [here](#).

Installing Webroot Kaseya VSA Cloud Module

If you have met all the prerequisites, use the following procedure.

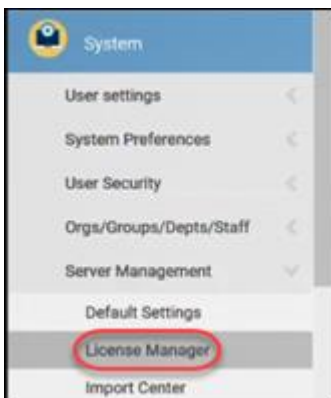
To install Webroot Kaseya VSA Cloud Module:

1. Download the Webroot Kaseya VSA Cloud Module **Webroot.vsaz** file [here](#). You can also get the latest module from Kaseya Automation Exchange under Webroot Kaseya Cloud Module.
2. Download the installer package to your device.

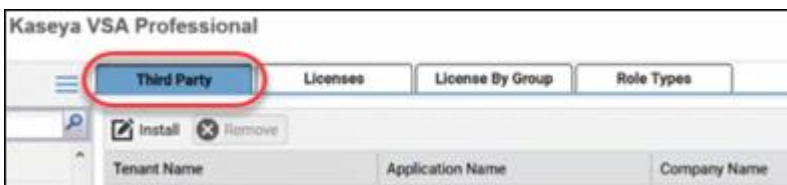


IMPORTANT NOTE: Please ensure the downloaded file is named **Webroot.vsaz** before proceeding to the next step (any other file names, such as “Webroot (1).vsaz” will NOT work).

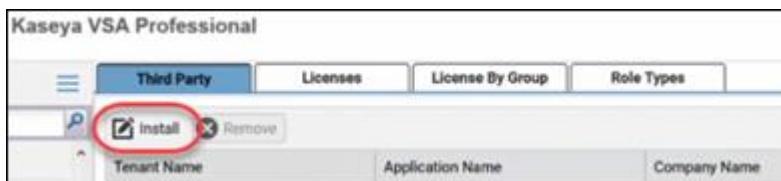
3. Within your Kaseya VSA Cloud Console, select **System > Server Management > License Manager**.



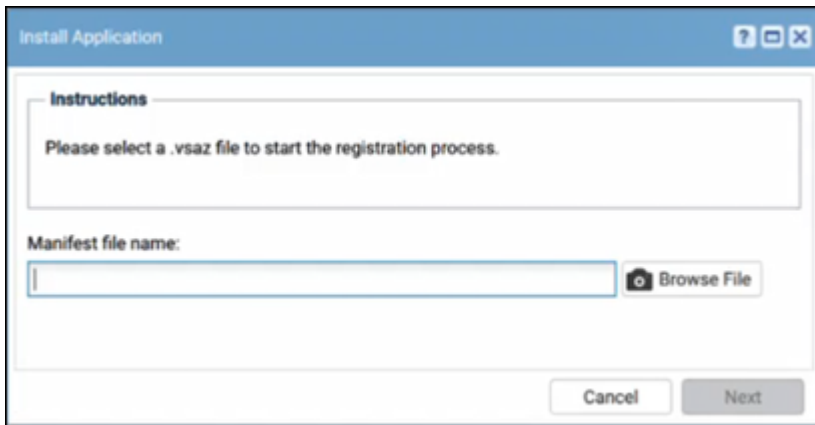
4. Click the **Third Party** tab.



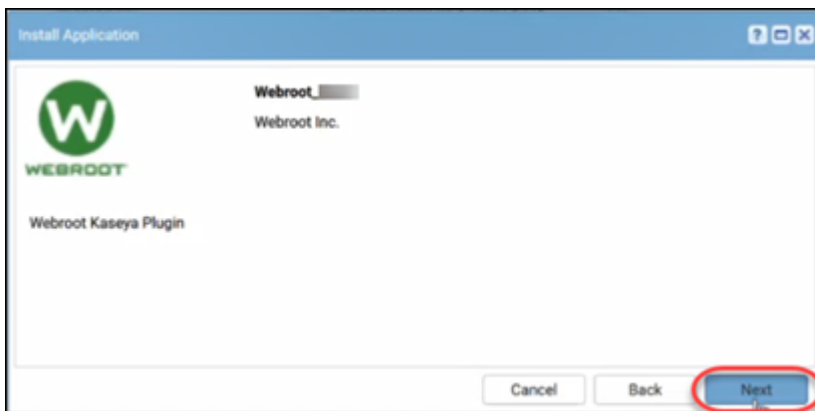
5. Click the **Install** icon.



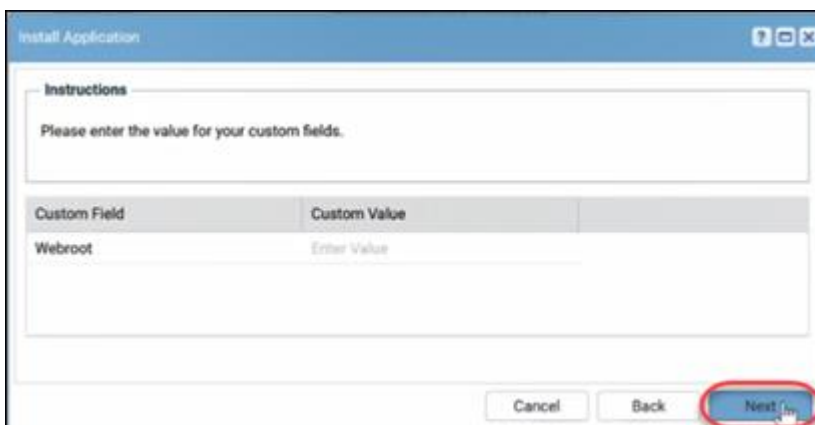
6. Use the **Browse File** button to locate downloaded VSAZ file.
7. Click the **Next** button to install.



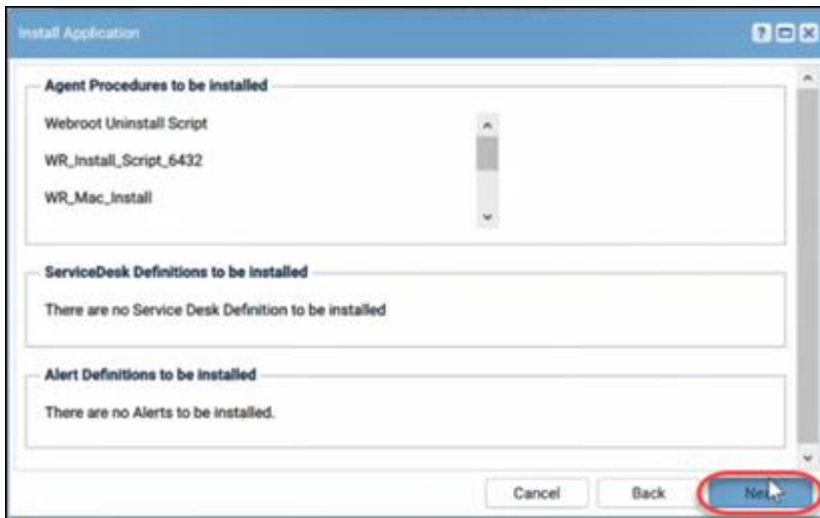
8. Click the **Next** button.



9. Click the **Next** button.



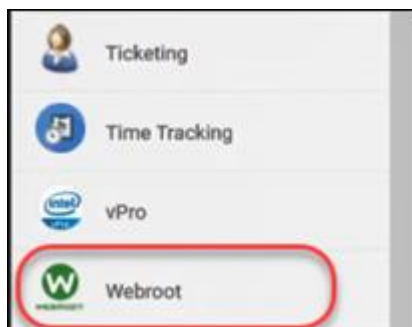
10. When you see the Agent Procedures to be installed window, click the **Next** button.



11. Click the **Finish** button to complete the installation.



12. Once installed, refresh the browser. You will be able to see the Webroot Module when you navigate to the bottom of the tree.



Controlling Access to Webroot Settings

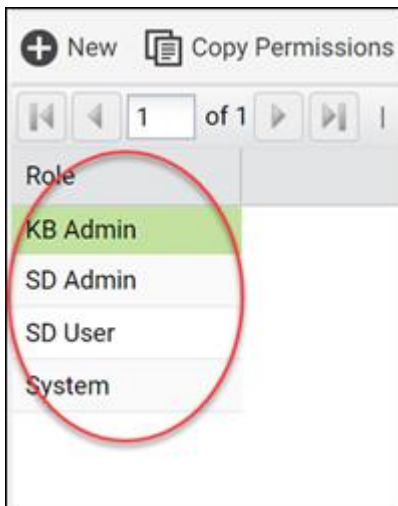
As needed, you can control an admin's access to Webroot settings. We recommend that you allow access to only those admins who will make GSM parent keycode assignments.

To control access to Webroot settings:

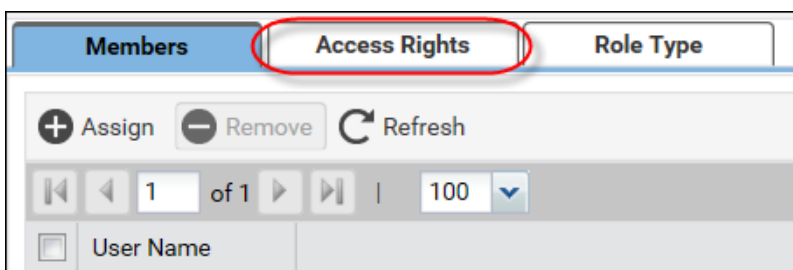
1. From the main menu, select **System > User Roles**.



2. In the Role pane, select the role you want to apply the permissions to.



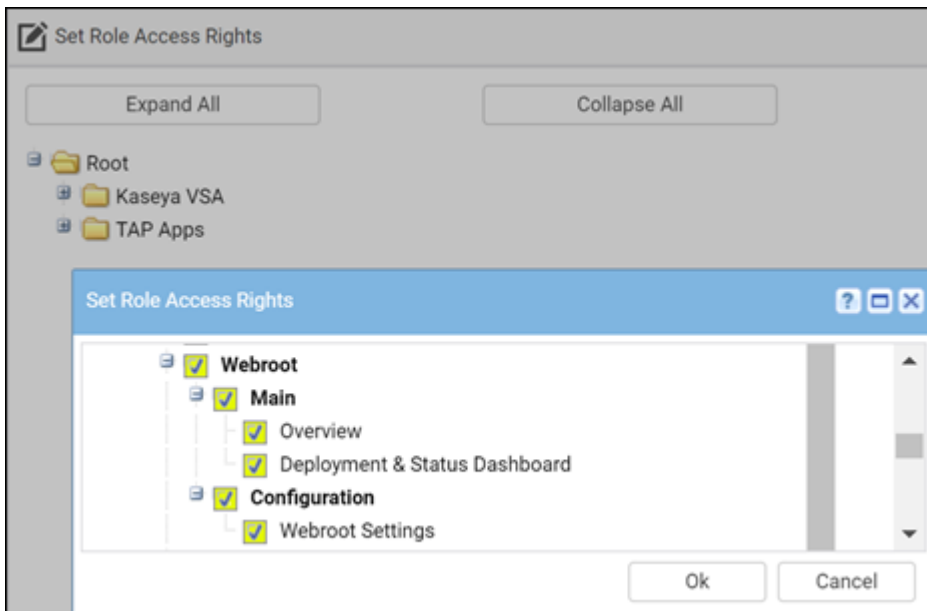
3. In the Set Role Access Rights pane, click the **Access Rights** tab.



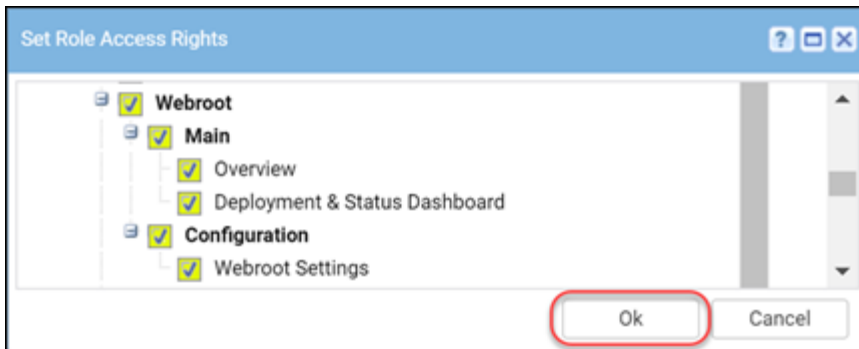
4. In the Access Rights tab, click the **Set Role Access Rights** button.



5. From the list, select **Master > Webroot** to expand the list.
6. Select the checkboxes next to the areas that you want to allow access to.
 - Webroot
 - Main
 - Overview
 - Deployment & Status Dashboard
 - Webroot Settings



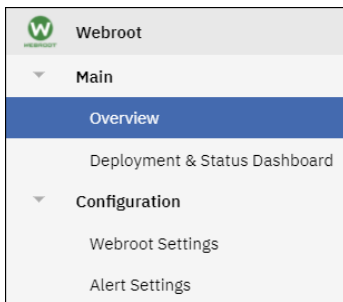
7. When you're done, click the **OK** button.



Getting Started and Deployment

The user interface within the Kaseya Module is designed to be easy to use and is broken down to three main menu items:

- **Overview** – Basic guide to steps required. See the [Overview Menu](#).
- **Deployment & Status Dashboard** – Allows simple GUI-driven deployments and menus for detailed status view as well as agent commands. See [Webroot Business Agent Deployment](#).
- **Webroot Settings** – Webroot specific settings, such as site or default keycode, Webroot console access, and auto WSAB adoption wizard. See [Adopting Existing Webroot Business Agents](#).



Overview Menu

The Overview menu is a very basic guide to the steps required to deploy and maintain your Webroot installation.

WEBROOT SETTINGS

Organizations must be assigned with a unique **Webroot Site Key**. The **Webroot Site Key** can be created by clicking "Webroot Settings/My Webroot". After signing-in, the Webroot Global Site Manager allows you to create multiple "Sites/Organizations", each with its own keycode.

DEPLOYMENT AND STATUS

Using the "Install" button, you can deploy a Webroot client on your Kaseya Agents. Once the installation is complete, your agent will be ready to take advantage of the Webroot Protection.

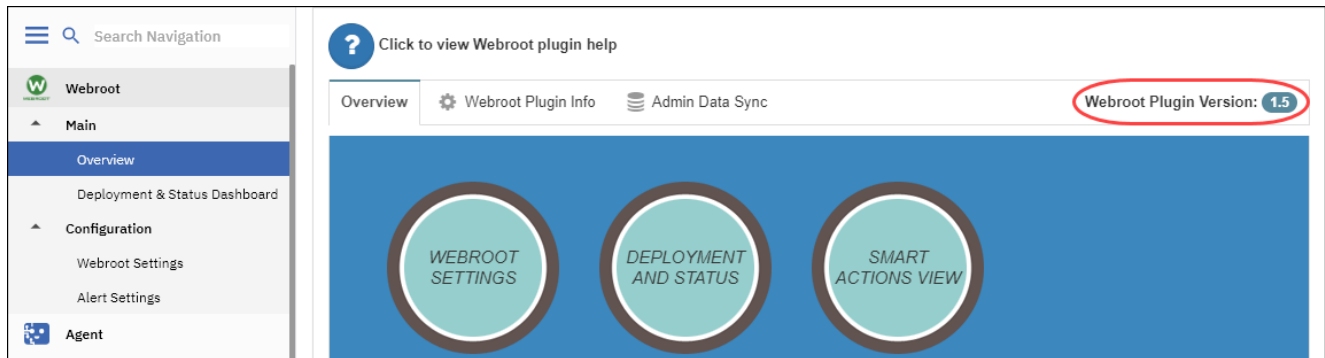
To Uninstall the Webroot client, select the target agents and then click the "Uninstall" button.

ⓘ Uninstallation will not Deactivate/Retire agents. Access the Webroot Console to deactivate retired endpoints

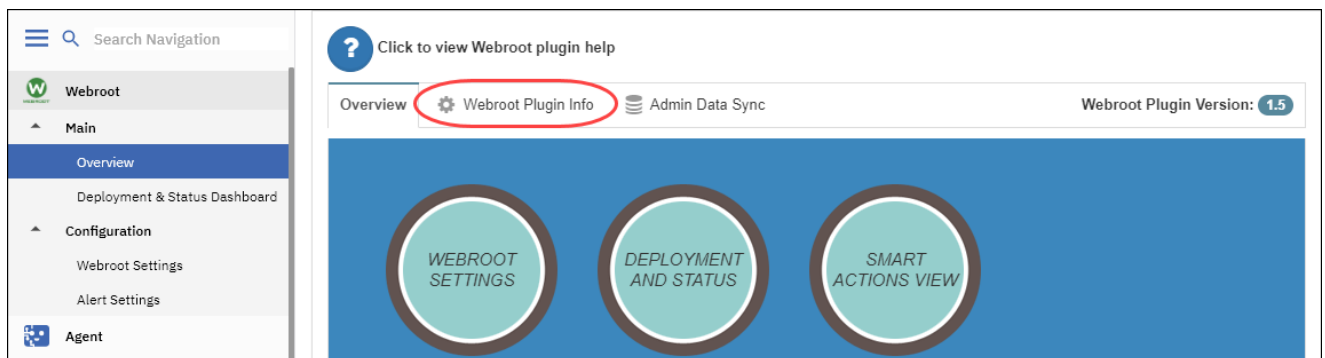
SMART ACTIONS VIEW

Provides UI for the viewing of the Status of the Webroot, the list of actions that can be initiated.

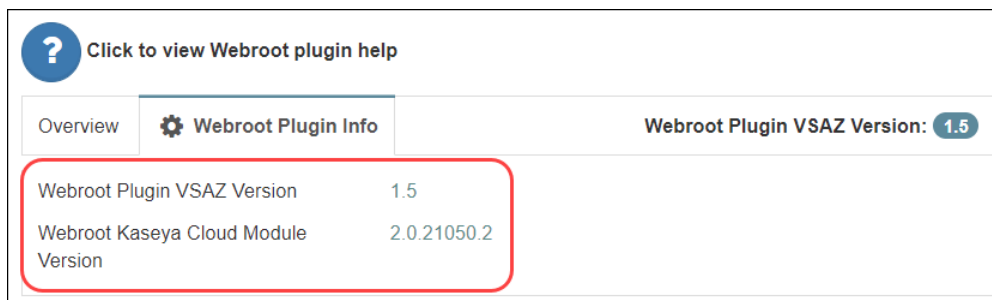
The major version info for the plugin is located in the upper right corner.



For additional information about the Webroot plugin, click the **Webroot Plugin Info** tab.

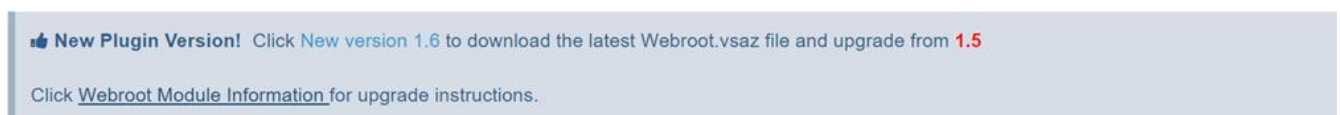


This displays information about the version of the **Webroot.vsz** file and the **Cloud Module Version**.



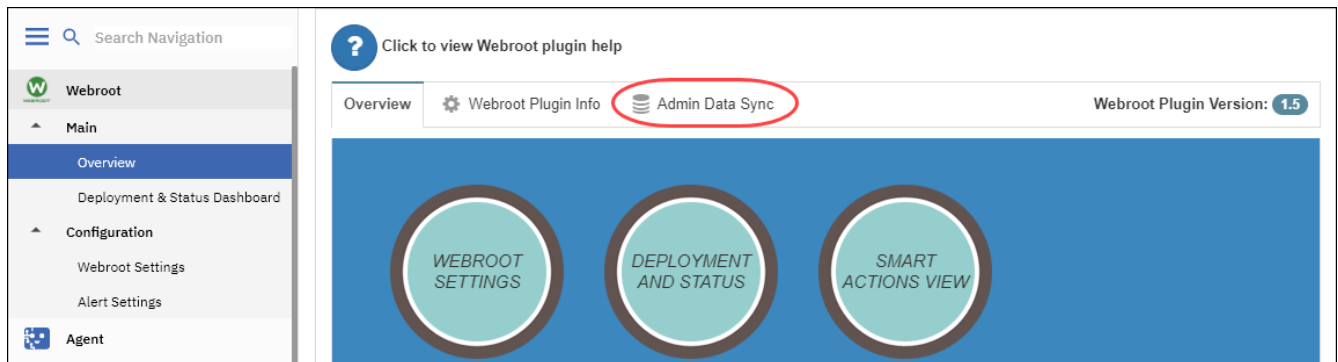
Plugin Version Notification

If you have an older version of the Webroot.vsz file that needs to be upgraded, you will be notified of a New Plugin Version within the Overview Page until you upgrade. Included in the notification is a link to the Kaseya Automation Exchange Webroot Cloud page, where you will find links to documentation, release info and the link to the latest Webroot Plugin Registration file.

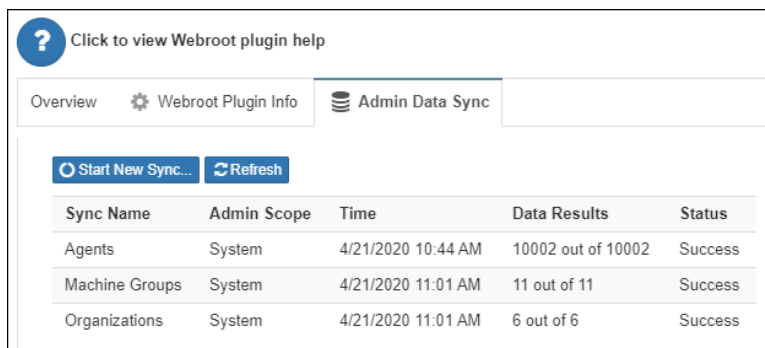


Admin Data Sync

To improve plugin responsiveness, an updated mechanism has been added that prefetches information, per admin. The sync is performed automatically if the admin is logged in and the data is more than 2 hours old.



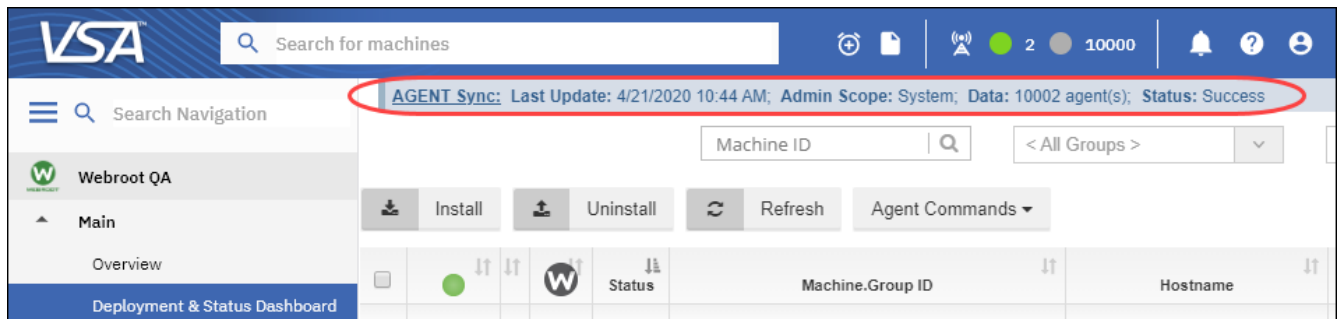
Clicking on the Admin Data Sync tab will open up the panel below.



A button to trigger a manual sync is on the admin data sync tab if needed. It will warn you if a sync process is already running. This page will update every 5 seconds when a button is pressed to give you feedback. **We suggest not changing admin Scope or logging out while this process is running, otherwise the process will fail.**

The Agent Sync Process is automatically triggered when the administrator accesses the Deployment & Status Dashboard. The AGENT Sync information is shown within the top messaging portion of the dashboard.

NOTE: Other messages may also be shown within Webroot product messaging window.



Webroot Business Agent Deployment

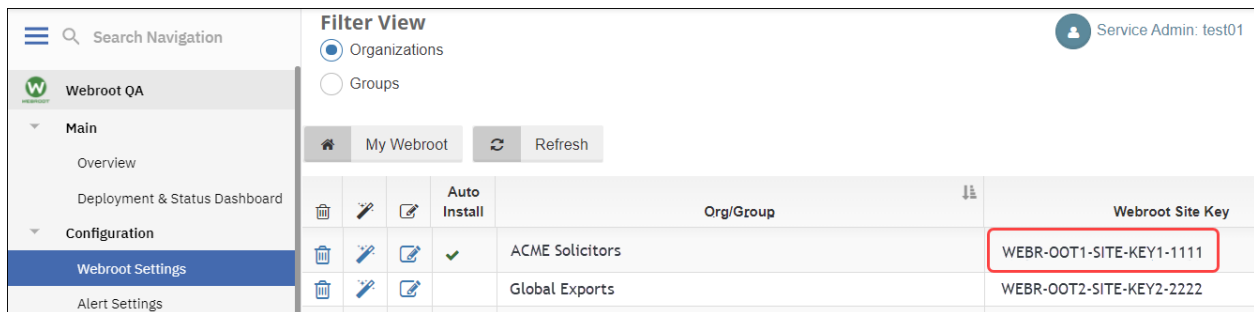
- Configuring and obtaining a unique Webroot site key. See [Configuring and Obtaining a Unique Webroot Site Key](#).
- Deploying Webroot Business agents through the Kaseya module. See [Deploying Webroot Agents via the Kaseya Module](#).
- Viewing installation and dashboard-level Webroot agent status. See [Viewing Installation and Dashboard Level Webroot Agent Status](#).

Note: If you have an existing Webroot Business deployment, you can adopt already installed endpoints into the Kaseya Module. For more information, see [Adopting Existing Webroot Business Agents](#).

Configuring and Obtaining a Unique Webroot Site Key

To configure:

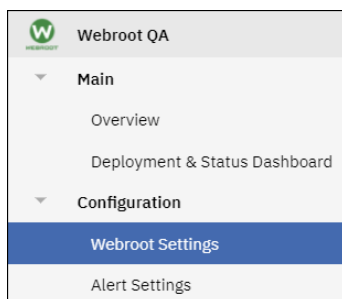
1. The Kaseya administrator must enter a valid Webroot site key, generated in the Webroot GSM, that matches the organization or group in the Kaseya VSA.



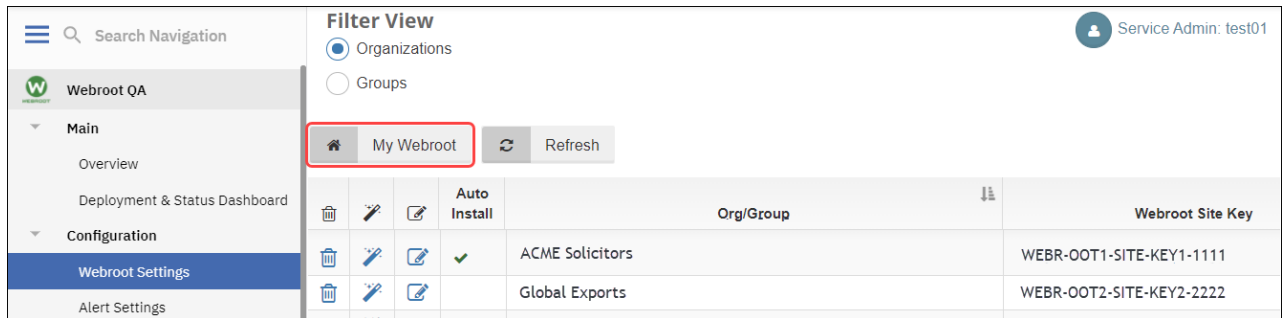
Org/Group	Webroot Site Key
ACME Solicitors	WEBR-OOT1-SITE-KEY1-1111
Global Exports	WEBR-OOT2-SITE-KEY2-2222

To obtain a unique site key:

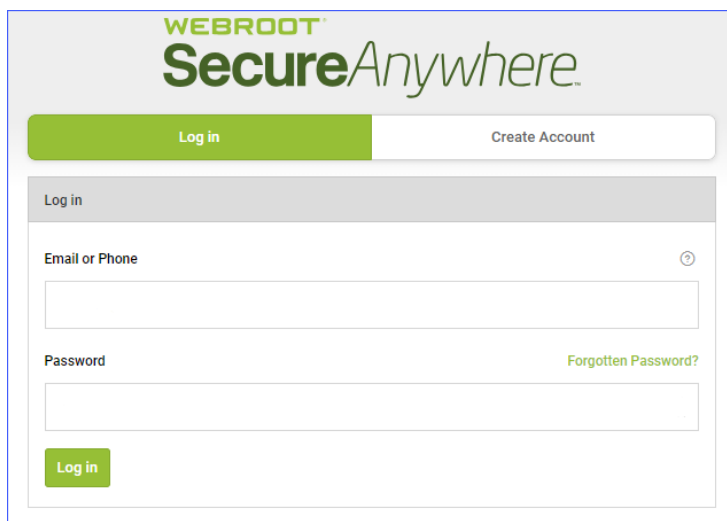
1. From the main menu, select **Webroot > Webroot Settings**.



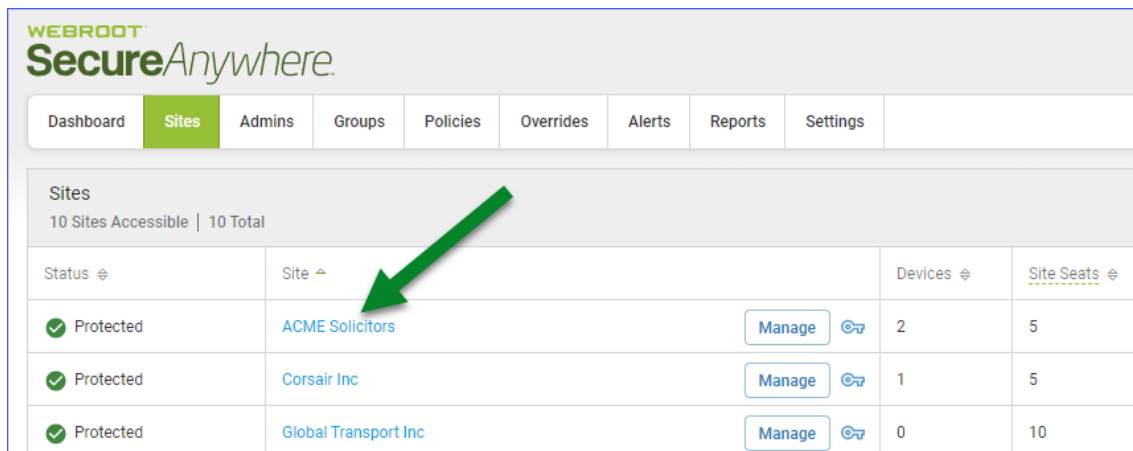
2. Click the **My Webroot** tab.



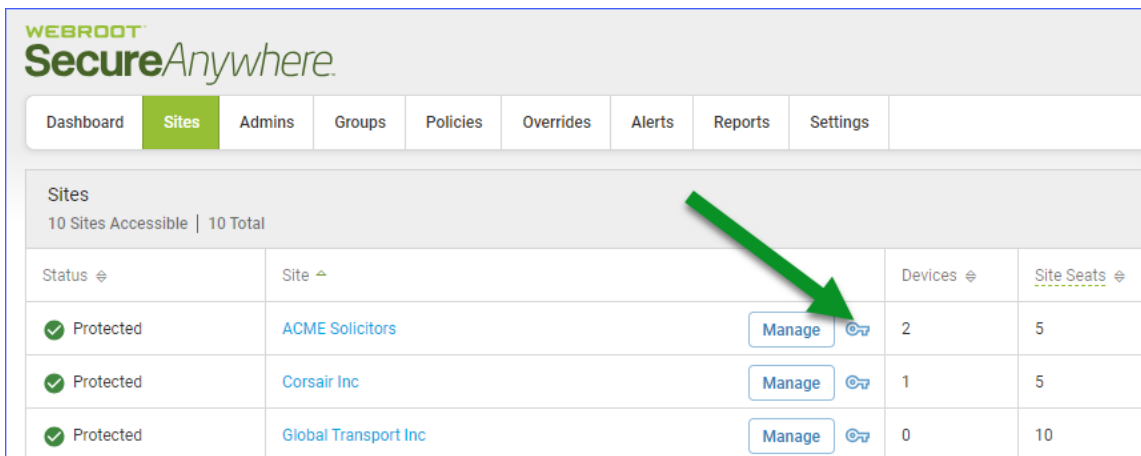
The [Webroot SecureAnywhere login page displays](#).



3. Log in using your Webroot credentials and selected 2 factor authentication
4. From the main panel, browse to your GSM console and create a new site that matches the organization in in the Kaseya VSA.



- Once the new site has been created, click on the corresponding key icon



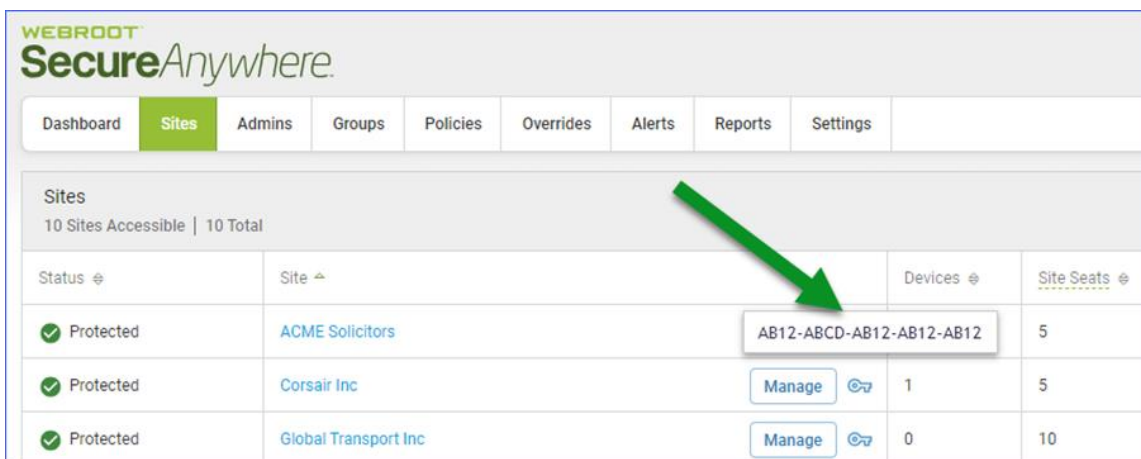
WEBROOT[®] SecureAnywhere

Dashboard **Sites** Admins Groups Policies Overrides Alerts Reports Settings

Sites
10 Sites Accessible | 10 Total

Status	Site		Devices	Site Seats
Protected	ACME Solicitors	Manage	2	5
Protected	Corsair Inc	Manage	1	5
Protected	Global Transport Inc	Manage	0	10

- In the Sites panel, copy the keycode from the Keycode column for that GSM site.



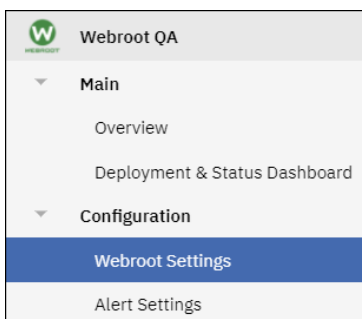
WEBROOT[®] SecureAnywhere

Dashboard **Sites** Admins Groups Policies Overrides Alerts Reports Settings

Sites
10 Sites Accessible | 10 Total

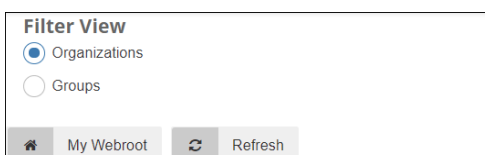
Status	Site		Devices	Site Seats
Protected	ACME Solicitors	AB12-ABCD-AB12-AB12-AB12		5
Protected	Corsair Inc	Manage	1	5
Protected	Global Transport Inc	Manage	0	10

- In Kaseya, from the main menu, select **Webroot > Webroot Settings**.



	Webroot QA
▼	Main
	Overview
	Deployment & Status Dashboard
▼	Configuration
	Webroot Settings
	Alert Settings

- The Filter View pane displays **Organizations** as default. You can select the **Groups** radio button, as needed.
- The Filter View pane allows you to filter by organization or group, which lets you assign Webroot site keycodes to Kaseya Organizations or Groups.

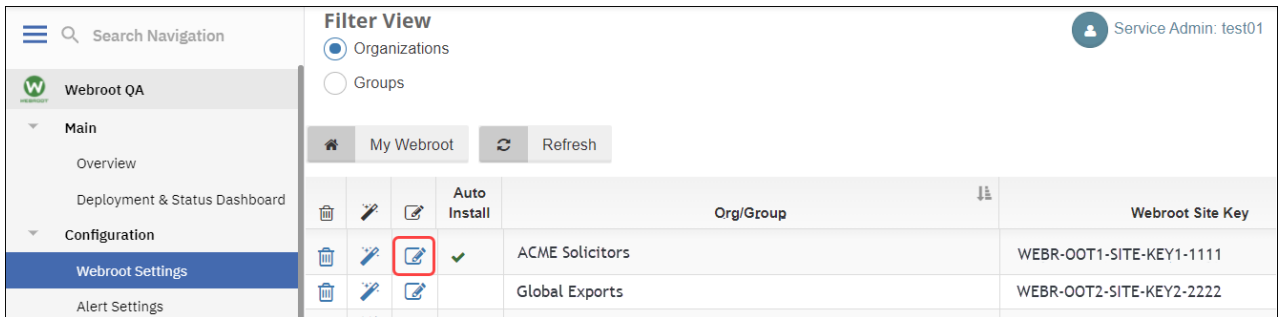


Filter View

☒ Organizations
☐ Groups

My Webroot Refresh

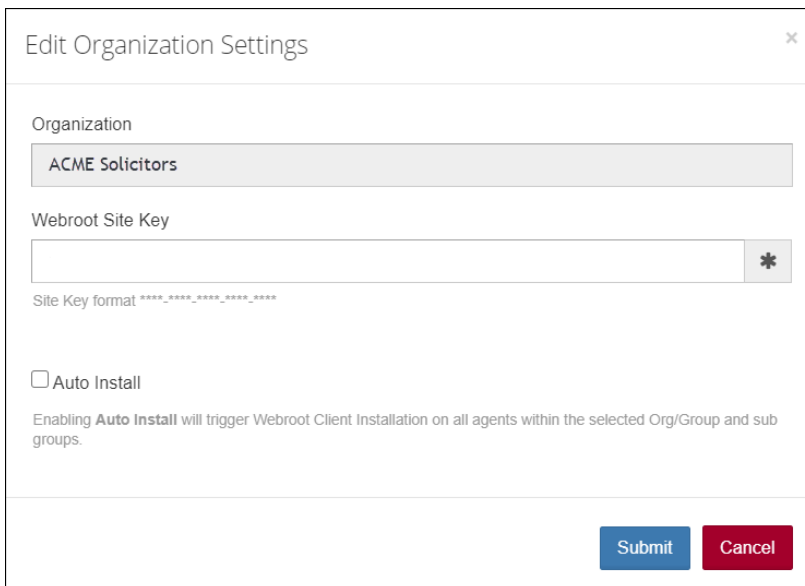
8. For the organization or group that you want to edit, click the **Edit** icon.



The screenshot shows the 'Filter View' for Organizations. The left sidebar contains a navigation menu with 'Webroot QA', 'Main' (Overview, Deployment & Status Dashboard), 'Configuration' (Webroot Settings, Alert Settings), and 'Webroot Settings'. The main area shows a table of organizations. The 'ACME Solicitors' organization is selected, and its 'Edit' icon (pencil) is highlighted with a red box. The table has columns for 'Org/Group' and 'Webroot Site Key'.

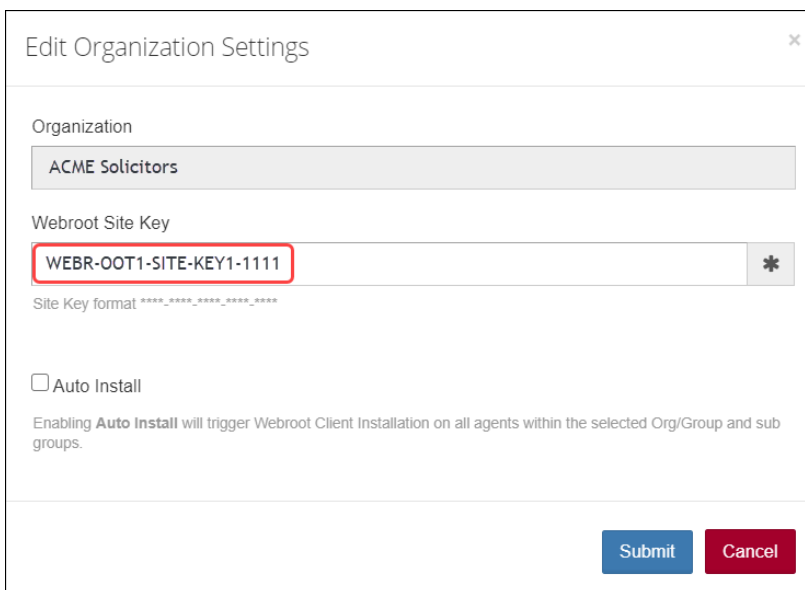
Org/Group	Webroot Site Key
ACME Solicitors	WEBR-OOT1-SITE-KEY1-1111
Global Exports	WEBR-OOT2-SITE-KEY2-2222

The Edit Organization Settings window displays the Organization field already populated.



The 'Edit Organization Settings' window shows the 'Organization' field populated with 'ACME Solicitors'. The 'Webroot Site Key' field is empty. The 'Auto Install' checkbox is unchecked. The window includes a 'Submit' button and a 'Cancel' button.

9. In the Webroot Site Key field, paste the keycode that you copied from the GSM console in step 5.



The 'Edit Organization Settings' window shows the 'Webroot Site Key' field populated with 'WEBR-OOT1-SITE-KEY1-1111'. The 'Auto Install' checkbox remains unchecked. The window includes a 'Submit' button and a 'Cancel' button.

10. To enable Auto Install of Webroot agents within the selected Org/Group, **Click Auto Install** check box.

IMPORTANT NOTE: If you do **NOT** want Webroot agents deployed on every single Computer in this Org/Group, please **Exclude** specific Computers within the Deployment & Status Dashboard **PRIOR** to setting Auto Install. See **Auto Deploy Exclusions** section below.

- Note:** If you do not have a GSM or if you use a single Webroot site key to manage all your organizations, you can use the same key on all Orgs/Groups within the Kaseya Module. **We recommend a site key per Organization, unless you have very small organizations consisting of one or two seats.**

- Webroot QA

Main

Overview

Deployment & Status Dashboard

Configuration

Webroot Settings

Alert Settings

Machine ID

ACME Solicitors

< No View >

Install

Auto Install

Uninstall

Refresh

Agent Commands

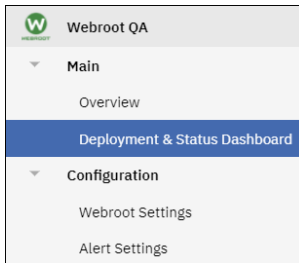
			Status	Machine.Group ID	Hostname	Attention Required	Infected	Policy	Active Threat
<input type="checkbox"/>				vrathwlnz840.root.1010	VRATHWLNZ840.qa.local				
<input type="checkbox"/>				vrathwlnz849.group-a.root.1010	VRATHWLNZ849	No	No	Yes	

Auto Deploy Exclusions

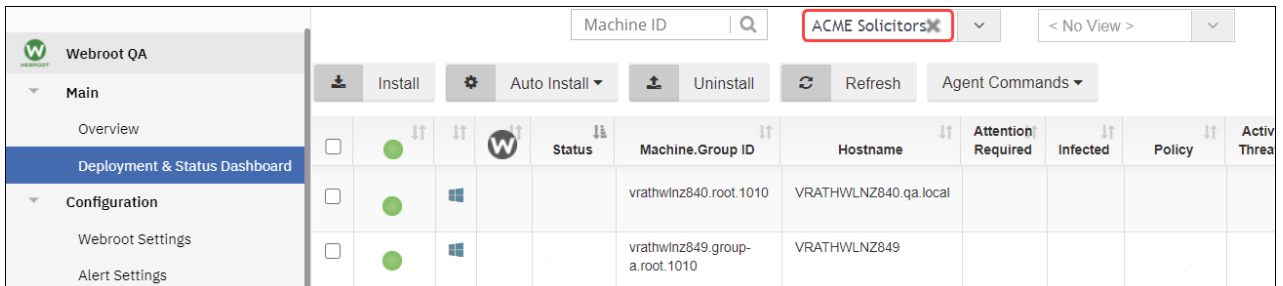
You can create Auto Deploy exclusions to prevent Webroot agent installation on specific Computers, even if Auto Deploy has been selected for Org/Group. We added the ability to exclude specific Computers within the Deployment & Status Dashboard.

To exclude specific Computers:

- From the main menu, select **Webroot > Deployment & Status Dashboard**

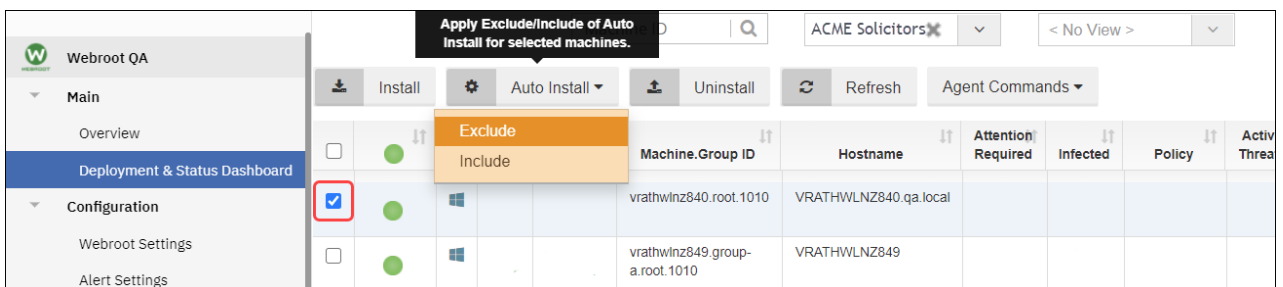



- Select the **Org/Group** from the drop down menu









Note: At this stage Auto Deploy has NOT yet been checked within the Webroot Settings and Webroot agents have NOT been deployed.







- Select **Computer** or **Computers** to be excluded from Auto Deploy and select **Exclude** from the **Auto Deploy** drop down menu.



The Deployment and Status Dashboard will display all **Auto Deploy Excluded** Computers, indicated by the Auto Deploy Excluded icon 

<div> <div>Webroot QA</div> <div> <div>Main</div> <div>Overview</div> <div>Deployment & Status Dashboard</div> <div>Configuration</div> <div>Webroot Settings</div> <div>Alert Settings</div> </div> </div>		<div> <div>Machine ID</div> <div>ACME Solicitors</div> <div>< No View ></div> </div> <div> <div>Install</div> <div>Auto Install</div> <div>Uninstall</div> <div>Refresh</div> <div>Agent Commands</div> </div>									
					Status	Machine.Group ID	Hostname	Attention Required	Infected	Policy	Activ Threa
		<input type="checkbox"/>				vrathwlnz840.root.1010	VRATHWLNZ840.qa.local				
		<input type="checkbox"/>				vrathwlnz849.group-a.root.1010	VRATHWLNZ849				

4. If **Auto Deploy** has been selected within an Org/Group in **Webroot Settings**, the Org/Group computers will show the Auto Deploy gear icon 

<div> <div>Webroot QA</div> <div> <div>Main</div> <div>Overview</div> <div>Deployment & Status Dashboard</div> <div>Configuration</div> <div>Webroot Settings</div> <div>Alert Settings</div> </div> </div>		<div> <div>Machine ID</div> <div>ACME Solicitors</div> <div>< No View ></div> </div> <div> <div>Install</div> <div>Auto Install</div> <div>Uninstall</div> <div>Refresh</div> <div>Agent Commands</div> </div>									
					Status	Machine.Group ID	Hostname	Attention Required	Infected	Policy	Activ Threa
		<input type="checkbox"/>				vrathwlnz840.root.1010	VRATHWLNZ840.qa.local				
		<input type="checkbox"/>				vrathwlnz849.group-a.root.1010	VRATHWLNZ849	No	No	Yes	

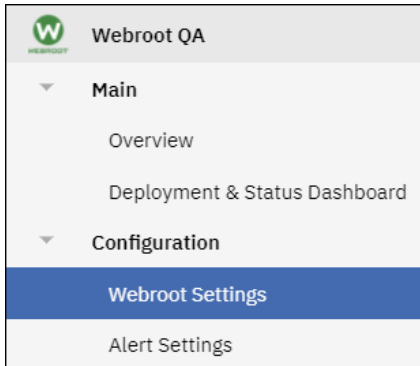
Note: It will take around 2 hours to Auto Deploy computers

Adopting Existing Webroot Business Agents

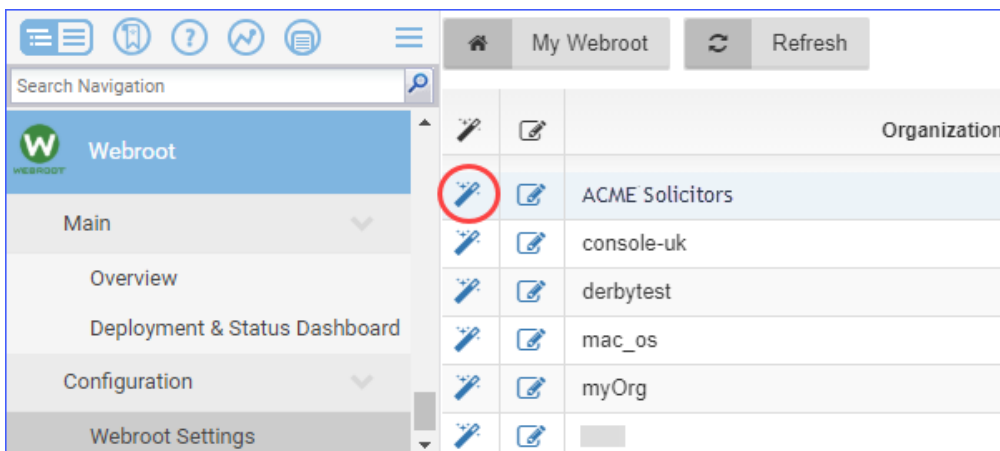
If you have existing WSAB deployments and want to adopt those endpoints, use the following procedure.

To adopt existing agents:

1. From the main menu, select **Webroot > Webroot Settings**.



2. For the row that lists the organization or group that you want to adopt, click the **Wizard** icon.



Webroot agents will be automatically discovered and pulled into the Kaseya Module. If the machine is online and, if there are no other agent procedures queued on that machine, it will happen within five minutes.

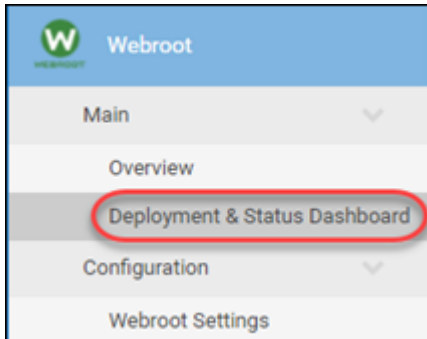
Note: Adopted Webroot endpoints that were initially installed manually, using Webroot installer executable (.exe), can only be uninstalled from within the Webroot console.

Deploying Webroot Agents via the Kaseya Module

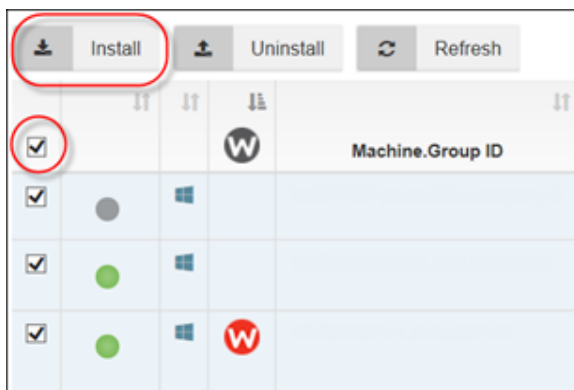
Deploying WSAB agents is very easy, provided a Kaseya agent is already installed. The site keycode for the group or organization containing these agents must be selected to display the Kaseya endpoints in the Deployment & Status Dashboard.

To deploy Webroot agents:

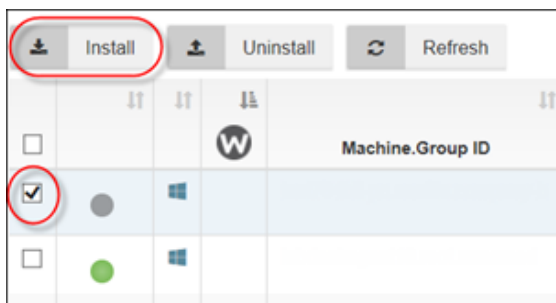
1. From the main menu, select **Webroot > Deployment & Status Dashboard**.



2. Do one of the following to deploy WSAB agents to just one endpoint or a range of endpoints.
 - To install WSAB agents on all endpoints in the filtered view, select the checkbox at the top of the column, and click the **Install** button. All endpoints are selected and installed.

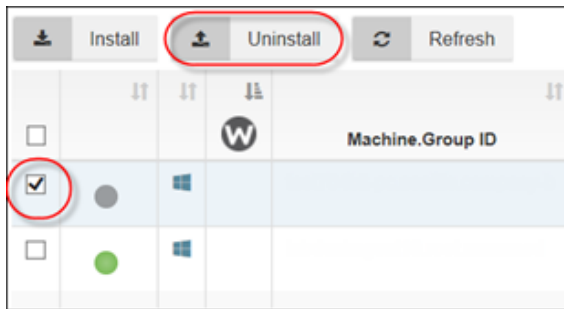


- To install WSAB agent on an individual Kaseya endpoint, select the checkbox of for the target endpoint, and click the **Install** button.



Progress during the installation process is indicated by an Installing status. Once the installation is complete, the installation status will change to Installed.

To uninstall individual endpoints, select the checkbox for the target endpoints, and click the **Uninstall** button.



Viewing Installation and Dashboard Level Webroot Agent Statuses

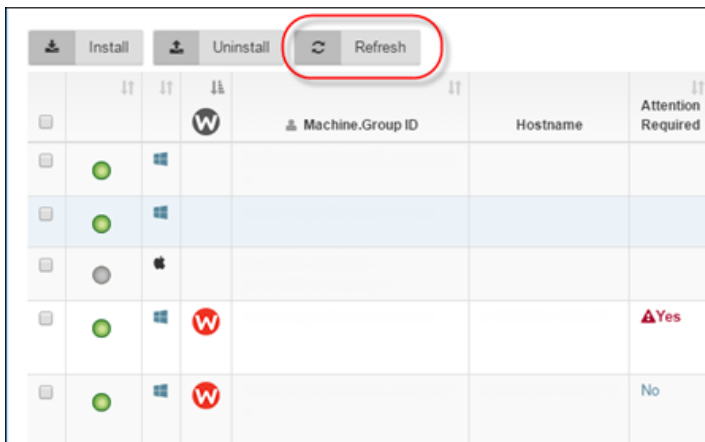
Once the desired WSAB agents are installed, you will be able to see their status at a glance.

Machine Group ID	Hostname	Attention Required	Expired	Expire Date	Infected	Policy Managed	Active Threats	Threats Removed	Last Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status
1	10.14.02.05-Feb-2018	No	No	01-Jan-2018	No	Yes	0	0	10:14:02 05-Feb-2018	11:36:28 05-Feb-2018	11:37:14 05-Feb-2018		Installed
2	00:46:01 05-Feb-2018	Yes	No	01-Jan-2018	Yes	Yes	2	0	00:46:01 05-Feb-2018	12:20:49 05-Feb-2018	12:21:28 05-Feb-2018		Installed
3	10:07:10 05-Feb-2018	No	No	01-Jan-2018	No	undetermined	0	0	10:07:10 05-Feb-2018	11:36:42 05-Feb-2018	11:37:14 05-Feb-2018		Installed
4	10:44:12 05-Feb-2018	No	No	01-Jan-2018	No	Yes	0	137	10:44:12 05-Feb-2018	11:30:14 05-Feb-2018	11:38:40 05-Feb-2018		Installed
5	10:11:08 05-Feb-2018	No	No	01-Jan-2018	No	undetermined	0	0	10:11:08 05-Feb-2018	11:36:43 05-Feb-2018	11:37:14 05-Feb-2018		Installed

Different operating systems for endpoints are identified by the following icons:

Icon	Description
	Windows OS
	Mac OS

- The interval to check for changes within the managed agents is one hour.



Indicators in the Deployment & Status Dashboard

Red W

If the endpoint is in an undesirable state, for example, if the endpoint is in an Attention Required state, the W icon is red. In addition to the Attention Required state, the W icon will be red if the agent is failing to retrieve status and threat information.

<div> <div>Install</div> <div>Uninstall</div> <div>Refresh</div> </div>					
			Machine.Group ID	Hostname	Attention Required
		W			
		W			Yes
		W			No

Warning Icon in Kaseya Agent Refresh Column

If an endpoint doesn't respond within three days or fails to gather data from the endpoint, the system alerts the administrator by a red triangle with an exclamation point in the center. This symbol will display in the Kaseya Agent Refresh column.

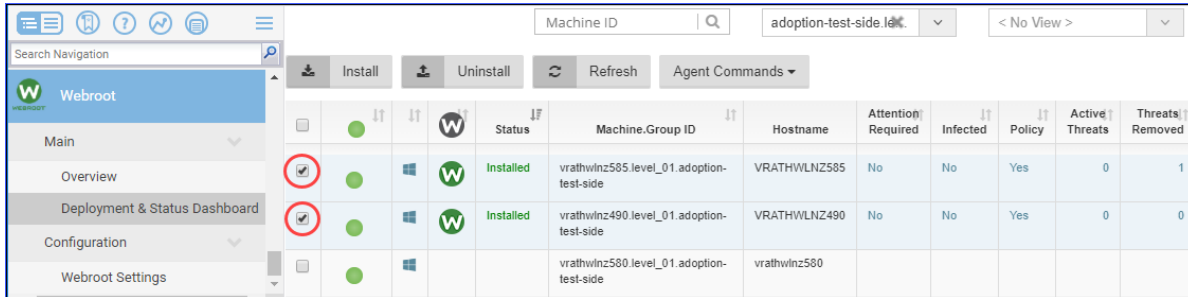
Endpoints	Last Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status
2	00:10:01 14-Mar-2017	00:21:53 14-Mar-2017	10:47:06 14-Mar-2017		Installed
0	08:00:01 14-Mar-2017	08:02:28 14-Mar-2017	08:42:20 14-Mar-2017		Installed
0	16:00:00 28-Feb-2017	16:33:32 28-Feb-2017	17:13:56 28-Feb-2017		Installed
0	02:41:00 10-Mar-2017	02:49:09 10-Mar-2017	04:37:07 13-Mar-2017		Installed

Running Webroot Agent Commands

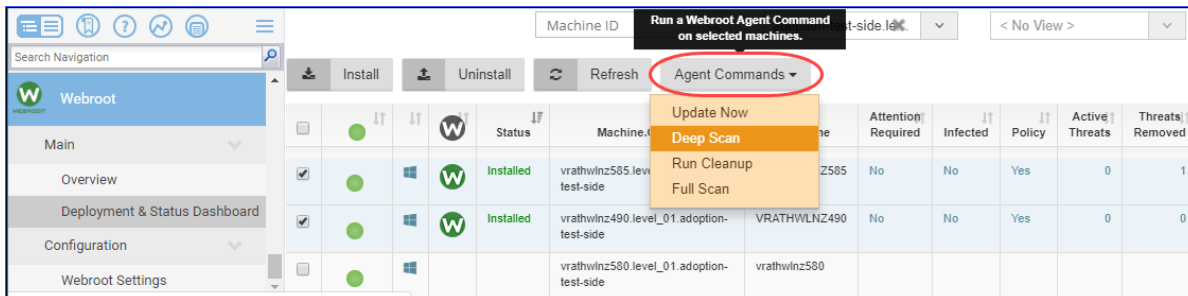
You can run Webroot Agent Commands on one or more Webroot Agents from the Deployment & Status Dashboard.

To run Webroot Agent Commands:

1. Go to **Webroot > Main > Deployment & Status Dashboard**.
2. Select the endpoints you want to run the commands on.



3. Click the **Agent Commands** button
4. Select the command, for example, *Deep Scan*.

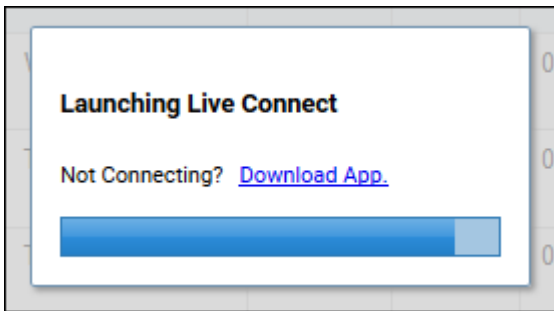
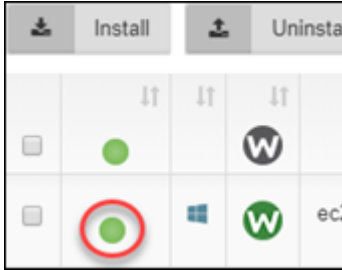


Launching Live Connect

The administrator can, as needed, validate the success of the Agent Procedures that execute Webroot activities and collect results.

To validate success:

1. In the Deployment & Status Dashboard, click on the green circular icon to directly get remote access to the selected device.

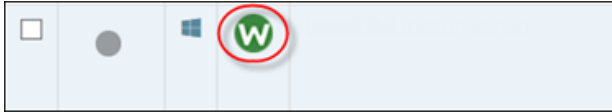


Detailed Webroot Agent Status & Agent Commands

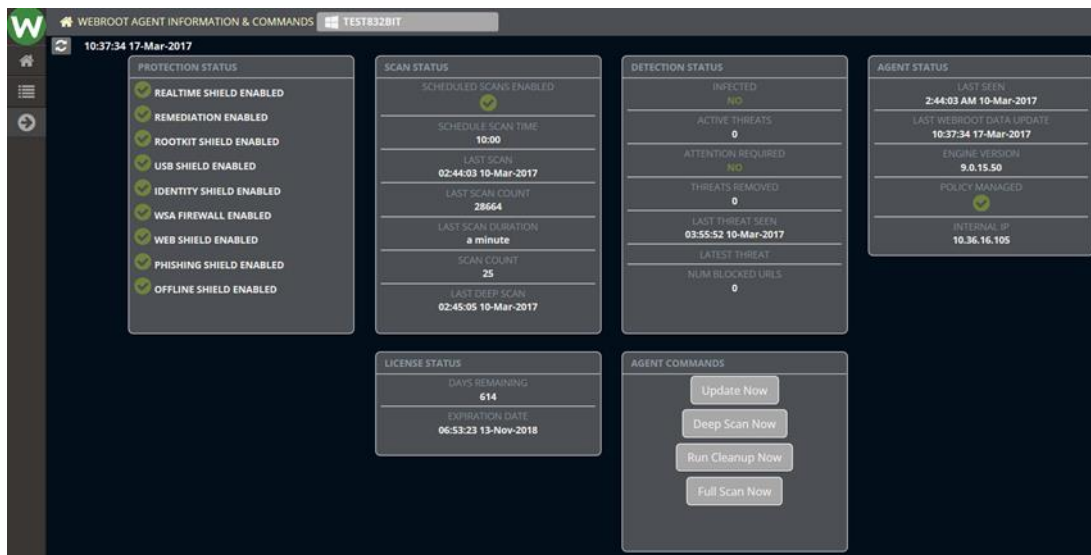
If you need detailed analysis of a specific WSAB agent or if you need to run WSAB Agent Commands, follow this procedure.

To generate analysis:

1. Click the desired **W** icon.



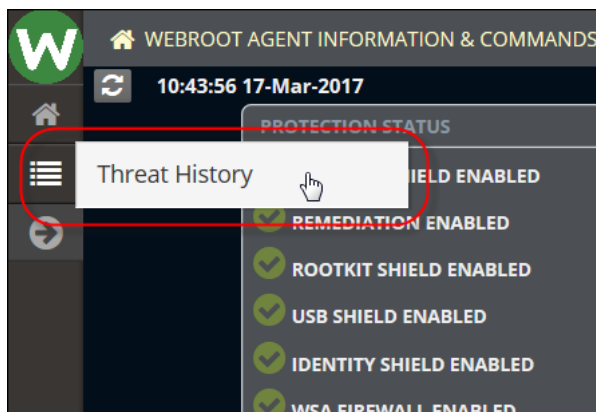
The system displays detailed Webroot Agent Information.



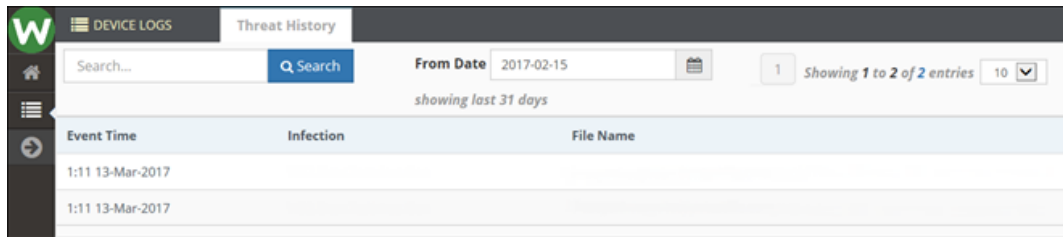
2. From this pane, you can run various commands, such as *Deep Scan Now* or *Run Cleanup Now*. These commands are executed within a few minutes.

Note: If Webroot agents are uninstalled and reinstalled, the Agent Status statistics are reset.

3. Click the **List** icon on the left side to view Webroot endpoint threat history.



Threat history information displays.



Note: Webroot endpoint threat history is persistent and will be available via the Executive Reports, even if endpoints are uninstalled or deactivated.

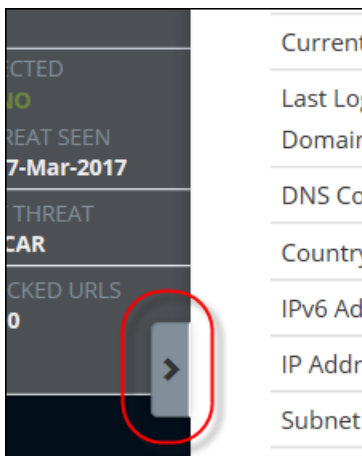
- For additional Kaseya-based information, click the **Expand** arrow.



The system expands the Machine Info window, which is scrollable.



5. To return to the Webroot Agent Information & Commands pane, click the **Side** arrow.



Integrated Alarm Parameters with Kaseya Alert Actions

If any installations, uninstallations, persistent threats or endpoint status failures occur on any Webroot agent, the module generates selected Kaseya Alert actions.

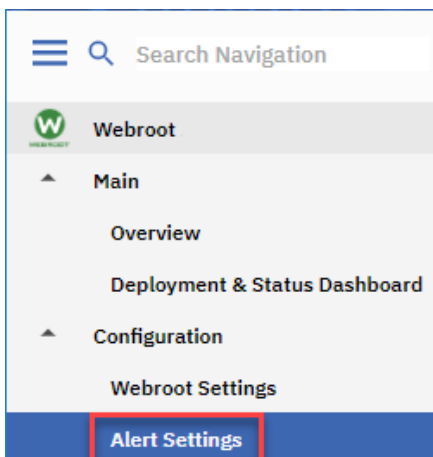
Note: To run alerts correctly **Kaseya emails and ticketing must be set up**, see section on **Setting Up Kaseya Emails and Ticketing** section below.

The following alerts can be selected:

- 1- **Install Failed** – if the install of a Webroot agent fails, an alert will be generated.
- 2- **Uninstall Failed** - if the Webroot agent fails to uninstall, an alert will be generated.
- 3- **Persistent Threats** – if there is a persistent threat that has not been removed for a selected period of time (0, 2, 4, 8, 16, 24) an alert will be generated.
- 4- **Endpoint Status** - If the agent procedure fails to gather information from the registry and can't load the status/data of the endpoint to the Webroot module server, an alert will be generated.

To set an alert:

1. From the Webroot menu, select **Alerts Settings**.



2. Select one or more of the **Webroot Alerts** checkboxes, such as *Persistent Threats*.

The screenshot shows the 'Webroot Alerts' configuration page. On the left is a navigation sidebar with the following items: Webroot, Main (Overview, Deployment & Status Dashboard), Configuration (Webroot Settings, Alert Settings), Agent, Agent Procedures, Anti-Malware, Antivirus, Audit, Backup, and Cloud Backup. The 'Alert Settings' section is currently selected. The main content area is titled 'Select Webroot Alerts' and includes the instruction 'Select the conditions for which you want to receive an alert'. Below this are four checkboxes: 'Install Failed', 'Uninstall Failed', 'Persistent Threat' (which is checked), and 'Endpoint Status Failure'. Each checkbox has an 'Edit details...' link to its right. Below the alert selection section is another section titled 'Select Alert Actions' with the instruction 'Select the actions to take when an enabled alert occurs'. This section contains three checkboxes: 'Create Alarm', 'Create Ticket', and 'Run Script after alert on the machine the alert occurred'. The 'Run Script' checkbox is currently selected. Below it is a dropdown menu labeled 'Select Agent Procedure' and a 'Clear' button. There is also a 'Send Email' checkbox and a text field for 'Email recipients (Comma separate multiple addresses)'. At the bottom of the main content area is an 'Apply' button.

3. Click on *Edit details*.

This is a close-up view of the 'Select Webroot Alerts' section. It shows the same four checkboxes as the previous screenshot: 'Install Failed', 'Uninstall Failed', 'Persistent Threat' (checked), and 'Endpoint Status Failure'. Each checkbox has an 'Edit details...' link to its right. The 'Edit details...' link for the 'Persistent Threat' checkbox is highlighted with a red rectangular box.

4. Modify the **Alert Details** as necessary the click on **Save**.

Edit Alert Details - Persistent Threat

Alert re-arm interval
Enable additional alerts of this type from an endpoint after hours.

Alert Template
Customize the template for the alert.
Alarm Summary / Ticket Summary / Email Subject

Active Threats on <id>

Alarm Message / Ticket Note / Email Body
Active Threats on <id> at <ts> (UTC).
Latest Threat: <wr-lt>

Available template parameters

Key	Description
<id>	endpoint on which event occurred
<ts>	date/time (in UTC) at which alert is sent
<wr-lt>	Webroot Latest Threat seen

[Restore Defaults](#)

[Save](#) [Close](#)

Note: Alerts for **Endpoint Status Failure** and **Persistent Threats** have a re-arm time of 0, 2, 4, 8, 16, 24 hours (if set to "0" the alert check cycle is once per hour). For example, if the Endpoint Status fails on the hourly check it would create an alert every hour, but with a selection of 8 hours, this alert would only trigger every 8 hours.

5. Select the relevant **Alert Criteria** checkbox, such as *Create Ticket* then click the **Apply** button.

Select Webroot Alerts
Select the conditions for which you want to receive an alert

☐ Install Failed [Edit details...](#)

☐ Uninstall Failed [Edit details...](#)

☒ Persistent Threat [Edit details...](#)

☐ Endpoint Status Failure [Edit details...](#)

Select Alert Actions
Select the actions to take when an enabled alert occurs

☐ Create Alarm

☒ Create Ticket

☐ Run Script after alert on the machine the alert occurred
Select Agent Procedure [Clear](#)

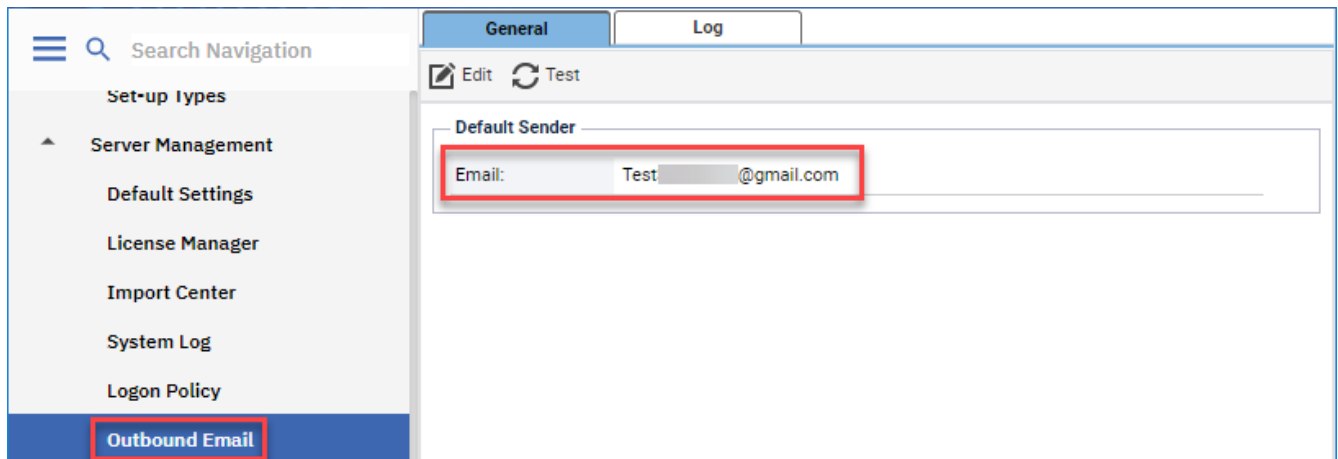
☐ Send Email
Email recipients (Comma separate multiple addresses)

[Apply](#)

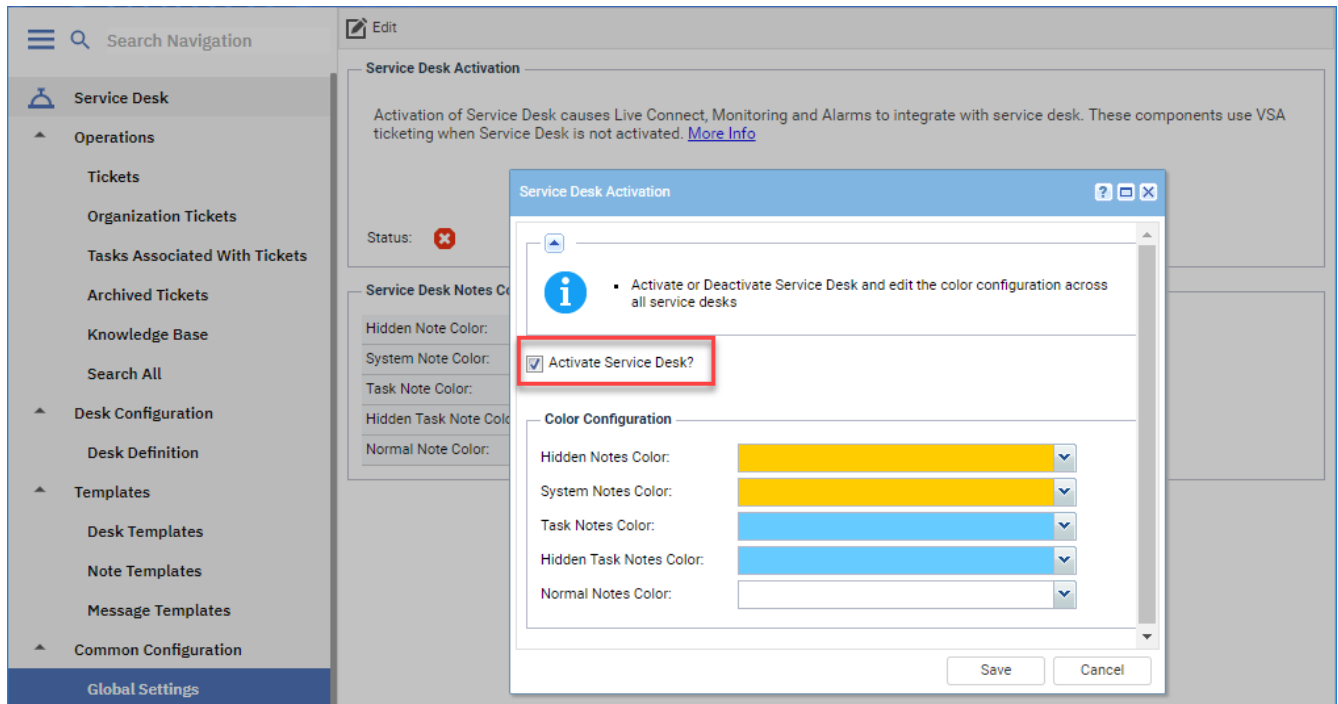
Note: In order to receive Alerts via email, you must enter a valid email address.

Setting Up Kaseya Emails and Ticketing

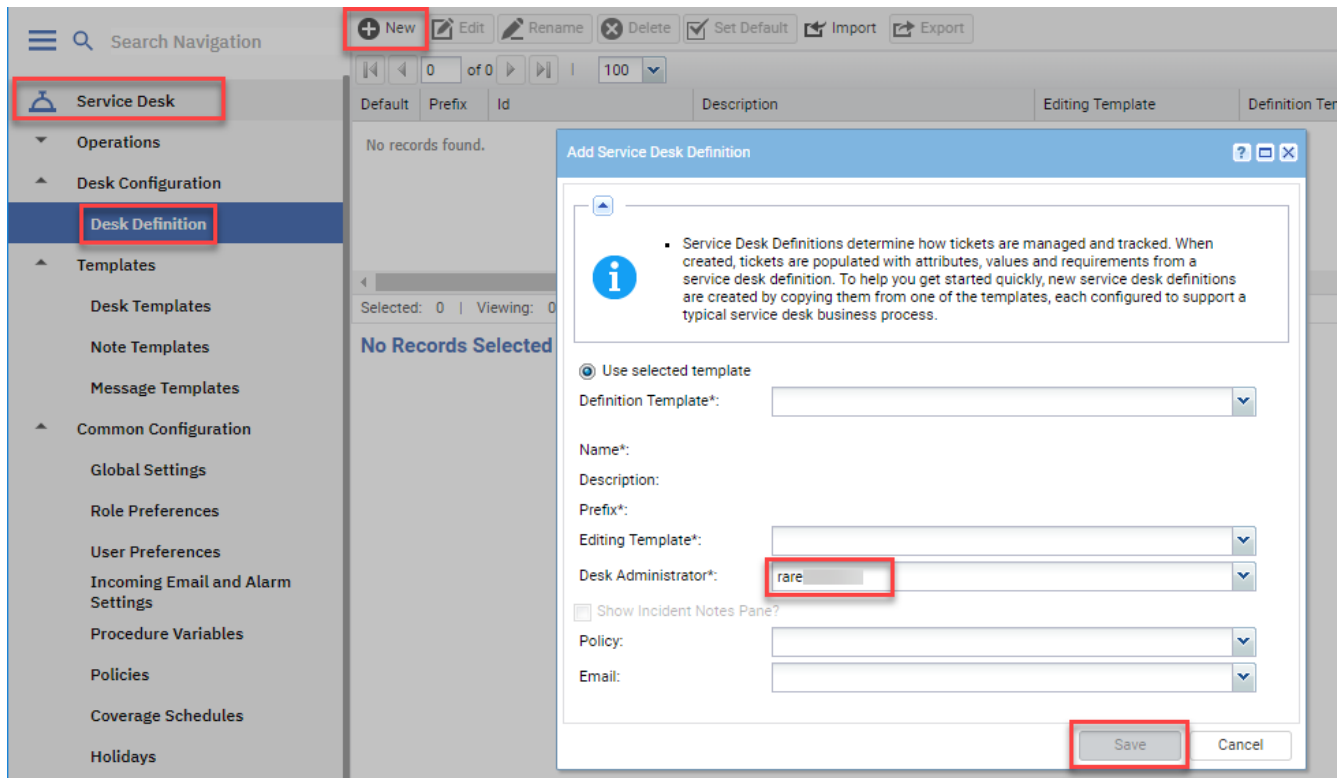
To setup the email capabilities, the outbound email must be setup within Kaseya **System > Server Management > Outbound Email**



If you want tickets to be created within **Service Desk**, you must activate Service Desk within function **Service Desk > Common Configuration > Global Settings**.



Once you have activated Service Desk then you will need to create a desk definition. Once complete the tickets will be generated.



Note: Depending on how you want to set up Service Desk, there may be other options you may need to enable. Please refer to Kaseya for full details.

If you do **not** want to use Service Desk, then make sure it's not enabled. Then by default the Webroot Plugin Alerts will create tickets within the ticketing module.

The screenshot displays the Webroot VSA Cloud Module V2.0 Ticketing interface. The sidebar on the left contains navigation options: Ticketing, Manage Tickets, View Summary, Create/View, Delete/Archive, Migrate Tickets, Configure Ticketing, Notify Policy, Access Policy, Assignee Policy, Due Date Policy, Edit Fields, Email Reader, Email Mapping, Agent, Agent Procedures, Anti-Malware, Antivirus, Audit, Backup, and Cloud Backup. The main area shows a list of tickets with columns: ID, Machine ID, Assignee, Category, Status, Priority, SLA Type, Dispatch Tech, Approval, Hours Worked, Last Modified Date, Creation Date, and Due Date. The tickets are filtered by 'Open' status and 'High' priority. The list shows several tickets related to 'Active Threats' and 'Collection of data on vrathwinz505.root.brada-org01 is not working'.

ID	Machine ID	Assignee	Category	Status	Priority	SLA Type	Dispatch Tech	Approval	Hours Worked	Last Modified Date	Creation Date	Due Date
637	wadmins-macbook-pro.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	9:10:49 am 5-Jun-19	9:10:49 am 5-Jun-19	9:10:49 am 12-Jun-19
636	vrathwinz505.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	9:02:48 am 5-Jun-19	9:02:48 am 5-Jun-19	9:02:48 am 12-Jun-19
635	vrathwinz506.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	1:08:14 am 5-Jun-19	1:08:14 am 5-Jun-19	1:08:14 am 12-Jun-19
634	wadmins-macbook-pro.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	12:11:12 am 5-Jun-19	12:11:12 am 5-Jun-19	12:11:12 am 12-Jun-19
633	vrathwinz505.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	12:02:12 am 5-Jun-19	12:02:12 am 5-Jun-19	12:02:12 am 12-Jun-19
632	wadmins-macbook-pro.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	4:10:39 pm 4-Jun-19	4:10:39 pm 4-Jun-19	4:10:39 pm 11-Jun-19
631	vrathwinz506.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	4:07:40 pm 4-Jun-19	4:07:40 pm 4-Jun-19	4:07:40 pm 11-Jun-19
630	vrathwinz505.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	3:02:38 pm 4-Jun-19	3:02:38 pm 4-Jun-19	3:02:38 pm 11-Jun-19
629	wadmins-macbook-pro.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	7:10:54 am 4-Jun-19	7:10:54 am 4-Jun-19	7:10:54 am 11-Jun-19
628	vrathwinz506.root.brada-org01	unassigned	Application problem	Open	High	None	No	Not required	0.0	7:07:54 am 4-Jun-19	7:07:54 am 4-Jun-19	7:07:54 am 11-Jun-19

Disclaimer

While every effort has been made to maintain document accuracy, product version updates may change or alter functionality and look of the screen shots. Please report document omissions or issues to your Webroot representative or post your comments in our Kaseya Partner Group [here](#).

This document is intended as a Getting Started Guide. For more information and product best practices, please contact your local Webroot representative.
