Kaseya VSA On-Prem Module
Version 2.5
Getting Started Guide

Table of Contents

Overview 1

What's New With 2.5 1

New Features 1

Enhancements 1

Prerequisites 2

Installing the Webroot Kaseya Module 3

Enabling Webroot API Settings 5

Setting up Single-Click Sign On to the Webroot Console 7

Controlling Access to Webroot Settings 8

Getting Started and Deployment 11

Overview Menu 11

Webroot Secure Anywhere Business Endpoint (Webroot Agent) Deployment 13

Configuring and Obtaining a Unique Webroot Site Key 13

Auto-Deploy Exclusion Rules 18

Adopting Existing Webroot Agents 21

Deploying Webroot Agents Through the Kaseya Module 22

Viewing Installation and Dashboard Level Webroot Agent Statuses 23

Indicators in the Deployment & Status Dashboard 25

Red W 25

Warning Icon in Kaseya Agent Refresh Column 25

Validating Success of Agent Procedures 26

Running Webroot Agent Commands 28

Detailed Webroot Agent Status and Agent Commands 29

Integrated Alarm Parameters With Kaseya Alert Actions 32

Running Executive Reports 34

Uninstalling the Kaseya Plugin 37

Disclaimer 37

Overview

The Webroot Kaseya Module is designed to increase operational efficiency by tightly integrating Webroot SecureAnywhere Business Endpoint Protection (Webroot) 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 deployment management, auto-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.

Note: This module is in complete compliance to all third party integration definitions for Kaseya on-prem VSA version 9.2 and up. At the time of publication, the module was tested up to VSA version 9.5.

What's New With 2.5

New Features

- Added agent commands drop down list to Deployment and Status Dashboard screen, reducing the number of clicks and allowing administrator to run agent commands on multiple machines.
- Single-click sign on to GSM, allowing single-click access to the Sites menu within the GSM console.
- Webroot Portal button added to the Deployment and Status Dashboard screen for faster access to the GSM console.
- Added Webroot policy name to Deployment and Status Dashboard grid.
- Manage mass install/uninstall actions to stop users accidentally removing or installing large numbers of endpoints. Added notification for the admin to positively acknowledge to make sure of a large install/uninstall and streamlined the background processes to handle large tasks.

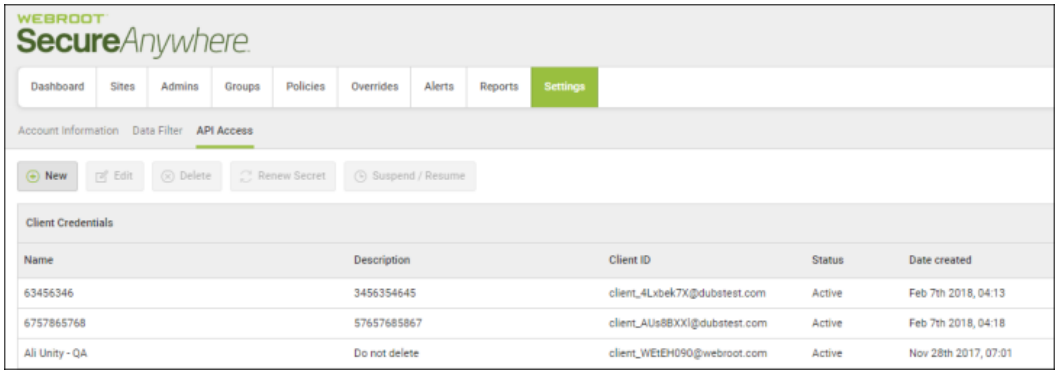
Enhancements

- Health check to make sure endpoints are uninstalled correctly. Added more tests to keep endpoint in sync with GSM.
- MID Collision enhancements, check hostname if duplicates are found. This allows Webroot API calls to update data for specific endpoints.
- Cleaned up Deployment and Status Dashboard grid, moved status to front of table.

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

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 on page 7.



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 9.2 and up.
- Kaseya administrator account.
- Kaseya Outbound Email Settings Administration.
- **Minumum - Microsoft SQL Server 2012 (SP3 Recommended)**
- Kaseya Module installer

  `WR_KPlugin_2.5.xx.xxxx.exe`
- The latest installer, which is available here.
- To install the Webroot Kaseya module, you must have access to the Kaseya server.

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

Installing the Webroot Kaseya Module

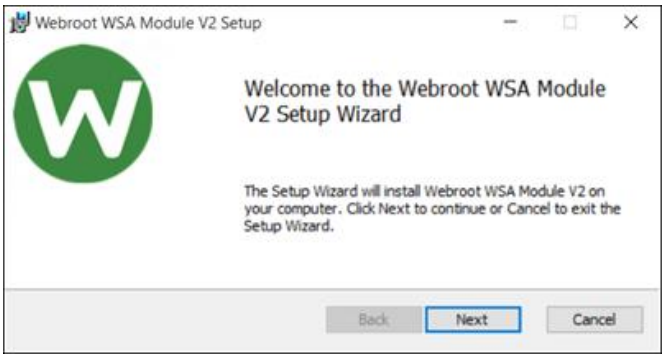
If you have met all the prerequisites, use the following procedure.

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_2.5.xx.xxxx.exe`

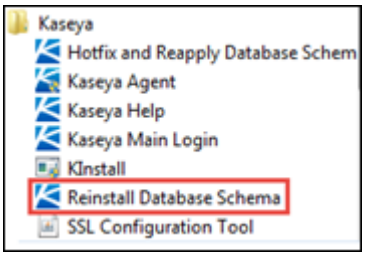
3. Follow the on-screen prompts.



Until the Setup Successful window displays.

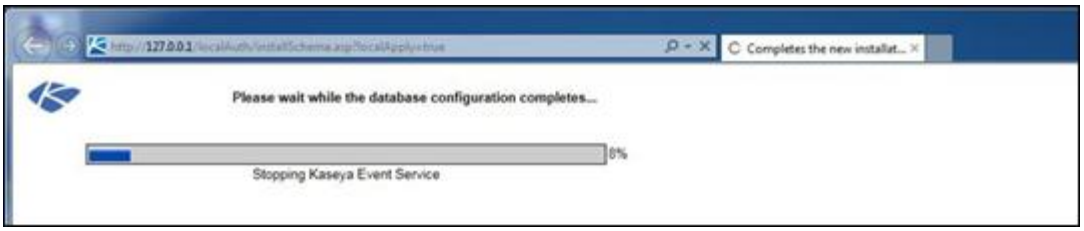
4. After the Webroot Kaseya Module has completed installation, you must reinstall the Database Schema. You can either use the link on the installer success screen, or access this from the Windows Start menu using the following path:

   Start > All Programs > Kaseya > Reinstall Database Schema



© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

The system installs the database schema.



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

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

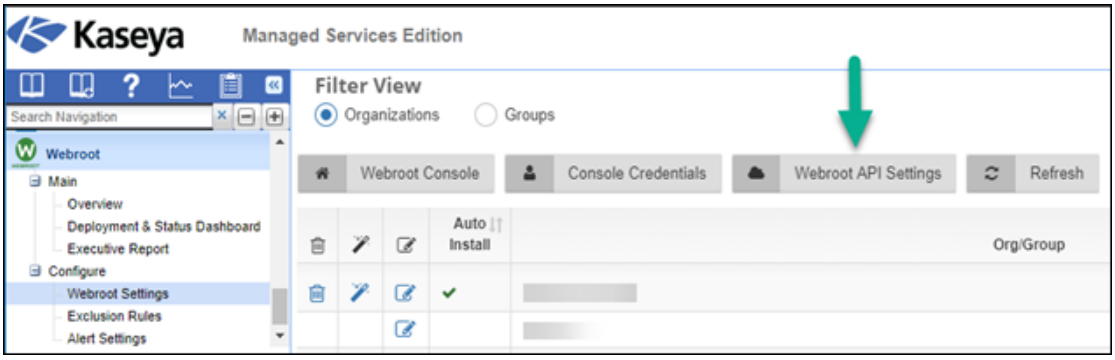
Enabling Webroot API Settings

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

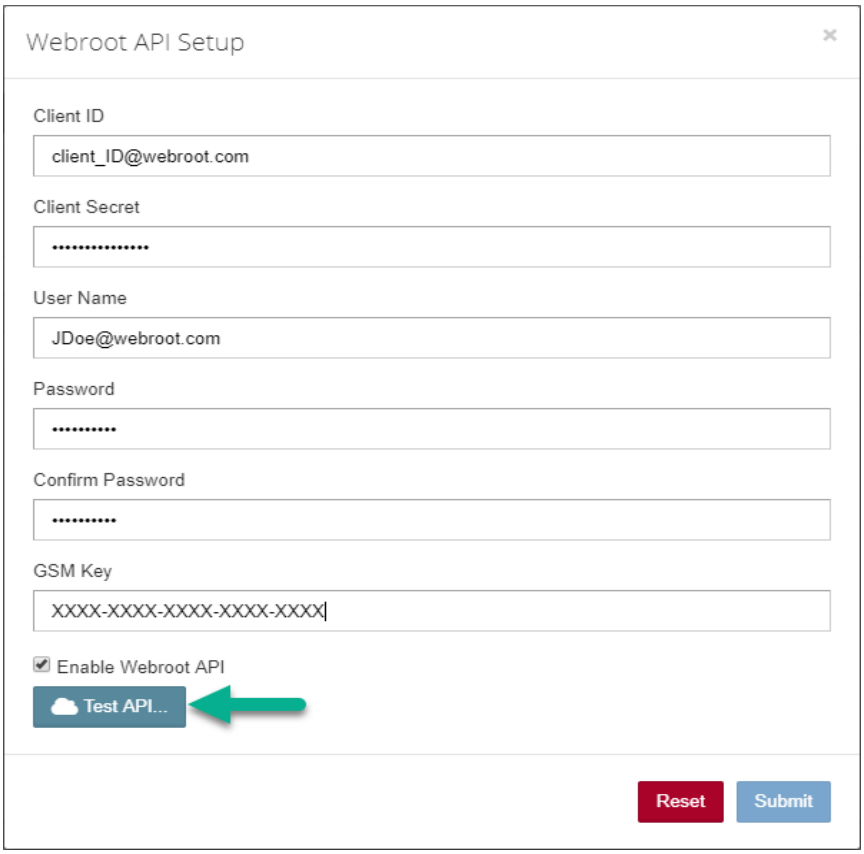
Alternatively, if you continue using the default settings, which utilize the Kaseya agent procedures, however you may experience higher loads on the Kaseya server.

To enable Webroot API settings:

1. After a successful installation, please enter valid Webroot API Settings. To do this, go to **Webroot** > **Configure** > **Webroot Settings.**
2. Click the **Webroot API Settings** button.



The Webroot API Setup window displays.

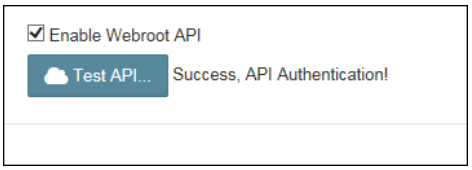


© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

If you don't have Unity API credentials yet, follow the instructions here to obtain them.

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

3. Click the **Test API** button.



4. When this test succeeded, click the **Submit** button.

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

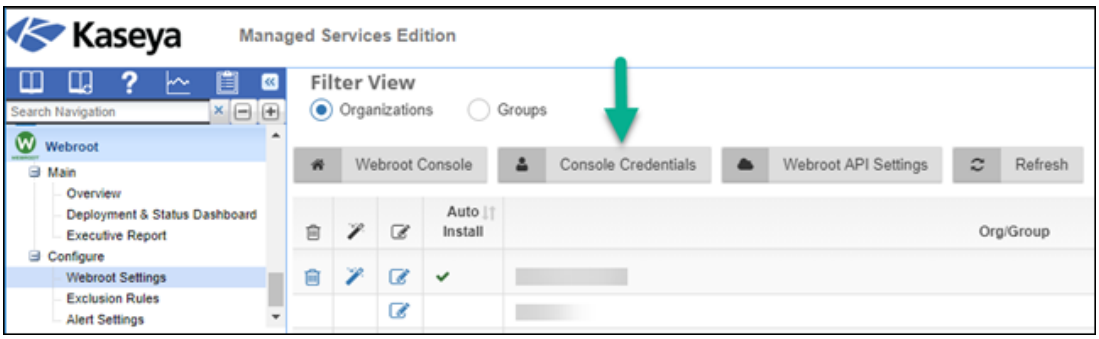
© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

Setting up Single-Click Sign On to the Webroot Console

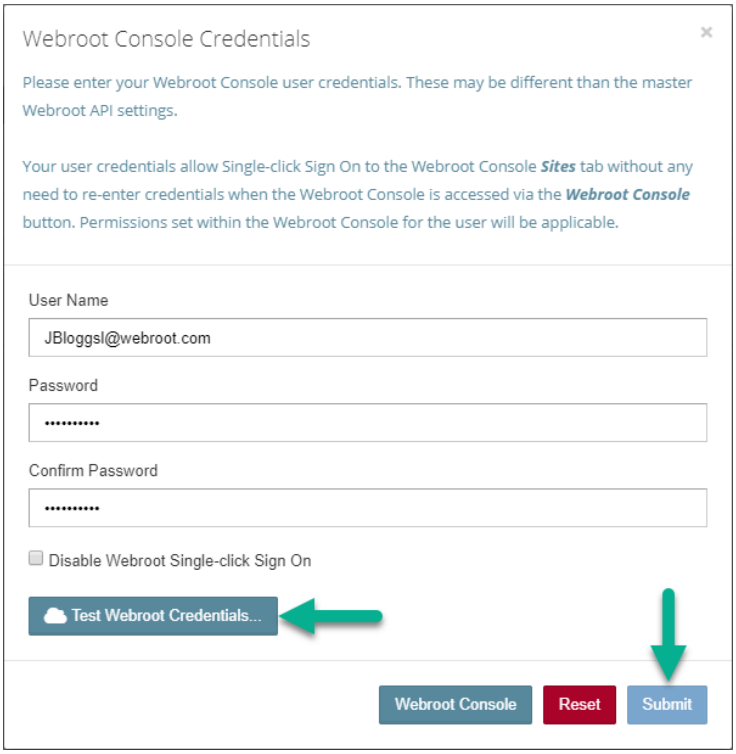
If you have enabled Unity API functionality, you can securely gain access to the Webroot Console Sites menu with a single click. This functionality is provided by a combination of Unity API credentials and your own Console Credentials that set your Webroot Console access level.

To enable single-click sign on to the Webroot Console:

1. Go to **Webroot** > **Configure** > **Webroot Settings**.
2. Click the **Console Credentials** button.



3. Enter your personal Webroot Console user access credentials. This may be diffenet then the API credentials you entered.
4. Click the **Test Webroot Credentia**ls button, then, if the test is successful, click the **Submit** button.



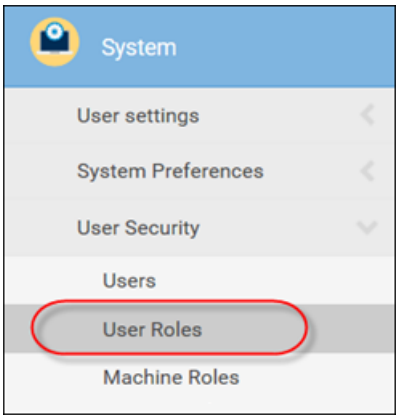
© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

Controlling Access to Webroot Settings

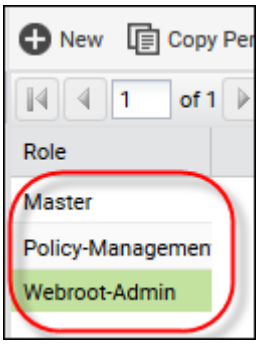
As needed, you can control an admin's access to Webroot settings. We recommend that you allow access to only those admins who will make GSM parent keycode assignments.

To control access to Webroot settings:

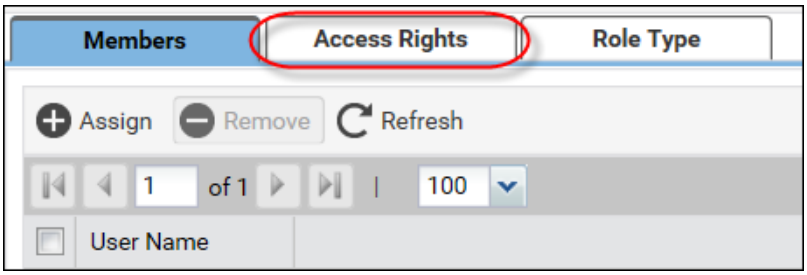
1. From the main menu, select **System** > **User Roles**.



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

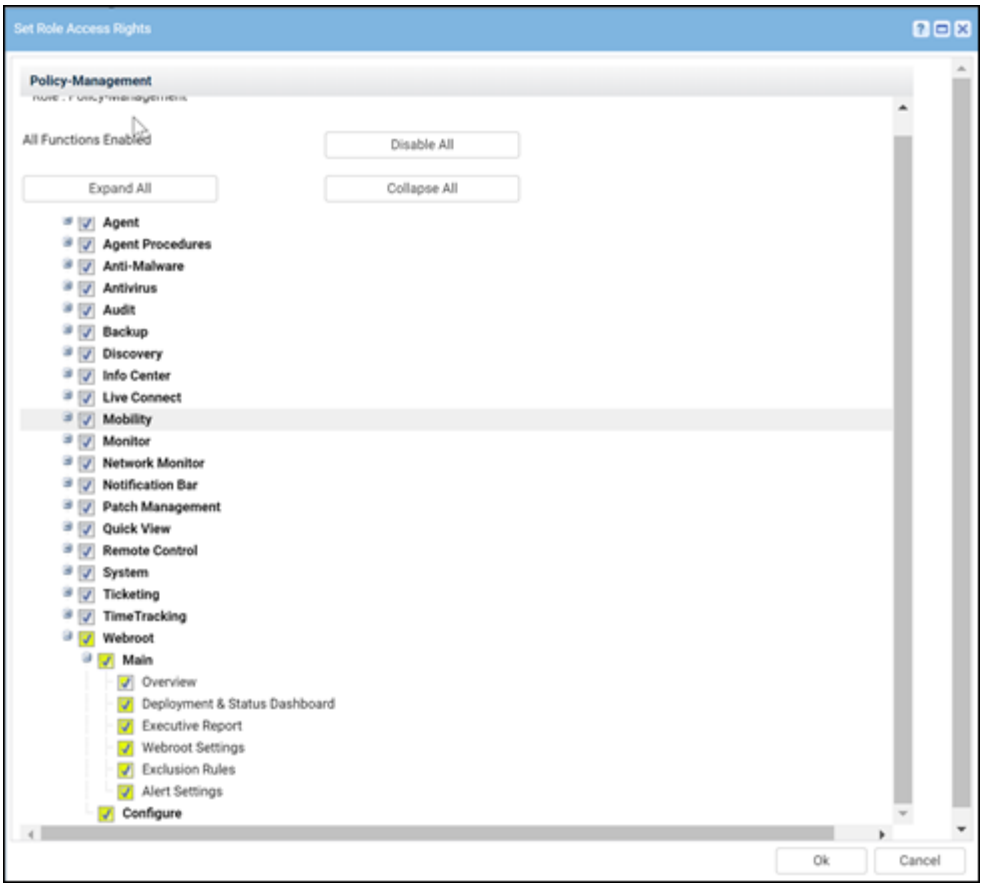


3. In the Set Role Access Rights pane, click the **Access Rights** tab.



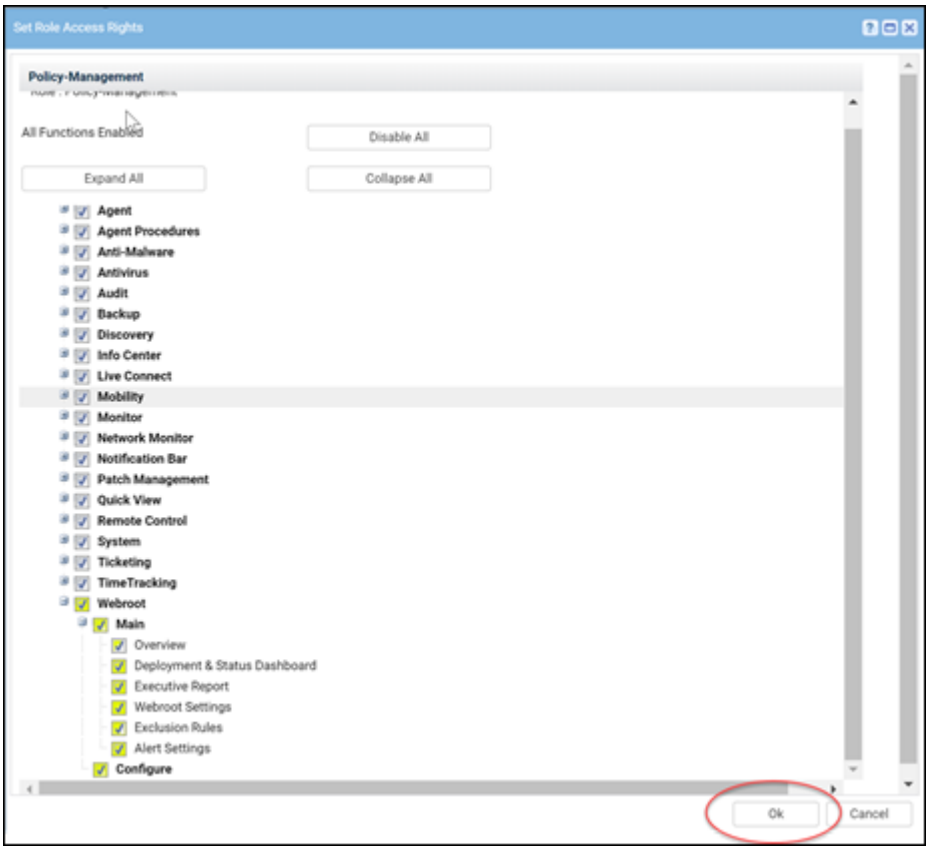
4. In the Access Rights tab, click the **Set Role Access Rights** button.

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
   - Exclusion Rules
   - Alert Settings
   - Executive Report



© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

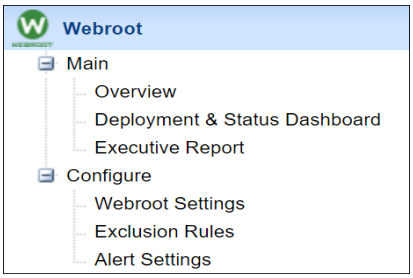
7. When you're done, click the **OK** button.



Getting Started and Deployment

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

- **Overview** – Basic guide to steps required. See the Overview Menu on page 11.
- **Deployment & Status Dashboard** – Allows simple GUI-driven deployments and menus for detailed status view as well as agent commands. See Webroot Agent Deployment on page 13.
- **Webroot Settings** – Webroot specific settings, such as site or default keycode, Webroot console access, and auto Webroot adoption wizard. See Adopting Existing Webroot Agents on page 21.
- **Alert Settings** – Alerts and alert criteria. See Integrated Alarm Parameters with Kaseya Alert Actions on page 32.
- **Executive Report** – Generating malware reports. See Running Executive Reports on page 34
- **Exclusion Rules** – Create exclusion rules to Install, Auto Install, and Adoption. See Auto-Deploy Exclusion Rules on page 18.

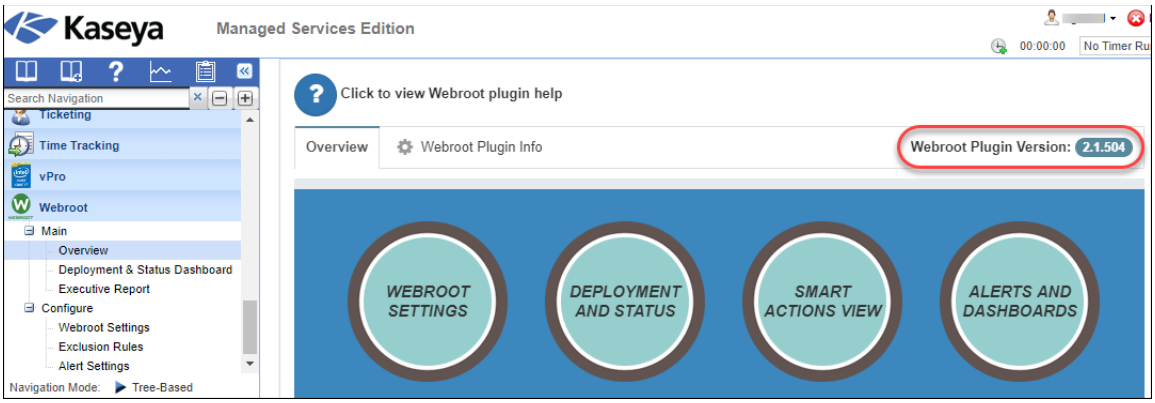


Overview Menu

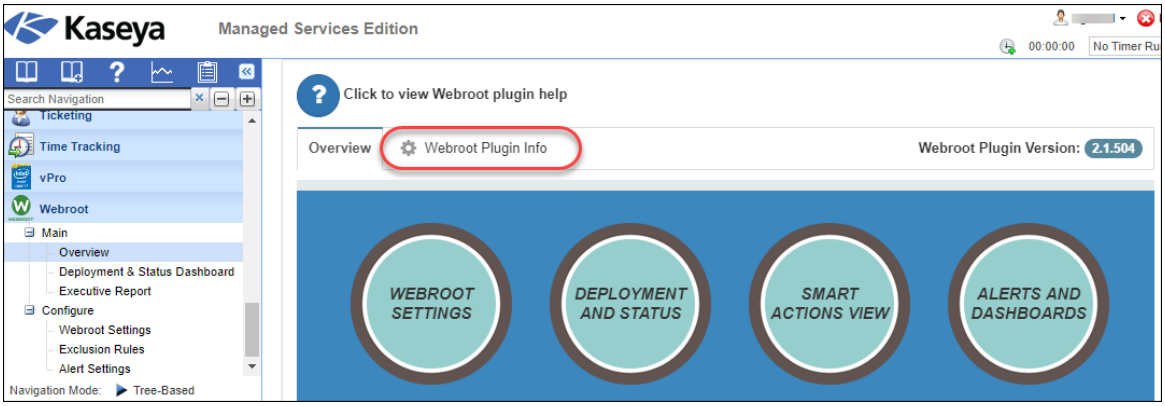
The Overview menu is a very basic guide to the steps required to deploy and maintain your Webroot installation.

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

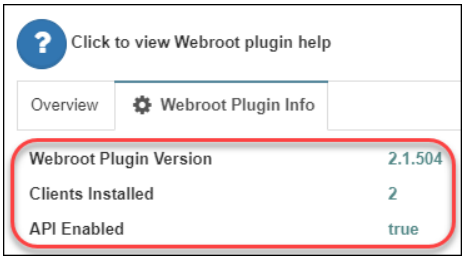
Included on the Overview tab is information about the plugin version, which is located in the upper right corner.



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



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



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 on page 13.
- Deploying Webroot agents through the Kaseya module. See Deploying Webroot Agents Through the Kaseya Module page 22.
- Viewing installation and dashboard-level Webroot agent status. See Viewing Installation and Dashboard Level Webroot Agent Status on page 23.

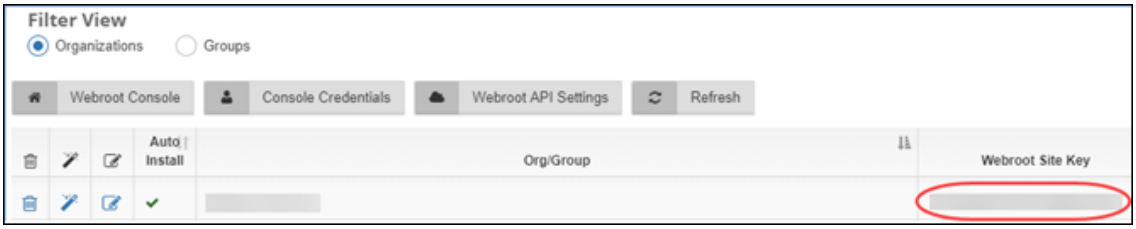
Note: If you have an existing Webroot deployment, you can adopt already installed endpoints in to the Kaseya Module. For more information, see Adopting Existing Webroot Agents on page 21.

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, follow the procedure that starts on page 15.

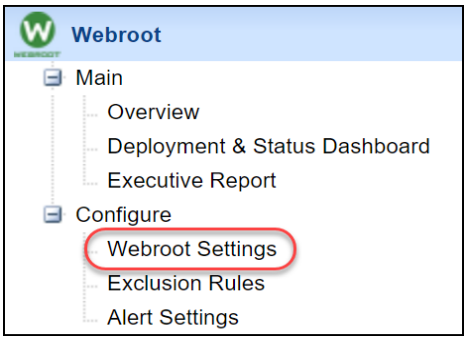
To configure with Webroot API enabled:

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.

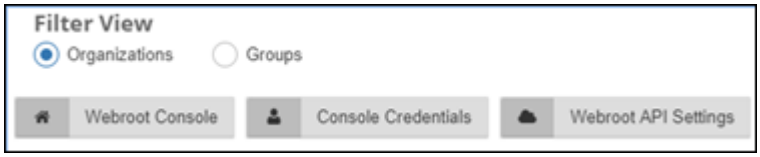


To obtain a unique site key:

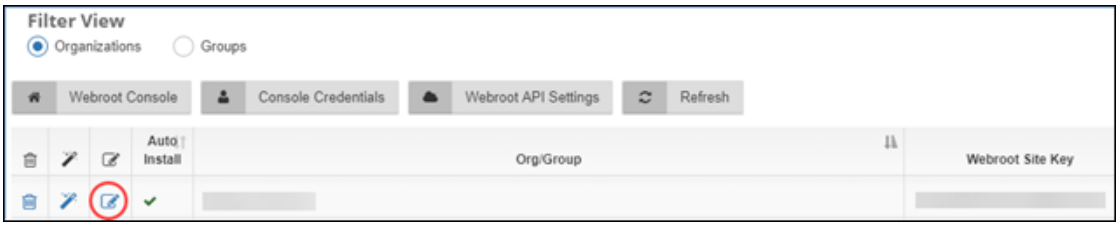
1. From the main menu, select **Webroot** > **Webroot Settings**.



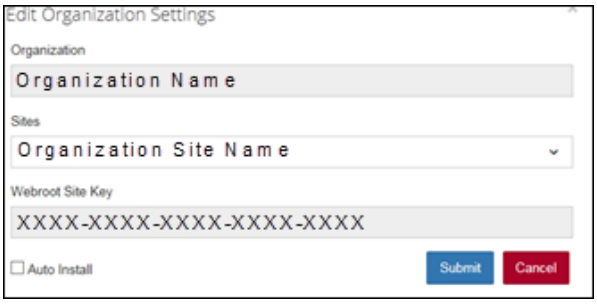
- The Filter View pane displays with the Organizations radio button active, though you can select the **Groups** radio button, as needed.
- The Filter View pane allows you to filter by organization or group, which lets you assign Webroot site keycodes to Kaseya organizations or groups.



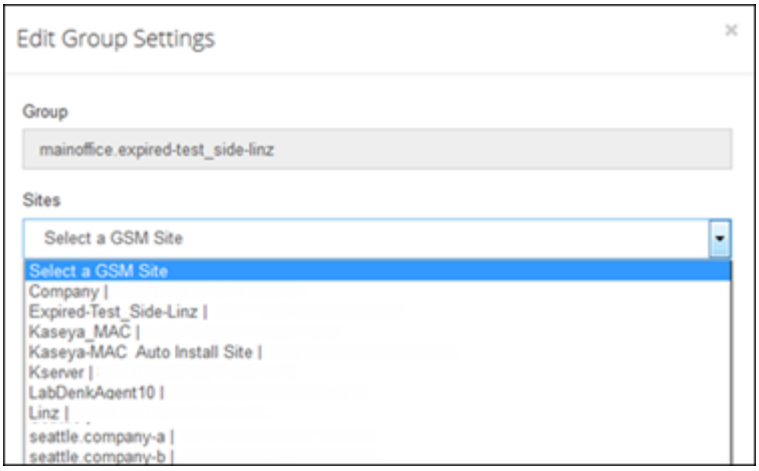
2. For the organization or group that you want to edit, click the **Edit** icon.



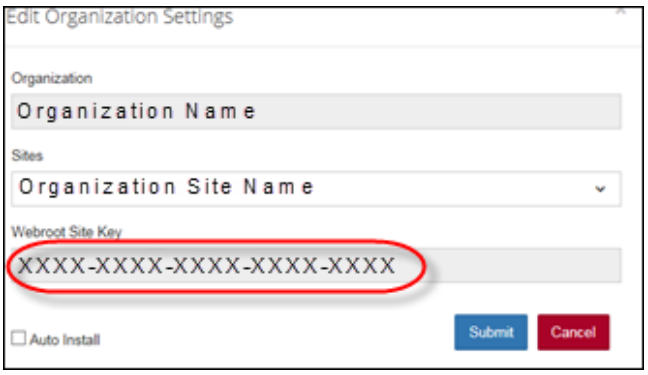
The Edit Organization Settings window displays with the organization field already populated.



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



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.



© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

- If you select the **Auto Install** checkbox, then Webroot agents will be deployed automatically to all Kaseya endpoints within the defined organization or group.
- With Auto Install, we deploy Webroot agents to any newly added Kaseya endpoints with a background task which runs once per hour. This will ensure that all Kaseya endpoints in the orgs/groups that are configured to auto install will have Webroot agents deployed.

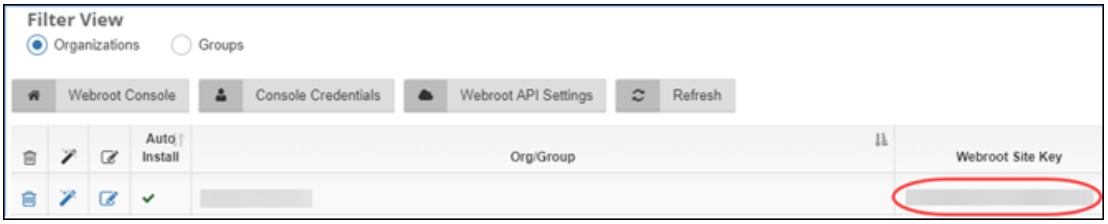
5. Click the **Submit** button to commit the key to the organization.

   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.

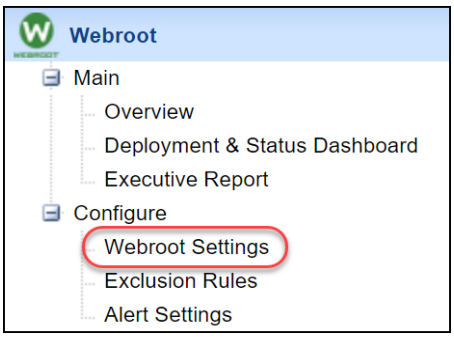
To configure without Webroot API enabled:

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.

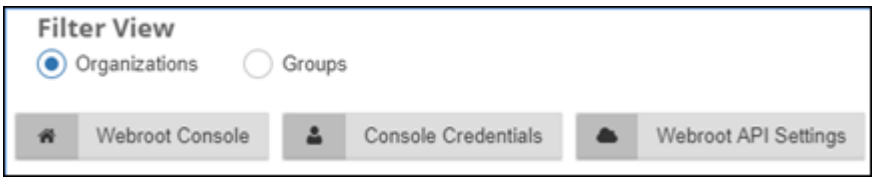


To obtain a unique site key:

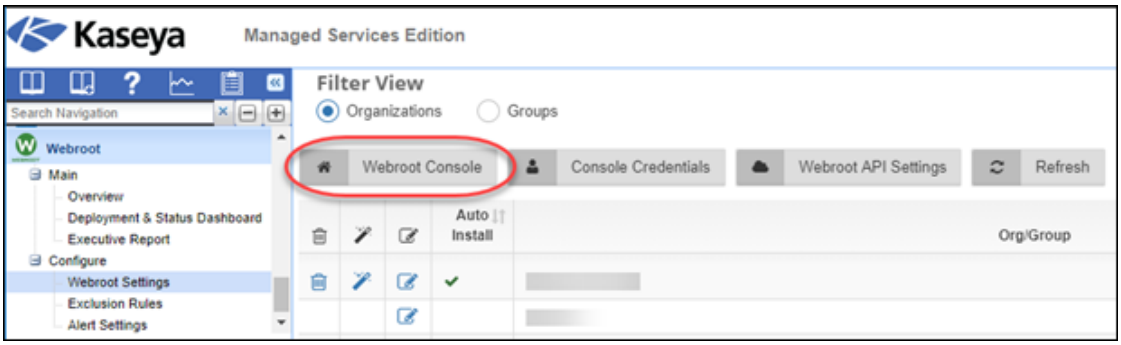
1. From the main menu, select **Webroot** > **Webroot Settings**.



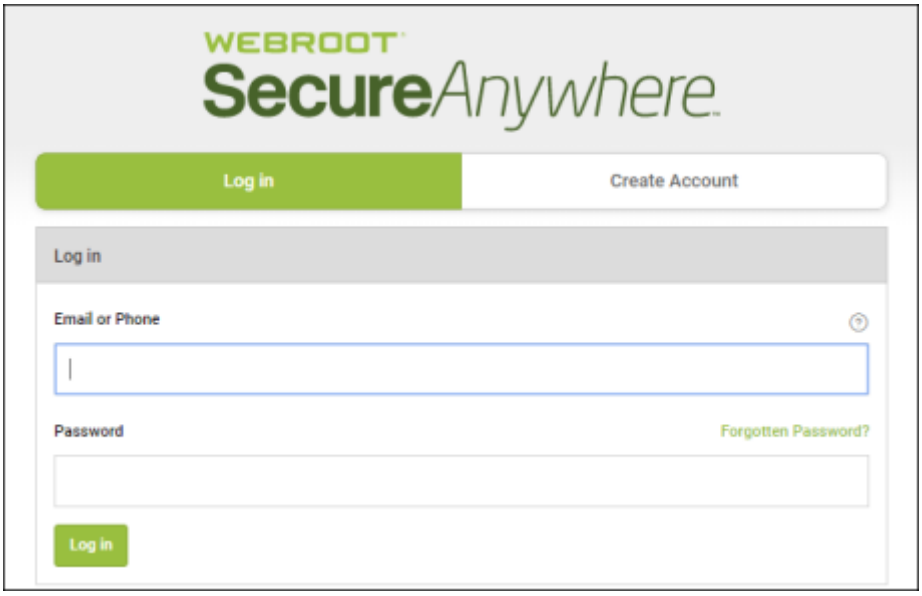
The Filter View pane displays with the Organizations radio button active, though you can select the **Groups** radio button, as needed.



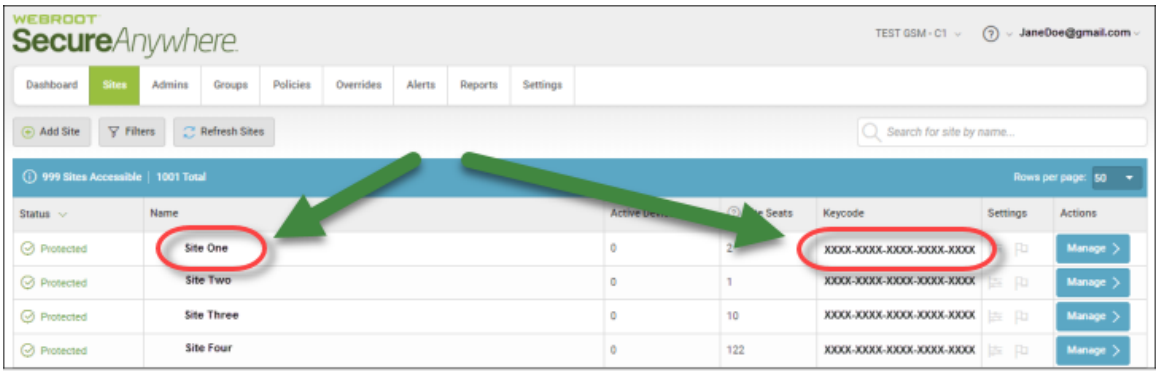
2. Click the **Webroot Console** button.



The Webroot SecureAnywhere login page displays.

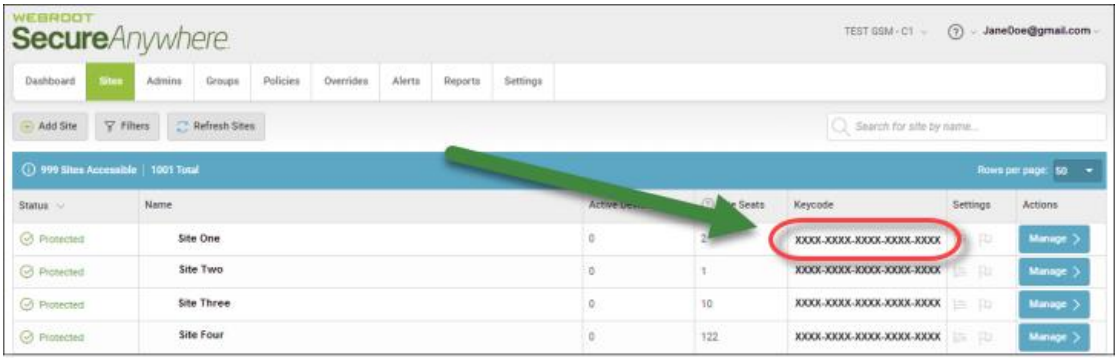


3. Log in using your Webroot credentials.
4. From the main panel, browse to your GSM console and create a new site that matches the organization in in the Kaseya VSA.

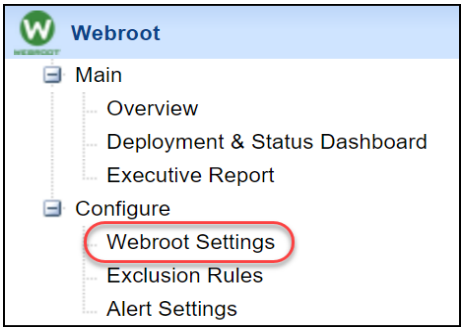


© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

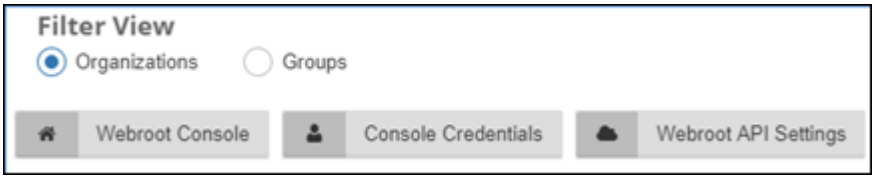
5. In the Sites panel, copy the keycode from the Keycode column for that GSM site.



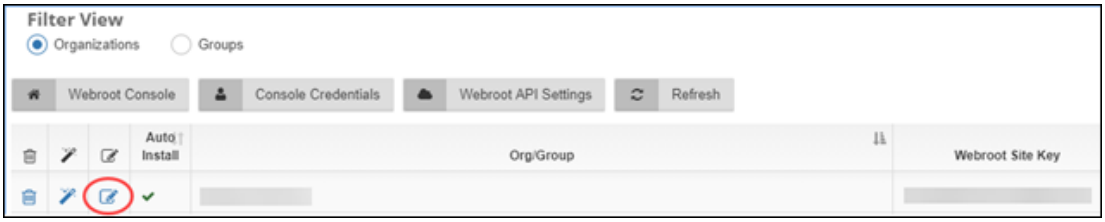
6. In Kaseya, from the main menu, select **Webroot** > **Webroot Settings**.



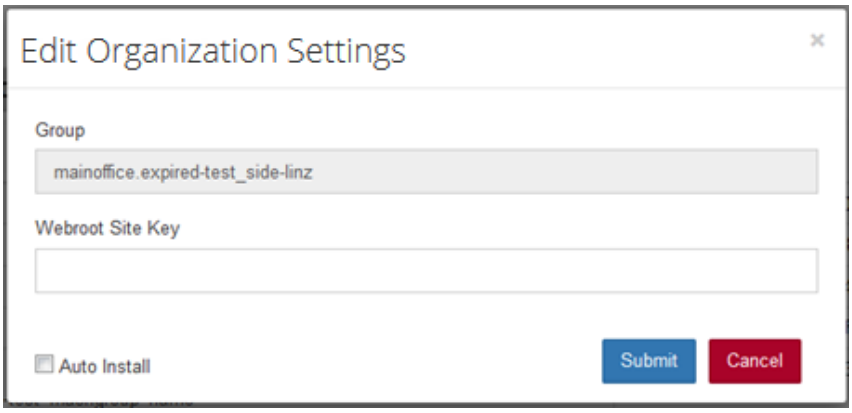
The Filter View pane allows you to filter by organization or group, which lets you assign Webroot site keycodes to Kaseya organizations or groups.



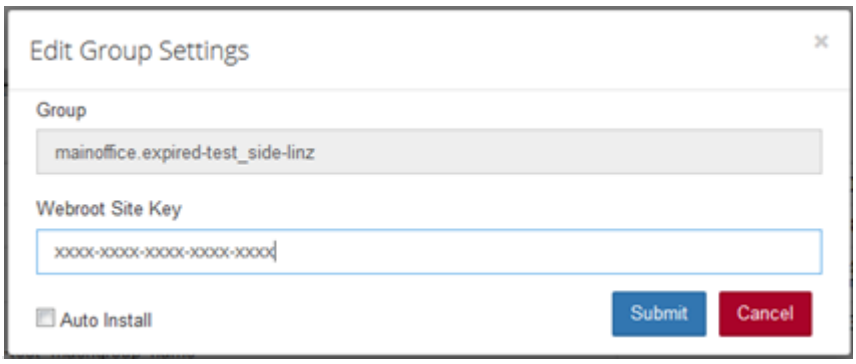
7. For the organization or group that you want to edit, click the **Edit** icon.



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



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



- If you select the **Auto Install** checkbox, then Webroot agents will be deployed automatically to all Kaseya endpoints within the defined organization or group.
- With Auto Install, we deploy Webroot agents to any newly added Kaseya endpoints with a background task, which runs once per hour. This will ensure that all Kaseya endpoints in the orgs/groups that are configured to auto install will have Webroot agents deployed.

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

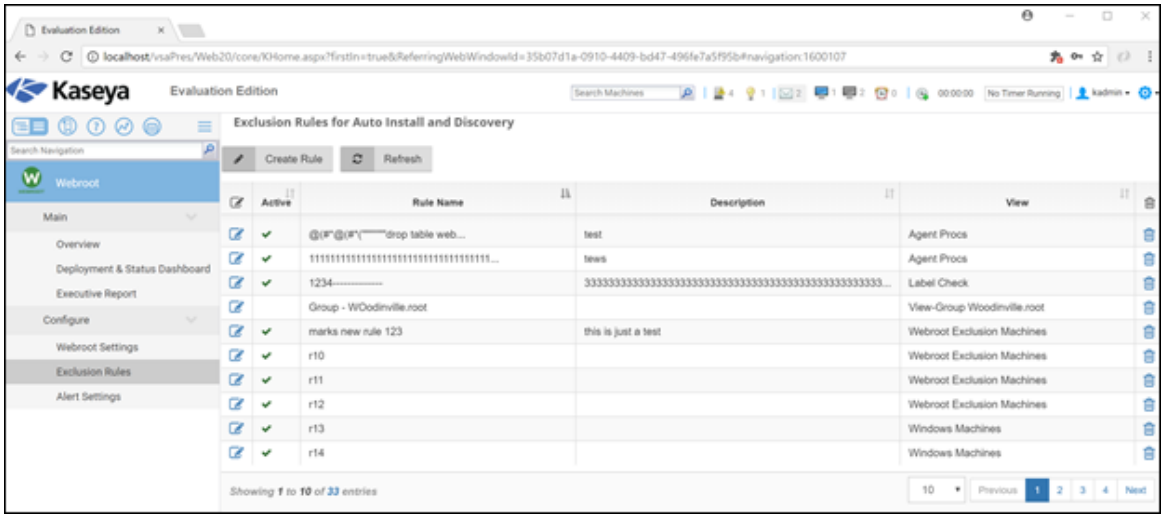
With version 2.1, it's now possible to create exclusion rules to Install, Auto Install, and Adoption. We added the ability to exclude specific machines within a group or organization by using Kaseya Views. For example, if you want to exclude machines from the install of the Webroot client, you can do 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.

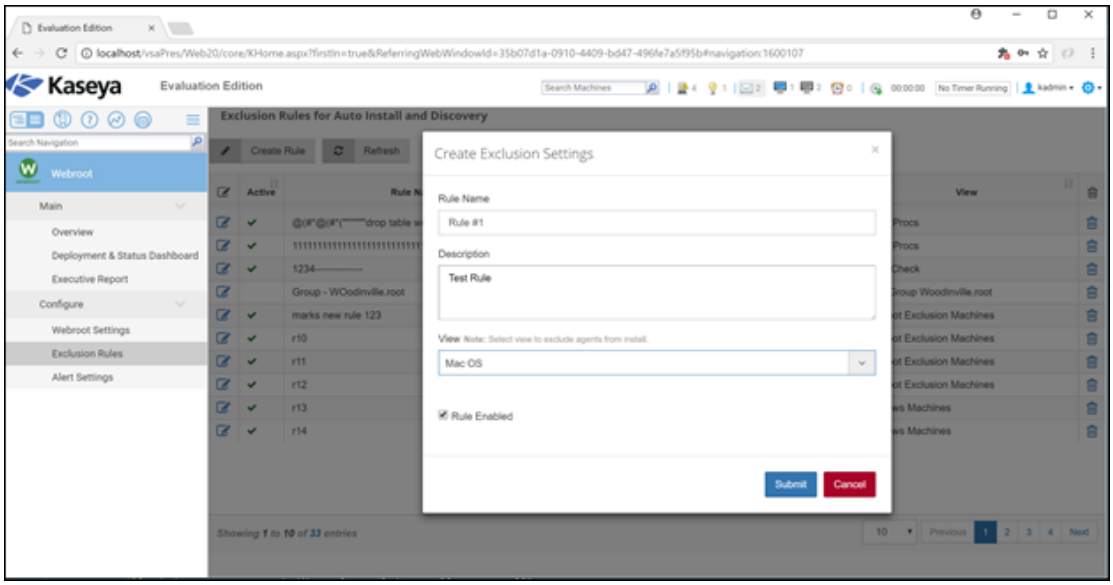
© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

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.

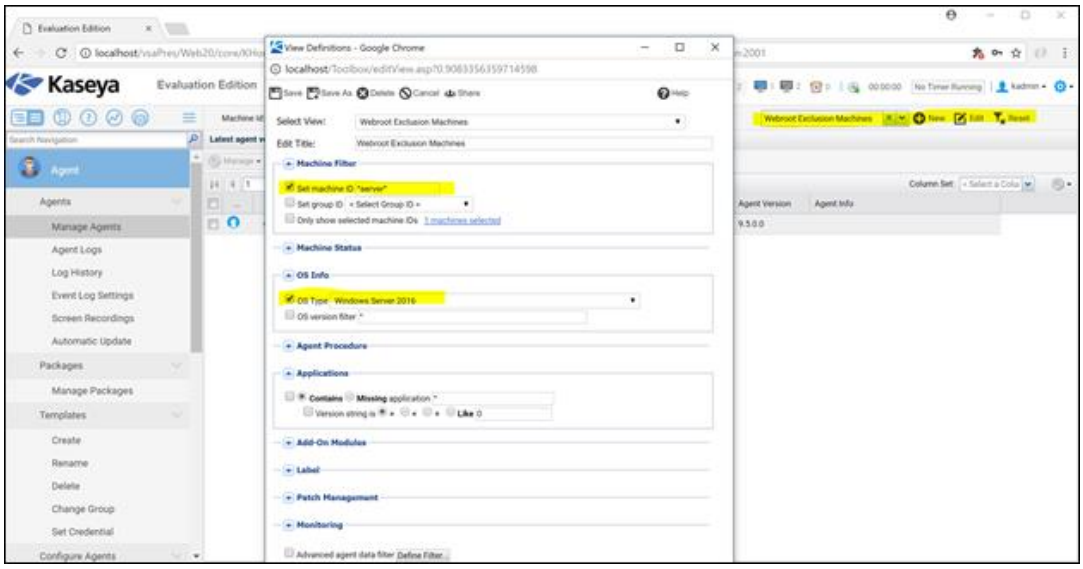


Create Exclusion Rule:

- 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.



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



Please keep in mind the following:

- 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.

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

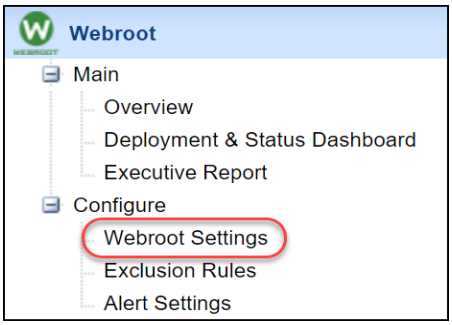
Adopting Existing Webroot Agents

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

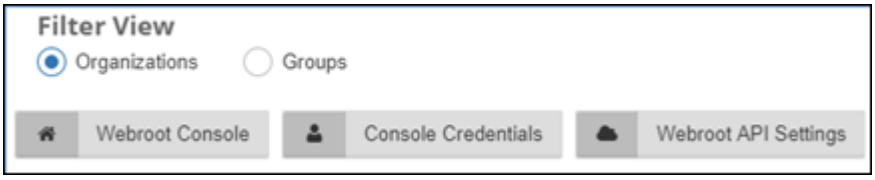
Note: Enabling Auto Install for those Organizations will do that automatically for you.

To adopt existing agents:

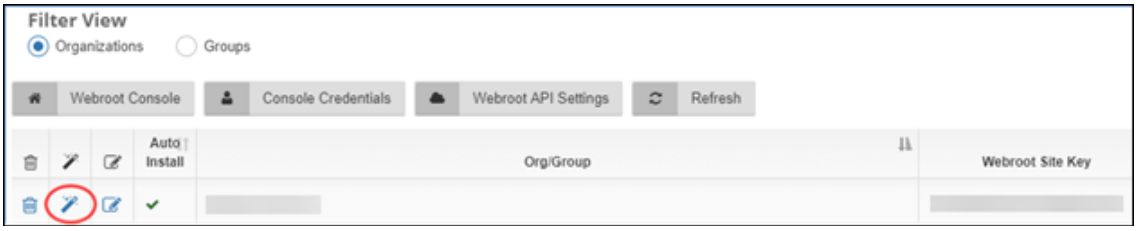
1. From the main menu, select **Webroot** > **Webroot Settings**.



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.

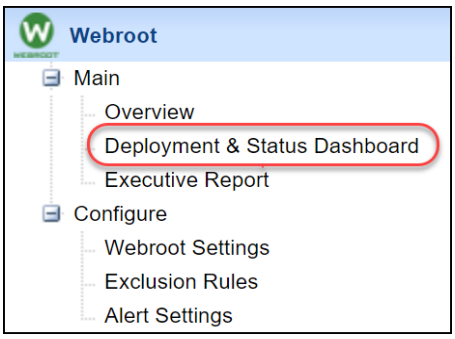
© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

Deploying Webroot Agents Through the Kaseya Module

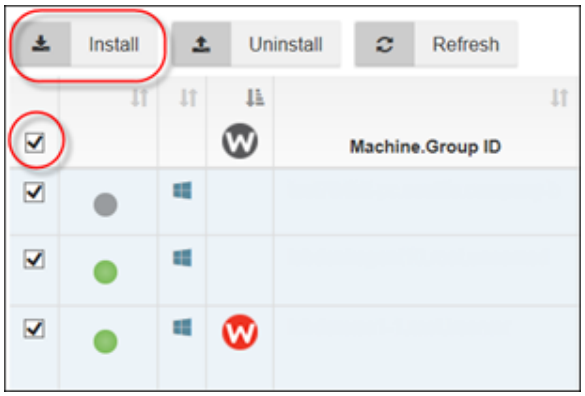
Deploying Webroot agents is very easy, provided a Kaseya agent is already installed. The site keycode for the group or organization containing these agents must be selected to display the Kaseya endpoints in the Deployment & Status Dashboard.

To deploy Webroot agents:

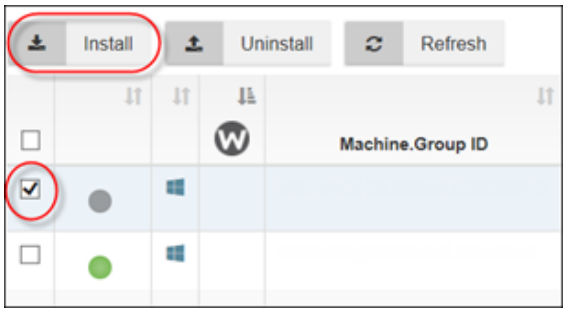
1. From the main menu, select **Webroot** > **Deployment & Status Dashboard**.



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.

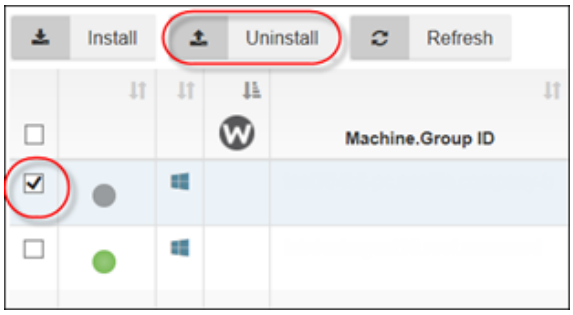


- To install Webroot agent on an individual Kaseya endpoint, select the checkbox of for the target endpoint , and click the **Install** button.



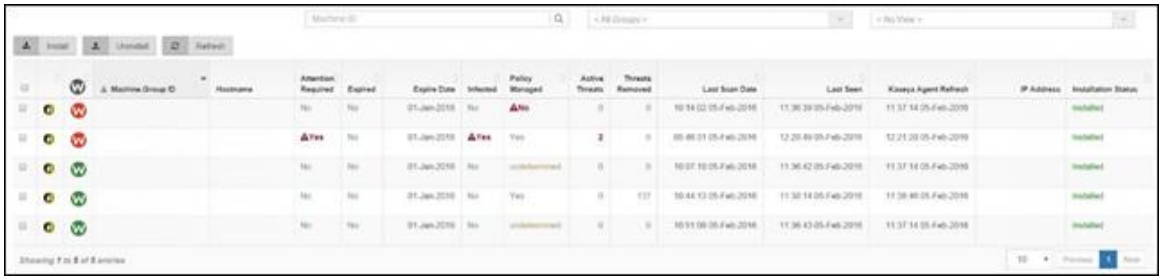
Progress during the installation process is indicated by an Installing status. Once the installation is complete, the installation status will change to Installed.

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



Viewing Installation and Dashboard Level Webroot Agent Statuses

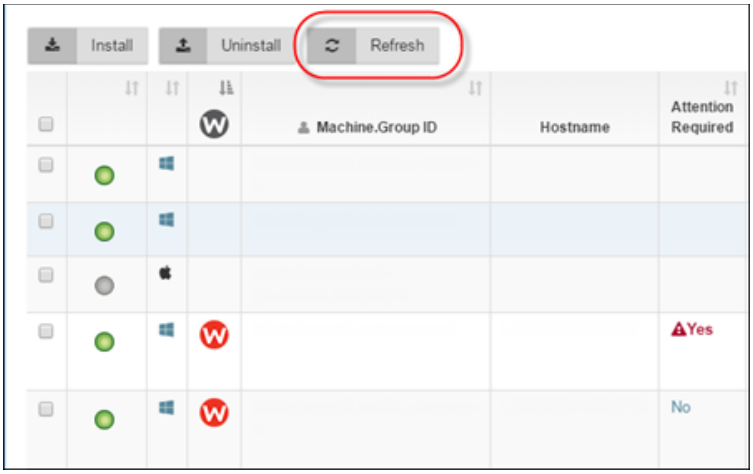
Once the desired Webroot agents are installed, you will be able to see their status at a glance.



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

Icon	Description
	Windows OS
	Mac OS

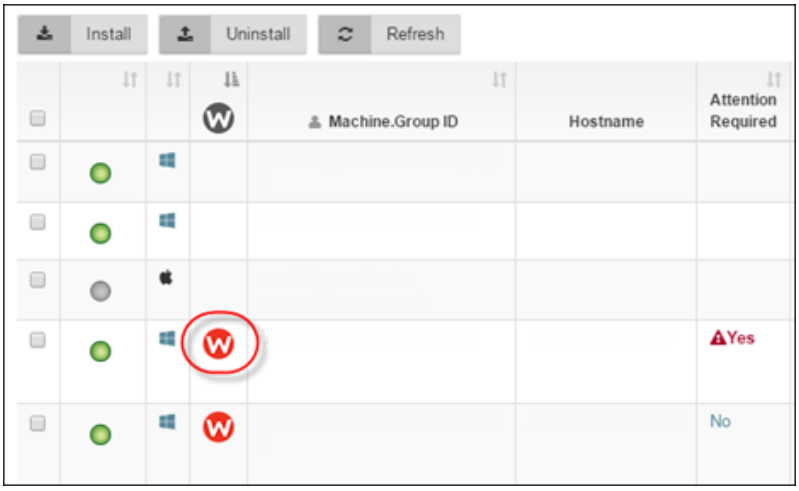
- If the Unity API is turned on, any changes within the managed agents will be checked every 15 minutes.
- If the API is not on, the interval to check for changes within the managed agents is one hour.



Indicators in the Deployment & Status Dashboard

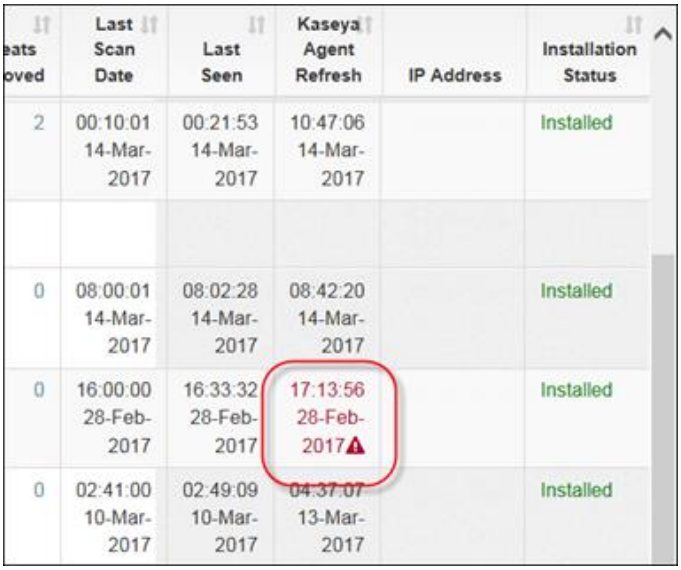
Red W

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.



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.



© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

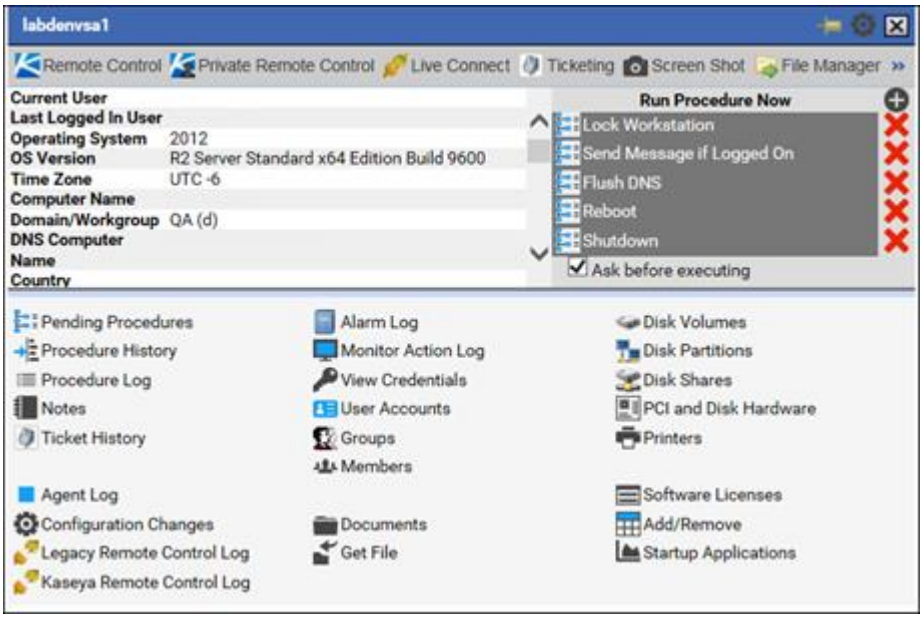
Validating Success of Agent Procedures

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

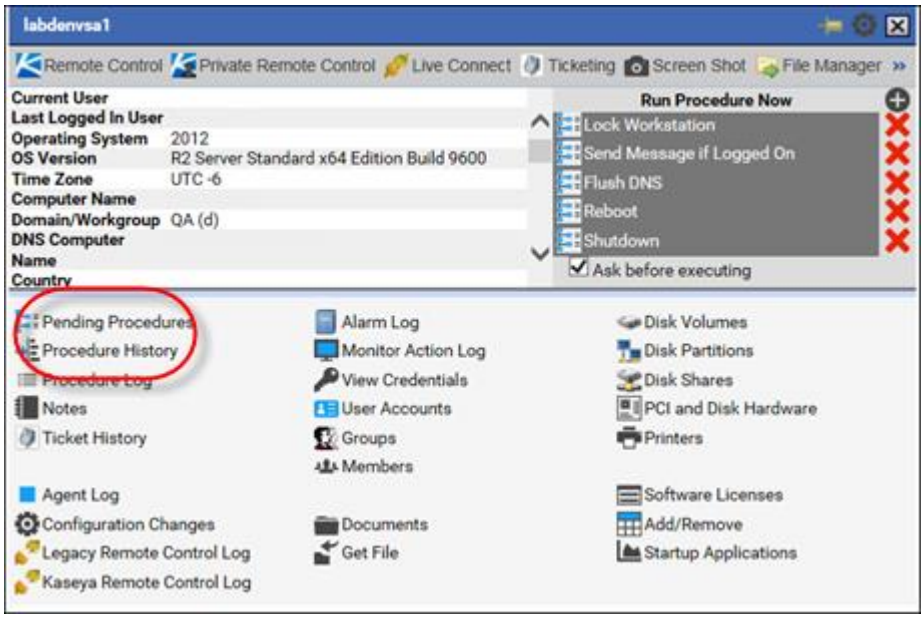
To validate success:

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

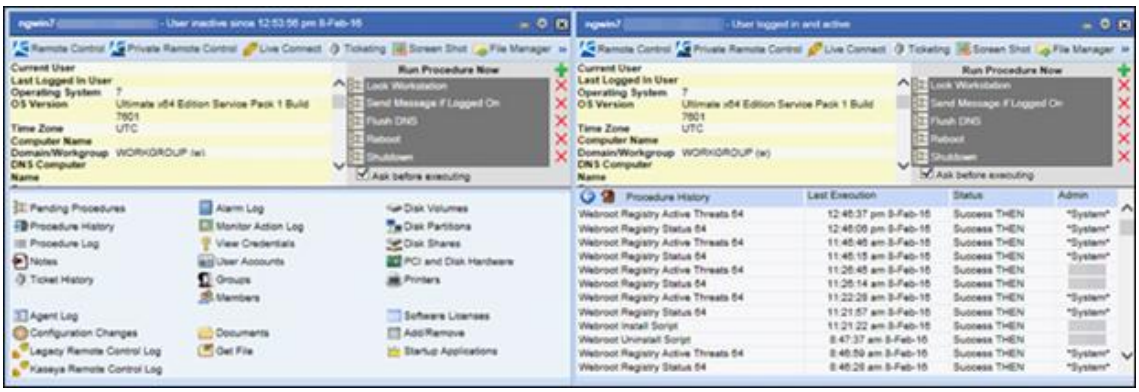
The Live Connect information window displays.



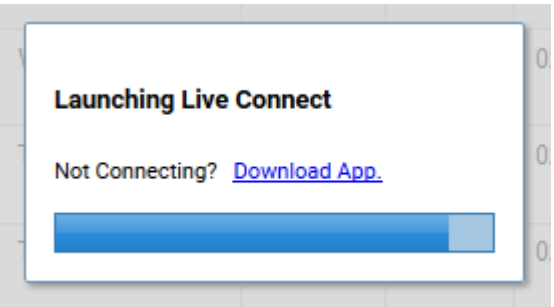
2. Select one of the following:
   - **Pending Procedures**
   - **Procedure History**



3. Review information, as needed.



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

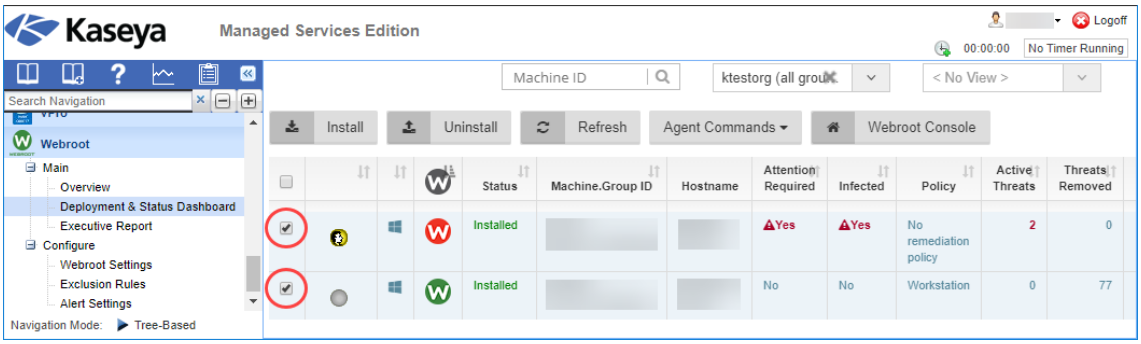


Running Webroot Agent Commands

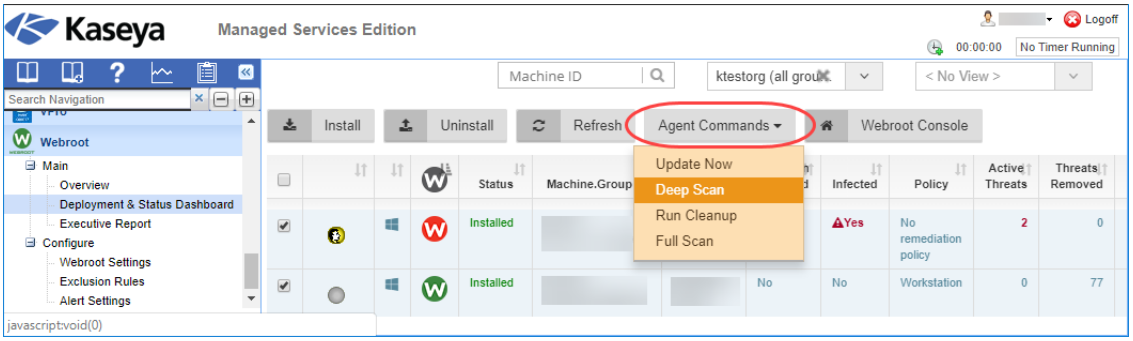
You can run Webroot Agent Commands on one or more Wbroot Agents from the Deployment & Status Dashboard.

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*.



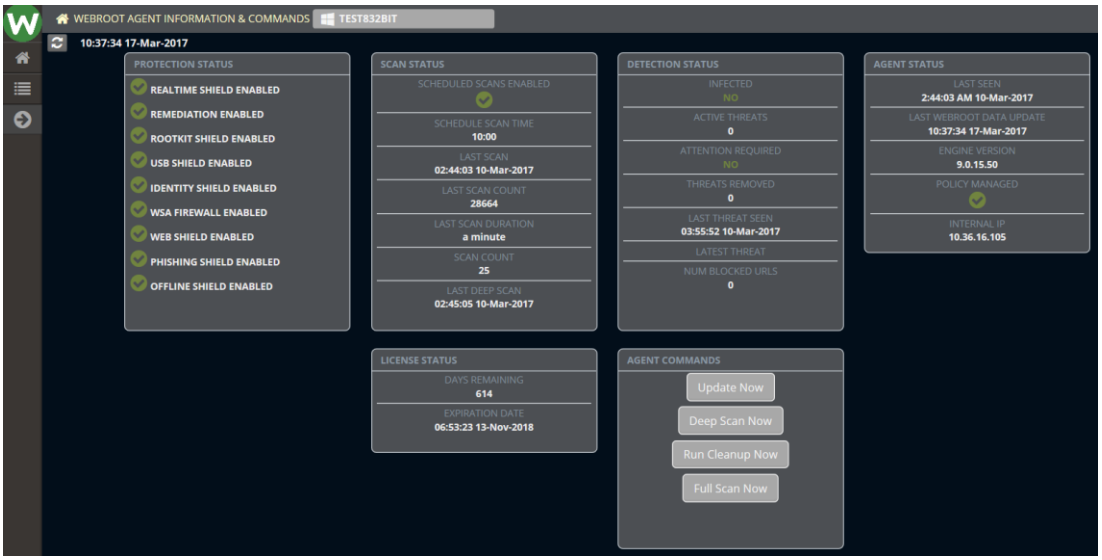
Detailed Webroot Agent Status and Agent Commands

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.

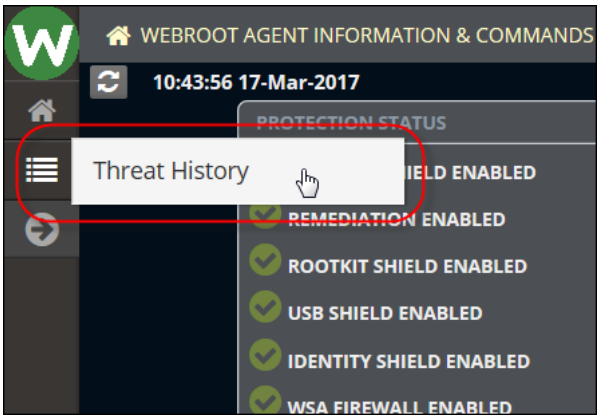
The system displays detailed Webroot Agent Information and Commands pane.



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.

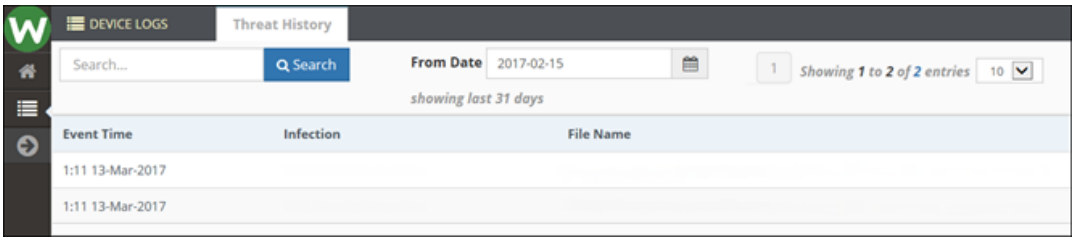
   Note: If Webroot agents are uninstalled and reinstalled, the Agent Status statistics are reset.

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



© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

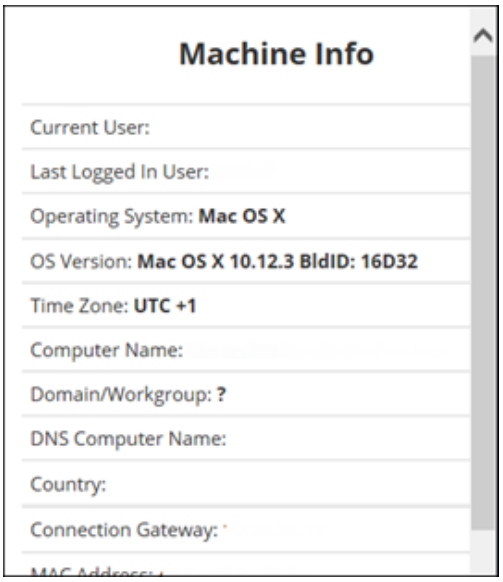
Threat history information displays.



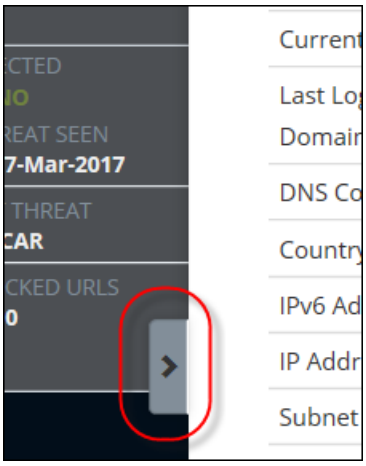
Note: Webroot endpoint threat history is persistent and will be available via the Executive Reports, even if endpoints are uninstalled or deactivated.

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

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

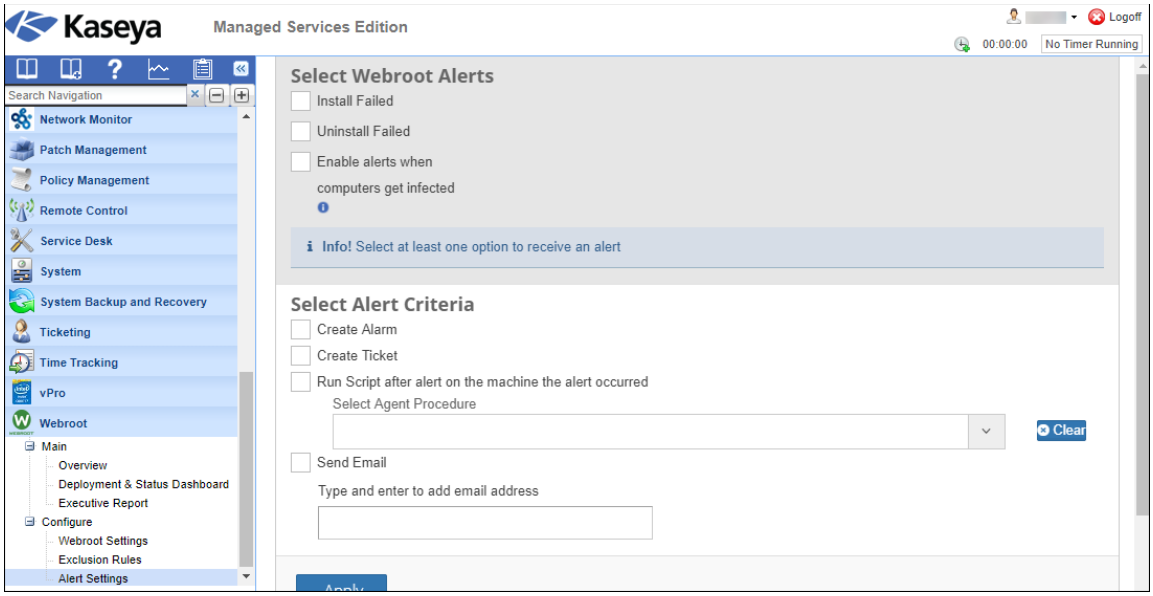


5. To return to the Webroot Agent Information & Commands pane, click the **Side** arrow.



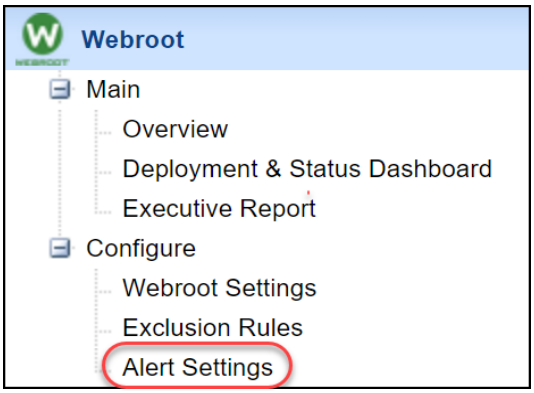
Integrated Alarm Parameters With Kaseya Alert Actions

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.



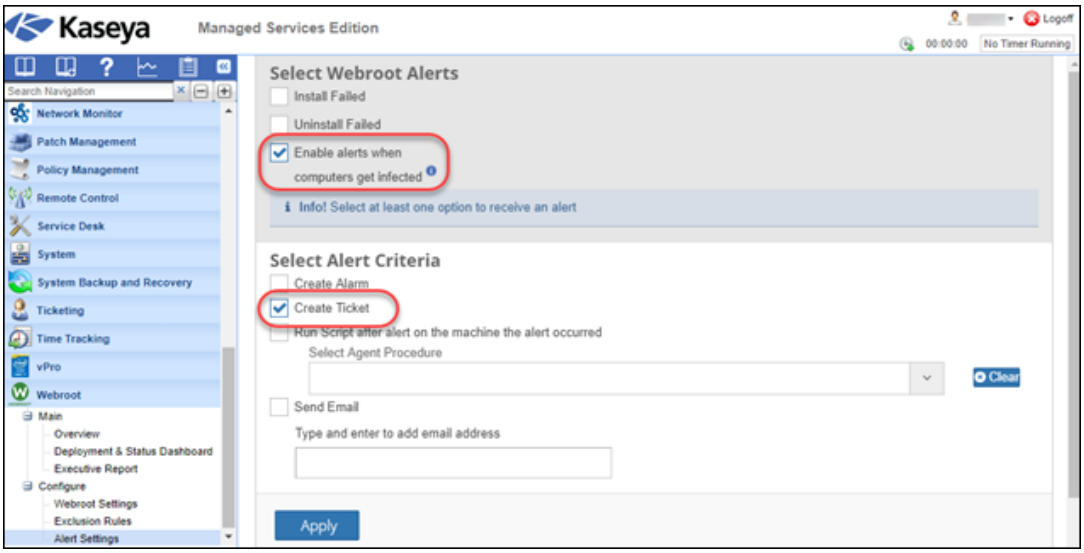
To set an alert:

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

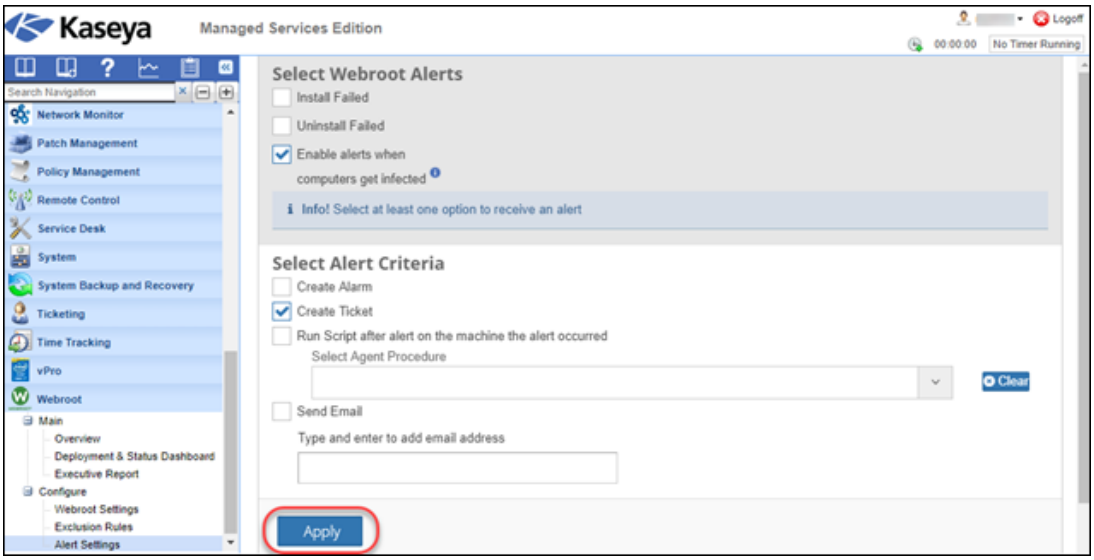


© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

The Webroot Alerts pane displays.



2. Select one or more of the **Webroot Alerts** checkboxes, such as *Enable alerts when computers get infected*.
3. Select the relevant **Alert Criteria** checkbox, such as *Create Ticket*.
4. When you're done, click the **Apply** button.

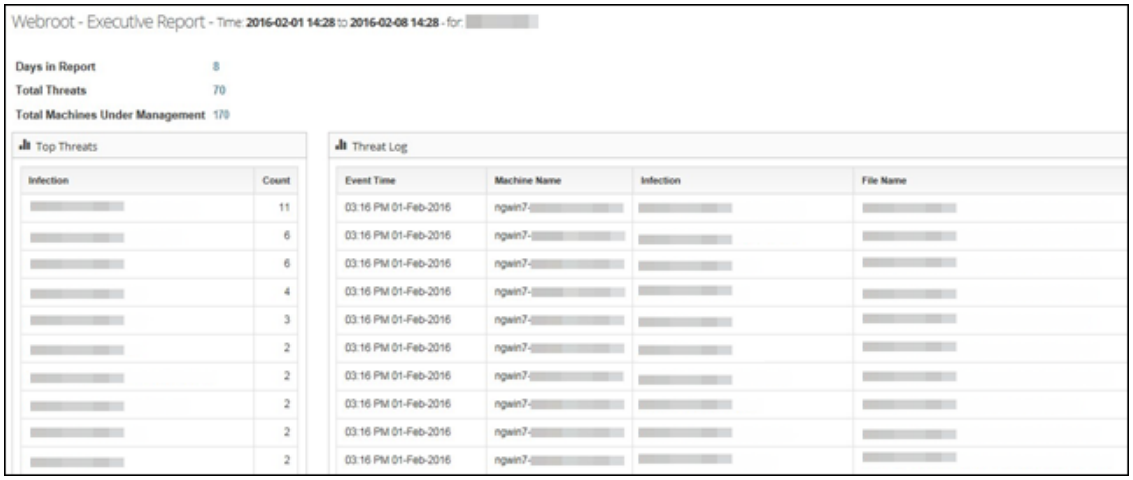


Note: In order to receive Alerts via email, you must enter a valid email address.

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

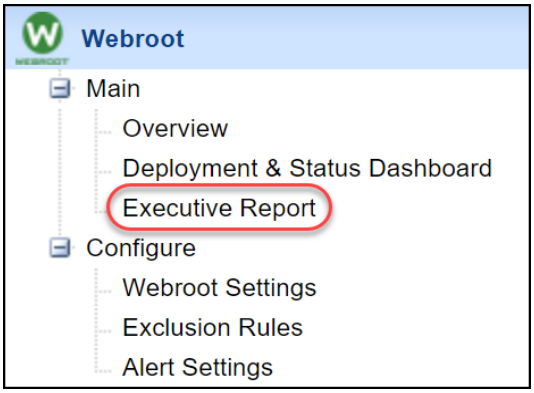
Running Executive Reports

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



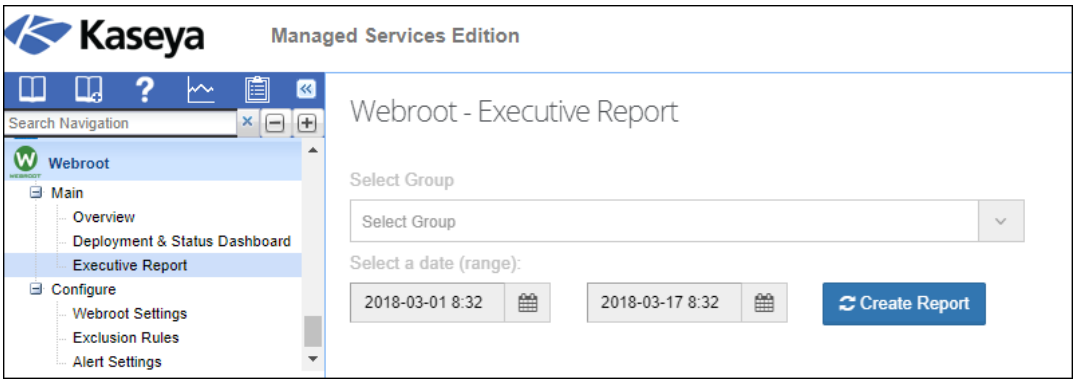
To generate an executive report:

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

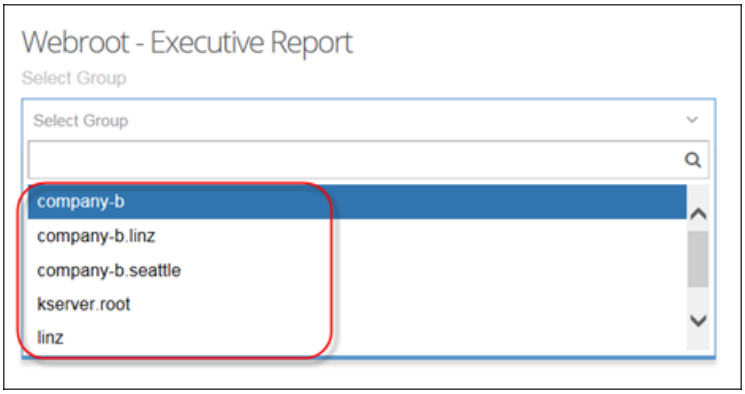


© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

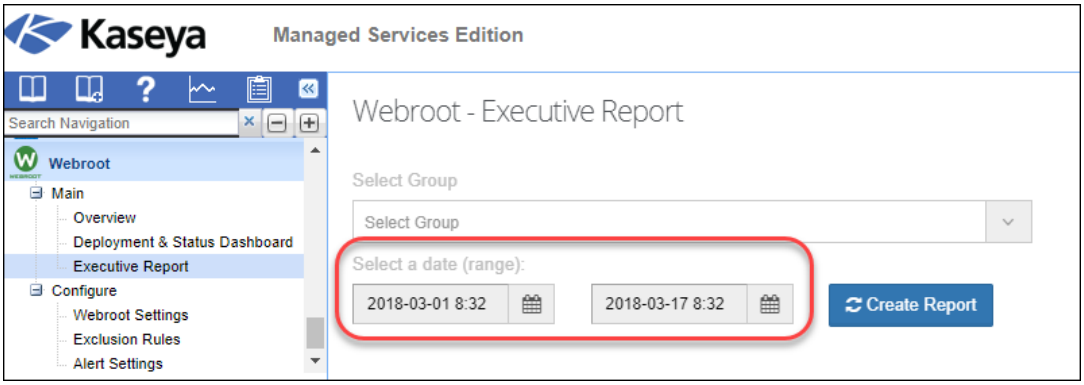
The Webroot – Executive Report pane displays.



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

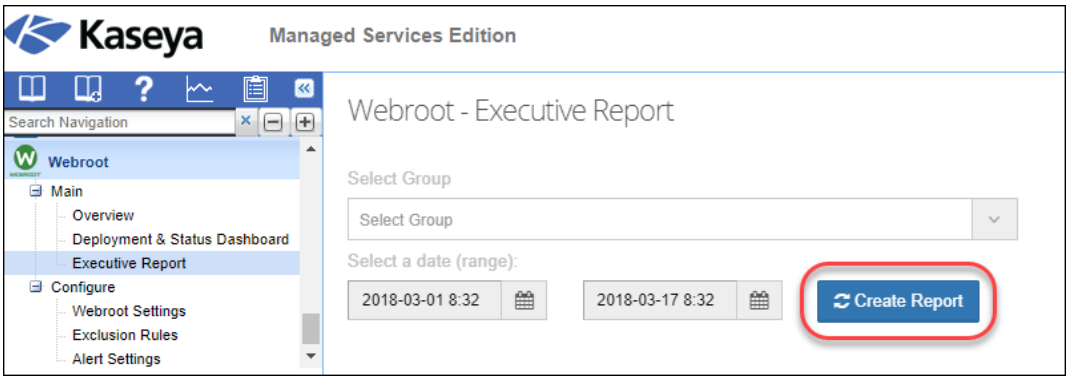


3. Using the two date fields, select an appropriate date range.



© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information

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

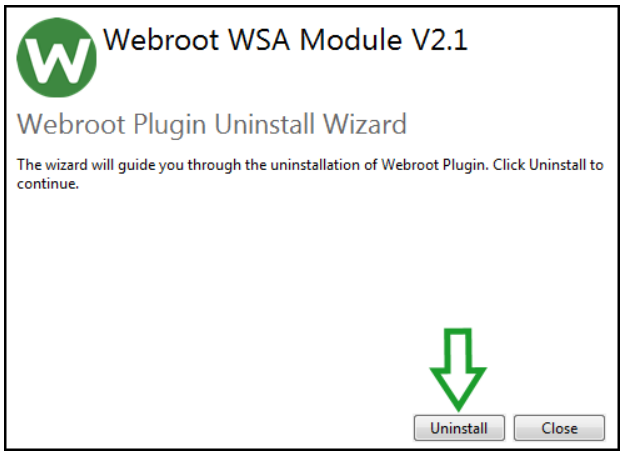


Note: Historical data is retained, even if Webroot endpoints are uninstalled or deactivated.

Uninstalling the Kaseya Plugin

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

Note: After uninstalling Kaseya module V2.1, 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.



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.

© 2018 Webroot Inc. All rights reserved. | Proprietary and Confidential Information