Kaseya VSA On-Prem Module

For Webroot Plugin Version 2.6.20149.1 and above

Getting Started Guide

Document Version 2.6.2

Table of Contents

Overview

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

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

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 this guide before deployment.

This module is in complete compliance to all third party integration definitions for Kaseya on-prem VSA version 9.3 and up. At the time of publication, the module was tested up to VSA version 9.5.

What's New With Version 2.6

New Features

- Added Customer Support Diagnostics command button to gather endpoint diagnostic information for Webroot support.
- Added the ability to retain Kaseya machine admin defaults to navigate different parts of the VSA without having to search machine filters again, making the integration more seamless between other modules.
- Added extensive Alert Setting features with different Alerts and actions.
- Added "Webroot Uninstalled or Removed" alert.

Enhancements

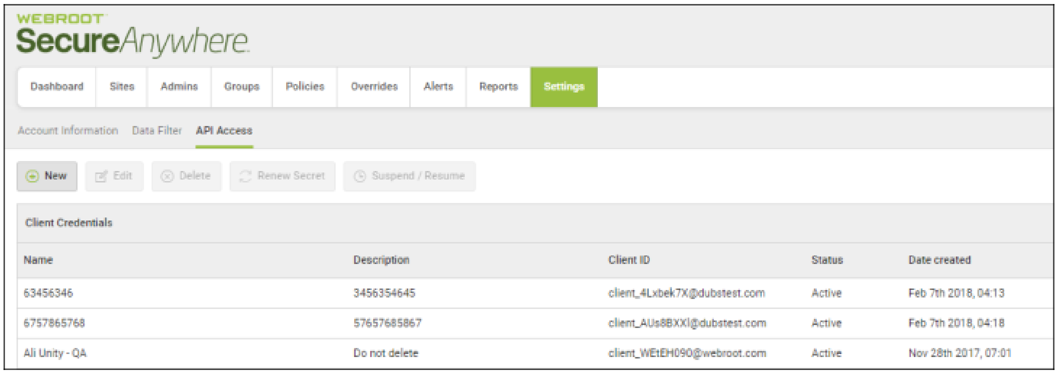
- Redesigned Unity API configuration screen to simplify API sign-on process and enhance security.
- Added self-healing process to try and fix stalled actions.
- Added enhanced error logging.
- Temporarily removed the Webroot Console SSO feature until it is re-purposed and reintroduced.

Bug Fixes

- Fixed Auto Deployment for machine with uninstall status.
- Fixed Agent procedure OS type check issue.
- Fixed Webroot Settings scope issue.
- Minor fixes and UI enhancements.

Prerequisites

- This guide.
- One of the following:
  - A Webroot GSM Super Admin account.
  - At least one Webroot SecureAnywhere site key.
  - GSM Account Settings for API Access. How to obtain the needed account settings for API access is described later in this document. For more information, see Controlling Access to Webroot Settings.



Client Credentials

Name	Description	Client ID	Status	Date created
63456346	3456354645	client_4Lxbek7X@dubstest.com	Active	Feb 7th 2018, 04:13
6757865768	57657685867	client_AUs8BXXl@dubstest.com	Active	Feb 7th 2018, 04:18
Ali Unity - QA	Do not delete	client_WEtEH090@webroot.com	Active	Nov 28th 2017, 07:01

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 your customers as different sites within Webroot GSM; one key per customer.
- Kaseya on-prem VSA Version 9.3 and up.
- Kaseya administrator account.
- Kaseya Outbound Email Settings Administration.
- **Minimum - Microsoft SQL Server 2012 (SP3 Recommended)**
- Kaseya Module installer

  `WR_KPlugin_2.6.xx.xxxx.exe`
- The latest installer, which is available here.
- To install the Webroot Kaseya module, you must have access to the Kaseya server.

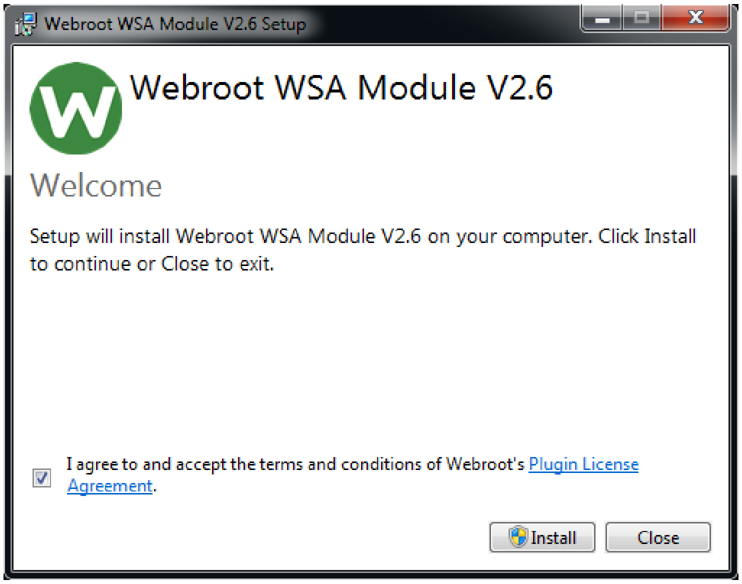
Installing the Webroot Kaseya Module

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

To install Webroot Kaseya Module:

1. Copy and unzip the installer package to your Kaseya server.
2. Install the Kaseya Module by running the following file:

   `WR_KPlugin_2.6.xx.xxxx.exe`
3. Follow the on-screen prompts.



Webroot WSA Module V2.6 Setup

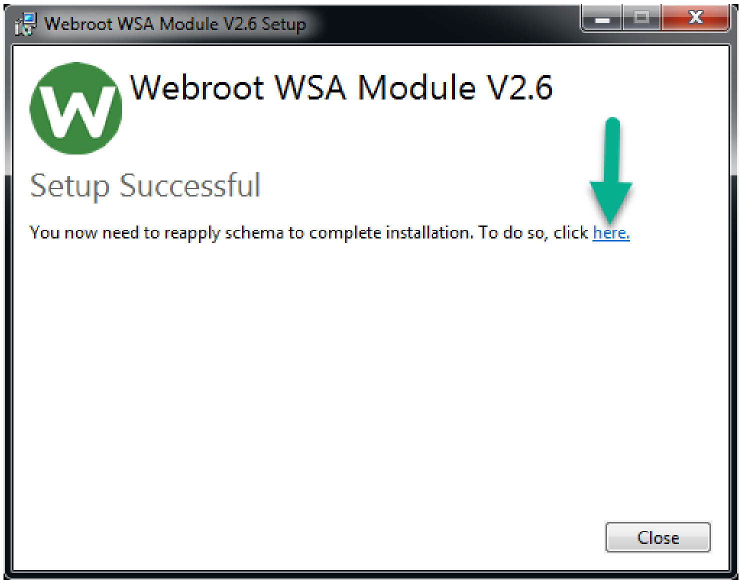
Webroot WSA Module V2.6

Welcome

Setup will install Webroot WSA Module V2.6 on your computer. Click Install to continue or Close to exit.

☑ I agree to and accept the terms and conditions of Webroot's Plugin License Agreement.

Until the Setup Successful window displays.



Webroot WSA Module V2.6 Setup

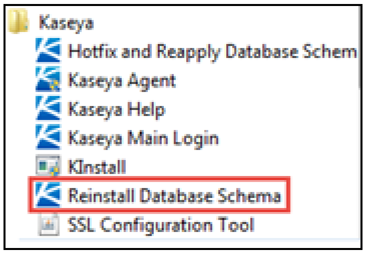
Webroot WSA Module V2.6

Setup Successful

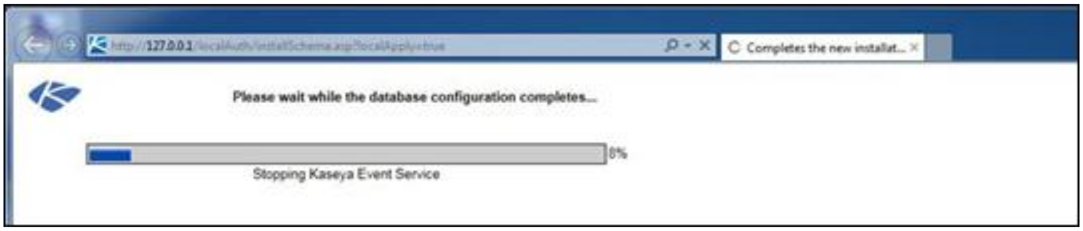
You now need to reapply schema to complete installation. To do so, click here.

4. After the Webroot Kaseya Module has completed installation, you must reinstall the Database Schema. You can either use the link on the installer success screen, or access this from the Windows Start menu using the following path:

   Start > All Programs > Kaseya > Reinstall Database Schema



The system installs the database schema.


http://127.0.0.1/localAuth/installSchema.asp?localApply=true
Completes the new installat...

Please wait while the database configuration completes...

8%

Stopping Kaseya Event Service

5. After this step has completed, you can access the Webroot Kaseya Module.

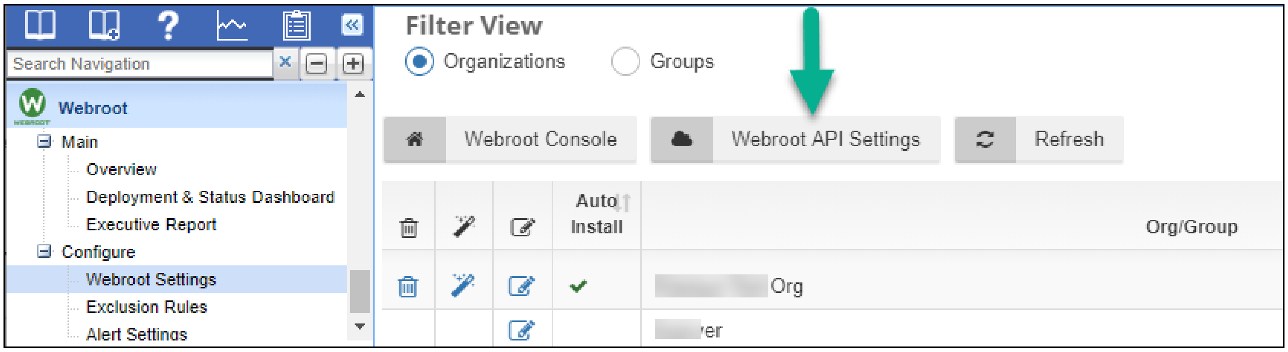
Enabling Webroot Unity API

We strongly recommend you enable Webroot Unity API functionality within your plug-in to take full advantage of the plugins improved performance, user experience and features.

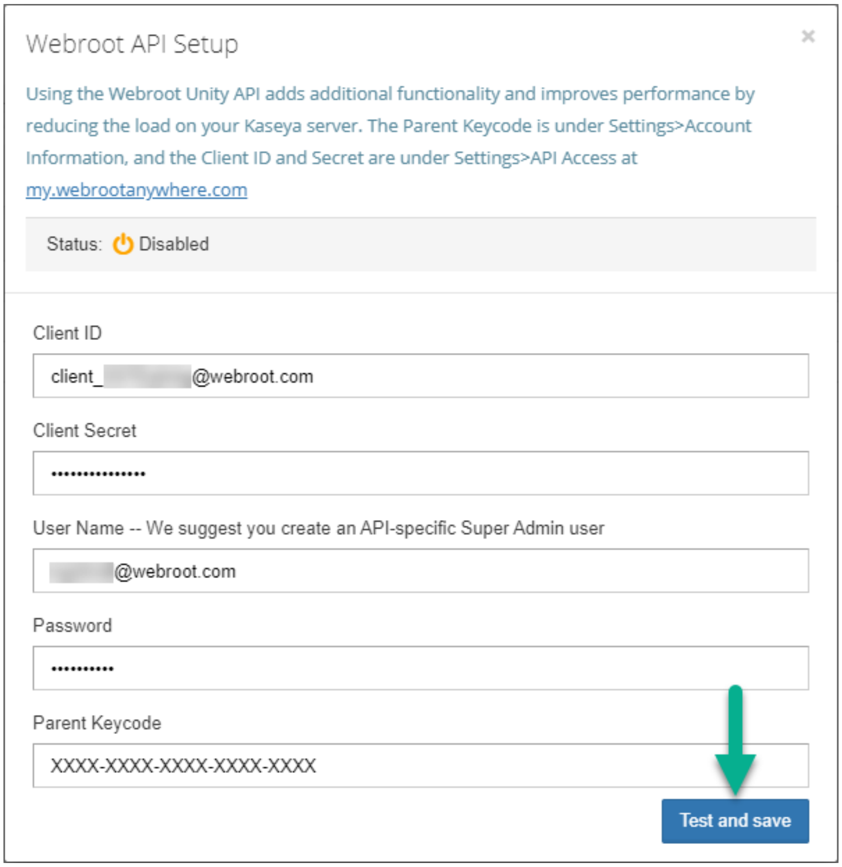
NOTE: You can use the default settings, which utilize Kaseya agent procedures to gather data. However, you may experience higher loads on the Kaseya server. In addition, certain data elements & actions will not be available without enabling the Webroot Unity API.

To enable the Webroot Unity API:

1. Please click on **Webroot API Settings** button and enter valid credentials. For further information on how to obtain credentials please follow the instructions here.



The Webroot API Setup window displays.



Webroot API Setup ×

Using the Webroot Unity API adds additional functionality and improves performance by reducing the load on your Kaseya server. The Parent Keycode is under Settings>Account Information, and the Client ID and Secret are under Settings>API Access at my.webrootanywhere.com

Status: Disabled

Client ID: client_[redacted]@webroot.com

Client Secret: •••••••••••••••

User Name -- We suggest you create an API-specific Super Admin user: [redacted]@webroot.com

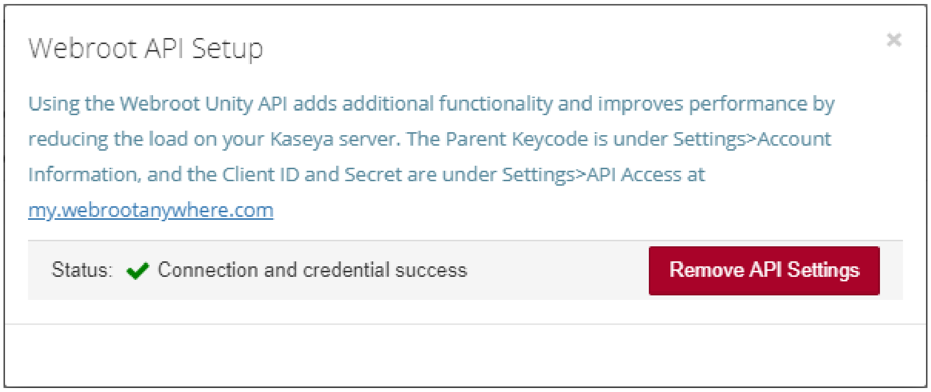
Password: ••••••••••

Parent Keycode: XXXX-XXXX-XXXX-XXXX-XXXX

2. Click the **Test and save** button illustrated above.

Note: If you don't have a GSM key/Parent Key, contact your Webroot sales representative.

3. If all credentials are correct, then the screen will auto-close – you are all set!
4. If you would like to **change** or **check the operation of the API**, just click on the **Webroot API Settings** button again. The following screen will pop-up. You can also check the API status by going to **Overview > Webroot Plugin Info** tab.



Webroot API Setup

Using the Webroot Unity API adds additional functionality and improves performance by reducing the load on your Kaseya server. The Parent Keycode is under Settings>Account Information, and the Client ID and Secret are under Settings>API Access at my.webrootanywhere.com

Status: ✓ Connection and credential success

5. To change the credentials or to disable the API, simply click on **Remove API Settings** button and start the whole process again.

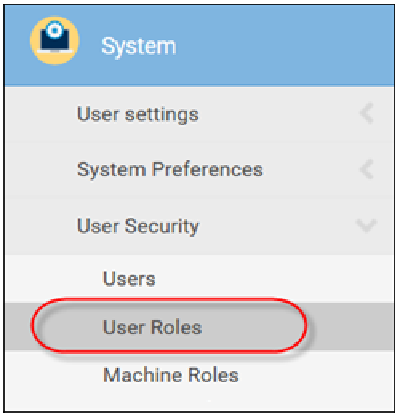
Note: If the test fails, the error message will indicate what's wrong with your settings. Fix the issue before proceeding.

Controlling Access to Webroot Settings

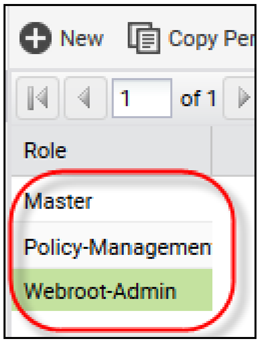
As needed, you can control an admin's access to Webroot settings. We recommend that you allow access to only those admins who will make GSM parent keycode assignments.

To control access to Webroot settings:

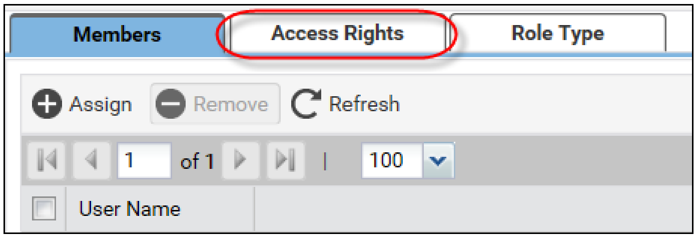
1. From the main menu, select **System > User Roles**.



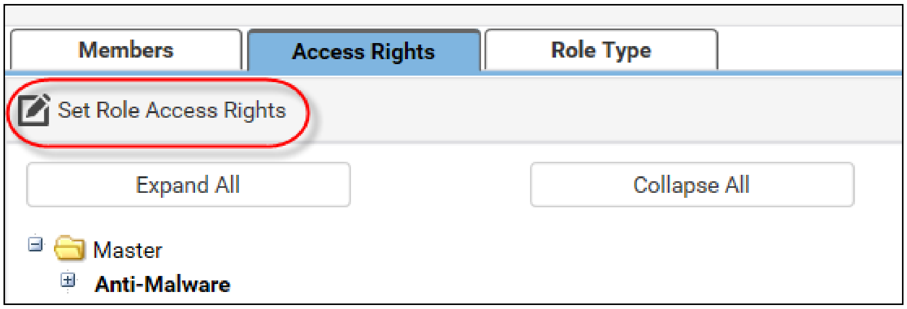
1. In the Role pane, select the role you want to apply the permissions to.



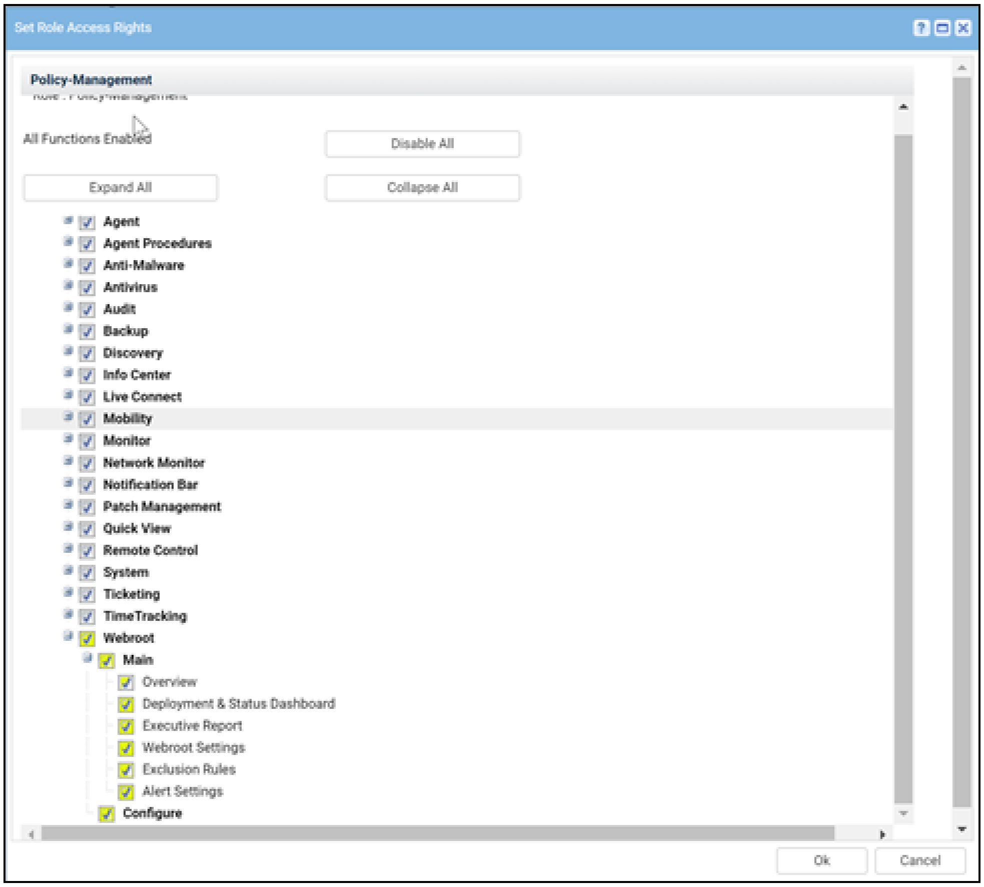
2. In the Set Role Access Rights pane, click the **Access Rights** tab.



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



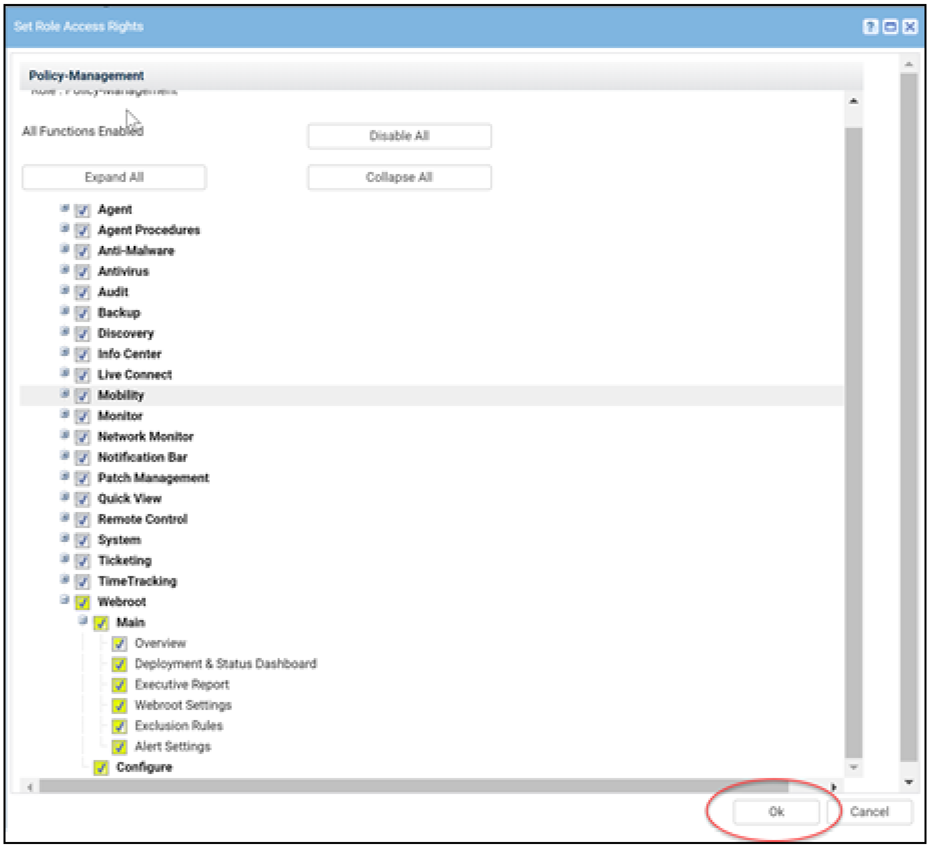
4. From the list, select **Master > Webroot** to expand the list.
5. Select the checkboxes next to the areas that you want to allow access to.
    - Webroot
    - Main
    - Overview
    - Deployment & Status Dashboard
    - Webroot Settings
    - Exclusion Rules
    - Alert Settings
    - Executive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



All Functions Enabled

- ☑ Agent
- ☑ Agent Procedures
- ☑ Anti-Malware
- ☑ Antivirus
- ☑ Audit
- ☑ Backup
- ☑ Discovery
- ☑ Info Center
- ☑ Live Connect
- ☑ Mobility
- ☑ Monitor
- ☑ Network Monitor
- ☑ Notification Bar
- ☑ Patch Management
- ☑ Quick View
- ☑ Remote Control
- ☑ System
- ☑ Ticketing
- ☑ TimeTracking
- ☑ Webroot
    - ☑ Main
        - ☑ Overview
        - ☑ Deployment & Status Dashboard
        - ☑ Executive Report
        - ☑ Webroot Settings
        - ☑ Exclusion Rules
        - ☑ Alert Settings
    - ☑ Configure

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



Policy-Management

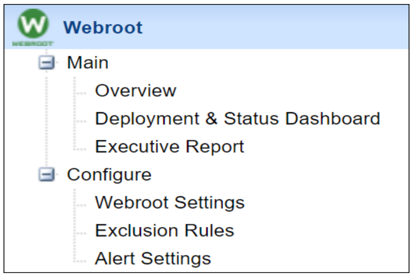
All Functions Enabled

- ☑ Agent
- ☑ Agent Procedures
- ☑ Anti-Malware
- ☑ Antivirus
- ☑ Audit
- ☑ Backup
- ☑ Discovery
- ☑ Info Center
- ☑ Live Connect
- ☑ Mobility
- ☑ Monitor
- ☑ Network Monitor
- ☑ Notification Bar
- ☑ Patch Management
- ☑ Quick View
- ☑ Remote Control
- ☑ System
- ☑ Ticketing
- ☑ TimeTracking
- ☑ Webroot
  - ☑ Main
    - ☑ Overview
    - ☑ Deployment & Status Dashboard
    - ☑ Executive Report
    - ☑ Webroot Settings
    - ☑ Exclusion Rules
    - ☑ Alert Settings
  - ☑ Configure

Getting Started and Deployment

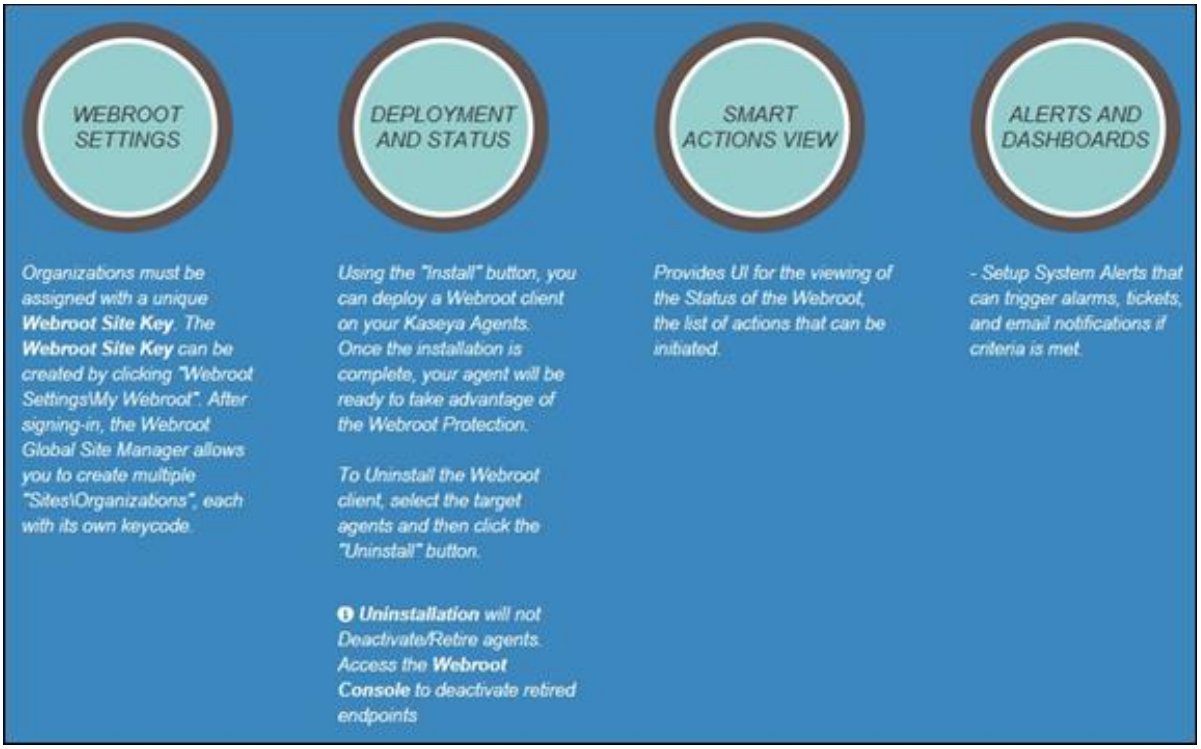
The user interface within the Kaseya Module is designed to be easy to use and is broken down to six main menu items:

- **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 Agent Deployment.
- **Webroot Settings** – Webroot specific settings, such as site or default keycode, Webroot console access, and auto Webroot adoption wizard. See Adopting Existing Webroot Agents.
- **Alert Settings** – Alerts and alert criteria. See Integrated Alarm Parameters with Kaseya Alert Actions.
- **Executive Report** – Generating malware reports. See Running Executive Reports.
- **Exclusion Rules** – Create exclusion rules to Install, Auto Install, and Adoption. See Auto-Deploy Exclusion Rules.



Overview Menu

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



*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.*

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.

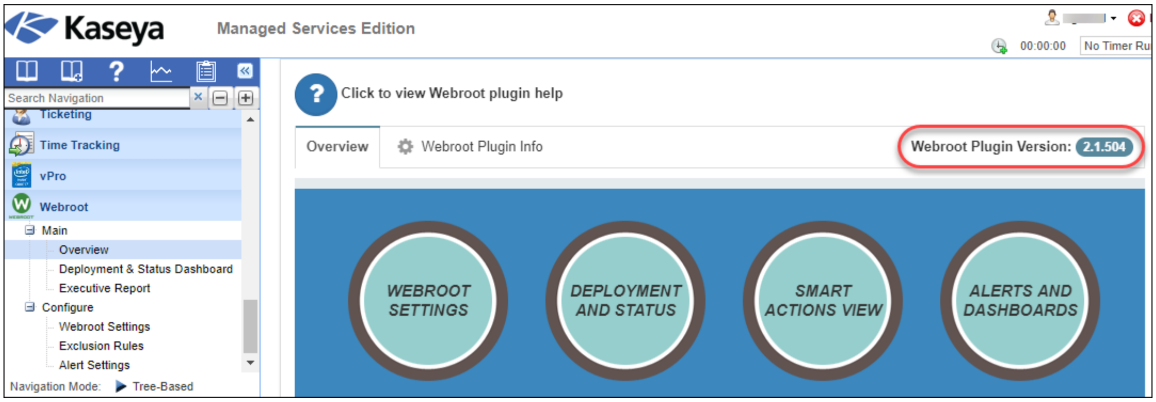
To Uninstall the Webroot client, select the target agents and then click the "Uninstall" button.

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

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

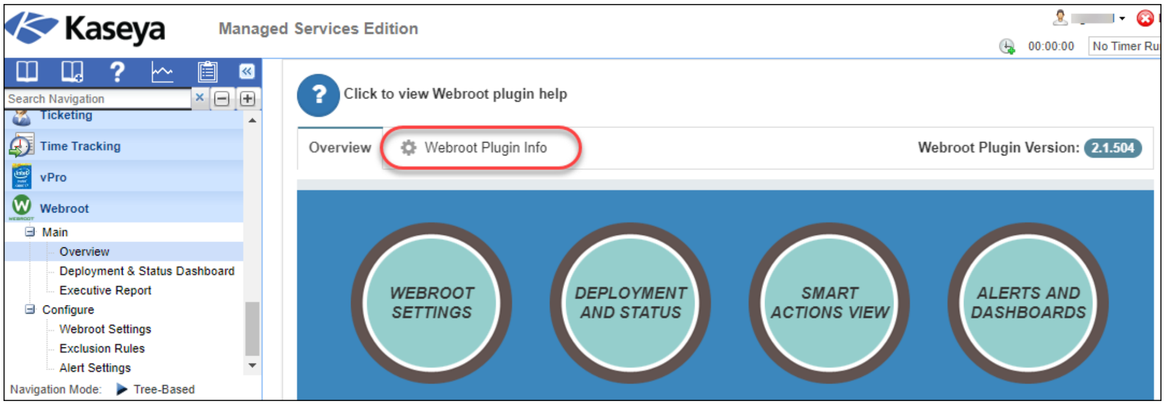
- Setup System Alerts that can trigger alarms, tickets, and email notifications if criteria is met.

Included on the Overview tab is information about the plugin version, which is located in the upper right corner.



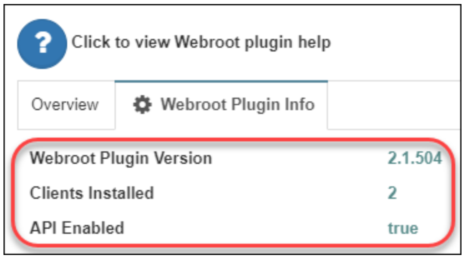
Webroot Plugin Version: 2.1.504

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



Webroot Plugin Version: 2.1.504

This displays information about the version, the number of clients installed, and whether or not API has been enabled.



Webroot Plugin Version	2.1.504
Clients Installed	2
API Enabled	true

Webroot Secure Anywhere Business Endpoint (Webroot Agent) Deployment

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

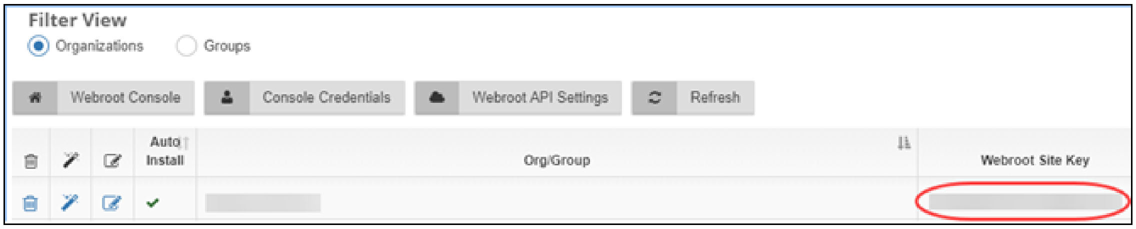
Note: If you have an existing Webroot deployment, you can adopt already installed endpoints in to the Kaseya Module. For more information, see Adopting Existing Webroot Agents.

Configuring and Obtaining a Unique Webroot Site Key

- If you have Webroot API enabled, follow the procedure that starts below.
- If you don't have Webroot API enabled, please go to Enabling Webroot Unity API.

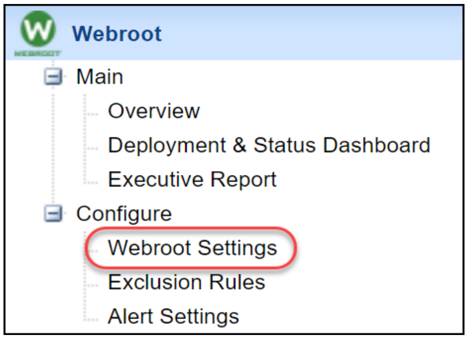
To configure with Webroot API enabled:

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

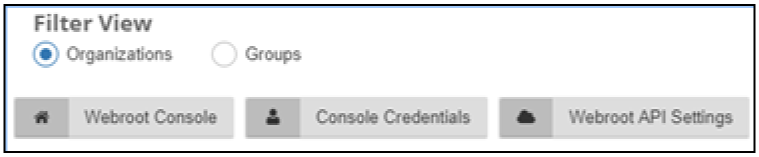


To obtain a unique site key:

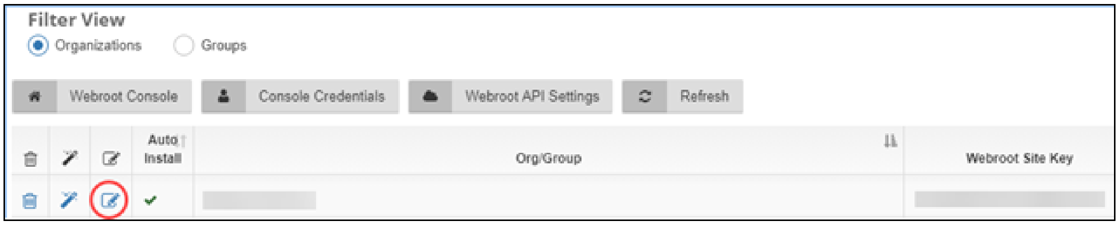
1. From the main menu, select **Webroot > Webroot Settings**.



- 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.

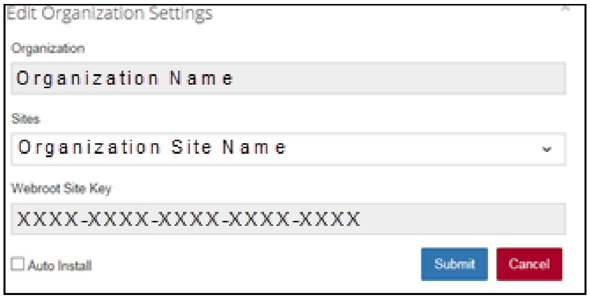


2. For the organization or group that you want to edit, click the **Edit** icon.



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

Note: If you select the **Auto Install** checkbox, a background task that runs once per hour ensures Webroot agents are deployed automatically to all Kaseya endpoints within the defined organization or group.



Edit Organization Settings

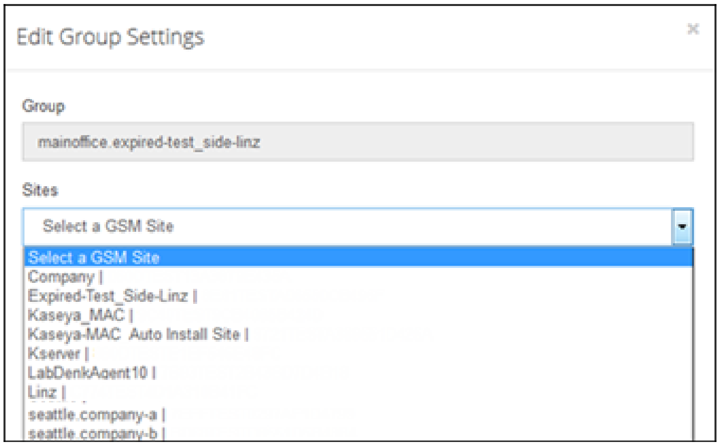
Organization: Organization Name

Sites: Organization Site Name

Webroot Site Key: XXXX-XXXX-XXXX-XXXX-XXXX

□ Auto Install

3. From the Sites drop-down menu, select the site you want to use.

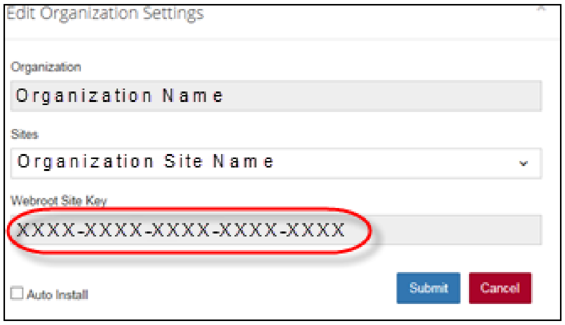


Edit Group Settings

Group: mainoffice.expired-test_side-linz

Sites: Select a GSM Site

4. Since Webroot API is enabled, the Webroot Site Key field is already populated as soon as a site has been selected from the drop-down menu.



Edit Organization Settings

Organization: Organization Name

Sites: Organization Site Name

Webroot Site Key: XXXX-XXXX-XXXX-XXXX-XXXX

□ Auto Install

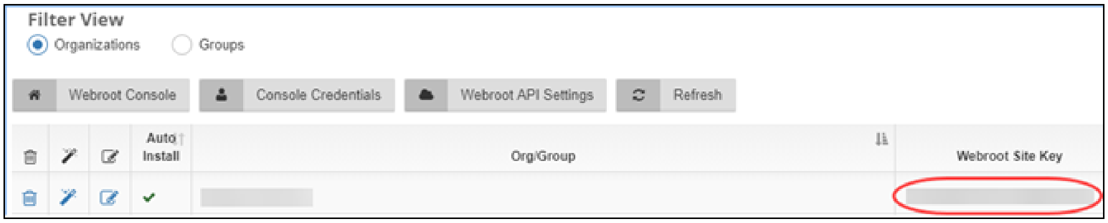
5. Click the **Submit** button to commit the key to the organization.

   Note: Version 2.0 and above allows assignment of keycodes, Auto Install, and adoption to the first level groups. Version 2.1 has added the ability to assign keycodes, auto install, and adoption to all Kaseya Group Levels.

   - Kaseya customers can now add keycodes to subgroups.
   - Lowest Group has priority.
   - Auto Install can be applied to subgroups.
   - Adoption Wizard will apply to subgroups.

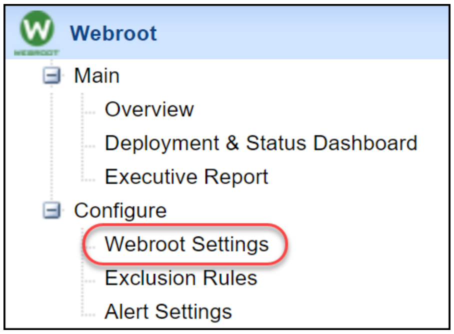
To configure without Webroot API enabled:

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.

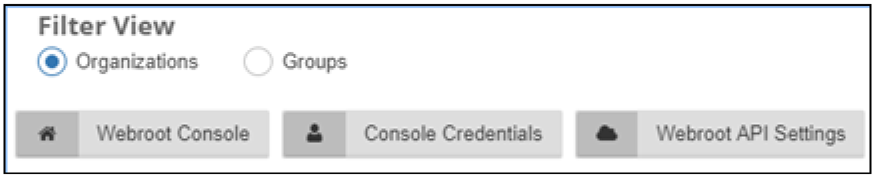


To obtain a unique site key:

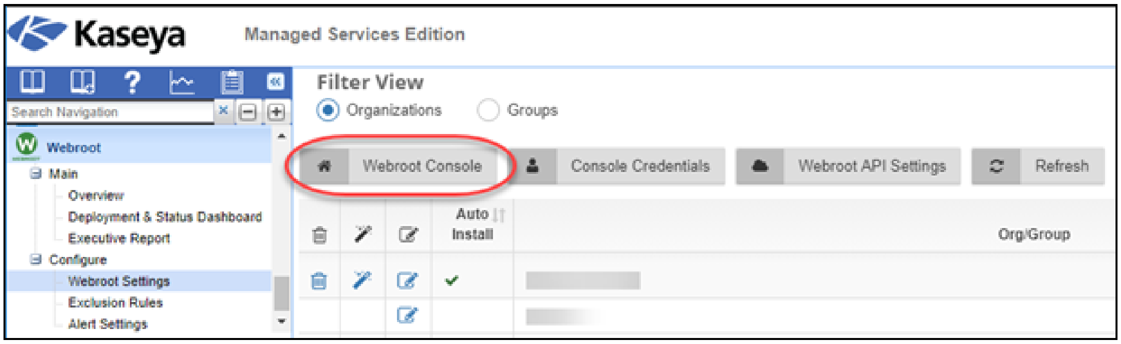
1. From the main menu, select **Webroot > Webroot Settings**.



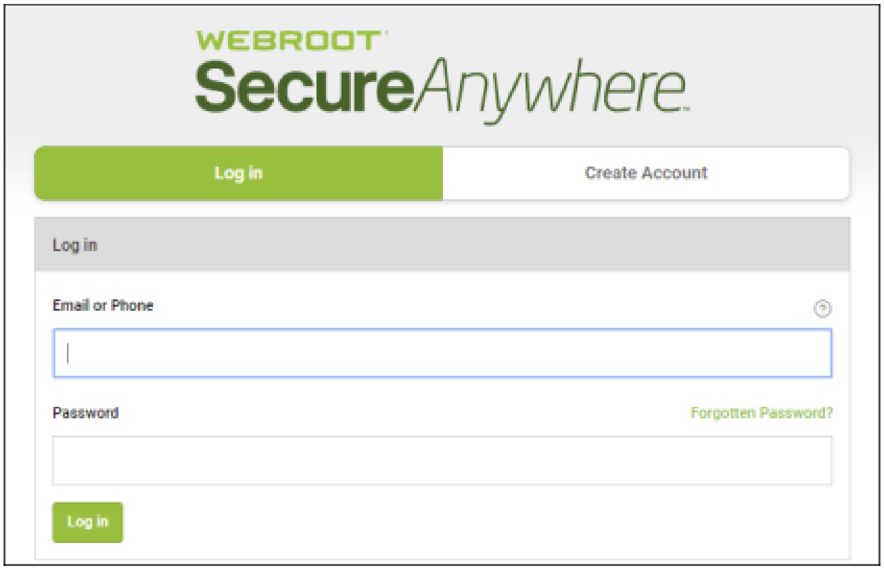
The Filter View pane displays with the Organizations radio button active, though you can select the **Groups** radio button, as needed.



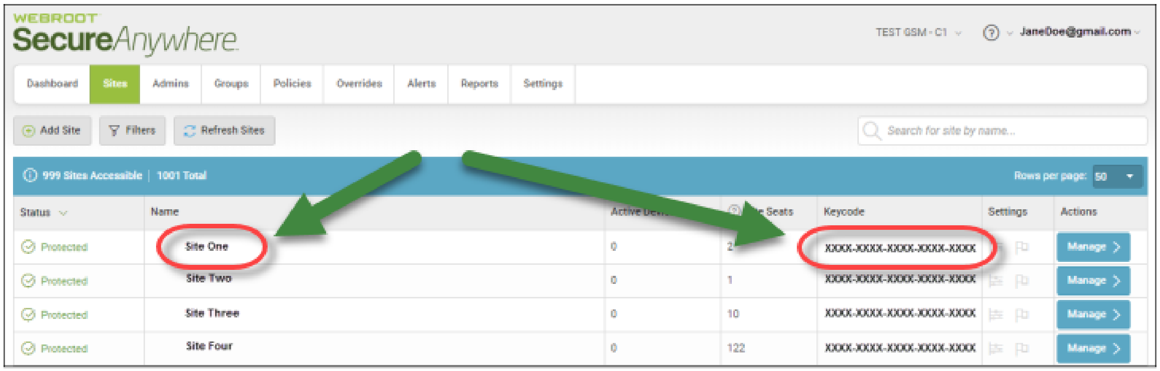
2. Click the **Webroot Console** button.



The Webroot SecureAnywhere login page displays.

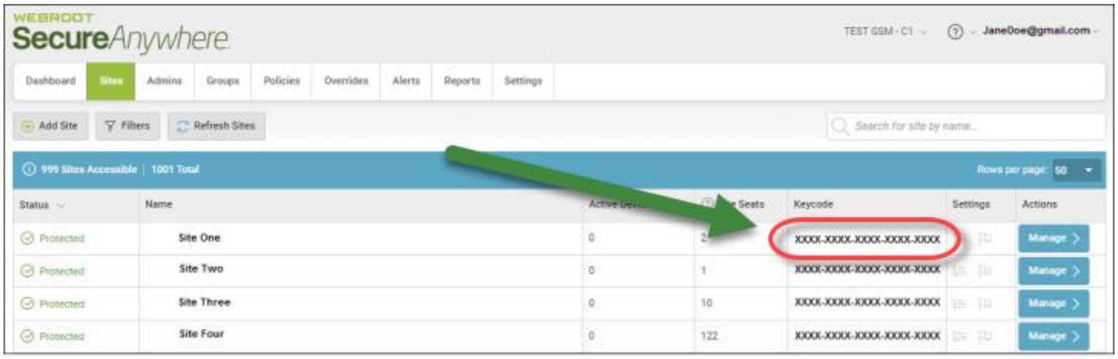


3. Log in using your Webroot credentials.
4. From the main panel, browse to your GSM console and create a new site that matches the organization in in the Kaseya VSA.



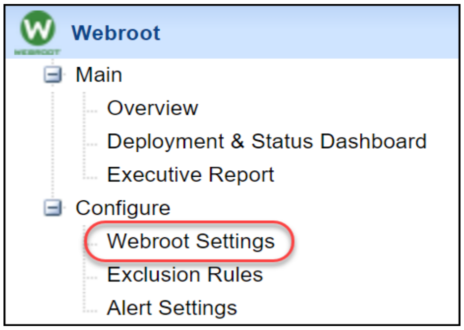
Status	Name	Active Dev	e Seats	Keycode	Settings	Actions
Protected	Site One	0	2	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >
Protected	Site Two	0	1	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >
Protected	Site Three	0	10	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >
Protected	Site Four	0	122	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >

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

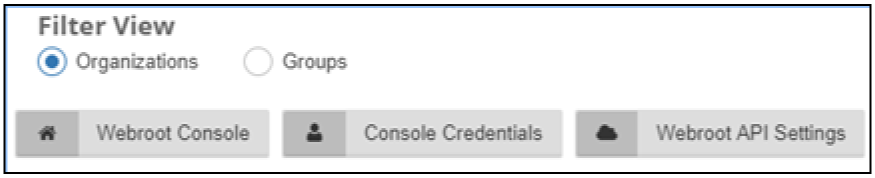


Status	Name	Active De	Seats	Keycode	Settings	Actions
Protected	Site One	0	2	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >
Protected	Site Two	0	1	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >
Protected	Site Three	0	10	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >
Protected	Site Four	0	122	XXXX-XXXX-XXXX-XXXX-XXXX		Manage >

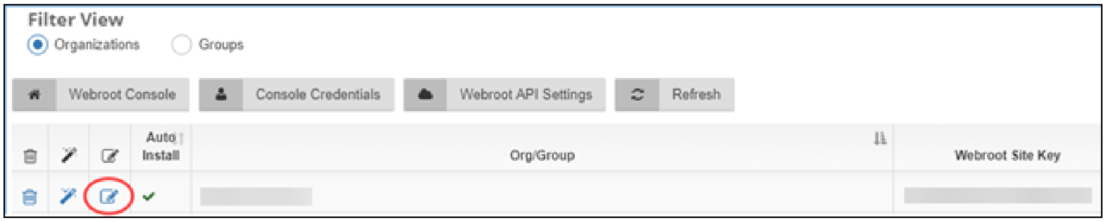
6. In Kaseya, from the main menu, select **Webroot > Webroot Settings**.



The Filter View pane allows you to filter by organization or group, which lets you assign Webroot site keycodes to Kaseya organizations or groups.



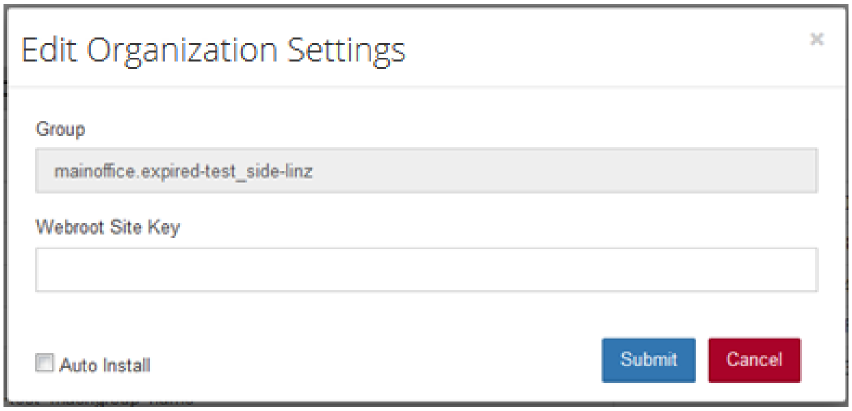
7. For the organization or group that you want to edit, click the **Edit** icon.



			Auto Install	Org/Group	Webroot Site Key
			✓		

Note: If you select the **Auto Install** checkbox, a background task that runs once per hour ensures Webroot agents are deployed automatically to all Kaseya endpoints within the defined organization or group.

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

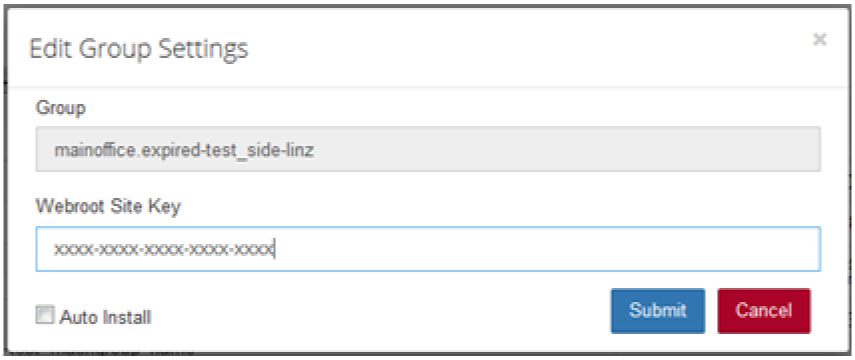


Edit Organization Settings

Group: mainoffice.expired-test_side-linz

Webroot Site Key:

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



Edit Group Settings

Group: mainoffice.expired-test_side-linz

Webroot Site Key: xxxx-xxxx-xxxx-xxxx-xxxx

9. Click the **Submit** button to commit the key to the organization.

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 organizations within the Kaseya Module. We recommend a site key per organization, unless you have very small organizations consisting of one or two seats.

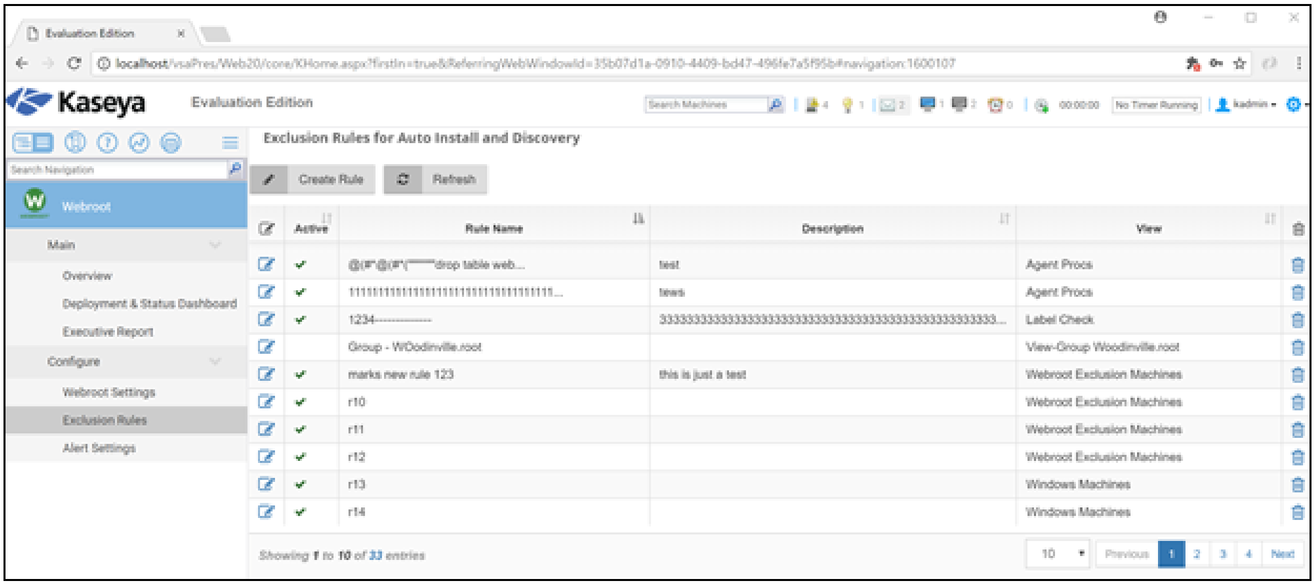
Auto-Deploy Exclusion Rules

With version 2.1 and above, you can create exclusion rules to **Install**, **Auto Install** and **Adoption**. We added the ability to exclude specific machines within a group or organization by using Kaseya Views. For example, if you want to prevent Webroot agents being Installed, you can configure it by:

- Machine name (ex. *server*)
- Software installed on a machine(ex. IIS, Sql Server)
- Operating System Type (ex. Windows 2012 Server)

Exclusion Rules is a Master Administrator function. All rules are global, and will be applied when the administrator selects a machine to install on. This will also apply to Auto Install and Discovery/Adoption.

Below is the Exclusion Rules grid. Kaseya Administrators will be able to create an exclusion rule by giving it a name and applying a Kaseya View to it.



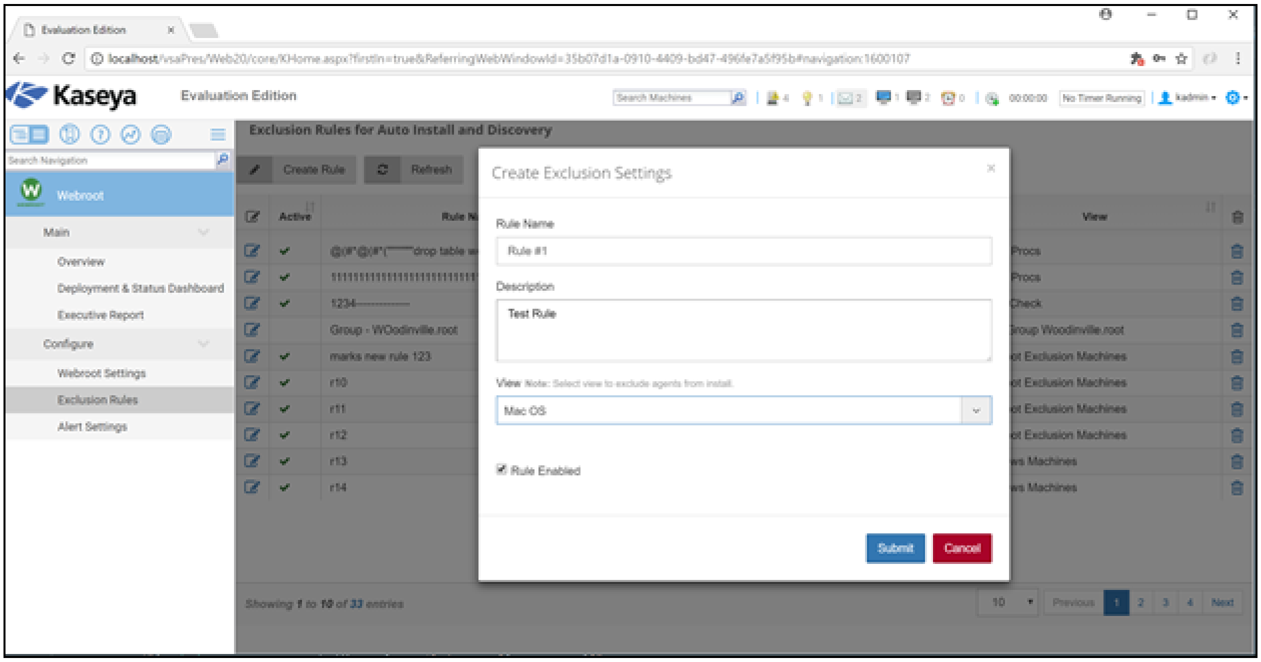
Exclusion Rules for Auto Install and Discovery

Active	Rule Name	Description	View
✓	@(#*@(#*(""""drop table web…	test	Agent Procs
✓	1111111111111111111111111111111111…	tews	Agent Procs
✓	1234--------------	3333333333333333333333333333333333333333333333333333…	Label Check
	Group - WOodinville.root		View-Group Woodinville.root
✓	marks new rule 123	this is just a test	Webroot Exclusion Machines
✓	r10		Webroot Exclusion Machines
✓	r11		Webroot Exclusion Machines
✓	r12		Webroot Exclusion Machines
✓	r13		Windows Machines
✓	r14		Windows Machines

Showing 1 to 10 of 33 entries

Create Exclusion Rule:

- Each Rule will have a name, which does not have to be unique.
- Each Rule will contain a description so that the administrators can store specific info on the rule.
- Each Rule contains a Kaseya View to filter out the machines. The machines that show up in the Kaseya View will be excluded from the Webroot Client install.
- Each Rule will have the ability to be disabled.


Evaluation Edition
localhost/vsaPres/Web20/core/KHome.aspx?firstIn=true&ReferringWebWindowId=35b07d1a-0910-4409-bd47-496fe7a5f95b#navigation:1600107
Kaseya
Evaluation Edition
Exclusion Rules for Auto Install and Discovery
Create Rule
Refresh
Webroot
Main
Overview
Deployment & Status Dashboard
Executive Report
Configure
Webroot Settings
Exclusion Rules
Alert Settings

Create Exclusion Settings

Rule Name: Rule #1

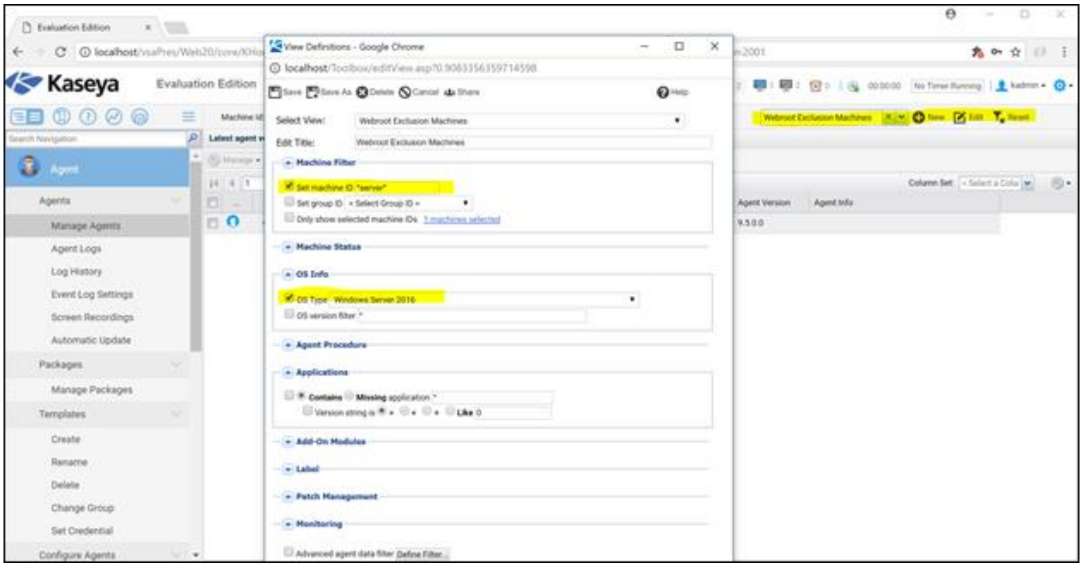
Description: Test Rule

View Note: Select view to exclude agents from install.

Mac OS

☑ Rule Enabled

Each Kaseya view must be created from a Kaseya Page Filter Bar.



Select View: Webroot Exclusion Machines

Edit Title: Webroot Exclusion Machines

Machine Filter

☑ Set machine ID "server"

□ Set group ID < Select Group ID >

□ Only show selected machine IDs 1 machines selected

OS Info

☑ OS Type Windows Server 2016

□ OS version filter *

Please keep the following in mind:

- We recommend keeping the views simple.
- We recommend naming the view with the Webroot prefix so they can easily be selected in the drop-down on the Exclusion rules page.
- Also, views can be deleted from outside the Webroot Plugin, which could cause install problems if the view doesn't exist.

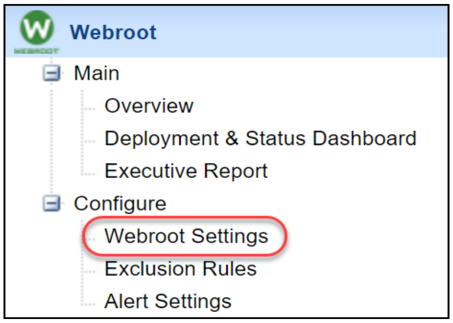
Adopting Existing Webroot Agents

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

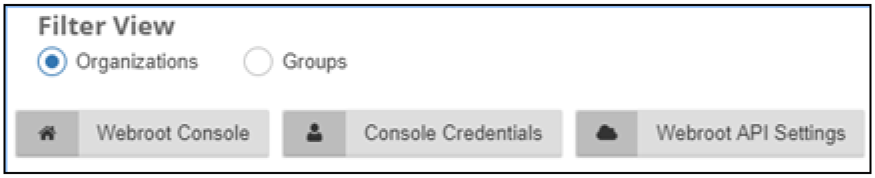
Note: Enabling Auto Install for those Organizations will do that automatically for you.

To adopt existing agents:

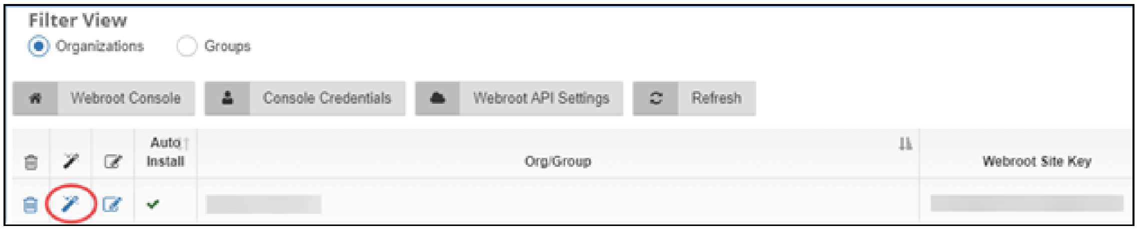
1. From the main menu, select **Webroot > Webroot Settings**.



The Filter View pane displays with the Organizations radio button selected, but you can select the Groups radio button, as needed.



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.

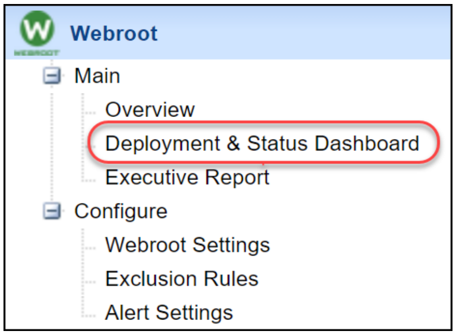
Note: Adopted Webroot endpoints that were initially installed manually, using Webroot installer executable, can only be uninstalled from within the Webroot console.

Deploying Webroot Agents Through the Kaseya Module

Deploying Webroot 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.

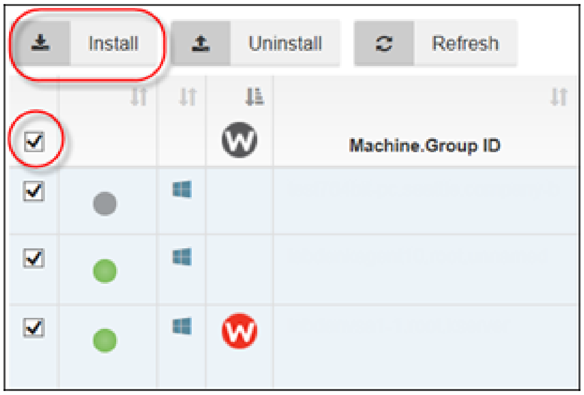
To deploy Webroot agents:

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

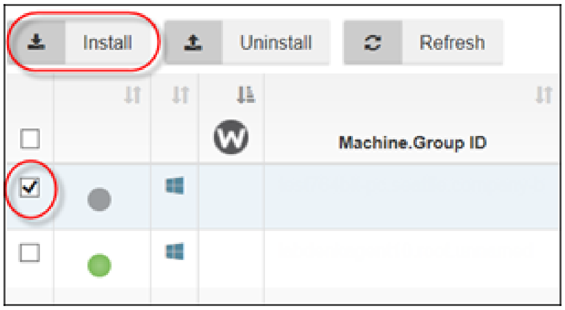


2. Do one of the following to deploy Webroot agents to just one endpoint or a range of endpoints.

- To install Webroot 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.

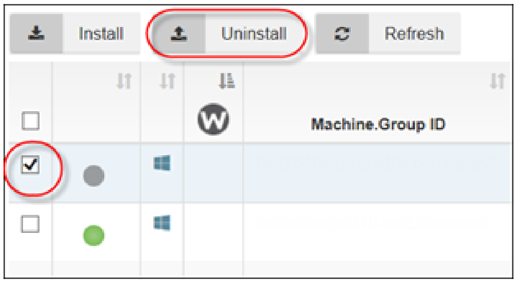


- To install Webroot agent on an individual Kaseya endpoint, select the checkbox of for the target endpoint , and click the **Install** button.



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

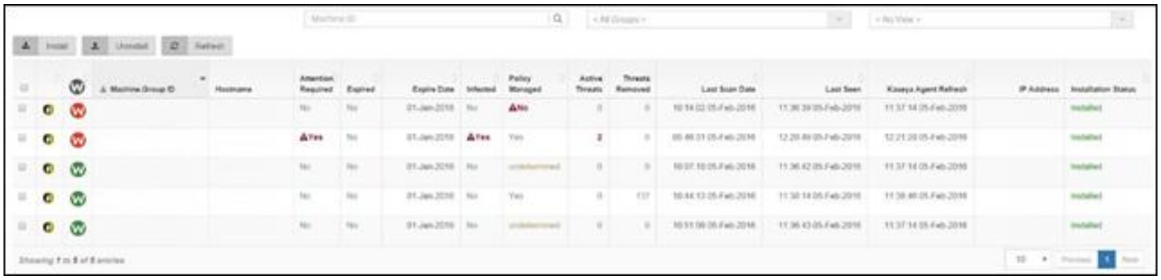
- To uninstall individual endpoints, select the checkbox for the target endpoints, and click the **Uninstall** button.



				Machine.Group ID
☑	●	⊞		
□	●	⊞		

Viewing Installation and Dashboard Level Webroot Agent Statuses

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



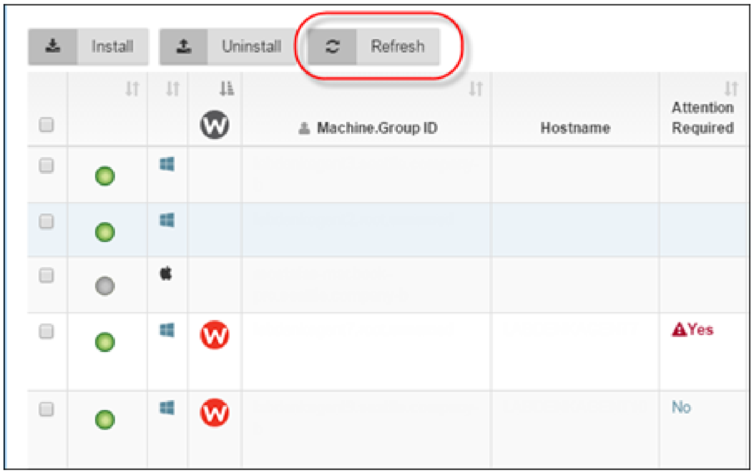
			Machine.Group ID	Hostname	Attention Required	Expired	Expire Date	Infected	Policy Managed	Active Threats	Threats Removed	Last Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status
□	●	W			No	No	01-Jan-2018	No	▲No	0	0	10:14:02 05-Feb-2018	11:36:39 05-Feb-2018	11:37:14 05-Feb-2018		Installed
□	●	W			▲Yes	No	01-Jan-2018	▲Yes	Yes	2	0	05:46:31 05-Feb-2018	12:20:49 05-Feb-2018	12:21:20 05-Feb-2018		Installed
□	●	W			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
□	●	W			No	No	01-Jan-2018	No	Yes	0	137	10:44:13 05-Feb-2018	11:30:14 05-Feb-2018	11:38:46 05-Feb-2018		Installed
□	●	W			No	No	01-Jan-2018	No	undetermined	0	0	10:51:08 05-Feb-2018	11:36:43 05-Feb-2018	11:37:14 05-Feb-2018		Installed

Showing 1 to 5 of 5 entries

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

Icon	Description
⊞	Windows OS
	Mac OS

- If the Unity API is turned on, any changes within the managed agents will be checked every 15 minutes.
- If the API is not on, the interval to check for changes within the managed agents is one hour.

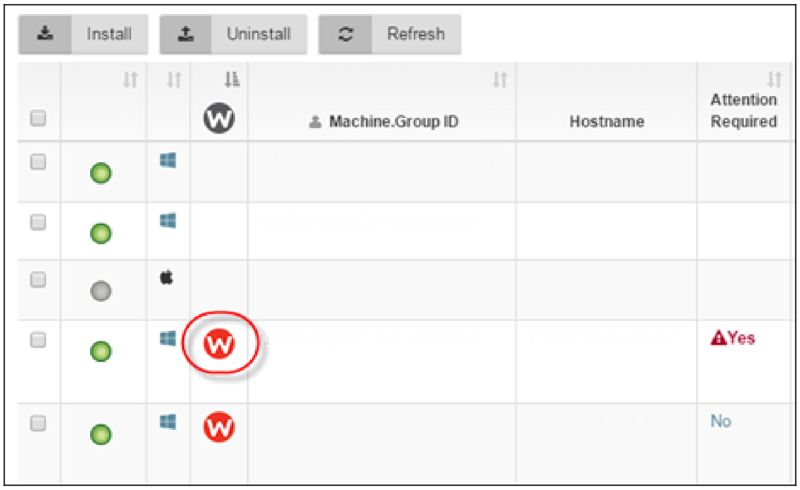


□				Machine.Group ID	Hostname	Attention Required
□	●	⊞				
□	●	⊞				
□	●					
□	●	⊞	W			▲Yes
□	●	⊞	W			No

Indicators in the Deployment & Status Dashboard

Red W

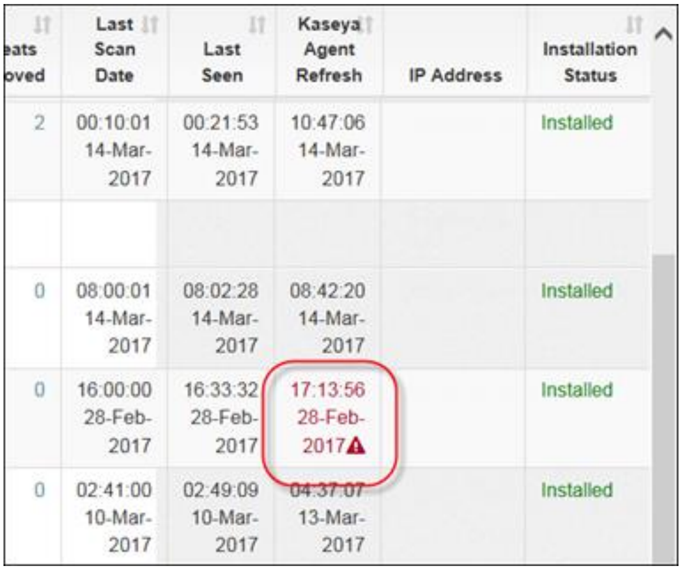
If the endpoint is in an undesirable state, for example, if the endpoint is in an Attention Required state, the W icon is red. In addition to the Attention Required state, the W icon will be red if the agent is failing to retrieve status and threat information.



☐			W	Machine.Group ID	Hostname	Attention Required
☐	●	⊞				
☐	●	⊞				
☐	●					
☐	●	⊞	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 API or 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.



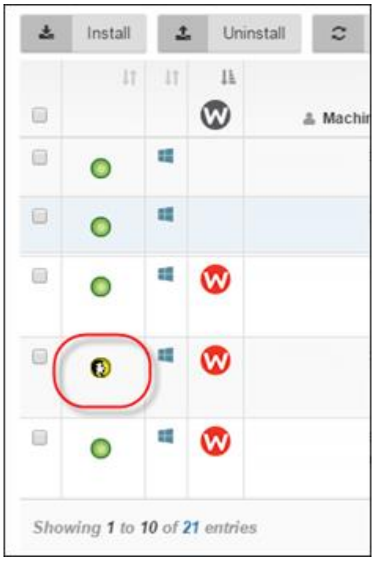
eats oved	Last Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status
2	00:10:01 14-Mar-2017	00:21:53 14-Mar-2017	10:47:06 14-Mar-2017		Installed
0	08:00:01 14-Mar-2017	08:02:28 14-Mar-2017	08:42:20 14-Mar-2017		Installed
0	16:00:00 28-Feb-2017	16:33:32 28-Feb-2017	17:13:56 28-Feb-2017⚠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

Validating Success of Agent Procedures

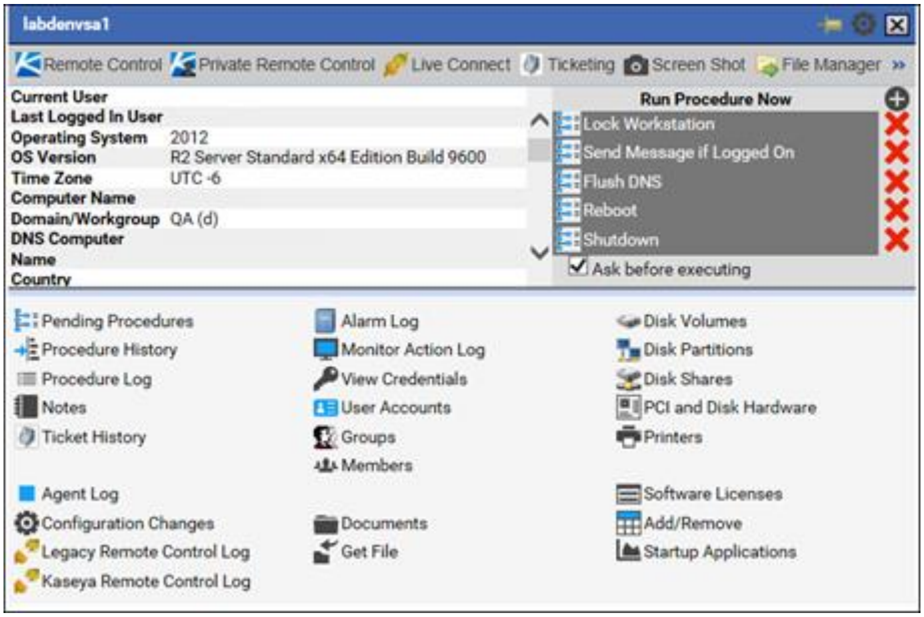
The administrator can, as needed, validate the success of the Agent Procedures that execute Webroot activities and collect results.

To validate success:

1. In the Deployment & Status Dashboard, hover over the **Kaseya** icon.



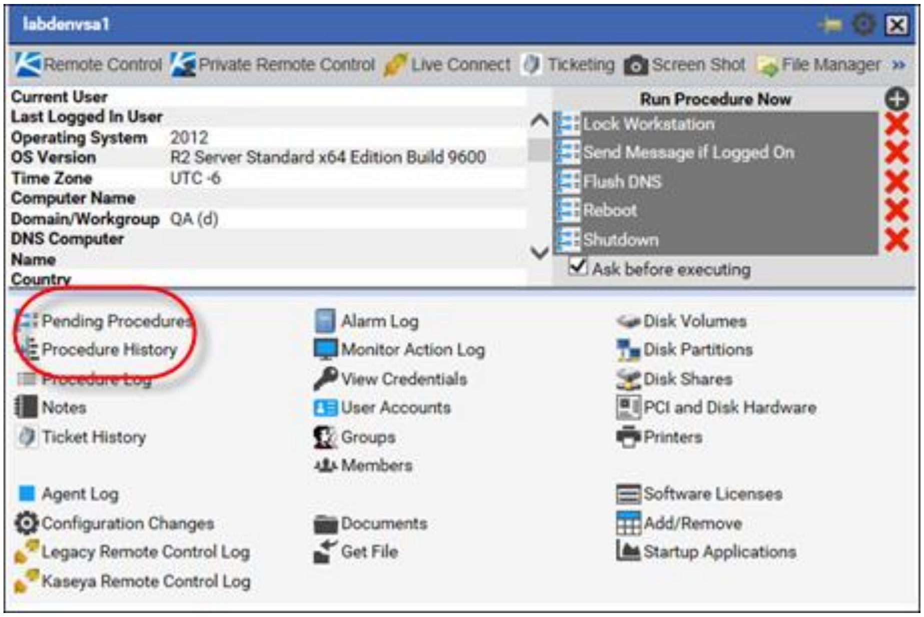
The Live Connect information window displays.



Current User
Last Logged In User
Operating System 2012
OS Version R2 Server Standard x64 Edition Build 9600
Time Zone UTC -6
Computer Name
Domain/Workgroup QA (d)
DNS Computer Name
Country

2. Select one of the following:

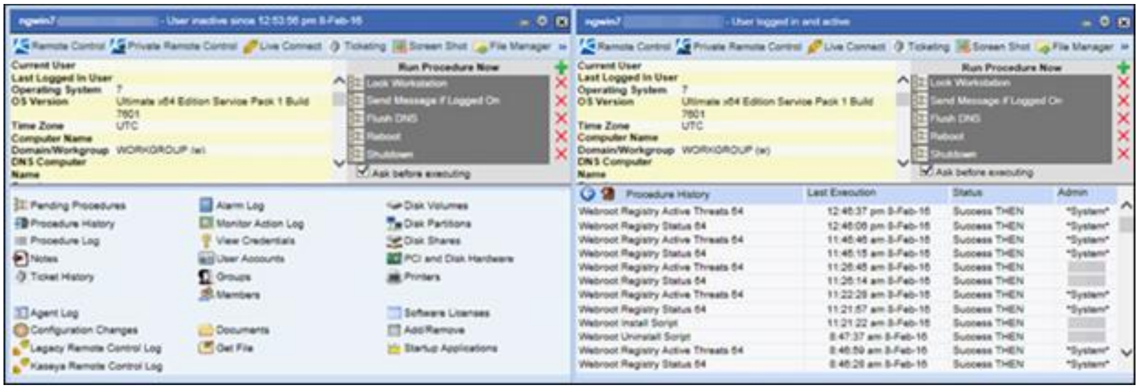
- **Pending Procedures**
- **Procedure History**



Current User	
Last Logged In User	
Operating System	2012
OS Version	R2 Server Standard x64 Edition Build 9600
Time Zone	UTC -6
Computer Name	
Domain/Workgroup	QA (d)
DNS Computer Name	
Country	

☑ Ask before executing

3. Review information, as needed.



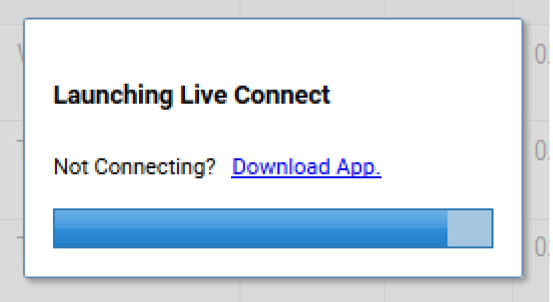
ngwin7 [redacted] - User inactive since 12:53:56 pm 8-Feb-16

ngwin7 [redacted] - User logged in and active

Current User	
Last Logged In User	
Operating System	7
OS Version	Ultimate x64 Edition Service Pack 1 Build 7601
Time Zone	UTC
Computer Name	
Domain/Workgroup	WORKGROUP (w)
DNS Computer Name	

Procedure History	Last Execution	Status	Admin
Webroot Registry Active Threats 64	12:46:37 pm 8-Feb-16	Success THEN	*System*
Webroot Registry Status 64	12:46:06 pm 8-Feb-16	Success THEN	*System*
Webroot Registry Active Threats 64	11:46:46 am 8-Feb-16	Success THEN	*System*
Webroot Registry Status 64	11:46:15 am 8-Feb-16	Success THEN	*System*
Webroot Registry Active Threats 64	11:26:48 am 8-Feb-16	Success THEN	[redacted]
Webroot Registry Status 64	11:26:14 am 8-Feb-16	Success THEN	[redacted]
Webroot Registry Active Threats 64	11:22:28 am 8-Feb-16	Success THEN	*System*
Webroot Registry Status 64	11:21:57 am 8-Feb-16	Success THEN	*System*
Webroot Install Script	11:21:22 am 8-Feb-16	Success THEN	[redacted]
Webroot Uninstall Script	8:47:37 am 8-Feb-16	Success THEN	[redacted]
Webroot Registry Active Threats 64	8:46:59 am 8-Feb-16	Success THEN	*System*
Webroot Registry Status 64	8:46:28 am 8-Feb-16	Success THEN	*System*

By clicking the icon, you can also use Live Connect to directly get remote access to the selected device.



Launching Live Connect

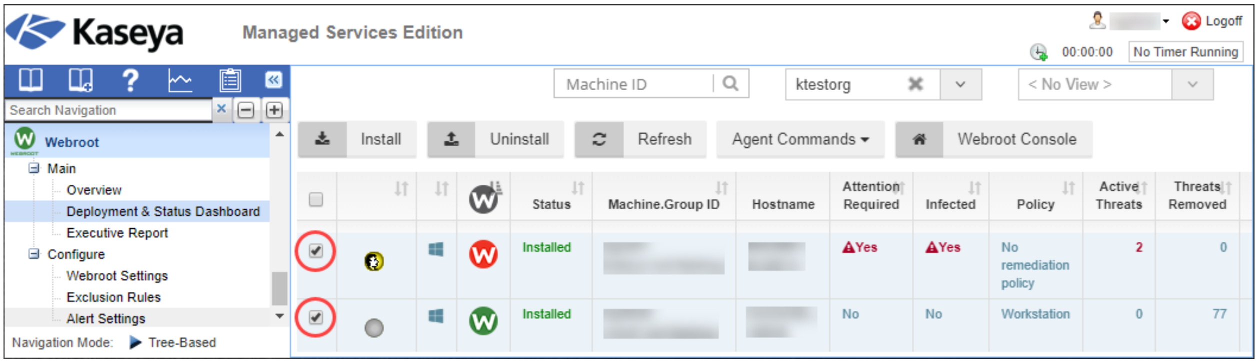
Not Connecting? Download App.

Running Webroot Agent Commands

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

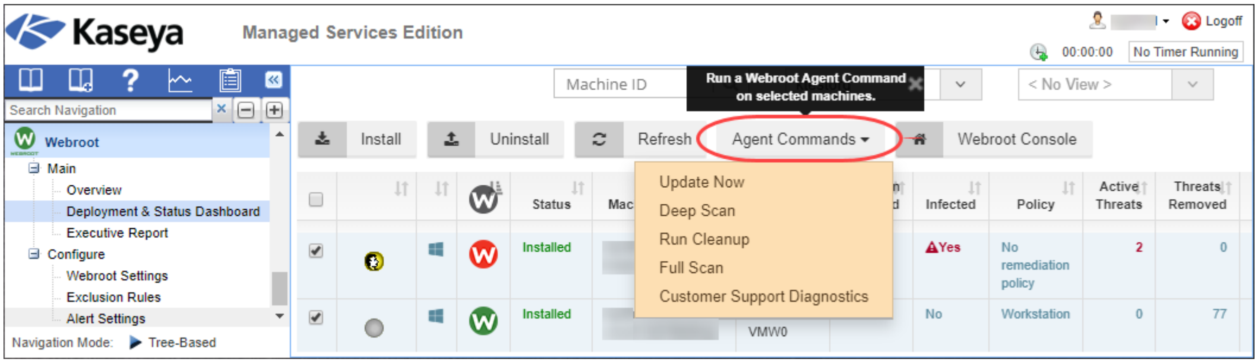
To run Webroot Agent Commands:

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



☐	Status	Machine.Group ID	Hostname	Attention Required	Infected	Policy	Active Threats	Threats Removed
☑	Installed	[redacted]	[redacted]	Yes	Yes	No remediation policy	2	0
☑	Installed	[redacted]	[redacted]	No	No	Workstation	0	77

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



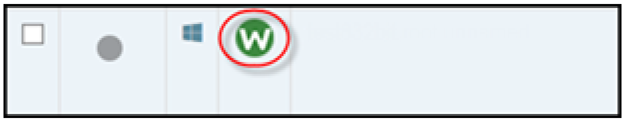
5. For more information on Webroot commands, please refer to the Webroot user guide in the Webroot Console.

Detailed Webroot Agent Status and Agent Commands

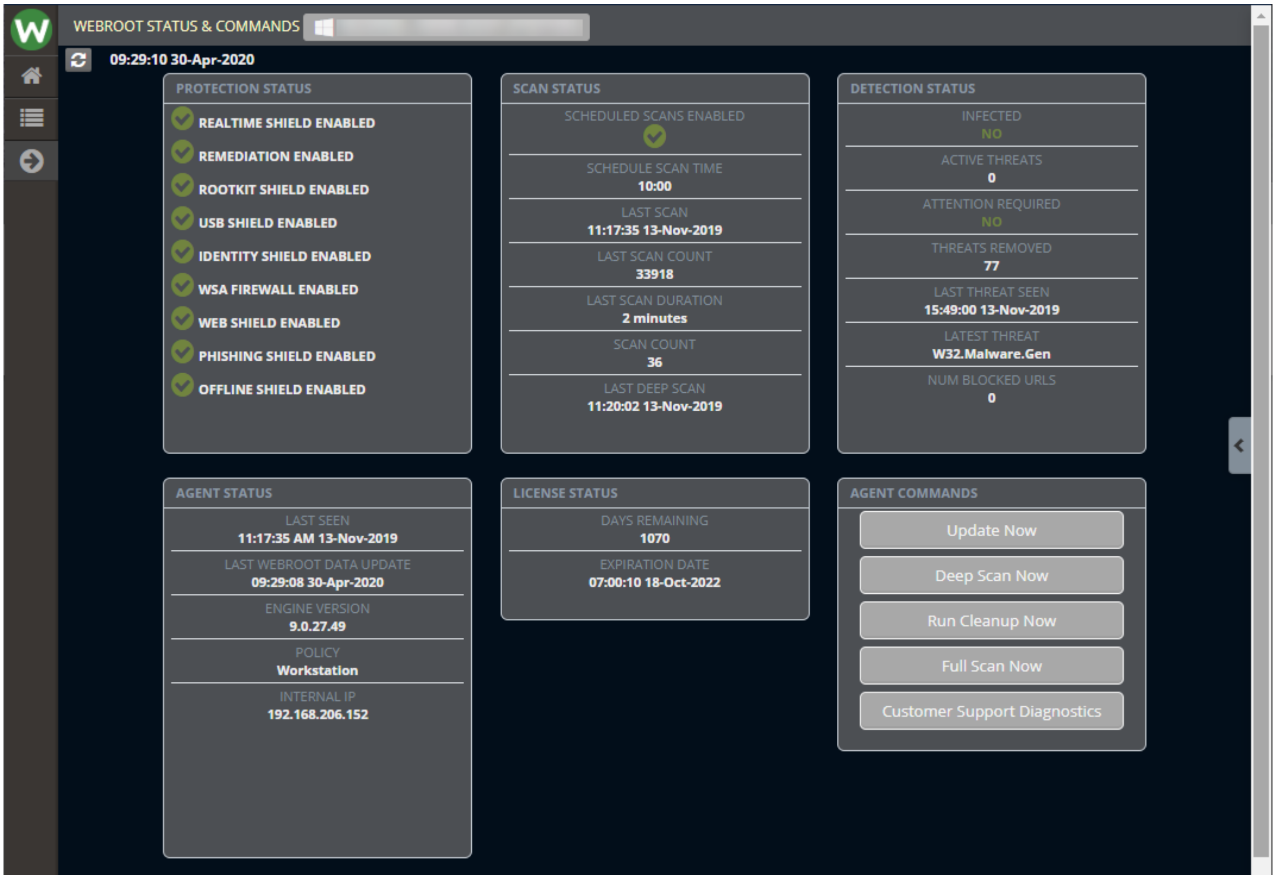
If you need detailed analysis of a specific Webroot agent or if you need to run Webroot Agent Commands, use this procedure.

To generate analysis or commands:

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



The system displays detailed Webroot Agent Information and Commands pane.



WEBROOT STATUS & COMMANDS

09:29:10 30-Apr-2020

PROTECTION STATUS

- ✓ REALTIME SHIELD ENABLED
- ✓ REMEDIATION ENABLED
- ✓ ROOTKIT SHIELD ENABLED
- ✓ USB SHIELD ENABLED
- ✓ IDENTITY SHIELD ENABLED
- ✓ WSA FIREWALL ENABLED
- ✓ WEB SHIELD ENABLED
- ✓ PHISHING SHIELD ENABLED
- ✓ OFFLINE SHIELD ENABLED

SCAN STATUS

SCHEDULED SCANS ENABLED ✓

SCHEDULE SCAN TIME 10:00

LAST SCAN 11:17:35 13-Nov-2019

LAST SCAN COUNT 33918

LAST SCAN DURATION 2 minutes

SCAN COUNT 36

LAST DEEP SCAN 11:20:02 13-Nov-2019

DETECTION STATUS

INFECTED NO

ACTIVE THREATS 0

ATTENTION REQUIRED NO

THREATS REMOVED 77

LAST THREAT SEEN 15:49:00 13-Nov-2019

LATEST THREAT W32.Malware.Gen

NUM BLOCKED URLS 0

AGENT STATUS

LAST SEEN 11:17:35 AM 13-Nov-2019

LAST WEBROOT DATA UPDATE 09:29:08 30-Apr-2020

ENGINE VERSION 9.0.27.49

POLICY Workstation

INTERNAL IP 192.168.206.152

LICENSE STATUS

DAYS REMAINING 1070

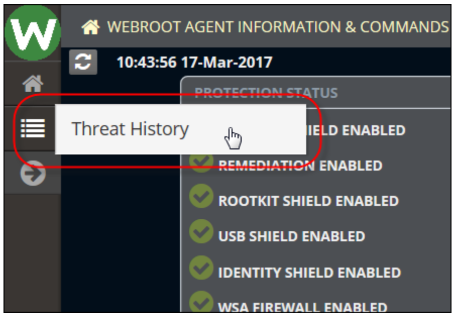
EXPIRATION DATE 07:00:10 18-Oct-2022

AGENT COMMANDS

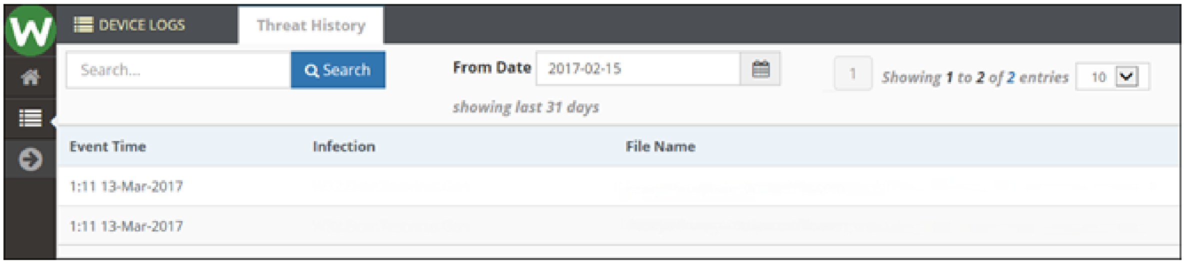
2. From this pane, you can run various commands, such as *Deep Scan Now* or *Run Cleanup Now*. These commands are executed within a few minutes.

   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.

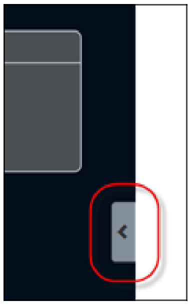


From Date 2017-02-15
showing last 31 days
Showing 1 to 2 of 2 entries

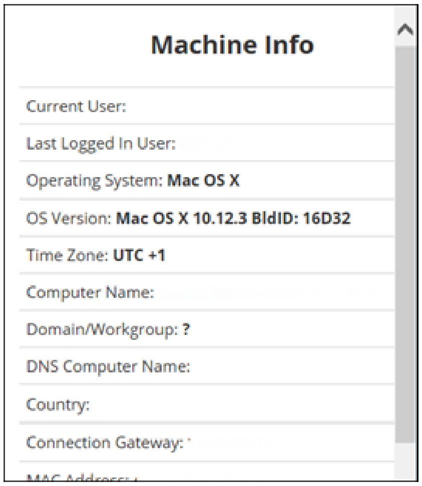
Event Time	Infection	File Name
1:11 13-Mar-2017		
1:11 13-Mar-2017		

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

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



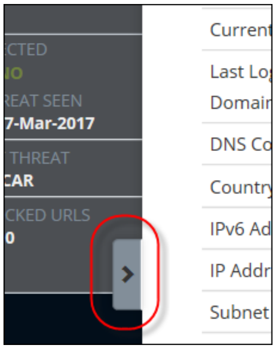
The system expands the Machine Info window, which is scrollable.



Machine Info

Current User:
Last Logged In User:
Operating System: **Mac OS X**
OS Version: **Mac OS X 10.12.3 BldID: 16D32**
Time Zone: **UTC +1**
Computer Name:
Domain/Workgroup: **?**
DNS Computer Name:
Country:
Connection Gateway:
MAC Address:

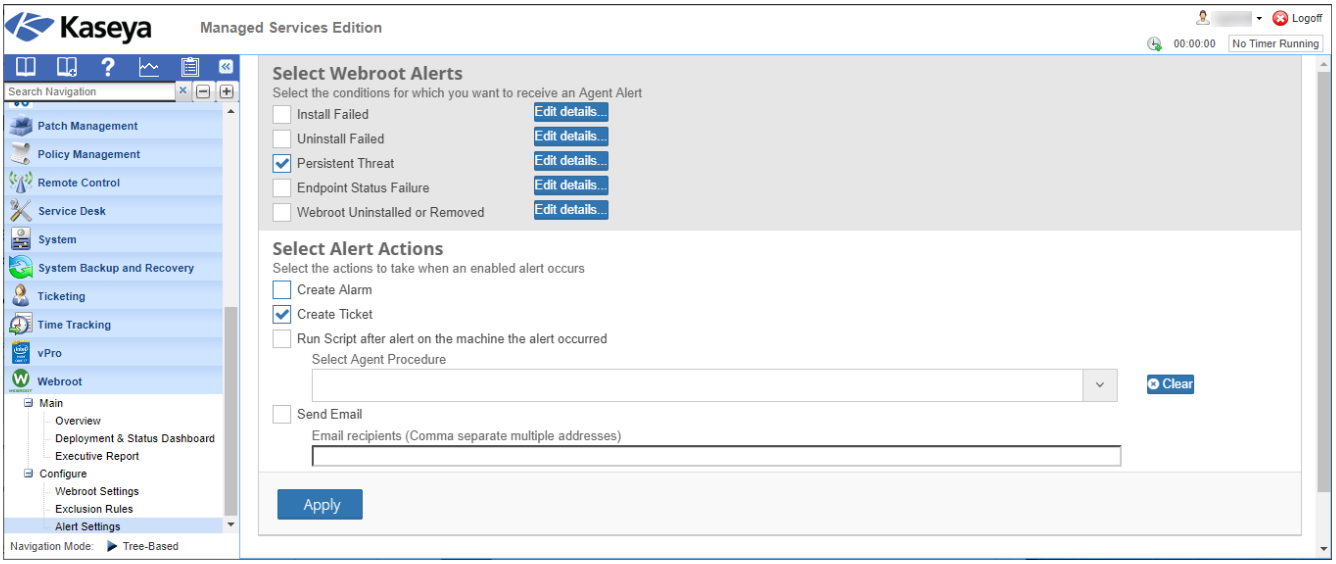
To return to the Webroot Agent Information & Commands pane, click the **Side** arrow.



Integrated Alarm Parameters With Kaseya Alert Actions

The Webroot Module is directly integrated into the Kaseya Alert Action metaphor. If any installations, uninstallations, or non-removable threats occur on any Agent, the module generates the common Kaseya Alert actions.

Note: To run alerts correctly **Kaseya emails and ticketing must be set up**.



Select Webroot Alerts

Select the conditions for which you want to receive an Agent Alert

- □ Install Failed — Edit details...
- □ Uninstall Failed — Edit details...
- ☑ Persistent Threat — Edit details...
- □ Endpoint Status Failure — Edit details...
- □ Webroot Uninstalled or Removed — 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
- □ Send Email
  - Email recipients (Comma separate multiple addresses)

The following alerts can be selected:

a. **Install Failed** – if the install of a Webroot agent fails, an alert will be generated.

b. **Uninstall Failed** - if the Webroot agent fails to uninstall, an alert will be generated.

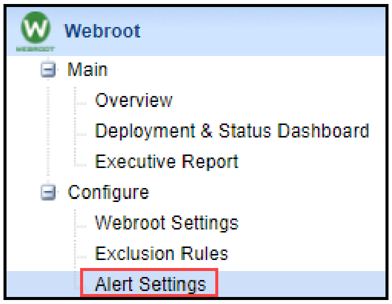
c. **Persistent Threats** – if there is a persistent threat that has not been removed for a selected period of time (0, 2, 4, 8, 16, 24) an alert will be generated.

d. **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.

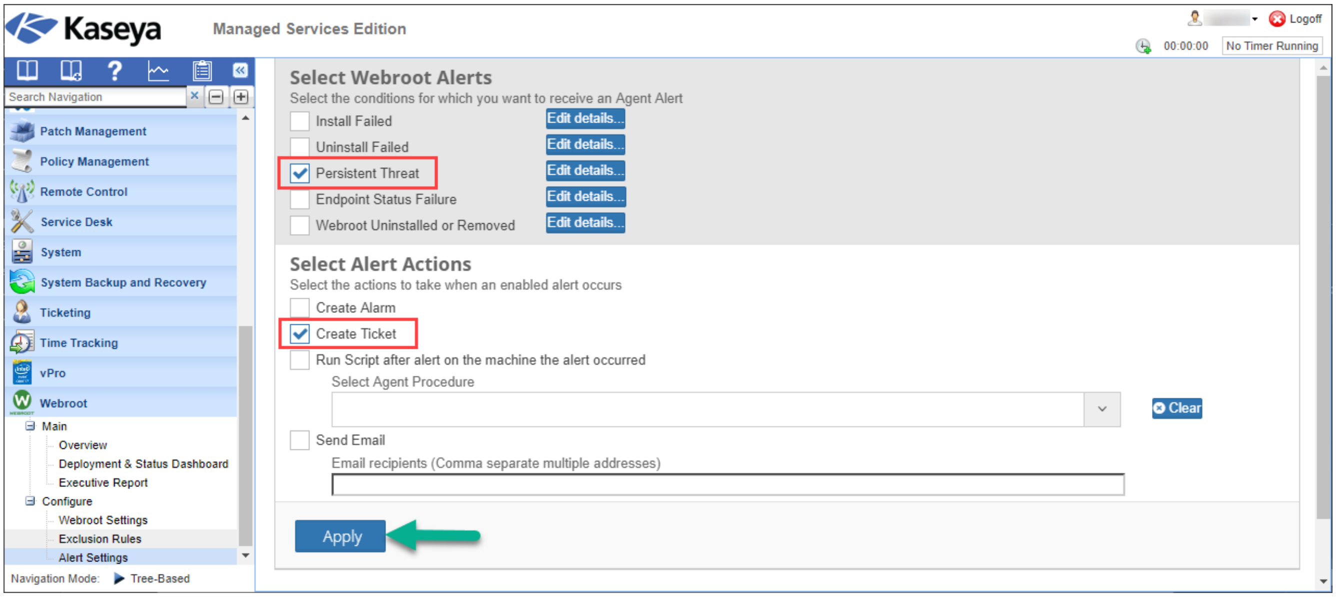
e. **Webroot Uninstalled or Removed** – If the Webroot agent is unexpectedly removed, an alert will be generated. Note this alert will be generated if endpoints are un-installed via the Webroot Console. If this is normal practice, we recommend this alarm is NOT set.

To set an alert:

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



The Webroot Alerts pane displays.



Select Webroot Alerts

Select the conditions for which you want to receive an Agent Alert

- □ Install Failed
- □ Uninstall Failed
- ☑ Persistent Threat
- □ Endpoint Status Failure
- □ Webroot Uninstalled or Removed

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

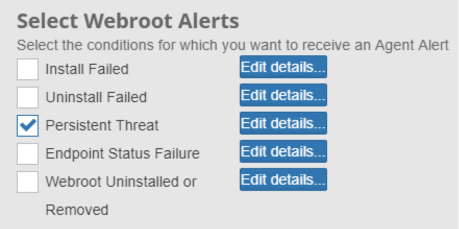
Select Agent Procedure

- □ Send Email

Email recipients (Comma separate multiple addresses)

2. Select one or more of the **Webroot Alerts** checkboxes, such as *Persistent Threats*.
3. Select the relevant **Alert Criteria** checkbox, such as *Create Ticket*.
4. When you're done, click the **Apply** button.

5. You can *Edit* each alert detail by clicking on **Edit details…**

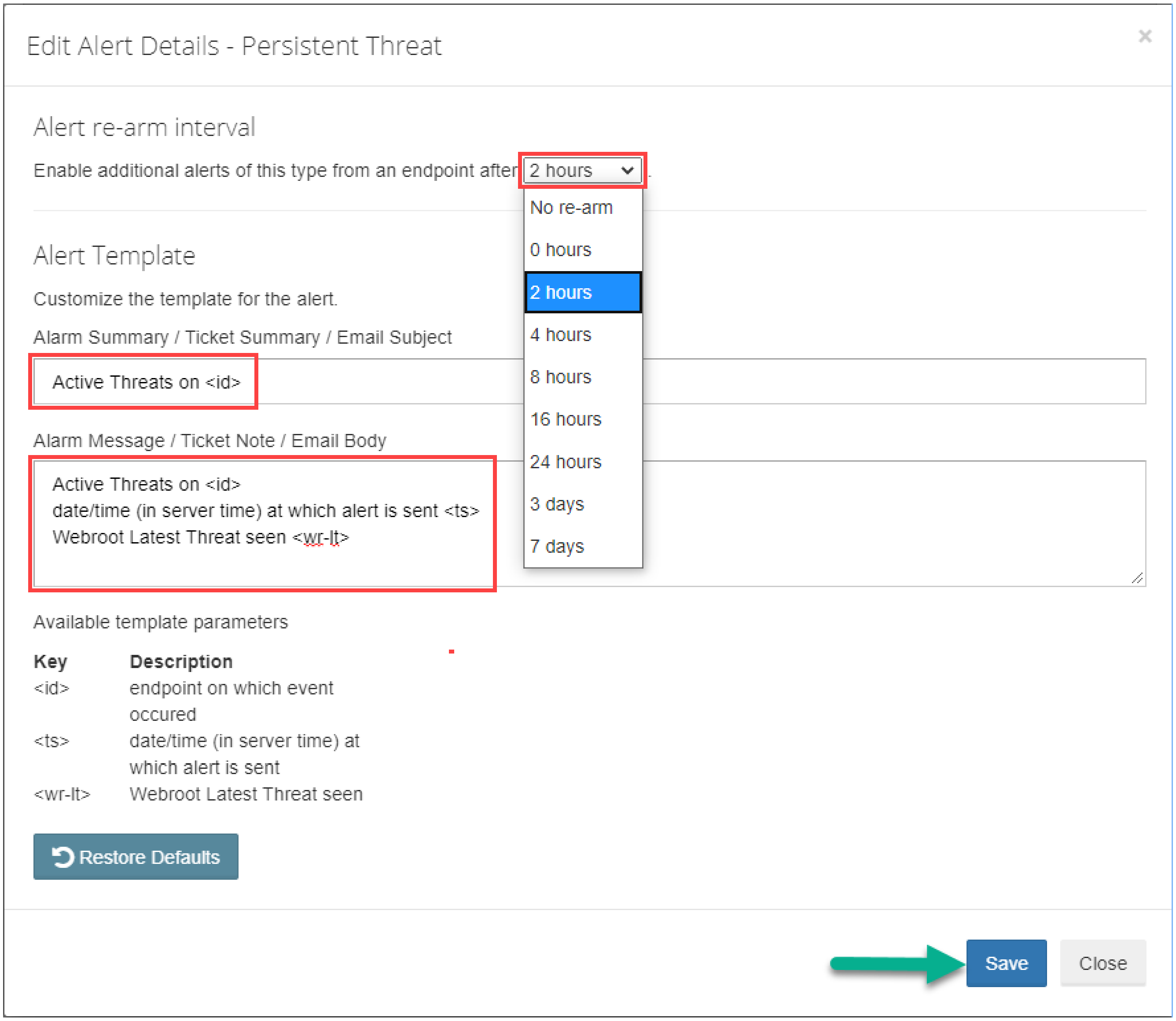


Select Webroot Alerts

Select the conditions for which you want to receive an Agent Alert

□	Install Failed	Edit details...
□	Uninstall Failed	Edit details...
☑	Persistent Threat	Edit details...
□	Endpoint Status Failure	Edit details...
□	Webroot Uninstalled or Removed	Edit details...

The Edit Alert Details pane displays.



Edit Alert Details - Persistent Threat

Alert re-arm interval

Enable additional alerts of this type from an endpoint after 2 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>
date/time (in server time) at which alert is sent <ts>
Webroot Latest Threat seen <wr-lt>

Available template parameters

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

6. Select the re-arm interval – how often an alert is re-sent.

Note:

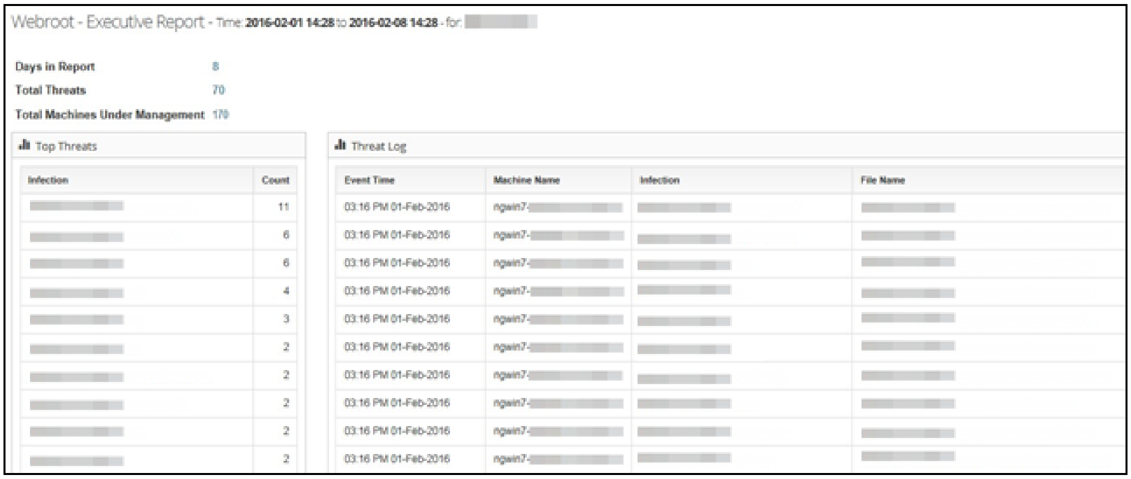
- Selecting "**0 hours**" will cause the **persistent** alert to be sent as soon it is detected. In general, this is every hour.
- Selecting "**no re-arm**" will limit persistent alarms to just one even if the alert condition is still active.

7. Select the detail of the **Alert Template** and add the fields you would like displayed within the alert.

Click on Save when finished.

Running Executive Reports

The Webroot Module provides a straightforward Threat Report for any of the Kaseya customer groups that are using Webroot.



Webroot - Executive Report - Time: 2016-02-01 14:28 to 2016-02-08 14:28 - for: [redacted]

Days in Report	8
Total Threats	70
Total Machines Under Management	170

Top Threats

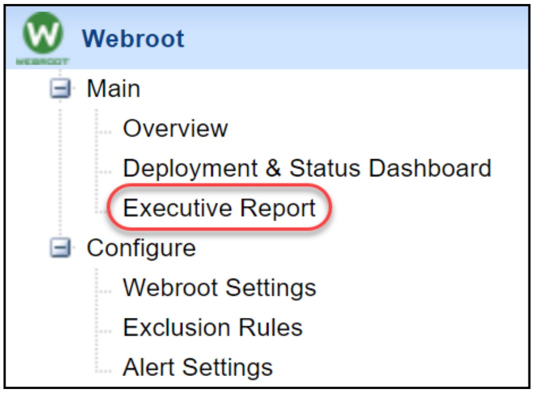
Infection	Count
[redacted]	11
[redacted]	6
[redacted]	6
[redacted]	4
[redacted]	3
[redacted]	2
[redacted]	2
[redacted]	2
[redacted]	2
[redacted]	2

Threat Log

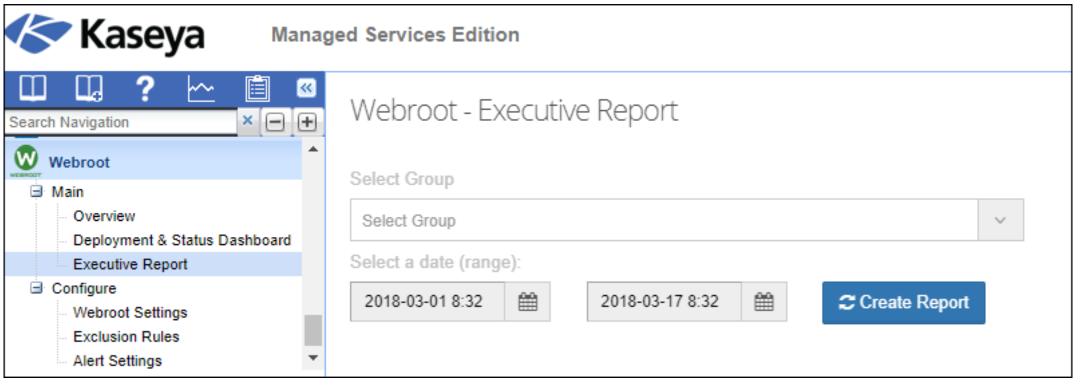
Event Time	Machine Name	Infection	File Name
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]

To generate an executive report:

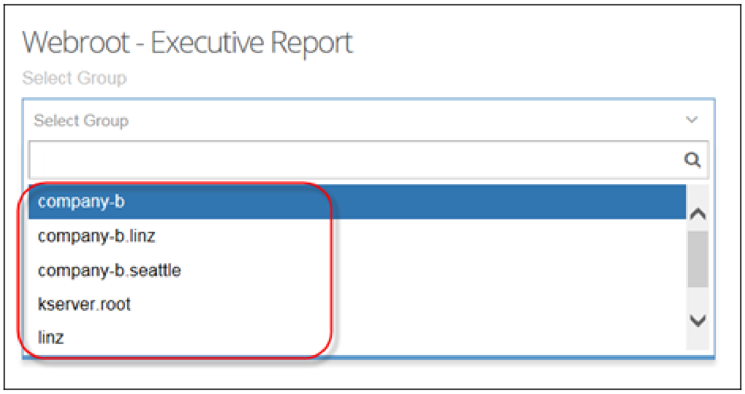
1. From the Webroot menu, select **Executive Report**.



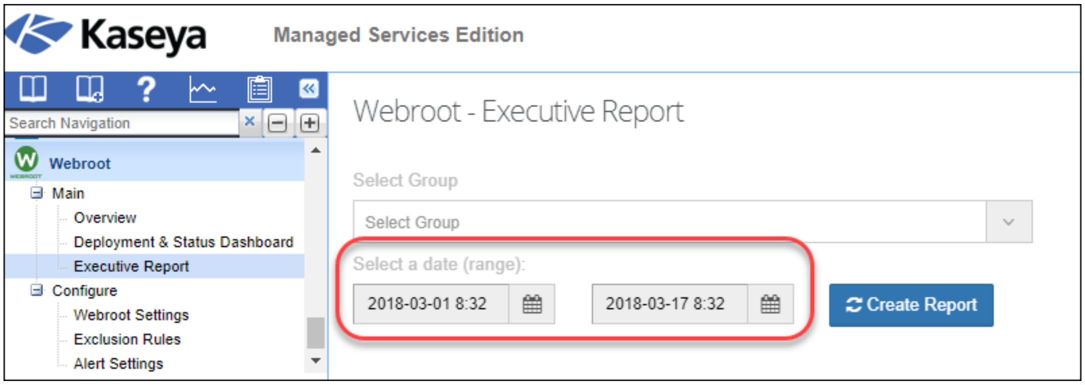
The Webroot – Executive Report pane displays.



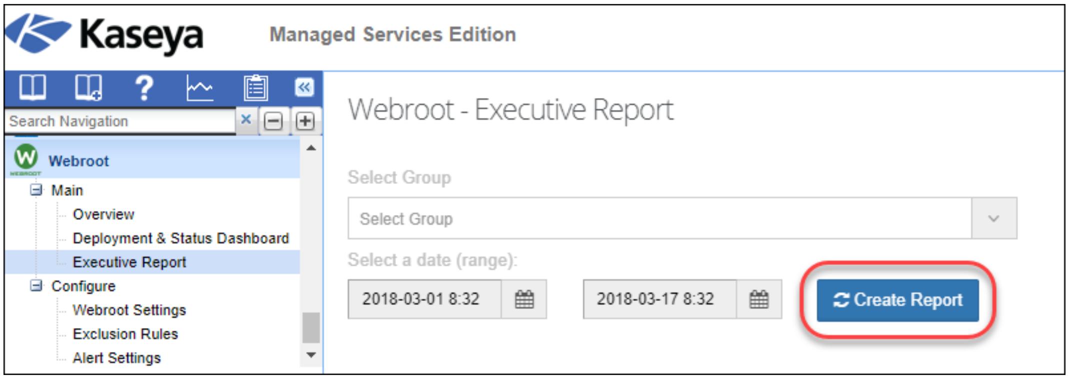
2. From the Select Group drop-down menu, select the **Kaseya** group for which you want to run the report.



3. Using the two date fields, select an appropriate date range.



4. When you're done, click the **Create Report** button.

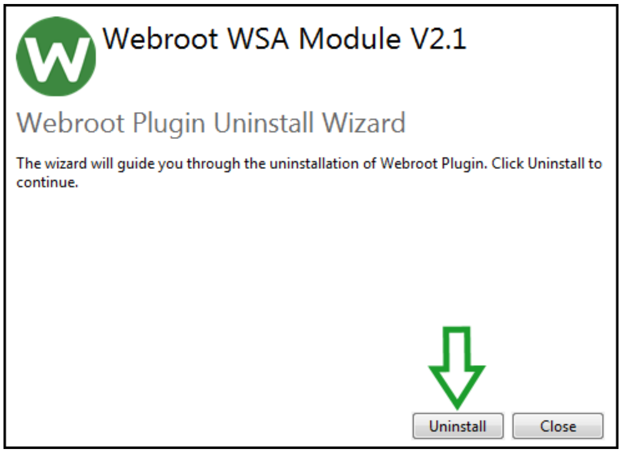


Note: Historical data is retained, even if Webroot endpoints are uninstalled or deactivated.

Uninstalling the Kaseya Plugin

To uninstall the Kaseya module, re-run the installer.

Note: After uninstalling Kaseya module V2.x, extra clean-up steps are required if you want to remove all the data relating to your installation. Steps to achieve this can be found here.



Webroot WSA Module V2.1

Webroot Plugin Uninstall Wizard

The wizard will guide you through the uninstallation of Webroot Plugin. Click Uninstall to continue.

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.

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