Kaseya Module
Version 2.0x
Getting Started Guide

Table of Contents

Overview

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

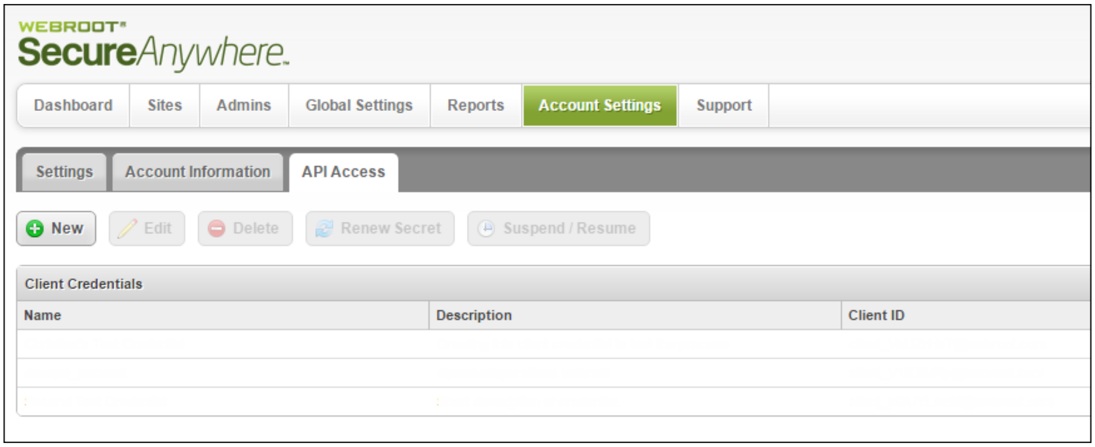
The Kaseya Module offers powerful features including deployment management, dashboards, auto-discovery, WSAB agent commands, actionable alerts, and threat history. This module is the first of a series of planned releases designed to optimize operational costs of WSAB security management via the Kaseya VSA platform. Further releases will add increased automation, efficiency features, and reporting.

The Module is designed to be extremely easy to install, requiring only a few clicks. It's intuitive to use, with helpful hints throughout; however, we recommend you read through this guide before deployment. This module is in complete compliance to all third party integration definitions for Kaseya on-prem VSA version 9.2 and up. At the time of publication, the module was tested up to VSA version 9.4.

Prerequisites

You will need the following to install the module:

- 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 9.



Note: If you are a first-time Webroot user, please complete your GSM account setup before going any further. For more information, see *Creating a Webroot Account*.

- 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
- Kaseya Module installer

  `WR_KPlugin_2.x.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

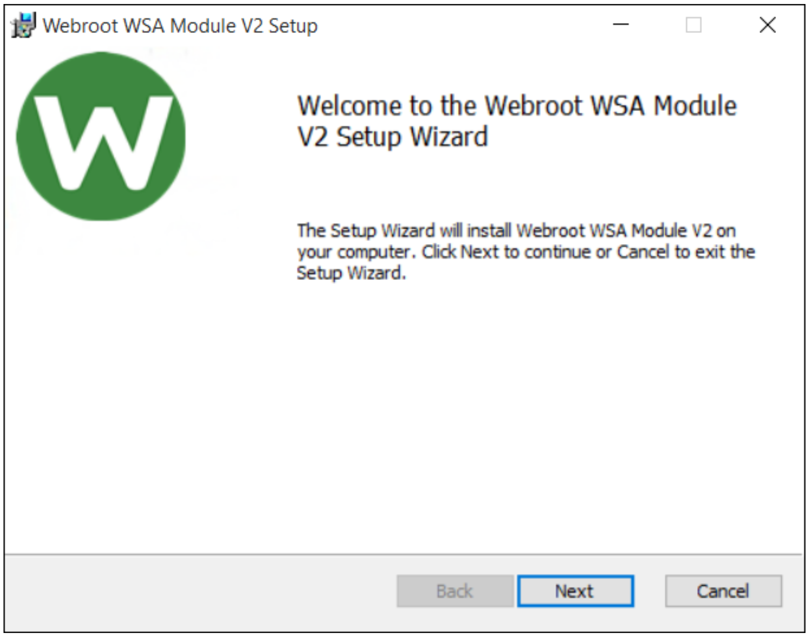
If you have met all the prerequisites, use the following procedure.

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.x.xx.xxxx.exe
   ```

3. Follow the on-screen prompts.

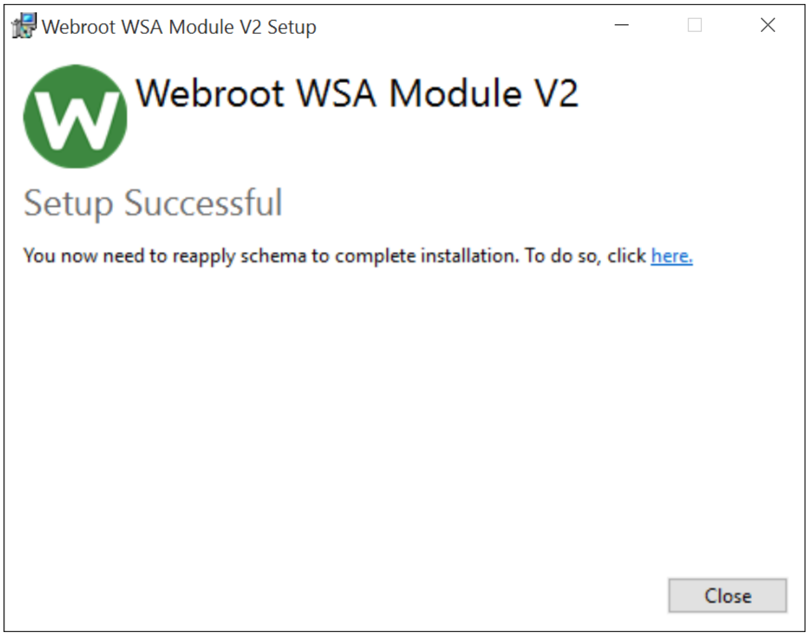


Webroot WSA Module V2 Setup

Welcome to the Webroot WSA Module V2 Setup Wizard

The Setup Wizard will install Webroot WSA Module V2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Until the Setup Successful window displays.



Webroot WSA Module V2 Setup

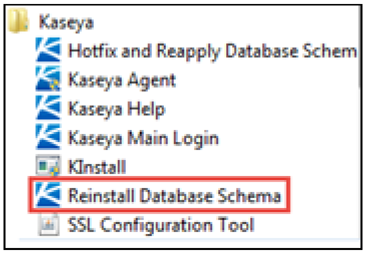
Webroot WSA Module V2

Setup Successful

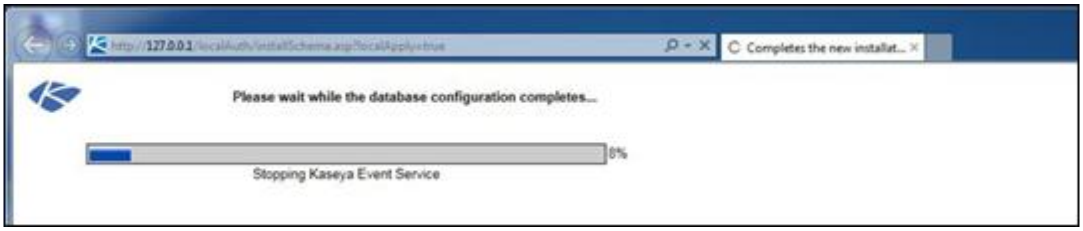
You now need to reapply schema to complete installation. To do so, click here.

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 (see screenshot above), 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.

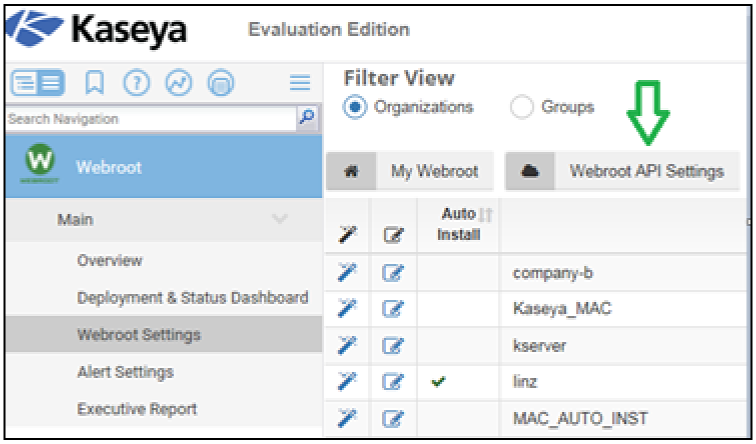
Enabling Webroot API Settings

In version two we have improved plug-in performance by utilizing Webroot Unity API. We strongly recommend that you enable the usage of Unity API in your plug-in to take advantage of this improved performance and user experience.

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

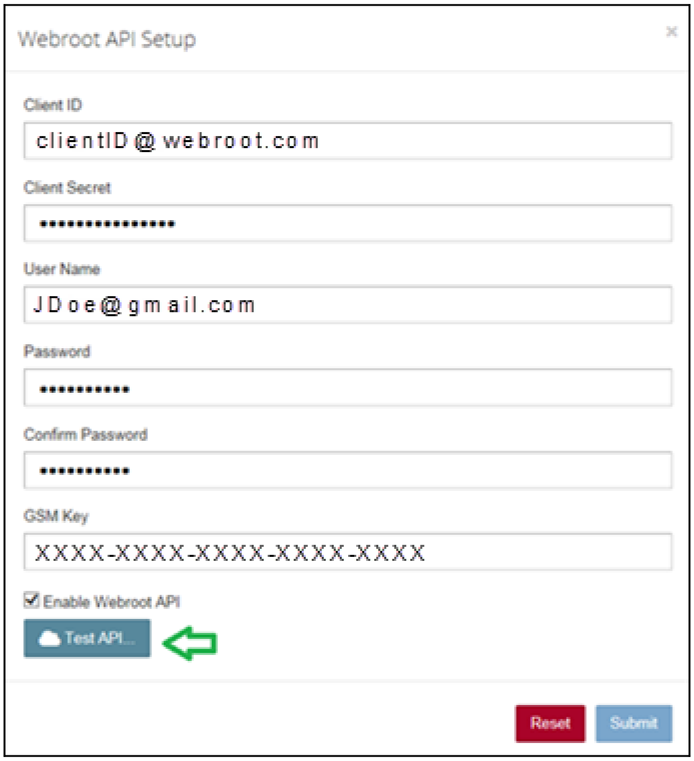
To enable Webroot API settings:

1. After the installation was successful, you must enter valid Webroot API Settings, (Webroot\Main\Webroot Settings\Webroot API Settings) and start a test.
2. Click the **Webroot API Settings** button.



		Auto Install	
			company-b
			Kaseya_MAC
			kserver
		✓	linz
			MAC_AUTO_INST

The Webroot API Setup window displays.



Client ID
clientID@webroot.com

Client Secret
••••••••••••••••

User Name
JDoe@gmail.com

Password
•••••••••••

Confirm Password
•••••••••••

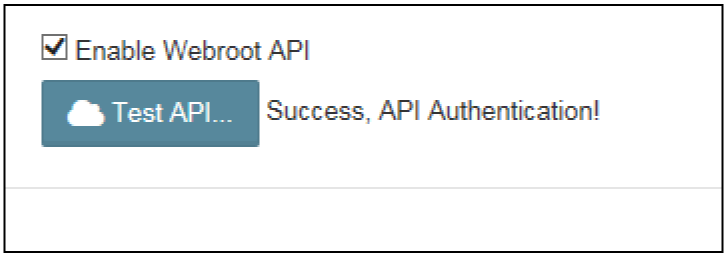
GSM Key
XXXX-XXXX-XXXX-XXXX-XXXX

☑ Enable Webroot API

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, contact your Webroot sales representative.

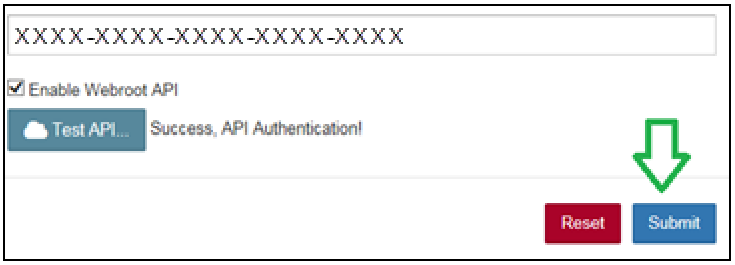
3. Click the **Test API** button.



☑ Enable Webroot API

Success, API Authentication!

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



XXXX-XXXX-XXXX-XXXX-XXXX

☑ Enable Webroot API

Success, API Authentication!

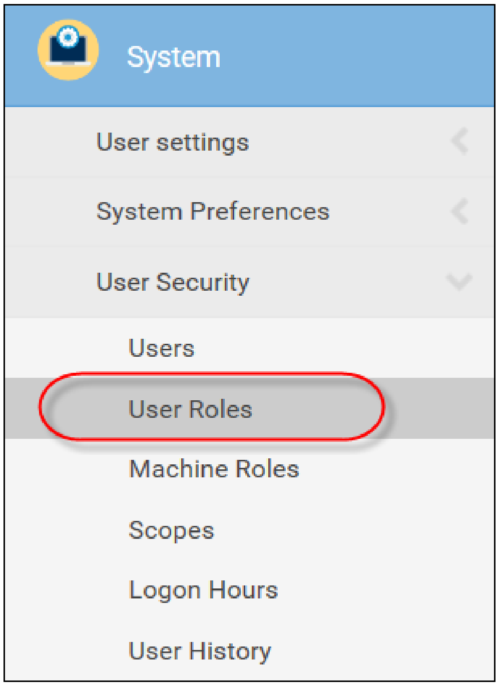
Note: In case the test fails, the error message should indicate what's wrong in your settings. Fix the issue before proceeding.

Controlling Access to Webroot Settings

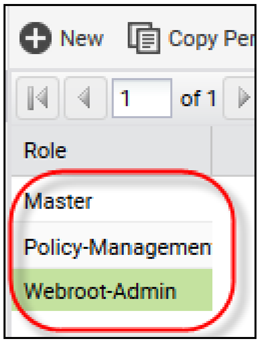
As needed, you can control an admin's access to Webroot settings. We recommend that you allow access to only those admins who will make GSM parent keycode assignments.

To control access to Webroot settings:

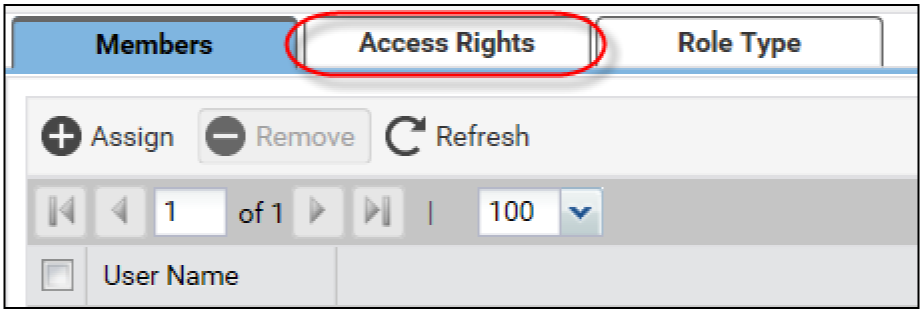
1. From the main menu, select **System** > **User Roles**.



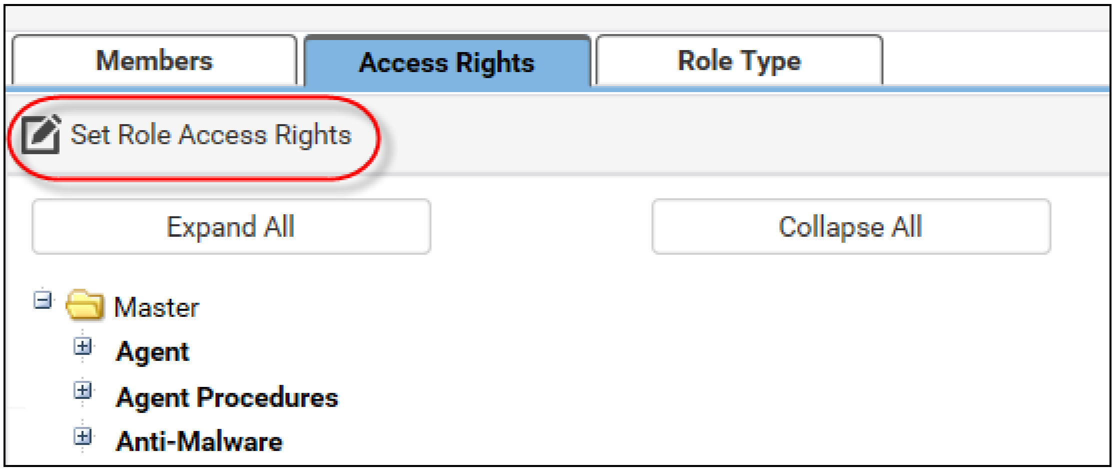
2. In the Role pane, select the role you want to apply the permissions to.



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



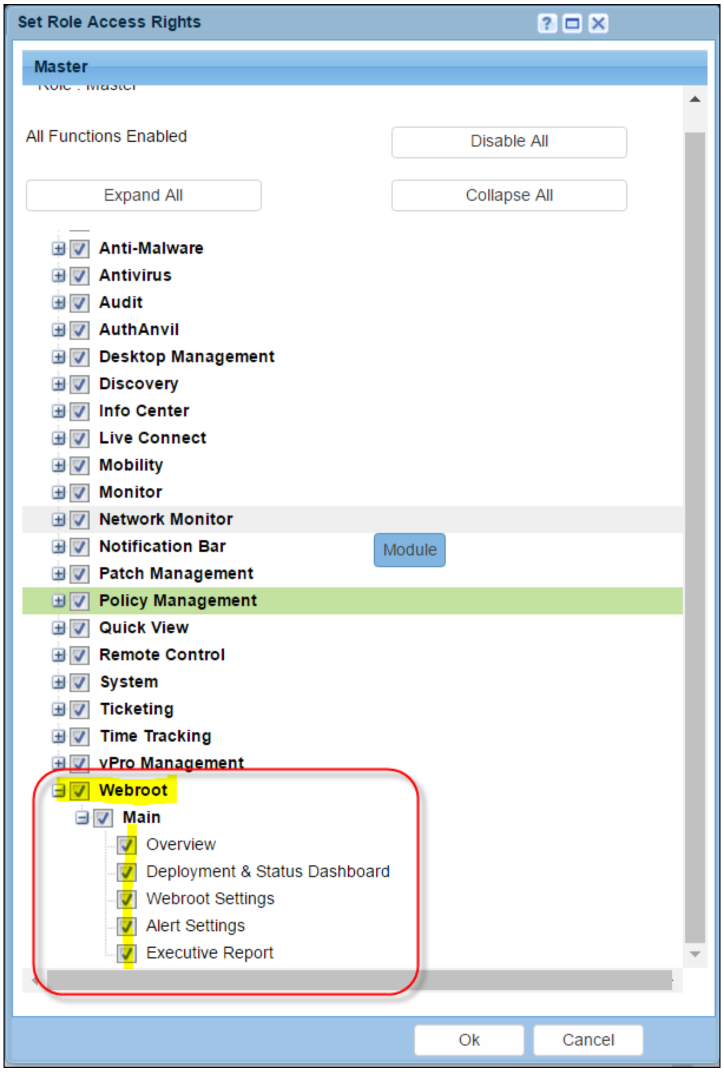
4. In the Access Rights tab, click the **Set Role Access Rights** button.



5. From the list, select **Master** > **Webroot** to expand the list.

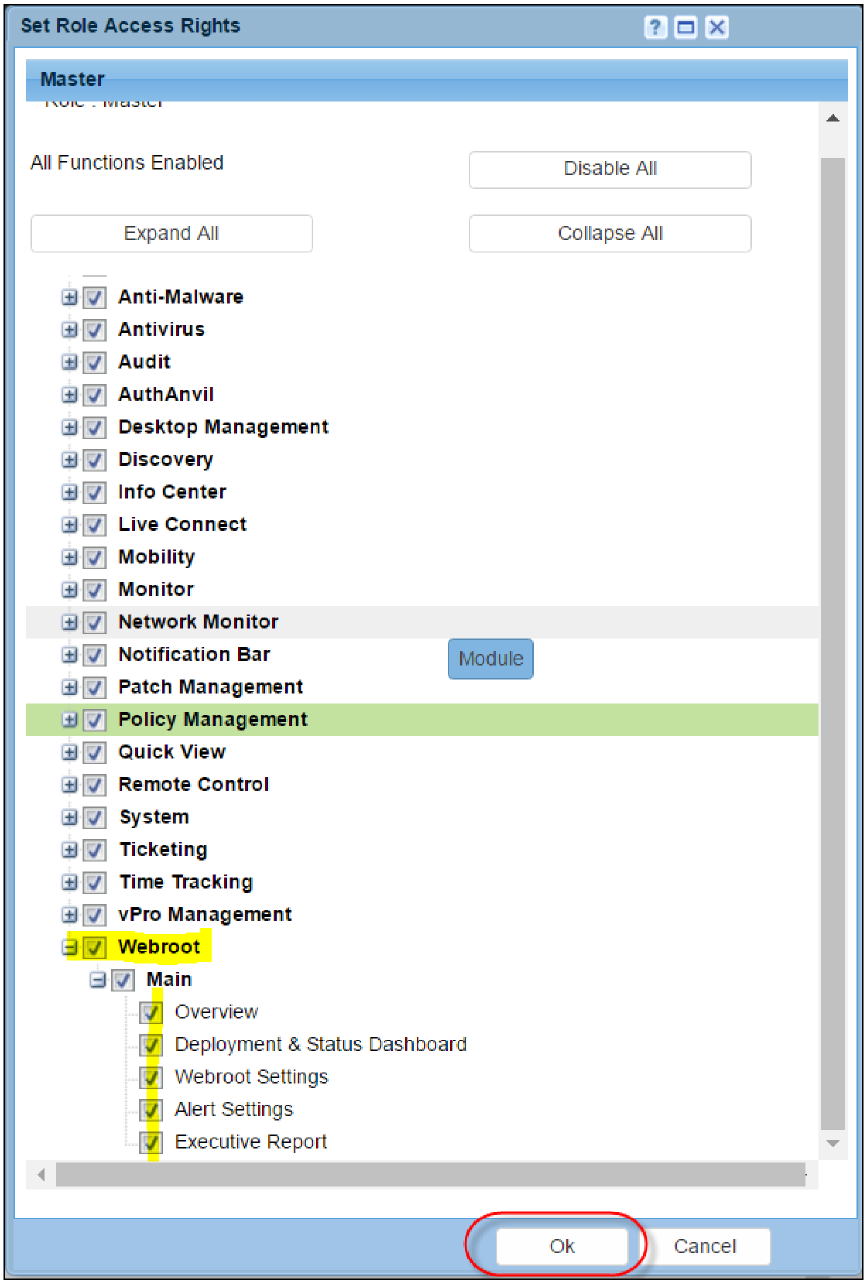
6. Select the checkboxes next to the areas that you want to allow access to.

   - Webroot
   - Main
   - Overview
   - Deployment & Status Dashboard
   - Webroot Settings
   - Alert Settings
   - Executive Report



- ☑ Anti-Malware
- ☑ Antivirus
- ☑ Audit
- ☑ AuthAnvil
- ☑ Desktop Management
- ☑ Discovery
- ☑ Info Center
- ☑ Live Connect
- ☑ Mobility
- ☑ Monitor
- ☑ Network Monitor
- ☑ Notification Bar
- ☑ Patch Management
- ☑ Policy Management
- ☑ Quick View
- ☑ Remote Control
- ☑ System
- ☑ Ticketing
- ☑ Time Tracking
- ☑ vPro Management
- ☑ Webroot
  - ☑ Main
    - ☑ Overview
    - ☑ Deployment & Status Dashboard
    - ☑ Webroot Settings
    - ☑ Alert Settings
    - ☑ Executive Report

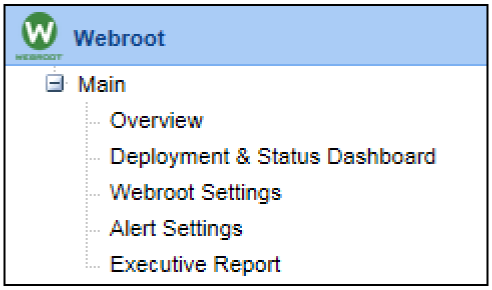
7. When you're done, click **OK**.



Getting Started and Deployment

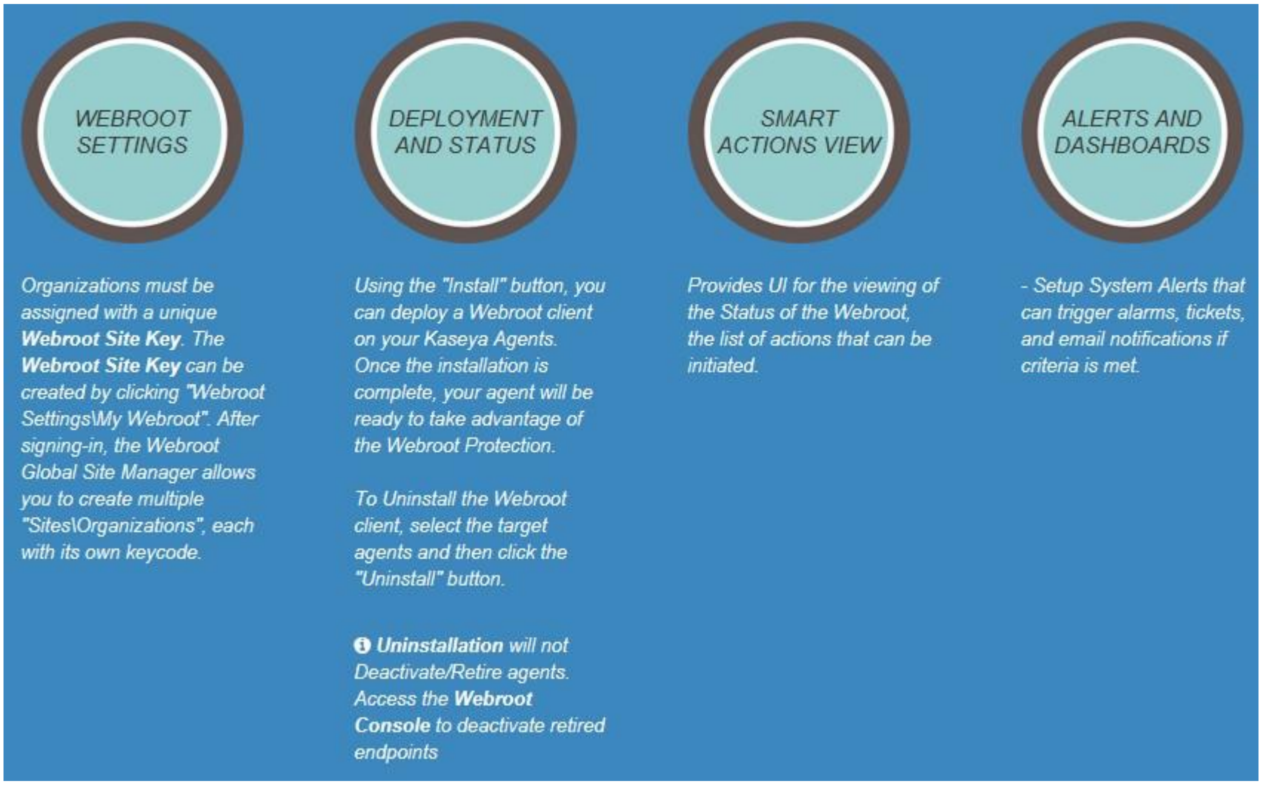
The user interface within the Kaseya Module is designed to be easy to use and is broken down to five main menu items:

- **Overview** – Basic guide to steps required. See How To Overview on page 14.
- **Deployment & Status Dashboard** – Allows simple GUI-driven deployments and menus for detailed status view as well as agent commands. See WSAB Agent Deployment on page 13.
- **Webroot Settings** – Webroot specific settings, such as site or default keycode, Webroot console access, and auto WSAB adoption wizard. See Adopting Existing WSAB Agents on page 16.
- **Alert Settings** – Alerts and alert criteria. See Integrated Alarm Parameters with Kaseya Alert Actions on page 38.
- **Executive Report** – Generating malware reports. See Running an Executive Report on page 41.



Overview Menu

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



WEBROOT SETTINGS

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

DEPLOYMENT AND STATUS

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

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

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

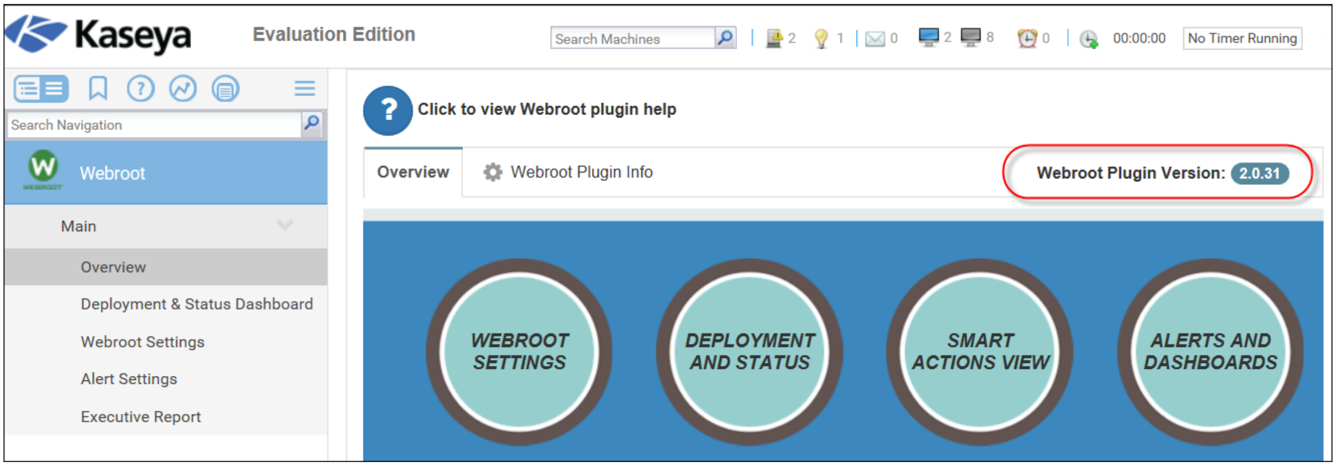
SMART ACTIONS VIEW

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

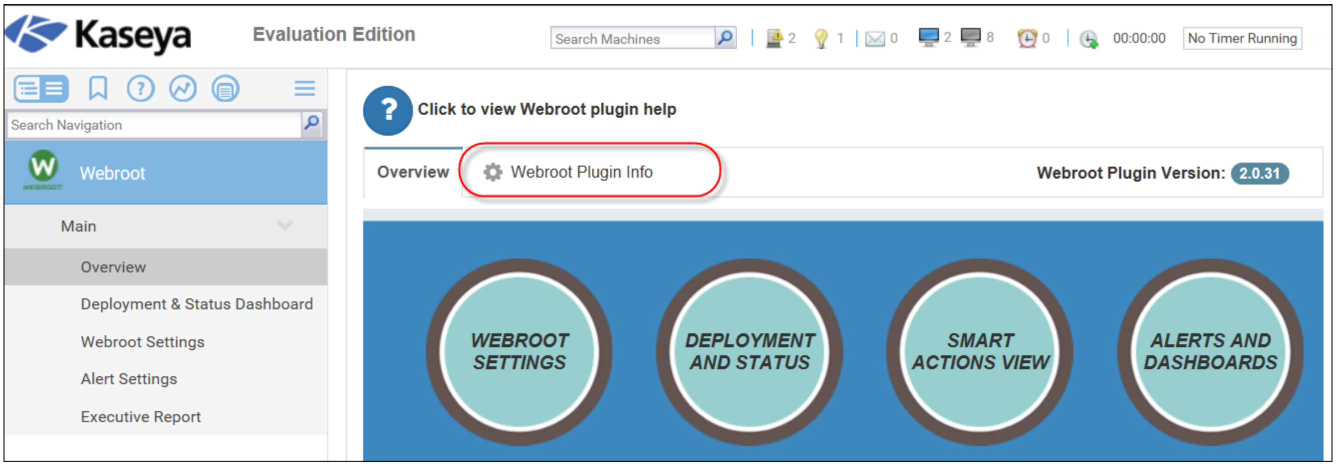
ALERTS AND DASHBOARDS

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

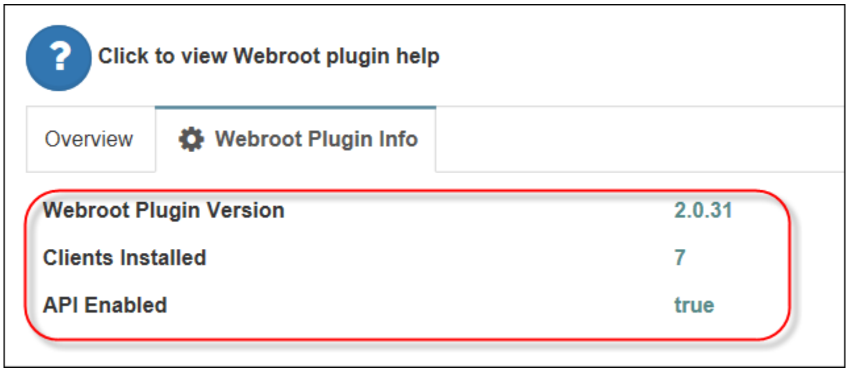
Included on the Overview tab is information about the plugin version, which is located in the upper right corner.



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 Plugin Version	2.0.31
Clients Installed	7
API Enabled	true

Webroot Secure Anywhere Business Endpoint (WSAB agent) Deployment

The following portion of the guide describes each of the steps needed to install the WSAB agents to selected endpoints. This process is broken into three main steps:

- Configuring and obtaining a unique Webroot site key. See Configuring and Obtaining a Unique Webroot Site Key on page 5.
- Deploying WSAB agents through the Kaseya module. See Deploying WSAB Agents Through the Kaseya Module page 28.
- Viewing installation and dashboard-level WSAB agent status. See Viewing Installation and Dashboard Level WSAB Agent Status on page 30.

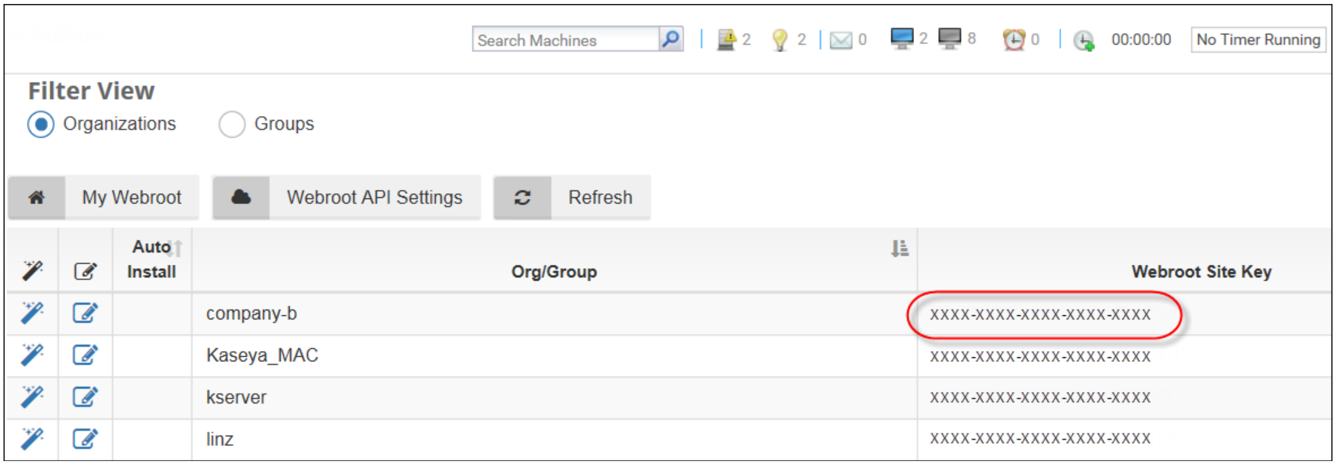
Note: If you have an existing WSAB deployment, you can adopt already installed endpoints in to the Kaseya Module. For more information, see Adopting Existing WSAB Agents on page 16.

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 20.

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.



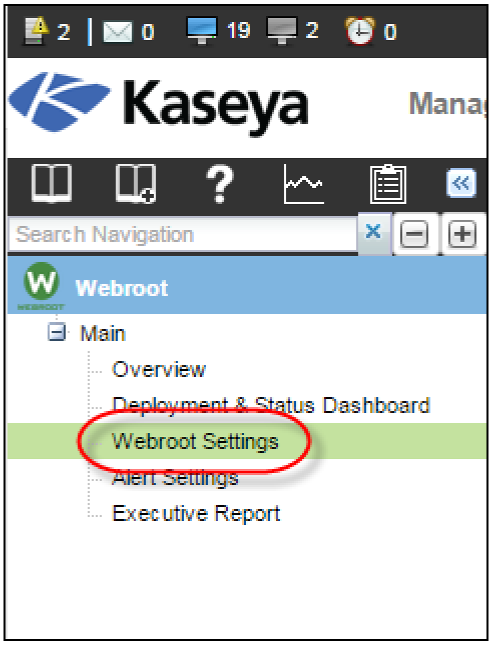
Filter View

● Organizations ○ Groups

		Auto Install	Org/Group	Webroot Site Key
			company-b	XXXX-XXXX-XXXX-XXXX-XXXX
			Kaseya_MAC	XXXX-XXXX-XXXX-XXXX-XXXX
			kserver	XXXX-XXXX-XXXX-XXXX-XXXX
			linz	XXXX-XXXX-XXXX-XXXX-XXXX

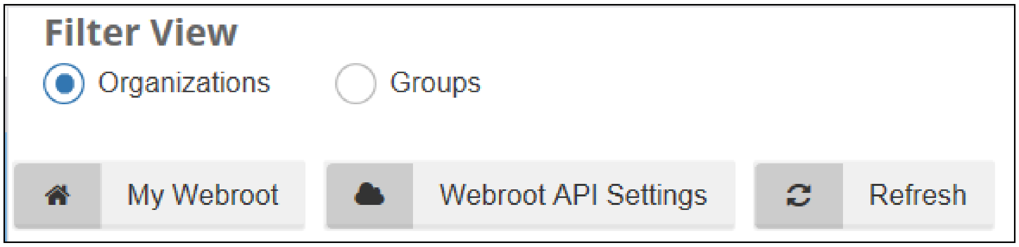
To obtain a unique site key:

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

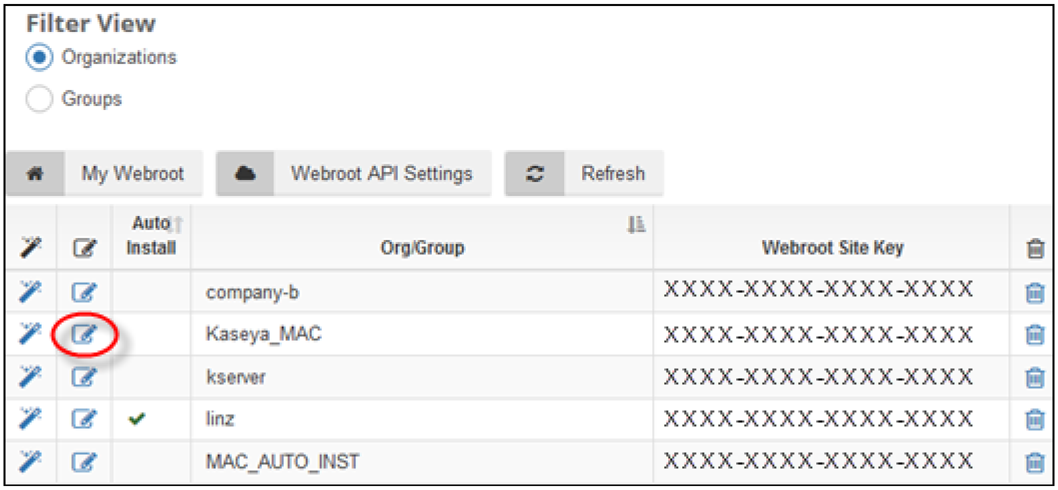


The Filter View pane displays with the Organizations radio button active, though you can select the **Groups** radio button, as needed.

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.



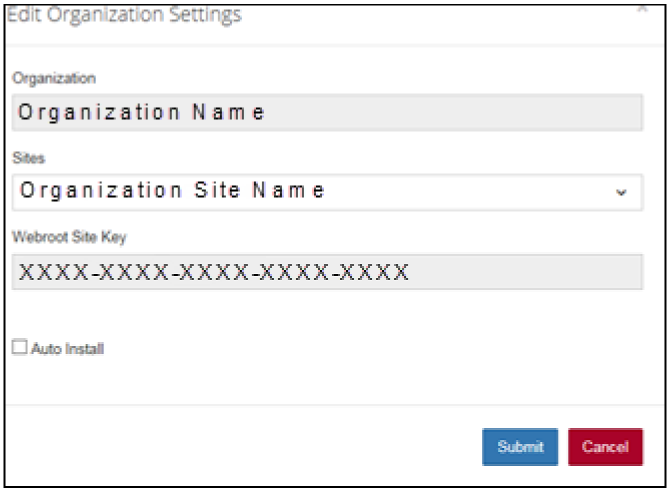
Filter View

● Organizations

○ Groups

		Auto Install	Org/Group	Webroot Site Key	
			company-b	XXXX-XXXX-XXXX-XXXX	
			Kaseya_MAC	XXXX-XXXX-XXXX-XXXX	
			kserver	XXXX-XXXX-XXXX-XXXX	
		✓	linz	XXXX-XXXX-XXXX-XXXX	
			MAC_AUTO_INST	XXXX-XXXX-XXXX-XXXX	

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



Edit Organization Settings

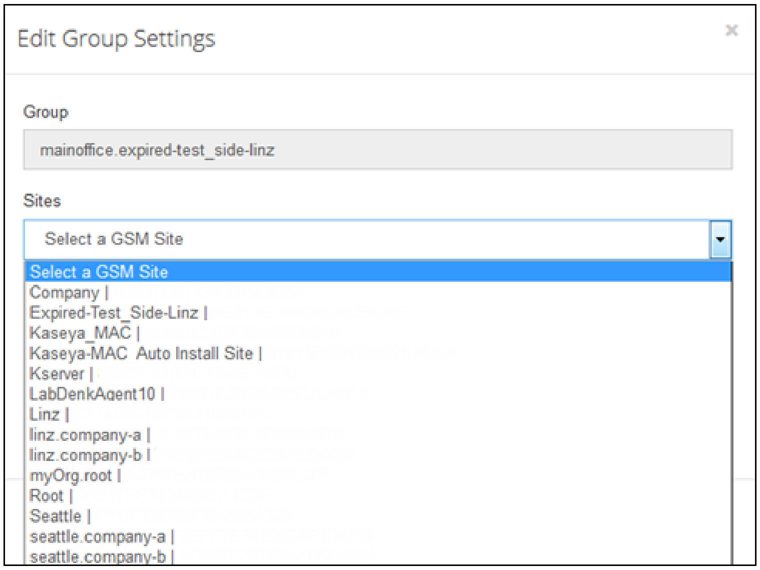
Organization: Organization Name

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

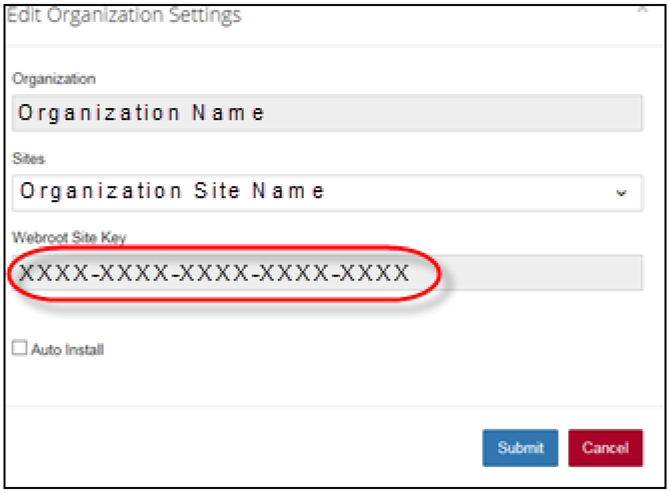
mainoffice.expired-test_side-linz

Sites

Select a GSM Site

Select a GSM Site
Company |
Expired-Test_Side-Linz |
Kaseya_MAC |
Kaseya-MAC Auto Install Site |
Kserver |
LabDenkAgent10 |
Linz |
linz.company-a |
linz.company-b |
myOrg.root |
Root |
Seattle |
seattle.company-a |
seattle.company-b |

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



Edit Organization Settings

Organization

Organization Name

Sites

Organization Site Name

Webroot Site Key

XXXX-XXXX-XXXX-XXXX-XXXX

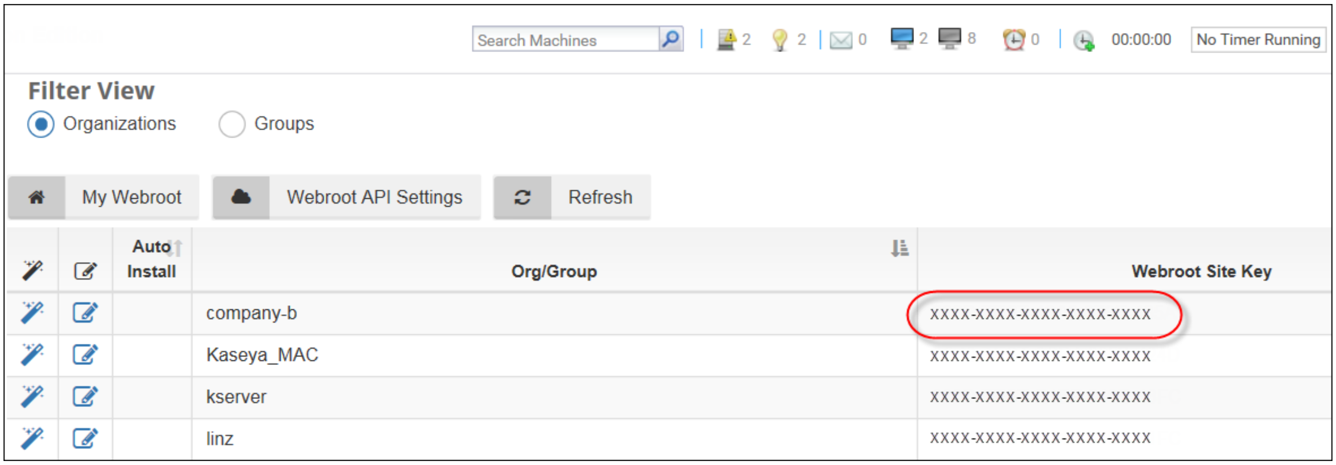
□ Auto Install

- If you select the Auto Install checkbox, then WSAB agents will be deployed automatically to all Kaseya endpoints within the defined organization or group.
- With Auto Install, we deploy WSAB 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 WSAB agents deployed.

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

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.



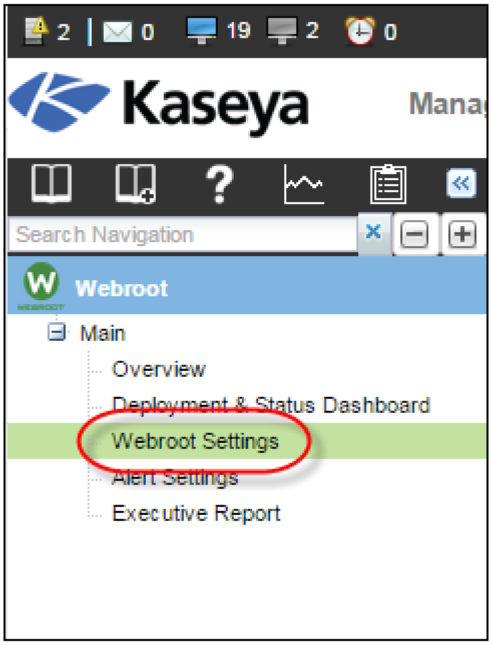
Filter View

● Organizations ○ Groups

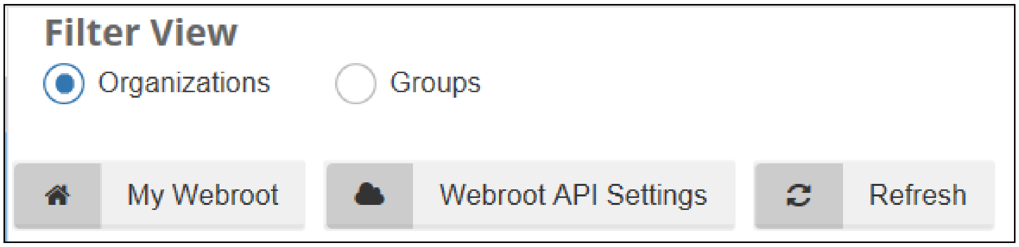
		Auto Install	Org/Group	Webroot Site Key
			company-b	XXXX-XXXX-XXXX-XXXX-XXXX
			Kaseya_MAC	XXXX-XXXX-XXXX-XXXX-XXXX
			kserver	XXXX-XXXX-XXXX-XXXX-XXXX
			linz	XXXX-XXXX-XXXX-XXXX-XXXX

To obtain a unique site key:

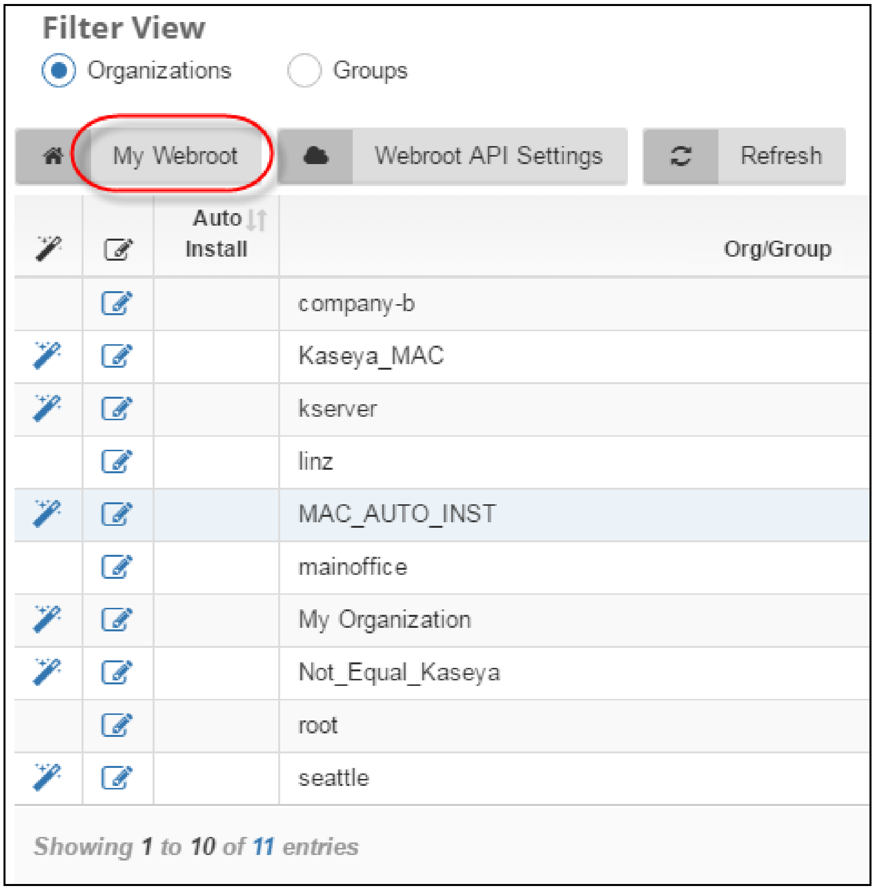
1. From the main menu, select **Webroot** > **Webroot Settings**.



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



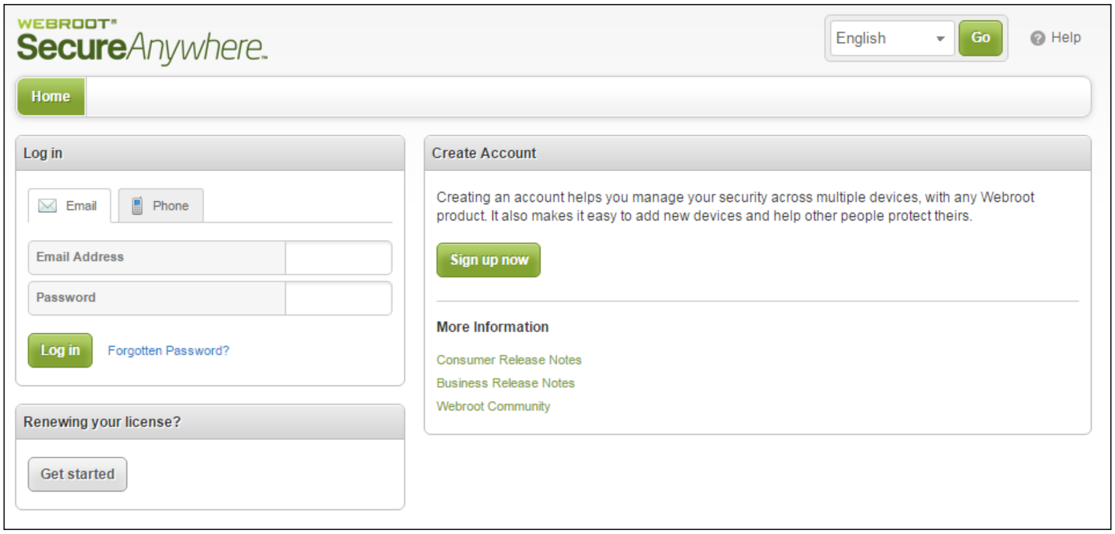
2. Click the **My Webroot tab**.



🪄	✎	Auto Install	Org/Group
	✎		company-b
🪄	✎		Kaseya_MAC
🪄	✎		kserver
	✎		linz
🪄	✎		MAC_AUTO_INST
	✎		mainoffice
🪄	✎		My Organization
🪄	✎		Not_Equal_Kaseya
	✎		root
🪄	✎		seattle

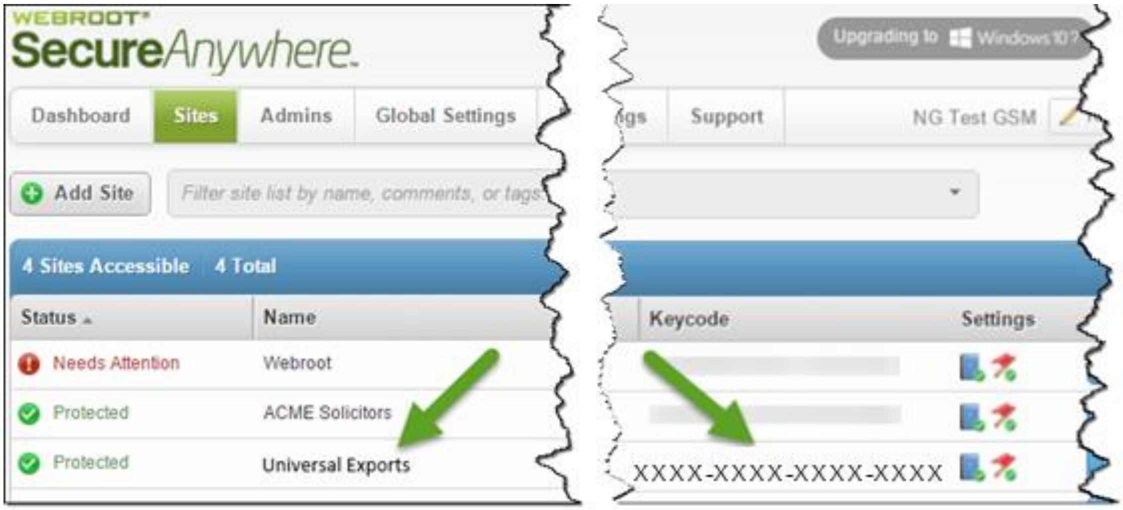
Showing ***1*** *to* ***10*** *of* ***11*** *entries*

The Webroot SecureAnywhere login page displays.



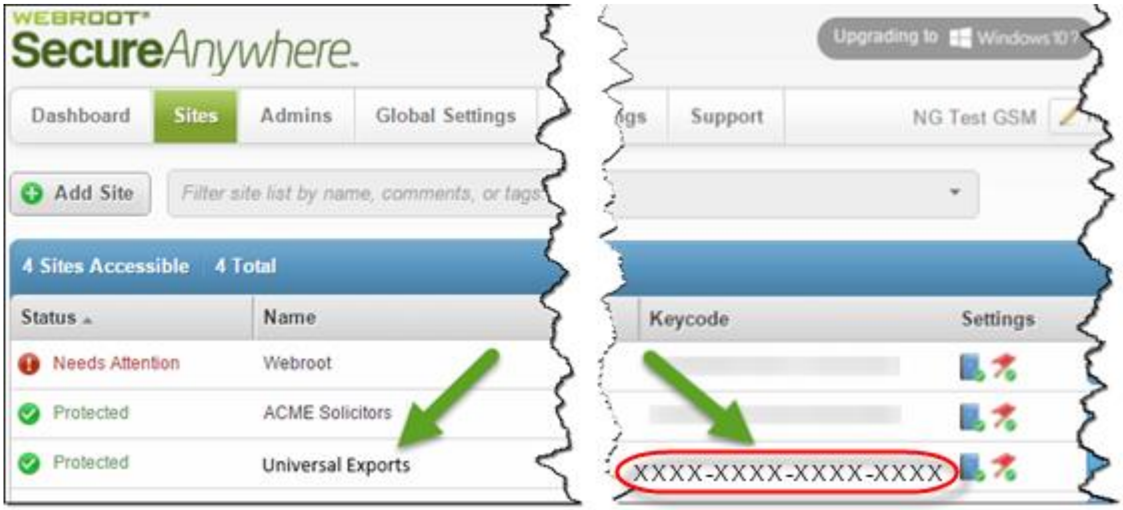
Creating an account helps you manage your security across multiple devices, with any Webroot product. It also makes it easy to add new devices and help other people protect theirs.

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.

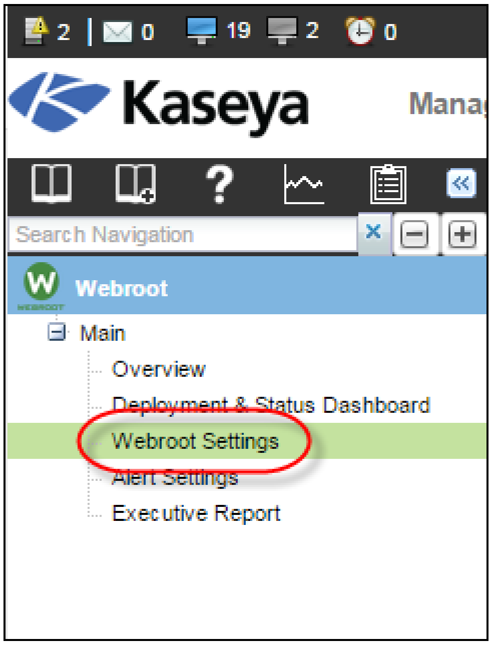


Status	Name	Keycode	Settings
Needs Attention	Webroot	[redacted]	
Protected	ACME Solicitors	[redacted]	
Protected	Universal Exports	XXXX-XXXX-XXXX-XXXX	

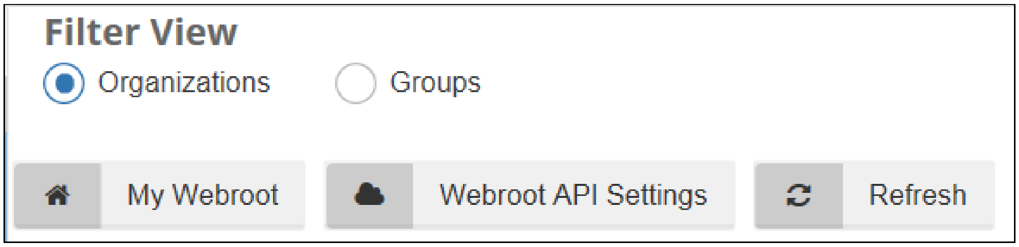
5. In the Sites panel, copy the keycode from the Keycode column for that GSM site.



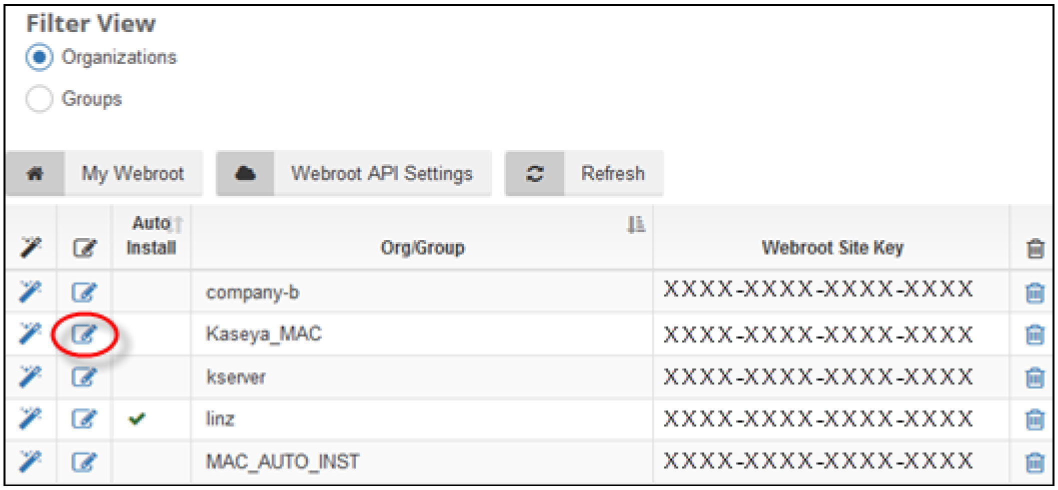
6. In Kaseya, from the main menu, select **Webroot** > **Webroot Settings**.



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.



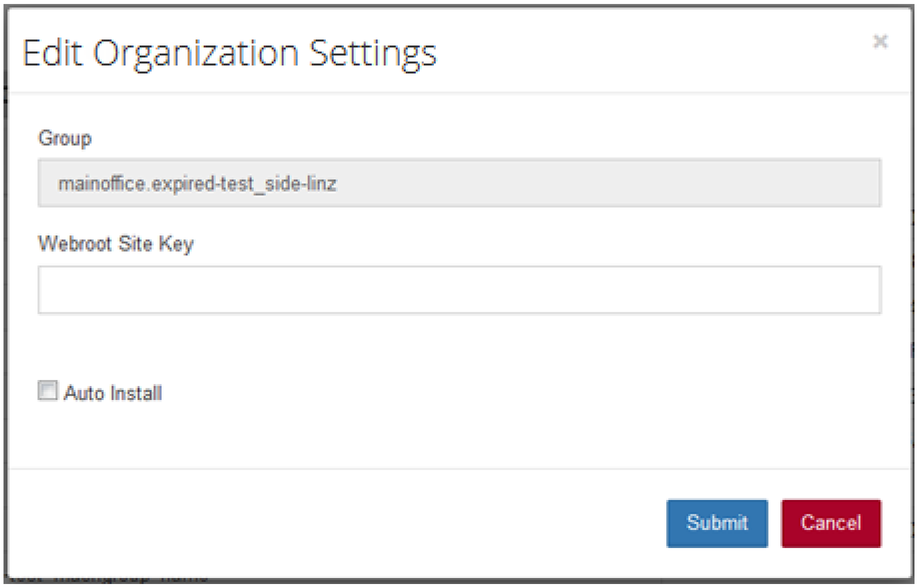
Filter View

● Organizations

○ Groups

		Auto Install	Org/Group	Webroot Site Key	
			company-b	XXXX-XXXX-XXXX-XXXX	
			Kaseya_MAC	XXXX-XXXX-XXXX-XXXX	
			kserver	XXXX-XXXX-XXXX-XXXX	
		✓	linz	XXXX-XXXX-XXXX-XXXX	
			MAC_AUTO_INST	XXXX-XXXX-XXXX-XXXX	

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



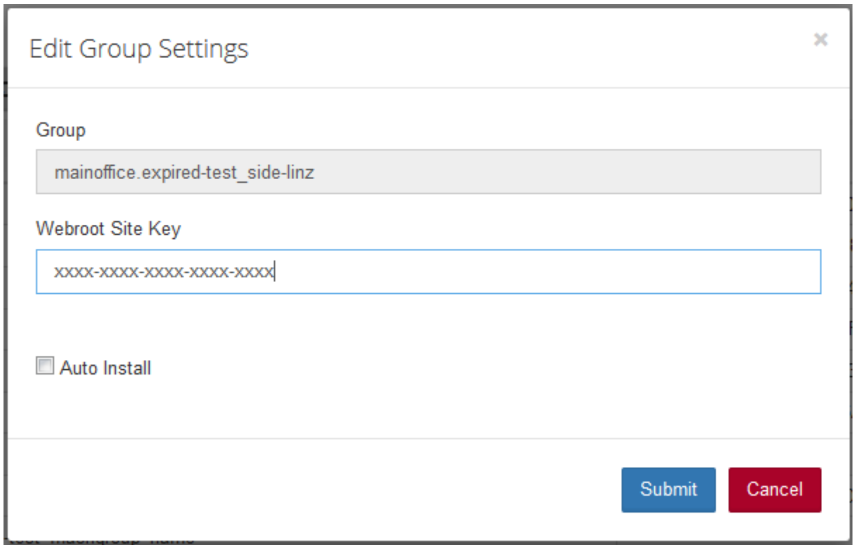
Edit Organization Settings

Group: mainoffice.expired-test_side-linz

Webroot Site Key:

□ Auto Install

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

□ Auto Install

- If you select the Auto Install checkbox, then WSAB agents will be deployed automatically to all Kaseya endpoints within the defined organization or group.
- With Auto Install we deploy WSAB 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 WSAB 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.

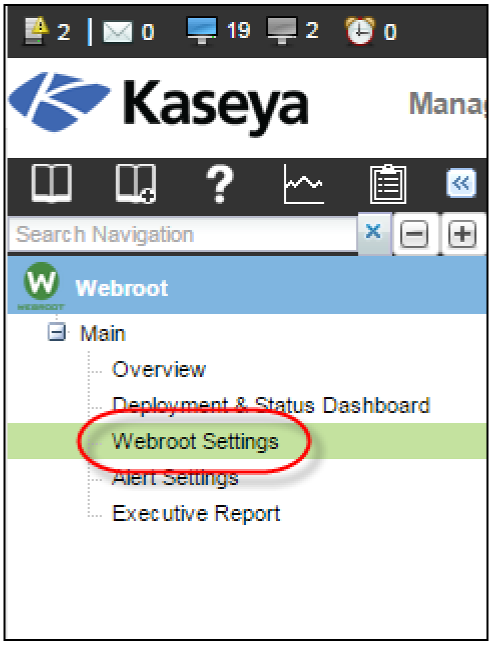
Adopting Existing WSAB Agents

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

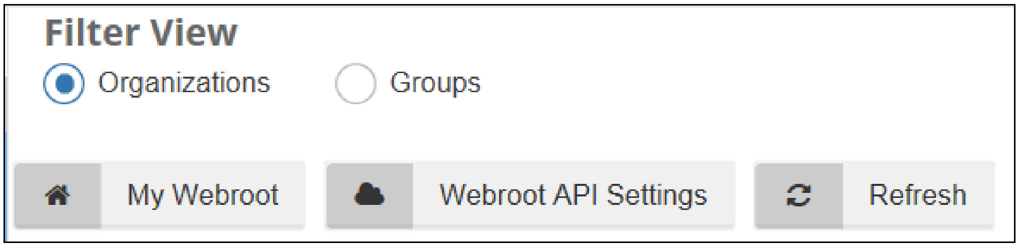
Note: Enabling Auto Install for those Organizations will do that automatically for you.

To adopt existing agents:

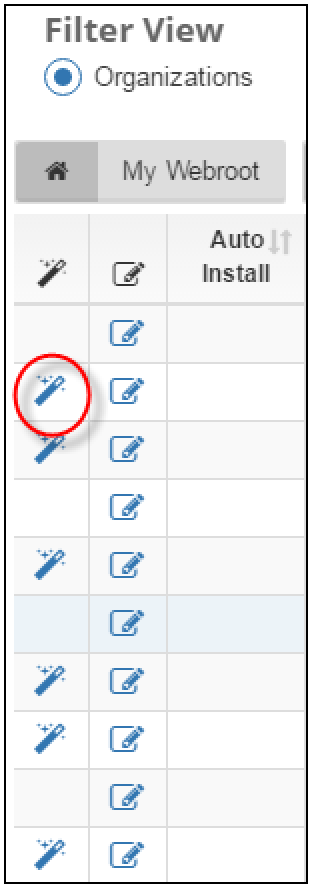
1. From the main menu, select **Webroot** > **Webroot Settings**.



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 on the **Wizard** icon.



WSAB 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.

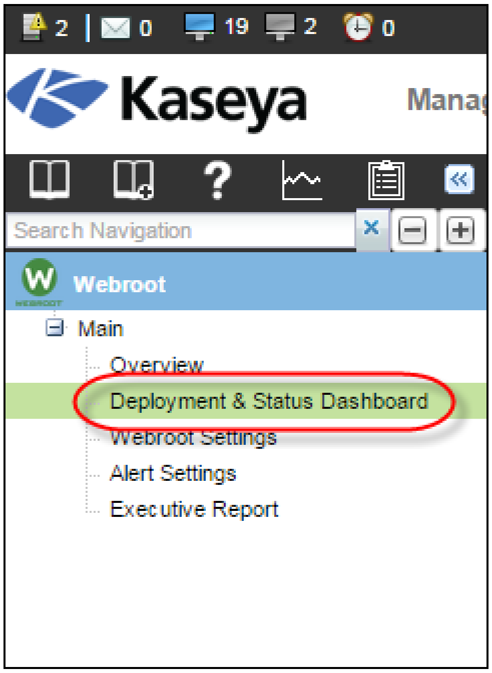
Note: Adopted WSAB endpoints that were initially installed manually (using WSAB installer executable) can only be uninstalled from within the Webroot console.

Deploying WSAB Agents Through the Kaseya Module

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

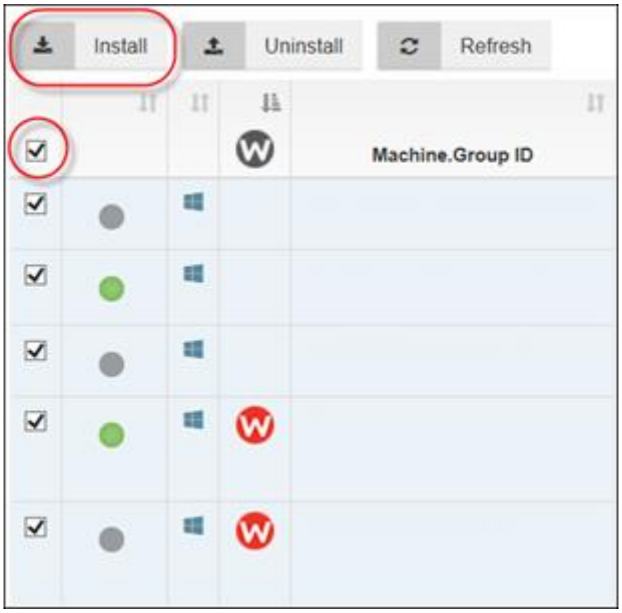
To deploy WSAB agents:

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

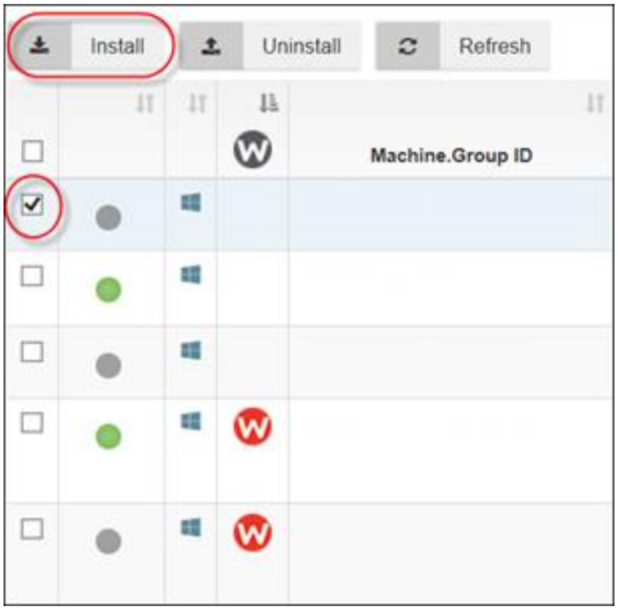


2. Do one of the following to deploy WSAB agents to just one endpoint or a range of endpoints.

   - To install WSAB agents on all endpoints in the filtered view, select the checkbox at the top of the column, and click the **Install** button. All endpoints are selected and installed.

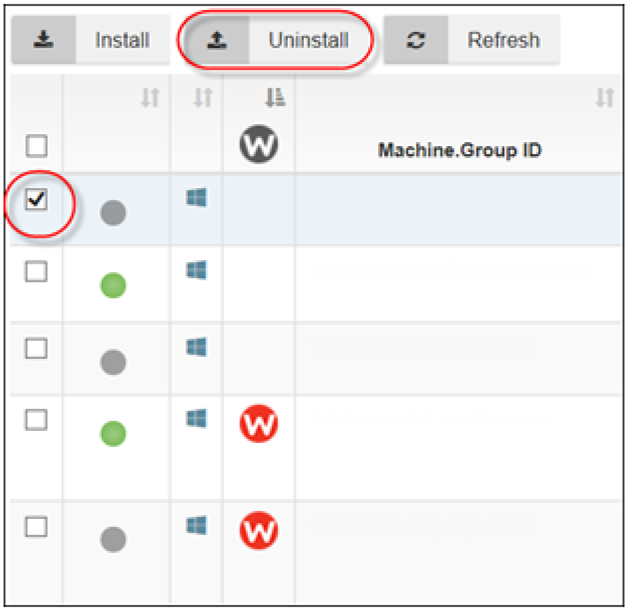


- To install WSAB agent on an individual Kaseya endpoint, select the checkbox of for the target endpoint , and click the **Install** button.



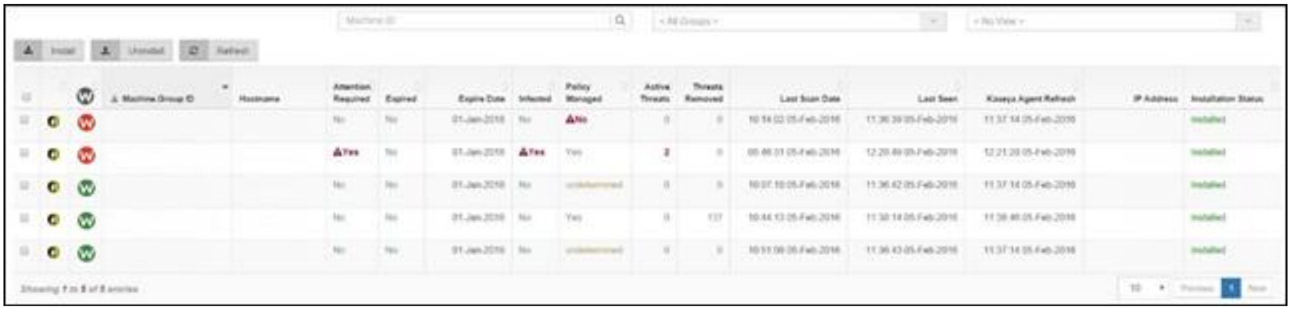
Progress during the installation process is indicated by an Installing status. Once the installation is complete the Installation status will change to Installed.

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



Viewing Installation and Dashboard Level WSAB Agent Status

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



			Machine.Group ID	Hostname	Attention Required	Expired	Expire Date	Infected	Policy Managed	Active Threats	Threats Removed	Last Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status
□	●	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	05:46:01 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	11:38:40 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

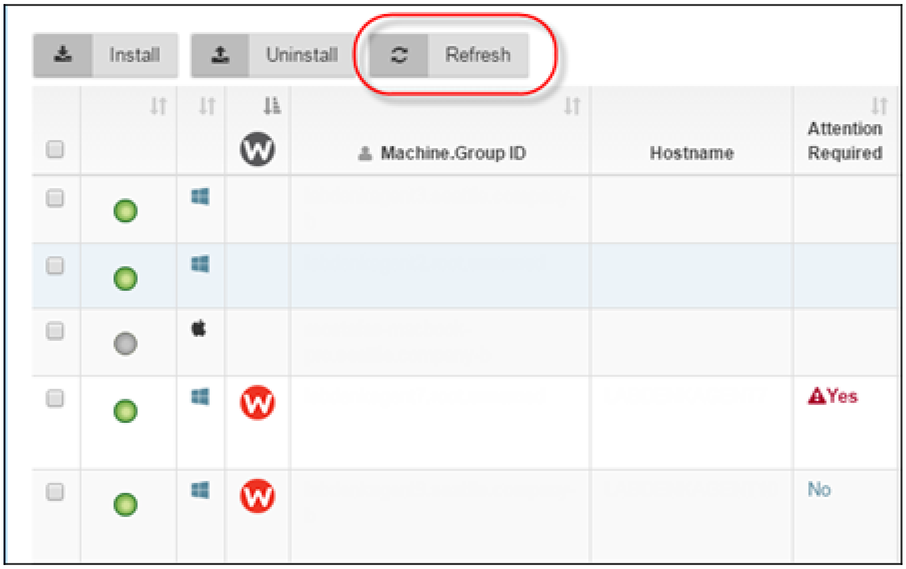
10 ▾ Previous 1 Next

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

Icon	Description
⊞	Windows OS
	Mac OS

The Refresh button pulls the latest agent information from the database.

- 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.

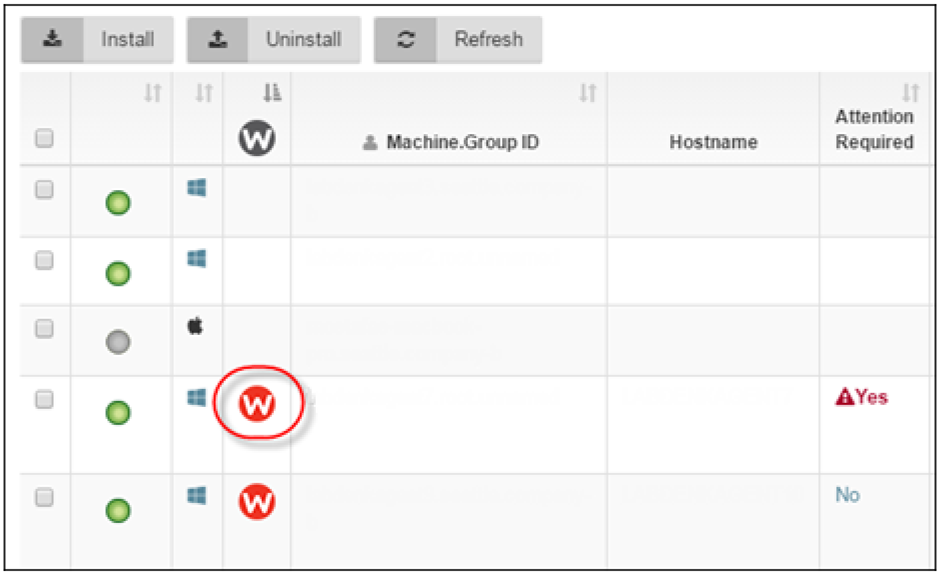


□			W	Machine.Group ID	Hostname	Attention Required
□	●	⊞				
□	●	⊞				
□	●					
□	●	⊞	W			▲Yes
□	●	⊞	W			No

Indicators in the Deployment & Status Dashboard

1. Red W

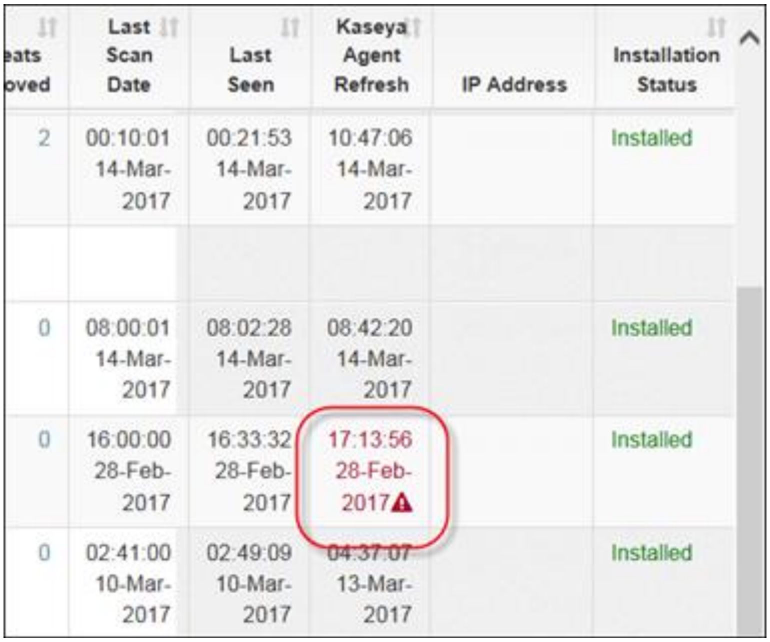
   If the endpoint is in an undesirable state, for example, if the endpoint is in an Attention Required state, the W icon is red. In addition to the Attention Required state, the W icon will be red if the agent is failing to retrieve status and threat information.



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

2. 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.



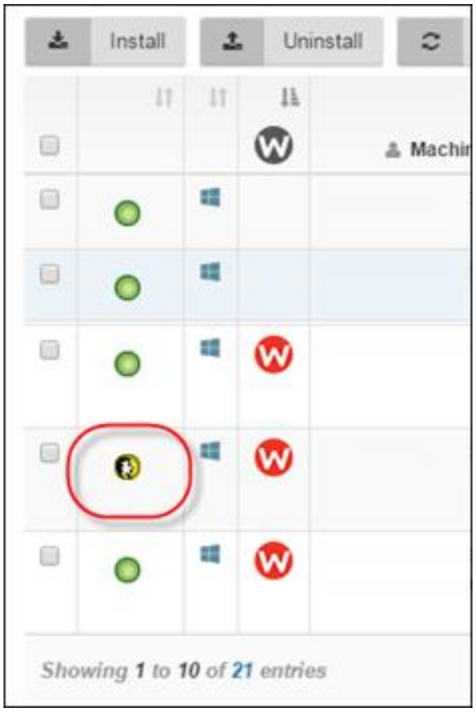
eats oved	Last Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status
2	00:10:01 14-Mar-2017	00:21:53 14-Mar-2017	10:47:06 14-Mar-2017		Installed
0	08:00:01 14-Mar-2017	08:02:28 14-Mar-2017	08:42:20 14-Mar-2017		Installed
0	16:00:00 28-Feb-2017	16:33:32 28-Feb-2017	17:13:56 28-Feb-2017▲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

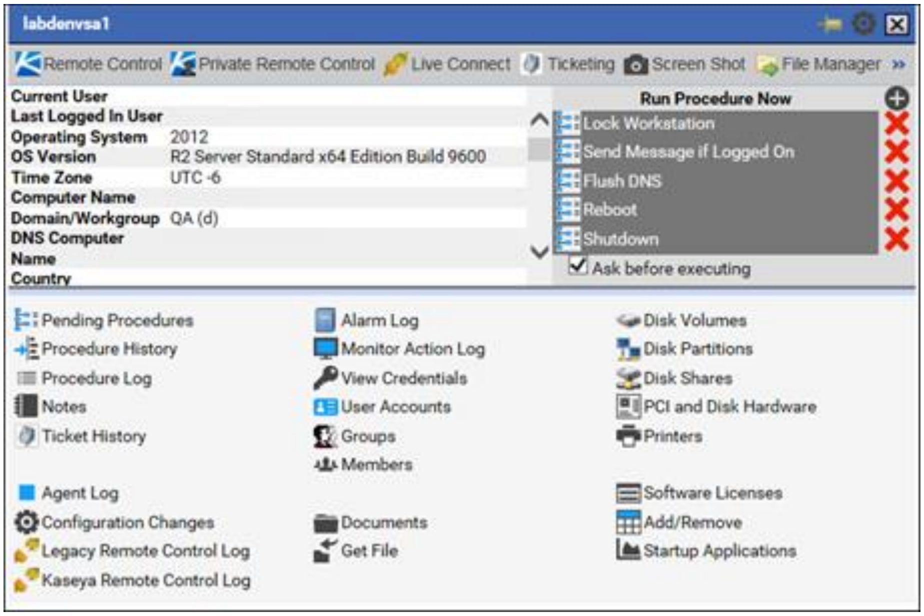
The administrator can, as needed, validate the success of the Agent Procedures that execute Webroot activities and collect results.

To validate success:

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

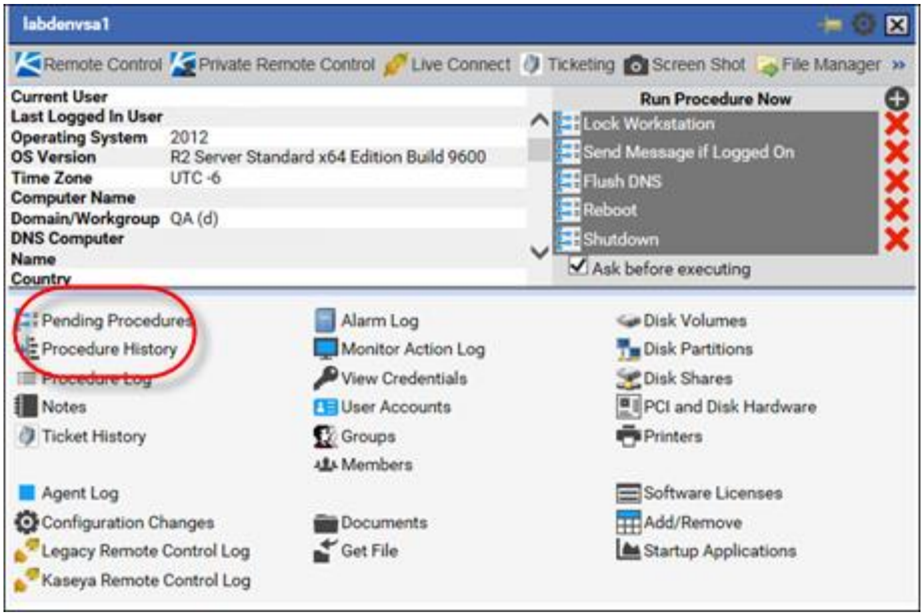


The Live Connect information window displays.



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

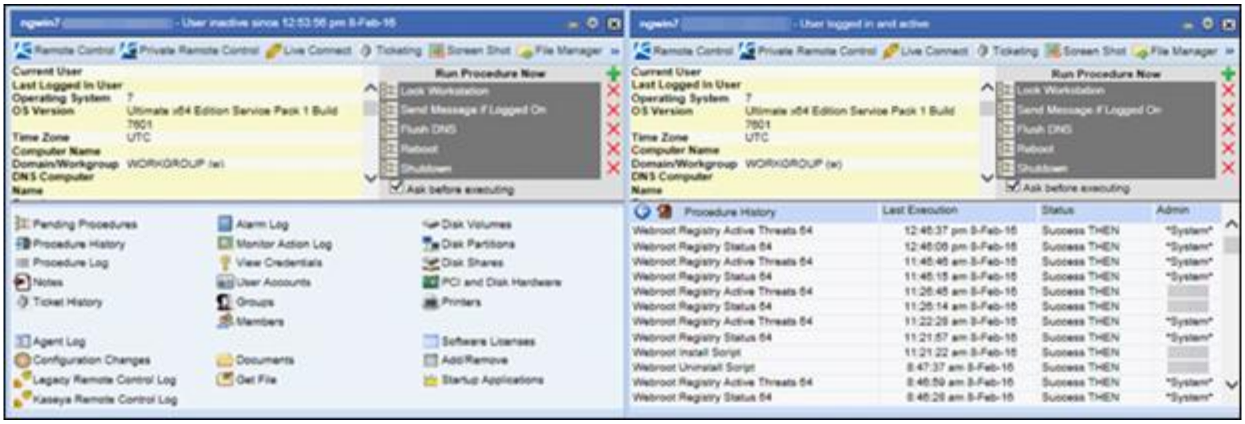


labdenvsa1

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

Review information, as needed.



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

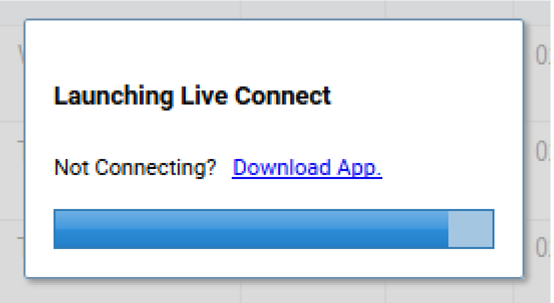
ngwin7 - User logged in and active

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	

☑ Ask before executing

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	11:26:45 am 8-Feb-16	Success THEN	
Webroot Registry Status 64	11:26:14 am 8-Feb-16	Success THEN	
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	
Webroot Uninstall Script	8:47:37 am 8-Feb-16	Success THEN	
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

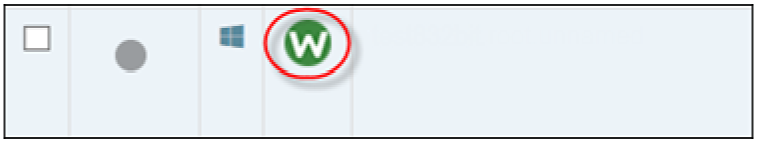
Not Connecting? Download App.

Detailed WSAB Agent Status and Agent Commands

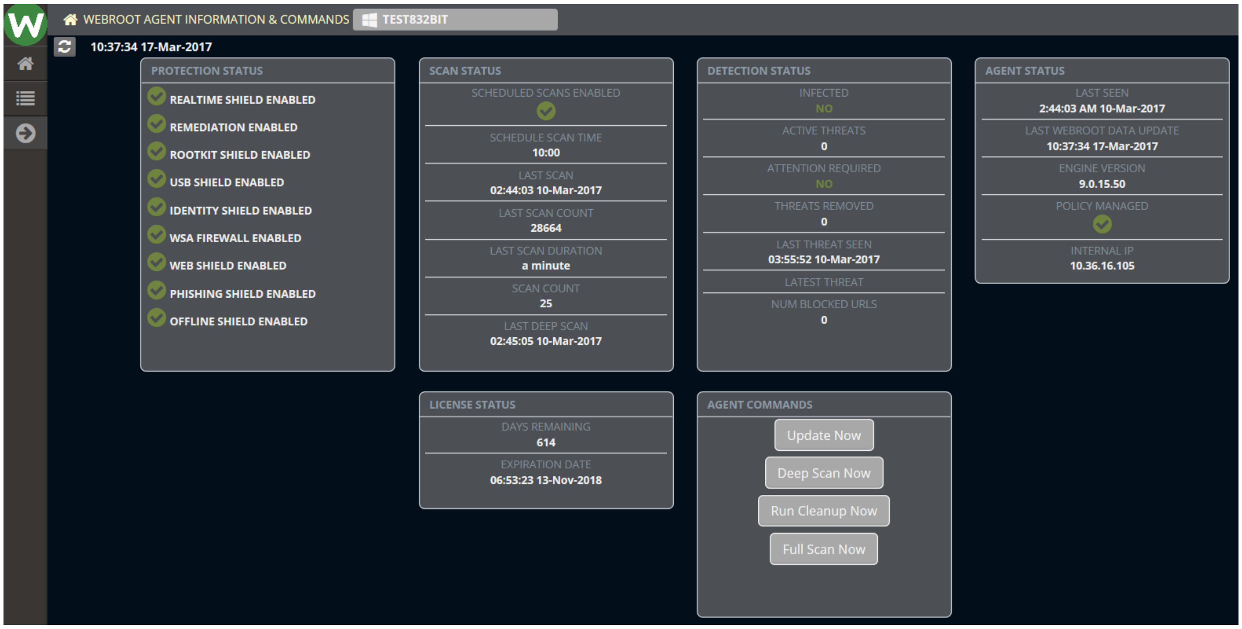
If you need detailed analysis of a specific WSAB agent or if you need to run WSAB Agent Commands, use this procedure.

To generate analysis or commands:

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



The system displays detailed Webroot Agent Information and Commands pane.



WEBROOT AGENT INFORMATION & COMMANDS TEST832BIT

10:37:34 17-Mar-2017

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 02:44:03 10-Mar-2017
LAST SCAN COUNT 28664
LAST SCAN DURATION a minute
SCAN COUNT 25
LAST DEEP SCAN 02:45:05 10-Mar-2017

DETECTION STATUS
INFECTED NO
ACTIVE THREATS 0
ATTENTION REQUIRED NO
THREATS REMOVED 0
LAST THREAT SEEN 03:55:52 10-Mar-2017
LATEST THREAT
NUM BLOCKED URLS 0

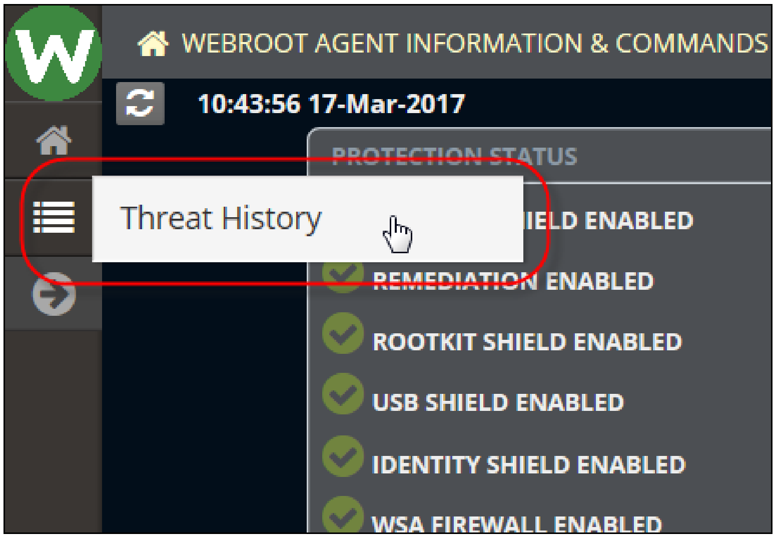
AGENT STATUS
LAST SEEN 2:44:03 AM 10-Mar-2017
LAST WEBROOT DATA UPDATE 10:37:34 17-Mar-2017
ENGINE VERSION 9.0.15.50
POLICY MANAGED ✓
INTERNAL IP 10.36.16.105

LICENSE STATUS
DAYS REMAINING 614
EXPIRATION DATE 06:53:23 13-Nov-2018

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 WSAB agents are uninstalled and reinstalled, the Agent Status statistics are reset.

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



WEBROOT AGENT INFORMATION & COMMANDS

10:43:56 17-Mar-2017

PROTECTION STATUS

…IELD ENABLED

REMEDIATION ENABLED

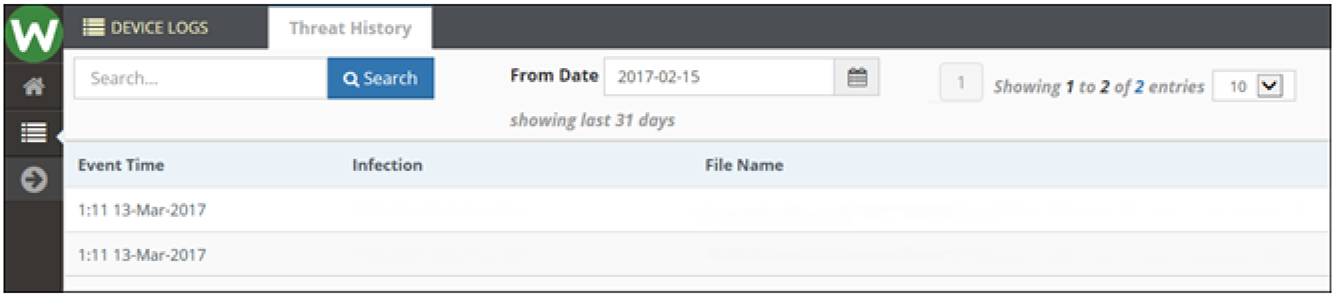
ROOTKIT SHIELD ENABLED

USB SHIELD ENABLED

IDENTITY SHIELD ENABLED

WSA FIREWALL ENABLED

Threat history information displays.



From Date 2017-02-15

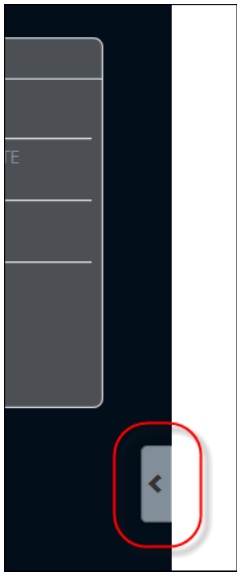
showing last 31 days

*Showing **1** to **2** of **2** entries*

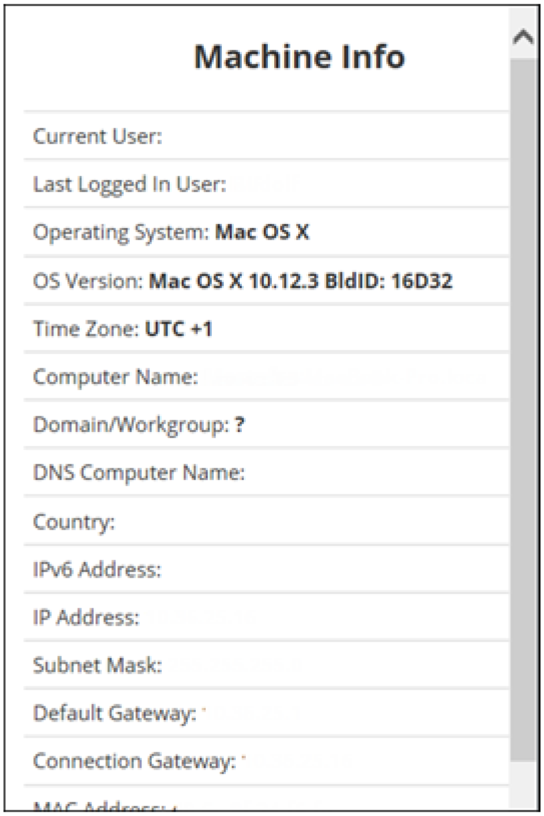
Event Time	Infection	File Name
1:11 13-Mar-2017	[redacted]	[redacted]
1:11 13-Mar-2017	[redacted]	[redacted]

Note: WSAB 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:

IPv6 Address:

IP Address:

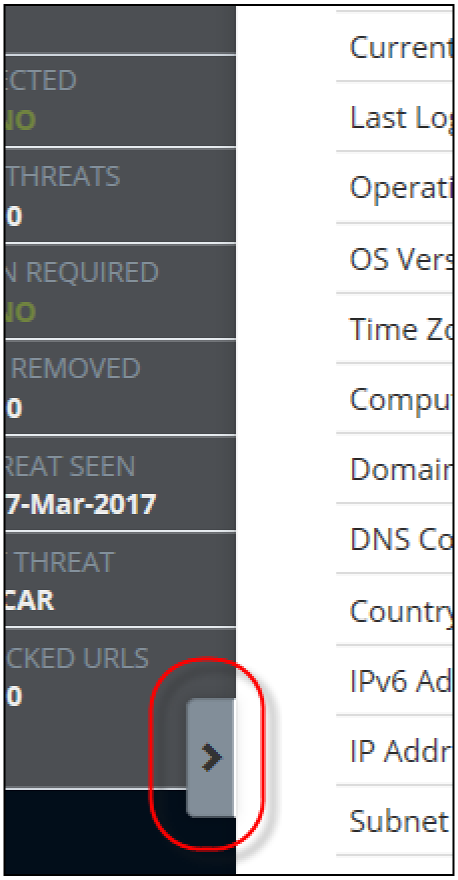
Subnet Mask:

Default Gateway:

Connection Gateway:

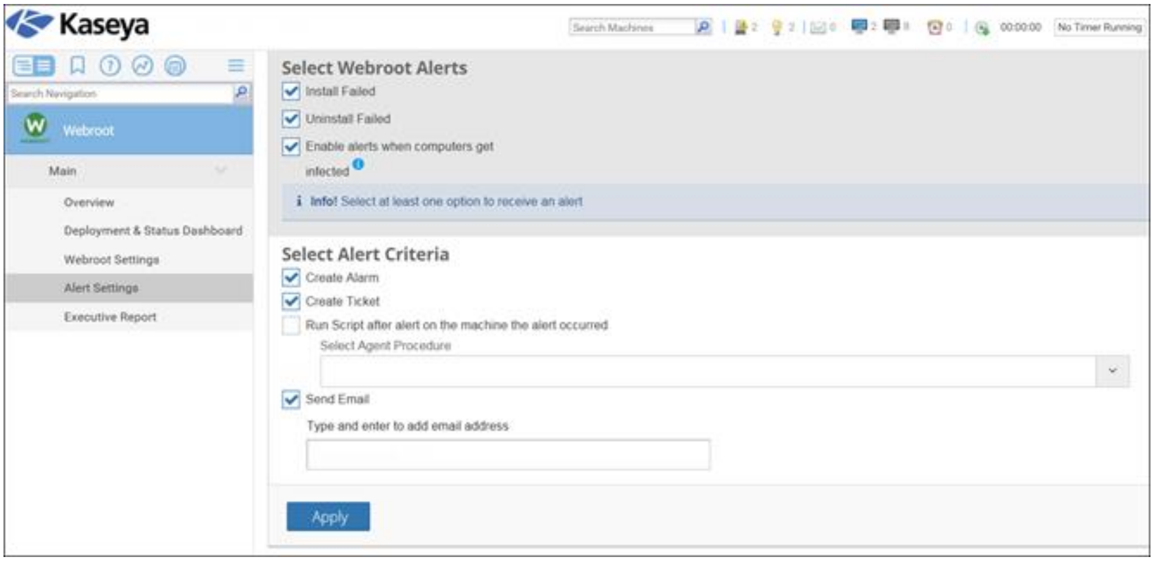
MAC Address:

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



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.



Select Webroot Alerts

☑ Install Failed

☑ Uninstall Failed

☑ Enable alerts when computers get infected

ℹ **Info!** Select at least one option to receive an alert

Select Alert Criteria

☑ Create Alarm

☑ Create Ticket

□ Run Script after alert on the machine the alert occurred

Select Agent Procedure

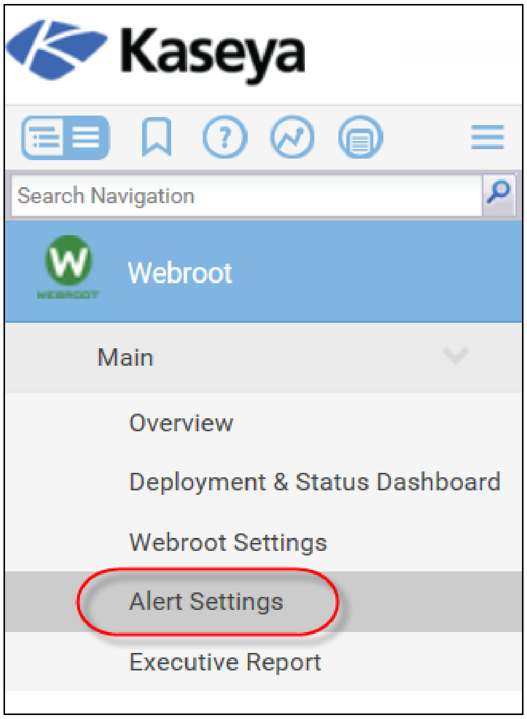
☑ Send Email

Type and enter to add email address

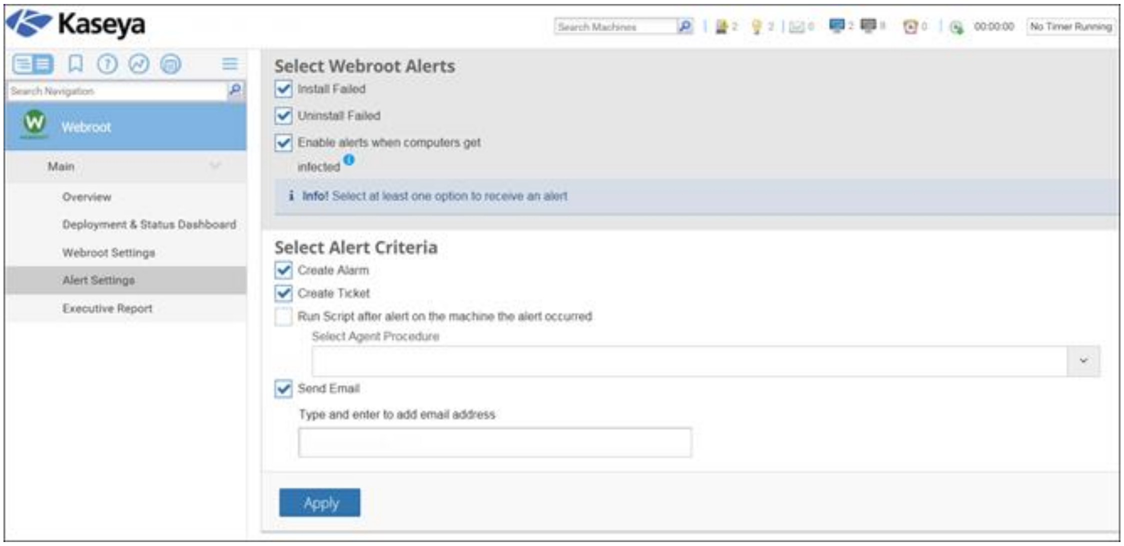
Apply

To set an alert:

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



The Webroot Alerts pane displays.



Select Webroot Alerts

☑ Install Failed

☑ Uninstall Failed

☑ Enable alerts when computers get infected

Info! Select at least one option to receive an alert

Select Alert Criteria

☑ Create Alarm

☑ Create Ticket

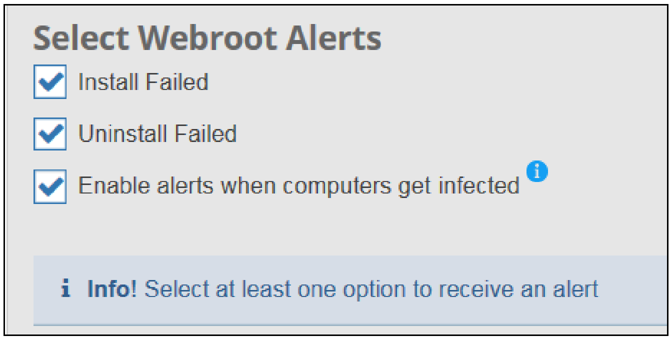
☐ Run Script after alert on the machine the alert occurred

Select Agent Procedure

☑ Send Email

Type and enter to add email address

2. Select one or more of the **Webroot Alerts** checkboxes, such as *Enable alerts when computers get infected*.



Select Webroot Alerts

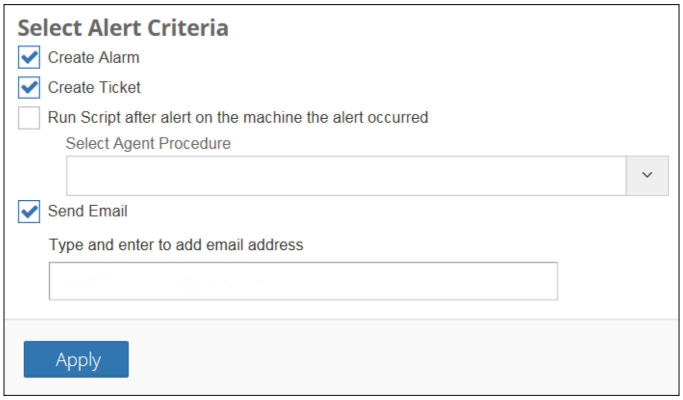
☑ Install Failed

☑ Uninstall Failed

☑ Enable alerts when computers get infected

Info! Select at least one option to receive an alert

3. Select the relevant **Alert Criteria** checkbox, such as *Create Ticket*.



Select Alert Criteria

☑ Create Alarm

☑ Create Ticket

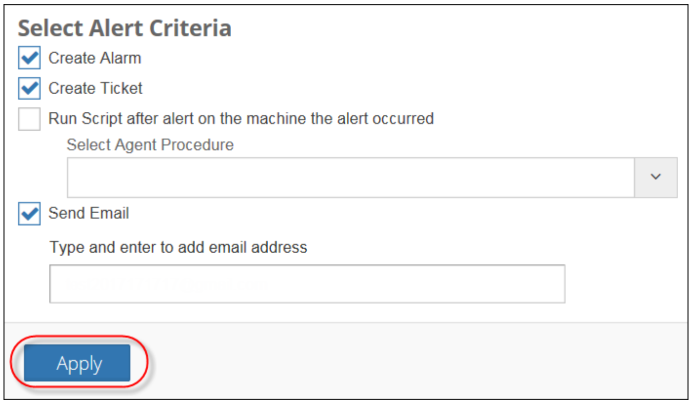
☐ Run Script after alert on the machine the alert occurred

Select Agent Procedure

☑ Send Email

Type and enter to add email address

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



Select Alert Criteria

☑ Create Alarm

☑ Create Ticket

□ Run Script after alert on the machine the alert occurred

Select Agent Procedure

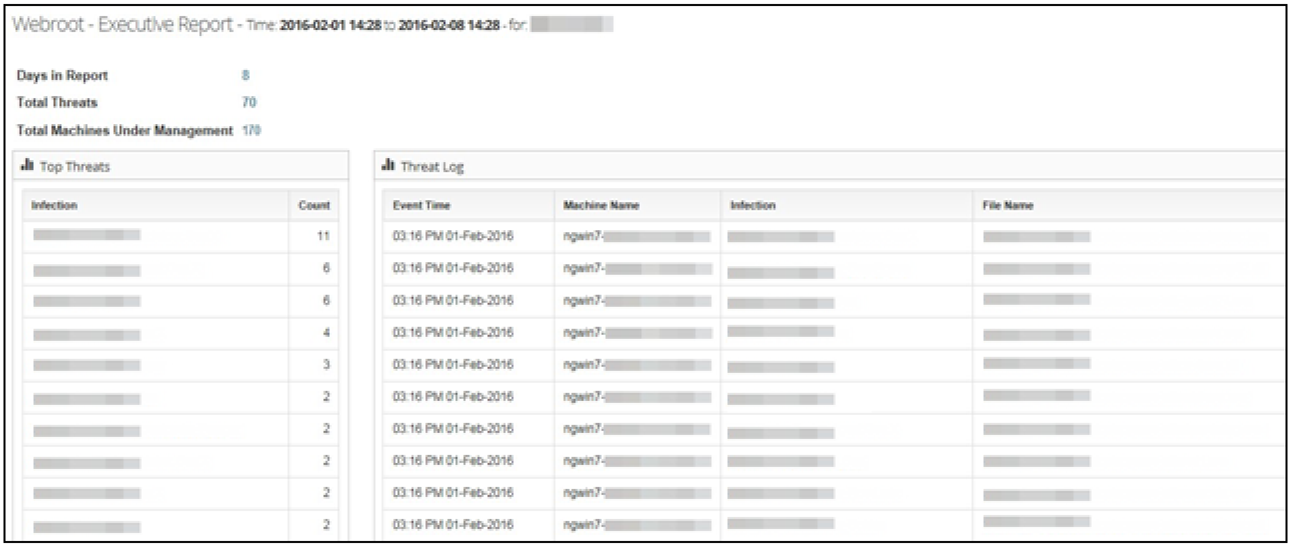
☑ Send Email

Type and enter to add email address

Note: In order to receive Alerts via e-mail you must enter a valid e-mail address.

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

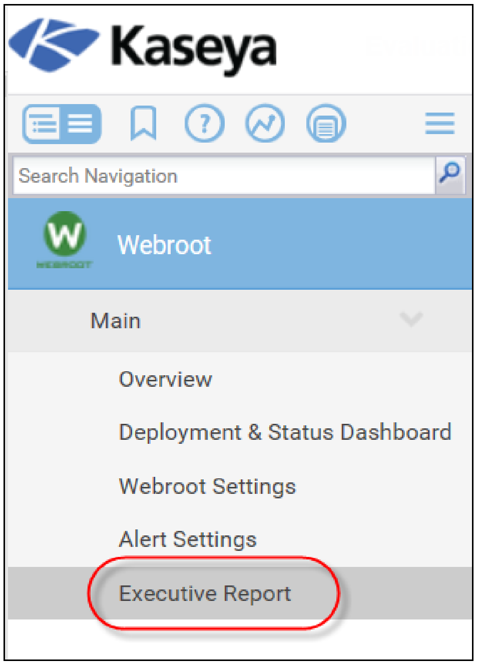
Infection	Count
[redacted]	11
[redacted]	6
[redacted]	6
[redacted]	4
[redacted]	3
[redacted]	2
[redacted]	2
[redacted]	2
[redacted]	2
[redacted]	2

Threat Log

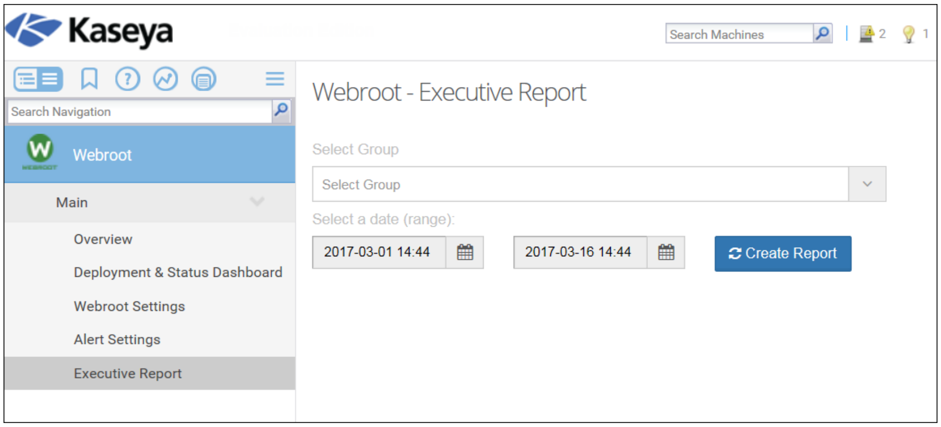
Event Time	Machine Name	Infection	File Name
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016	ngwin7-[redacted]	[redacted]	[redacted]
03:16 PM 01-Feb-2016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



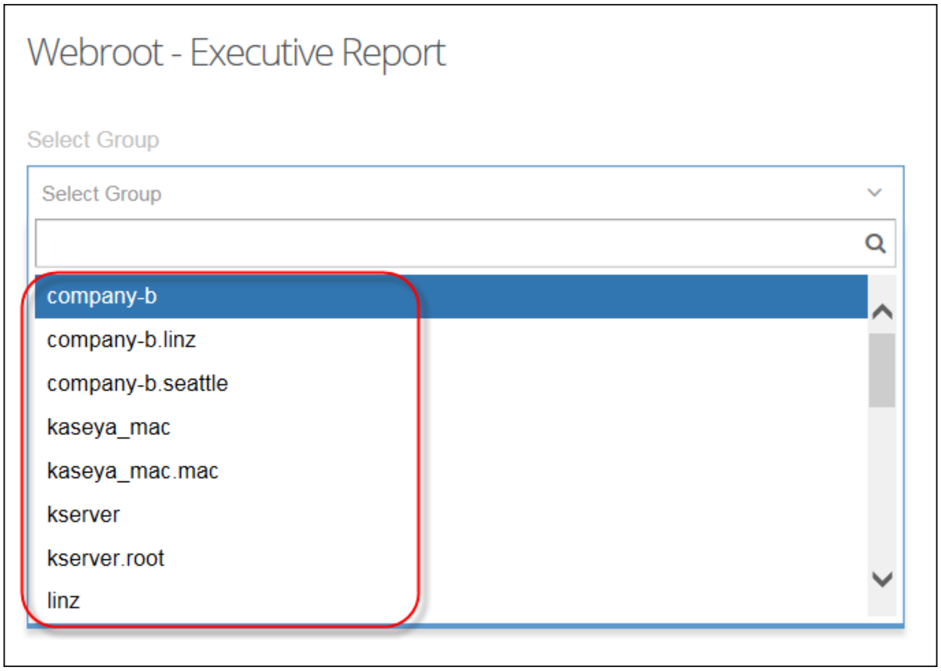
The Webroot – Executive Report pane displays.



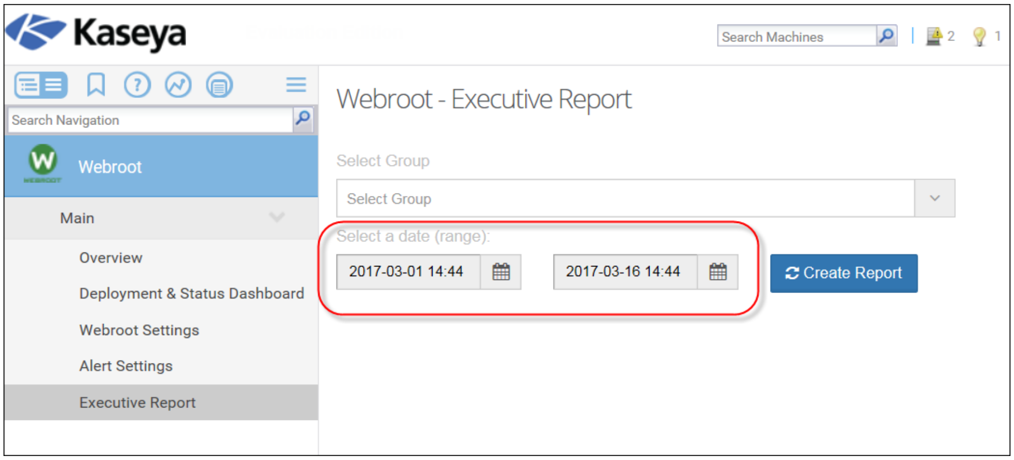
2017-03-01 14:44

2017-03-16 14:44

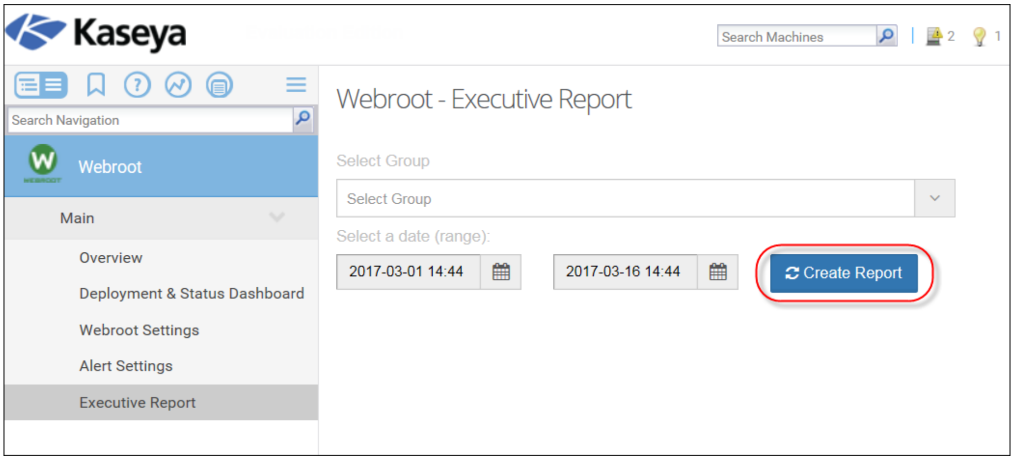
2. From the Select Group drop-down menu, select the **Kaseya** group for which you want to run the report.



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



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



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

Automatically Installing Webroot SecureAnywhere Agents Using Kaseya Agent Procedure in Policies

If you would like to have more control over the installation process than is possible with auto install, we recommend utilizing the Kaseya Agent Procedure in Policies, which you can set up using the following instructions.

This section describes how to import the Kaseya Agent Procedure package provided in the Webroot Kaseya v2.0 plugin and how to set up Kaseya Policies and Views to install Webroot SecureAnywhere only to selected machines.

Note: This will not work for endpoints unless they have set a site key for the Organization or Group within the Webroot Plugin.

Part One - Locating the WebrootAgentProcs.xml file

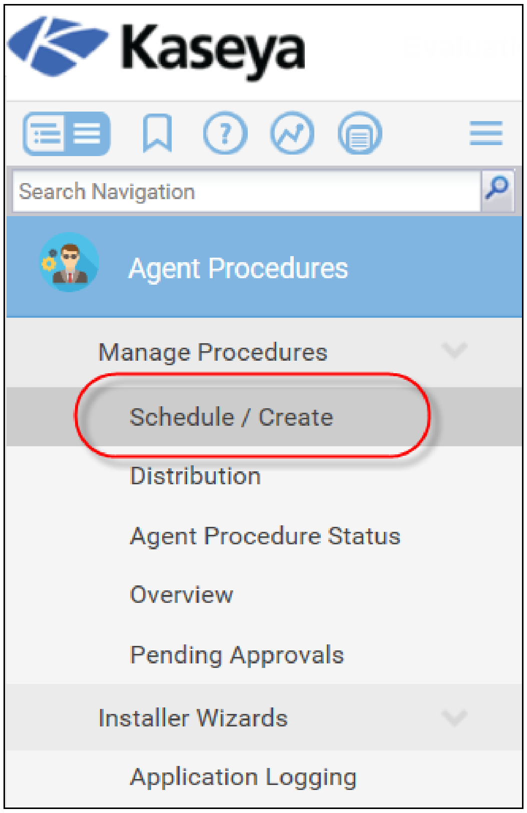
After successful installation of the Webroot Kaseya VSA Integration version 2.0 the Webroot Agent Procedure pack will be stored on your VSA Kaseya server.

Note: Editing these agent procedures will not be supported due to the use of core system agent procedures and workflow processes that follow the installation of the Webroot WSA client software.

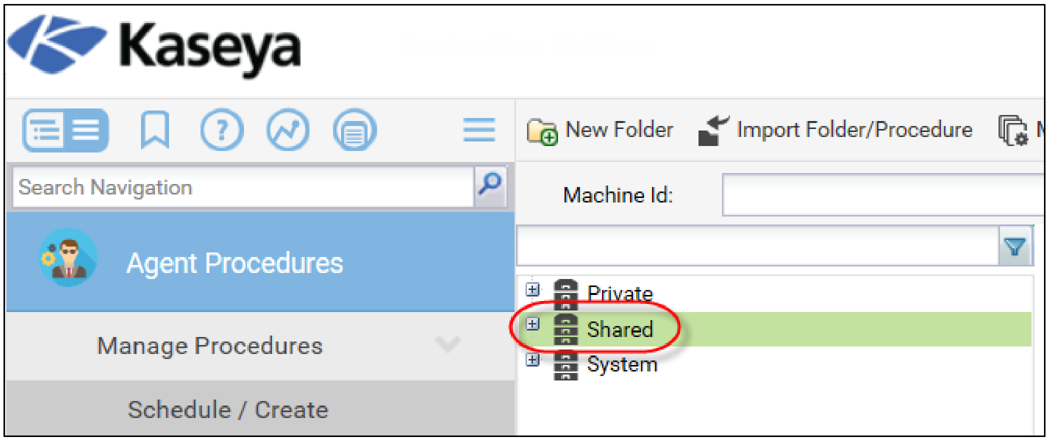
Within <install path>\kaseya\webpages\giwebrootaddon, there will be a WebrootAgentProcs.xml file. Use this XML file to import the agent procedures into your VSA environment so administrators can use them within policy or to schedule on specific machines.

Part Two - Importing Agent Procedures

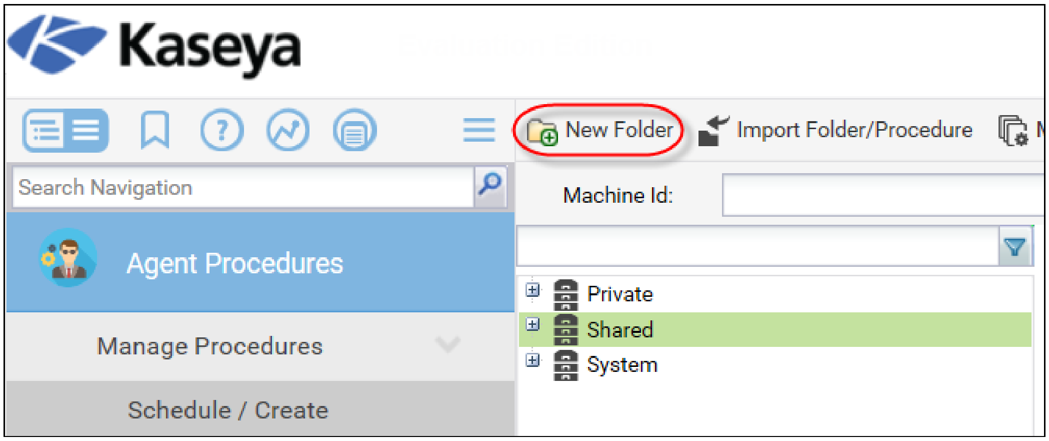
1. Copy the WebrootAgentProcs.xml from the VSA, see above for path, to share directory or local directory so the administrator can access them on the import.
2. Log in to your VSA.
3. From the main menu, select **Agent Procedure** > **Schedule / Create**.



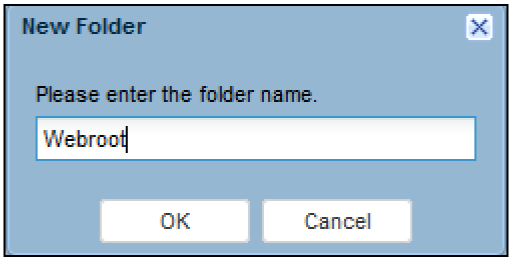
4. Select the **Shared** tree node.



5. Click the **New Folder** button.



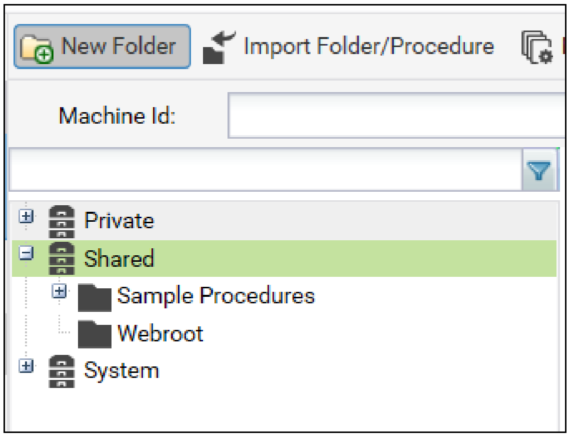
6. In the Please enter the folder name field, enter a name for the new folder, for example, *Webroot*.


New Folder

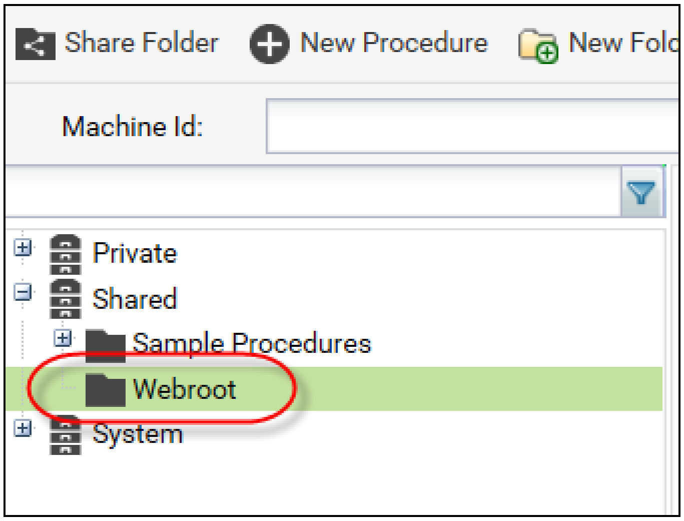
Please enter the folder name.

Webroot

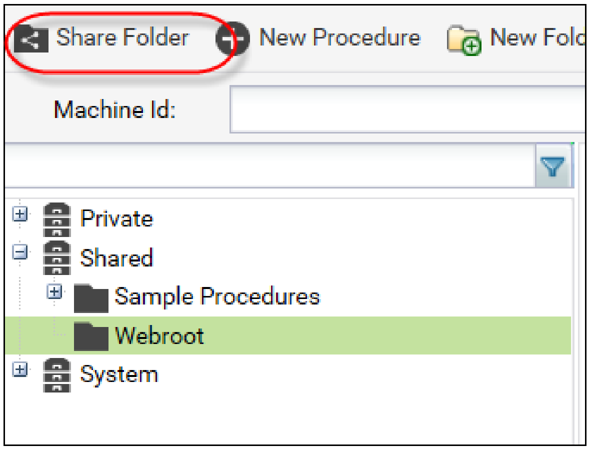
The system creates a new folder with that name.



7. Select the newly created folder. Note that the menu bar options change.

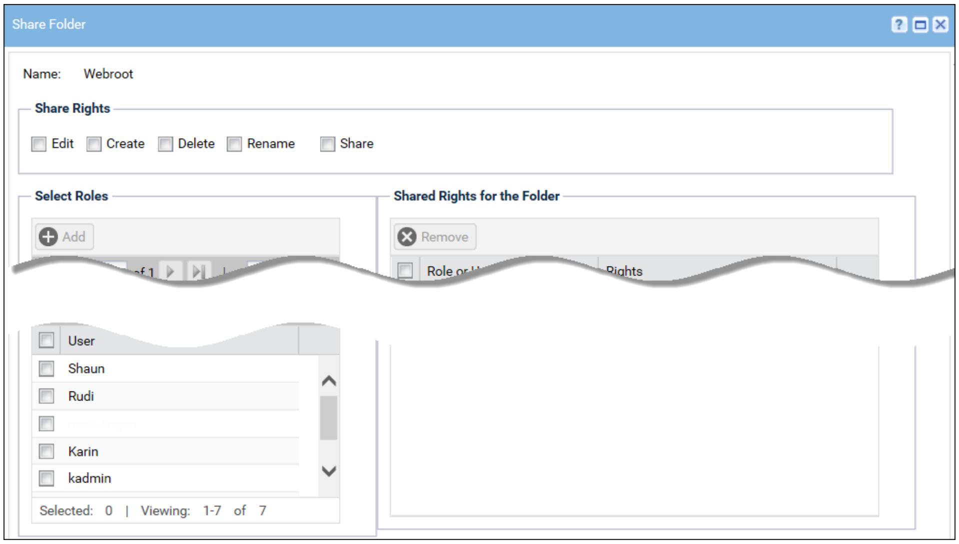


8. Click the **Share Folder** button in the toolbar to give shared access to the new folder.



Note: We recommend that you grant all Master Admins rights to this folder:

The Share Folder window displays.



Share Folder

Name: Webroot

Share Rights

□ Edit □ Create □ Delete □ Rename □ Share

Select Roles

Add

□	User
□	Shaun
□	Rudi
□	
□	Karin
□	kadmin

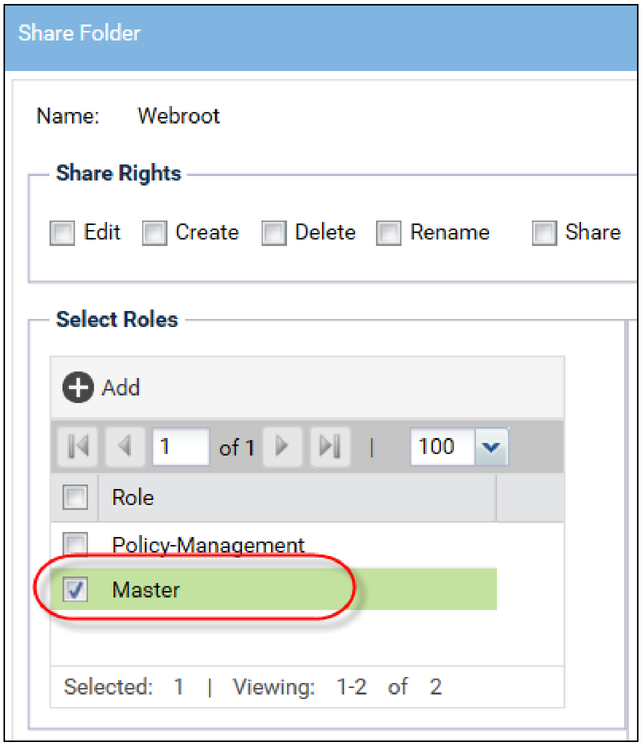
Selected: 0 | Viewing: 1-7 of 7

Shared Rights for the Folder

Remove

□	Role or U	Rights

9. In the Select Roles area, select the **Master** checkbox.



Share Folder

Name: Webroot

Share Rights

□ Edit □ Create □ Delete □ Rename □ Share

Select Roles

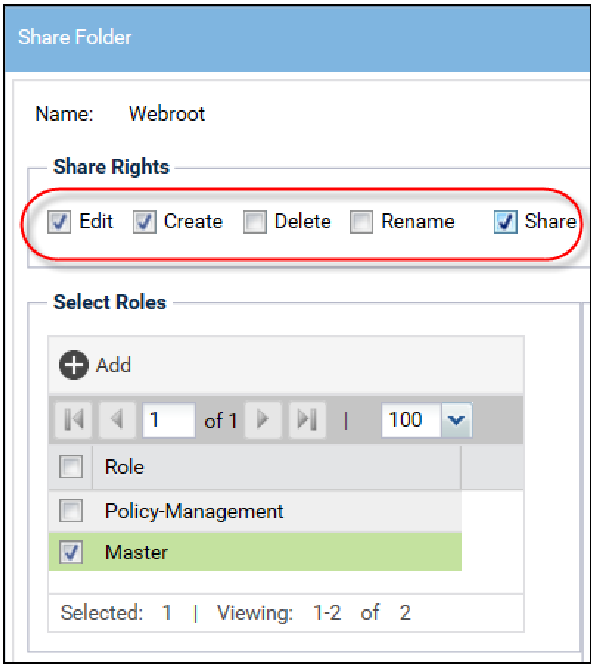
Add

1 of 1 | 100

□	Role
□	Policy-Management
☑	Master

Selected: 1 | Viewing: 1-2 of 2

10. In the Share Rights area, select the following checkboxes:
    - **Edit**
    - **Create**
    - **Share**



Share Folder

Name: Webroot

Share Rights

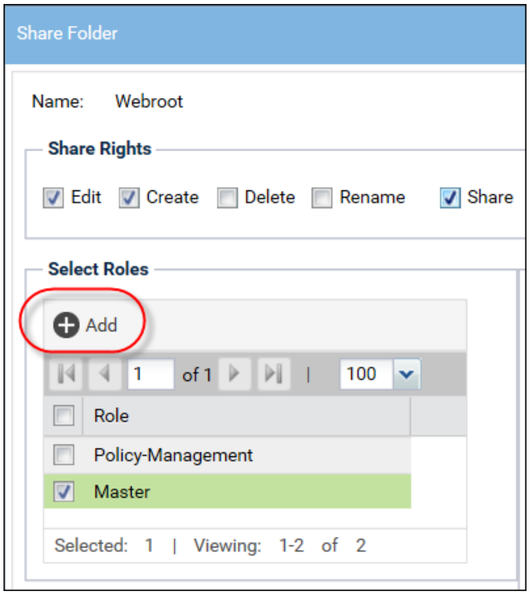
☑ Edit ☑ Create ☐ Delete ☐ Rename ☑ Share

Select Roles

☐	Role
☐	Policy-Management
☑	Master

Selected: 1 | Viewing: 1-2 of 2

11. When you're ready, click the **Add** button.



Share Folder

Name: Webroot

Share Rights

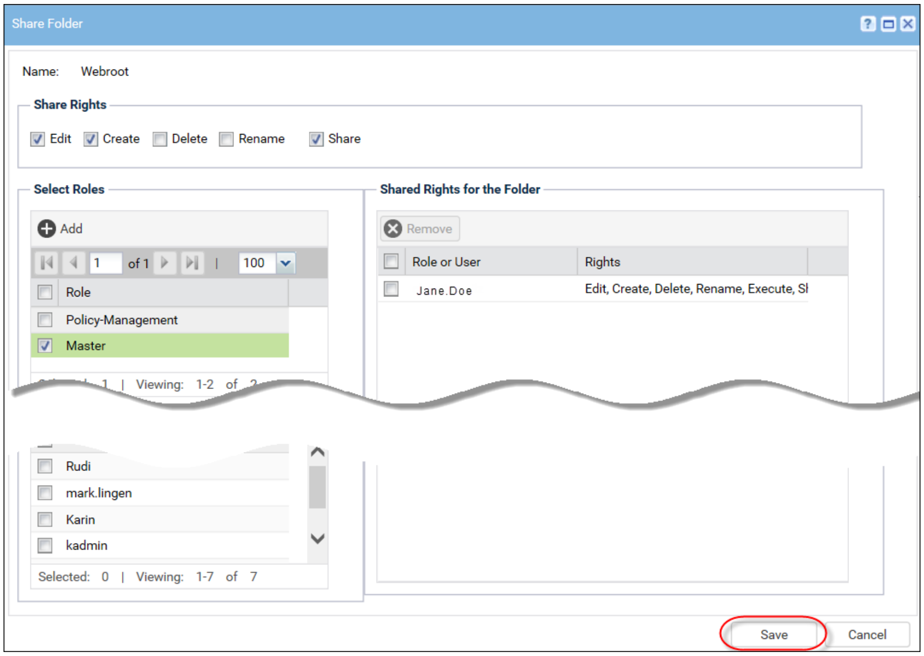
☑ Edit ☑ Create ☐ Delete ☐ Rename ☑ Share

Select Roles

☐	Role
☐	Policy-Management
☑	Master

Selected: 1 | Viewing: 1-2 of 2

12. When you're done, click the **Save** button to submit your changes.



Share Folder

Name: Webroot

Share Rights

☑ Edit ☑ Create □ Delete □ Rename ☑ Share

Select Roles

Add

□	Role
□	Policy-Management
☑	Master
□	Rudi
□	mark.lingen
□	Karin
□	kadmin

Selected: 0 | Viewing: 1-7 of 7

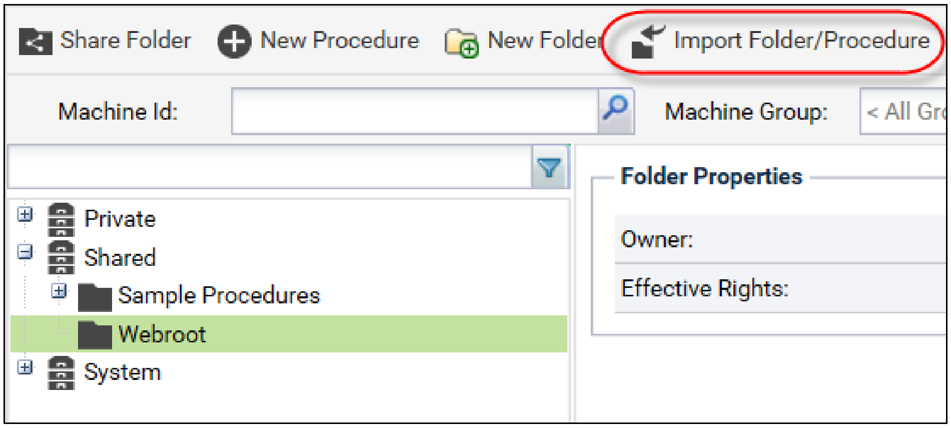
Shared Rights for the Folder

Remove

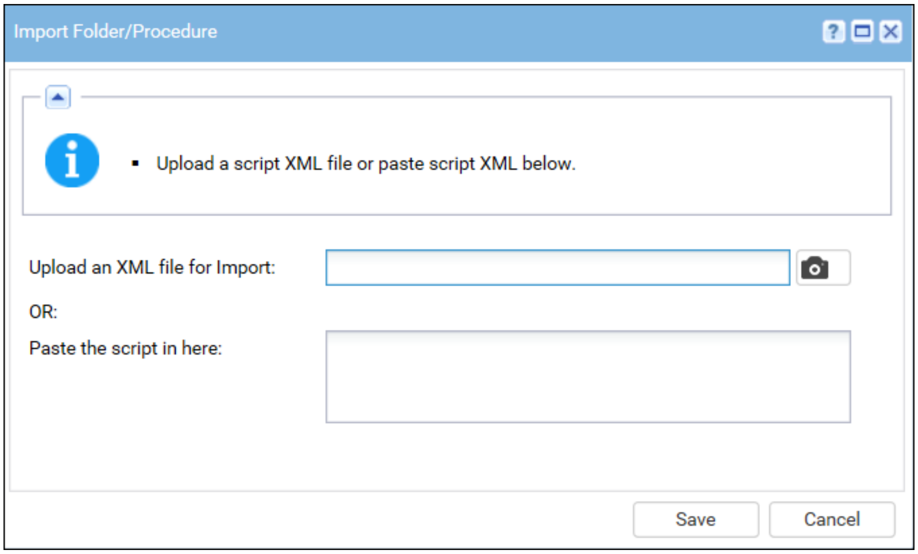
□	Role or User	Rights
□	Jane.Doe	Edit, Create, Delete, Rename, Execute, Sl

Save Cancel

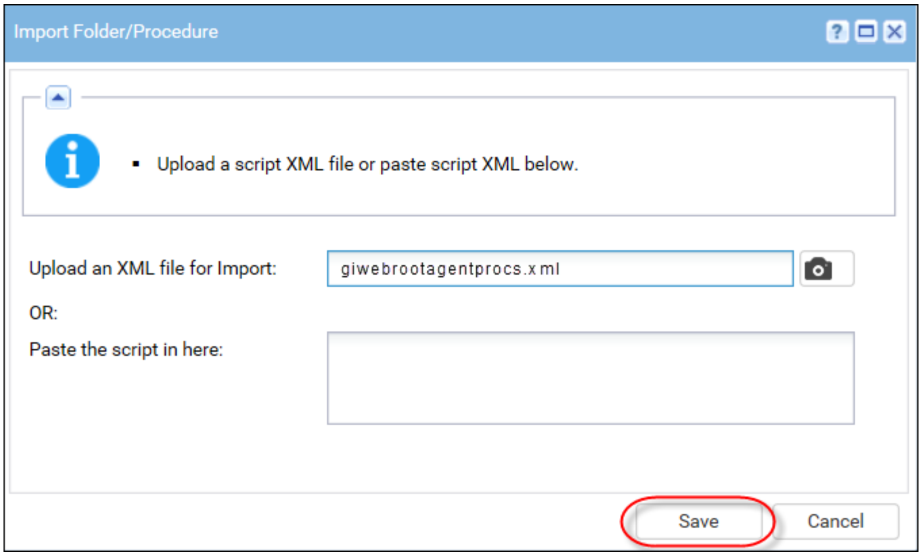
13. With the newly created folder still selected, click the **Import Folder/Procedure** icon in the toolbar.



The Import Folder/Procedure window displays.

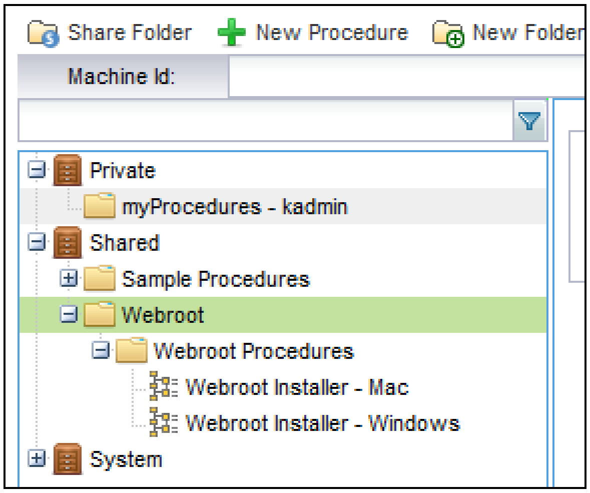

Import Folder/Procedure
Upload a script XML file or paste script XML below.
Upload an XML file for Import:
OR:
Paste the script in here:
Save
Cancel

14. Browse the share or local drive for the specific file and click the **Save** button.


Import Folder/Procedure
Upload a script XML file or paste script XML below.
Upload an XML file for Import:
OR:
Paste the script in here:
Save
Cancel

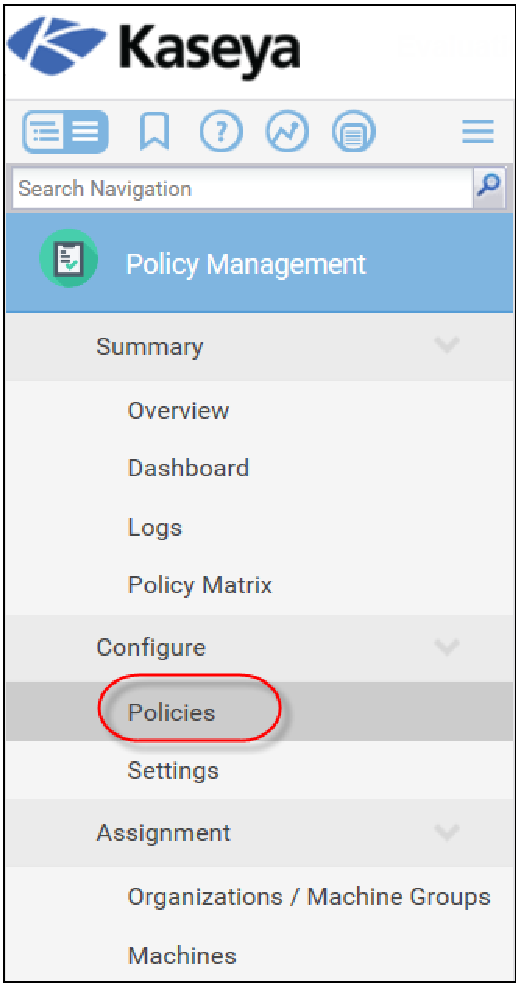
Upload an XML file for Import: giwebrootagentprocs.xml

15. After the import, you will have two new Webroot agent procedures for use with the VSA.

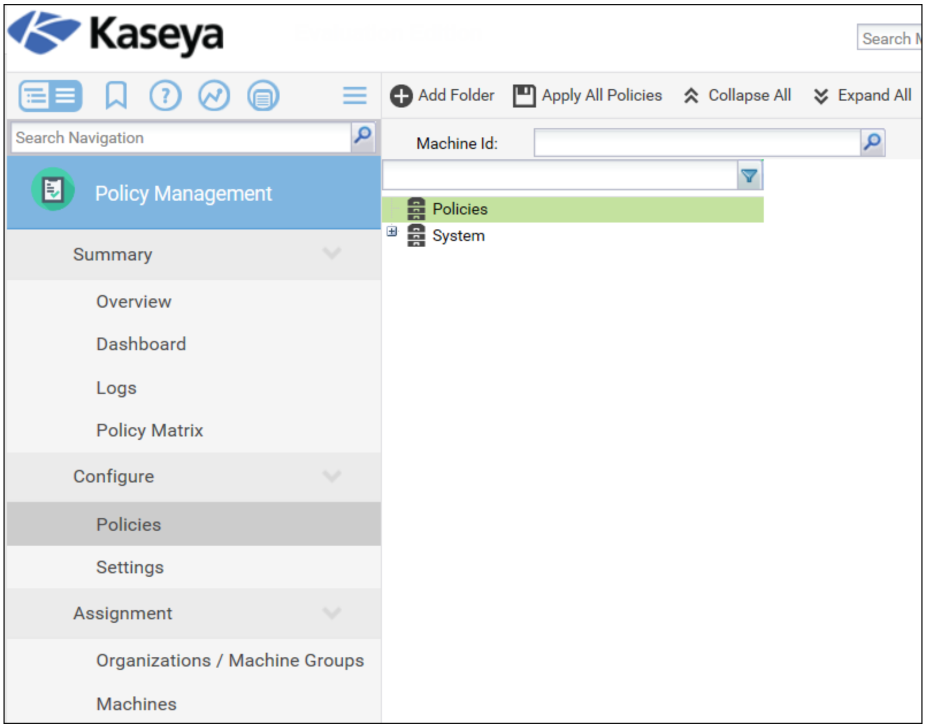


Part Three - Adding Agent Procedures to Policies

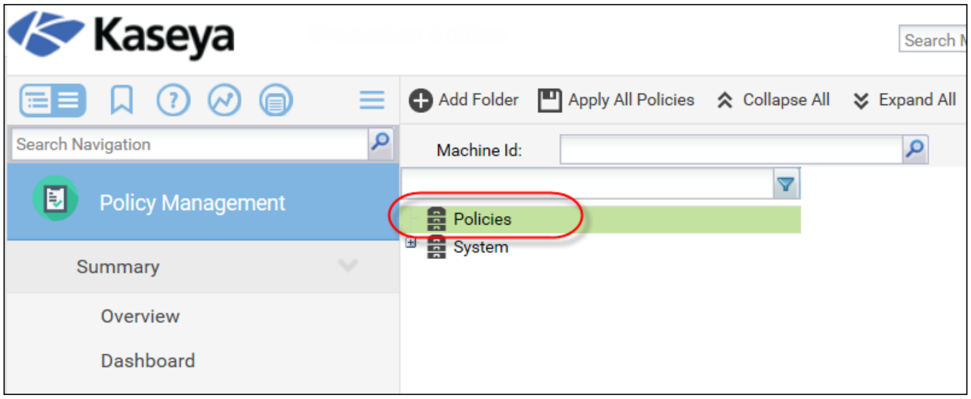
1. From the main menu, select **Policy Management** > **Configure** > **Policies**.



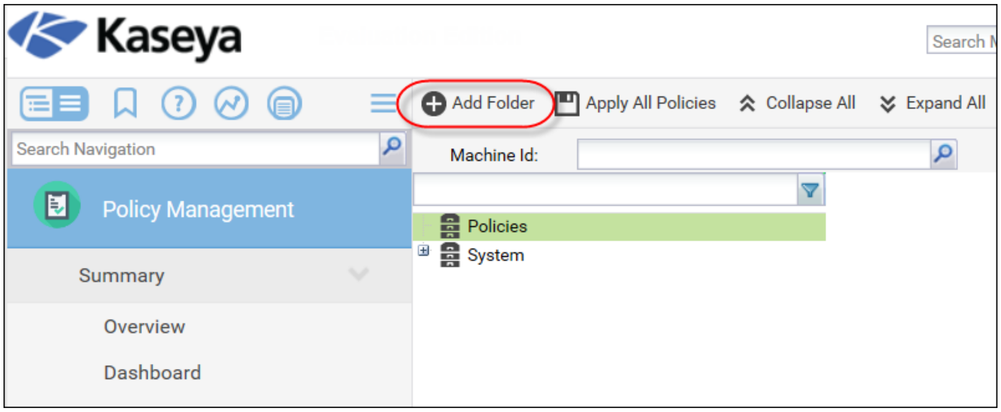
The Policies pane displays.



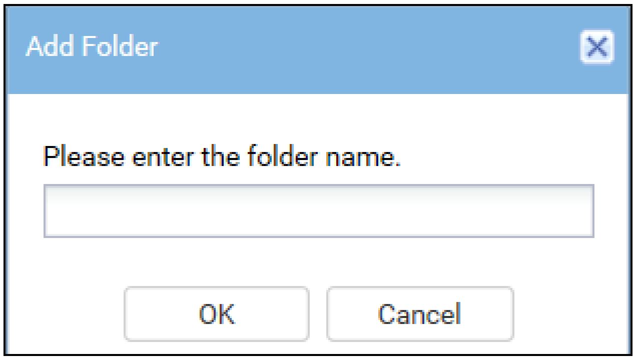
2. In the Policies pane, select **Policies**.



3. Click the **Add Folder** button.



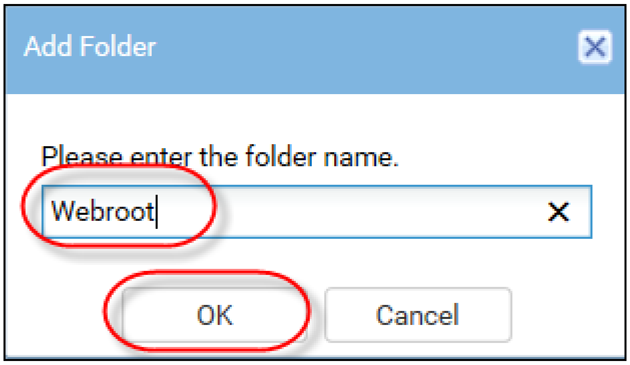
The Add Folder window displays.



Add Folder

Please enter the folder name.

4. In the Please enter the folder name field, enter a name for the folder, such as *Webroot*, then click the **OK** button.

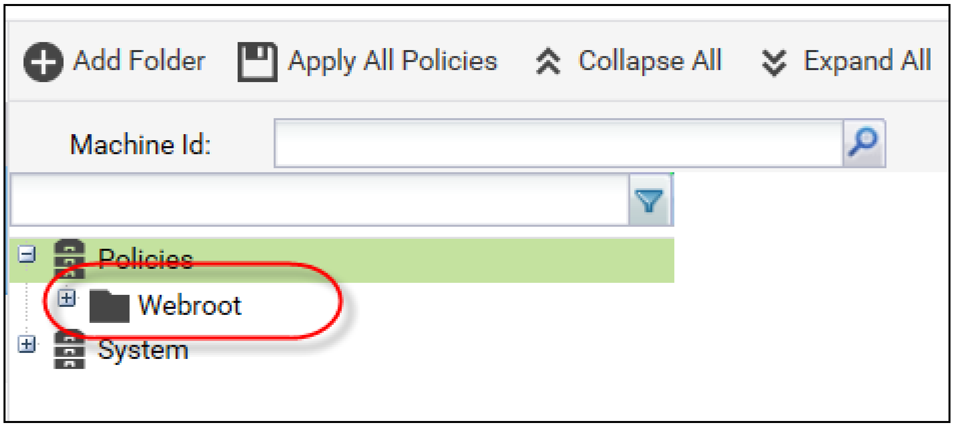


Add Folder

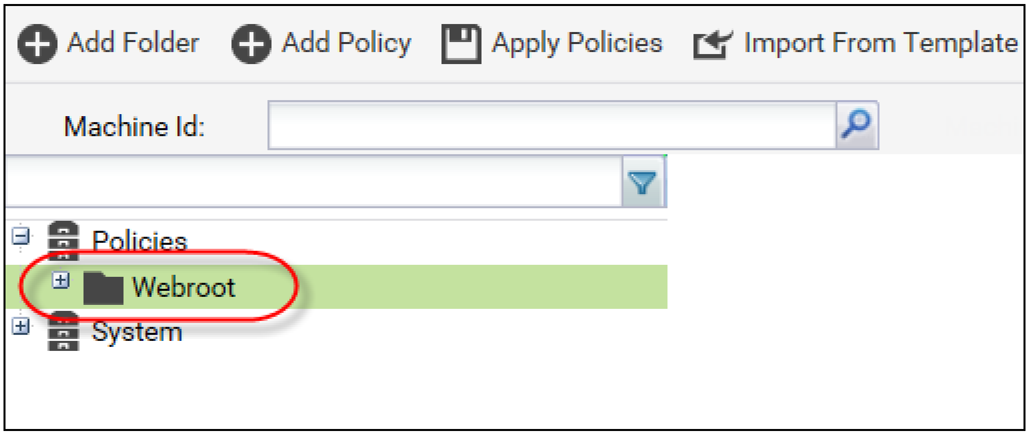
Please enter the folder name.

Webroot

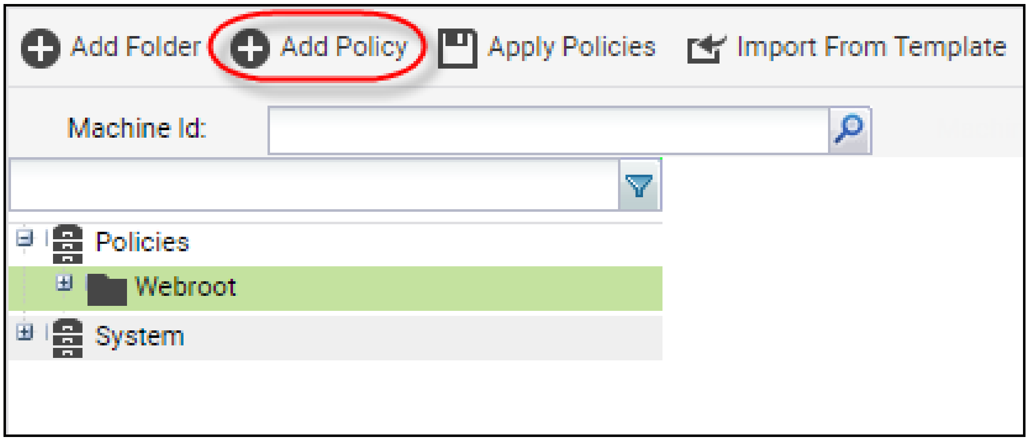
The new folder displays beneath the Policies tree.



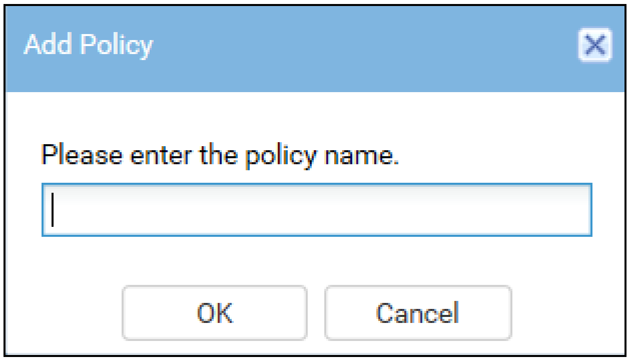
5. Select the new folder. Note that the menu bar options change.



6. Click the **Add Policy** button.

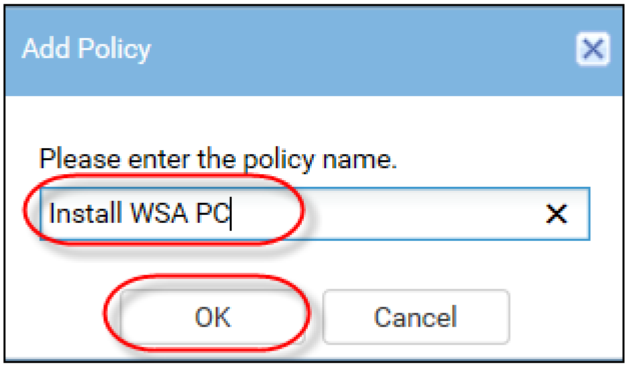


The Add Policy window displays.



Please enter the policy name.

7. In the Please enter the policy name, field, enter a policy name, for example, *Install WSA PC*, and click the **OK** button.

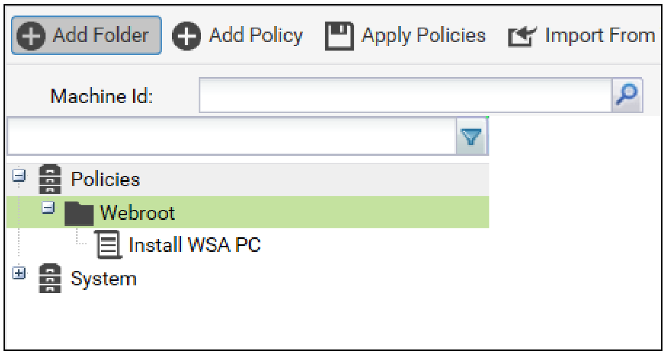


Add Policy

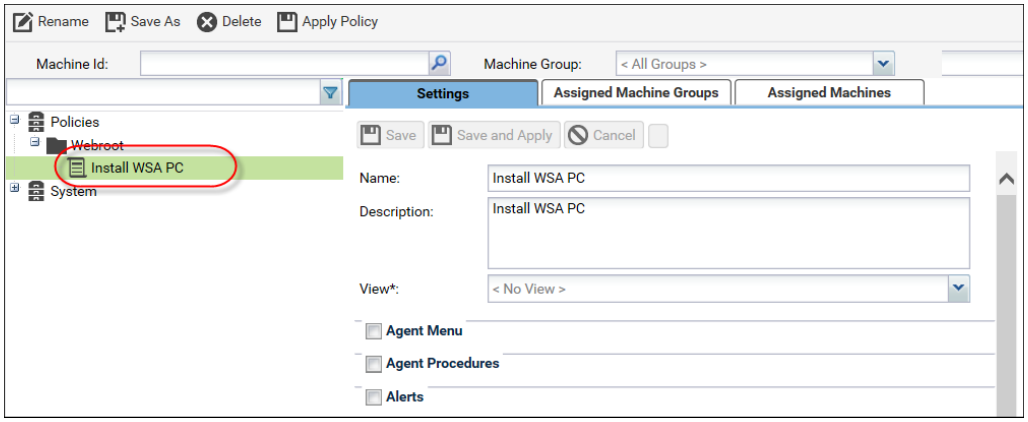
Please enter the policy name.

Install WSA PC

The new policy displays beneath the Policies tree.



8. Select the new policy to display the settings area for the policy.



Machine Group: < All Groups >

Name: Install WSA PC

Description: Install WSA PC

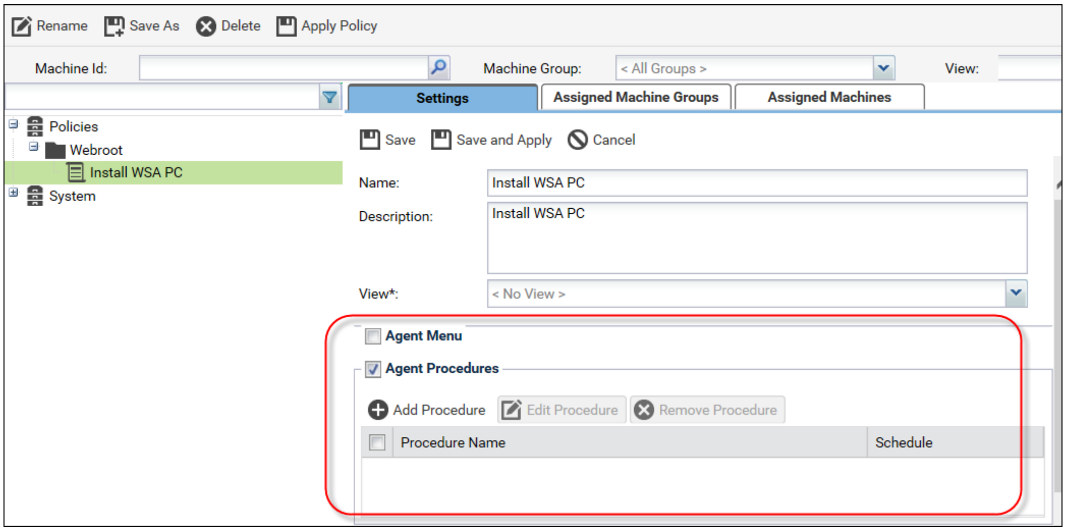
View*: < No View >

□ Agent Menu

□ Agent Procedures

□ Alerts

9. In the Settings tab, select the **Agent Procedures** checkbox to display the Agent Procedures settings area.



Name: Install WSA PC

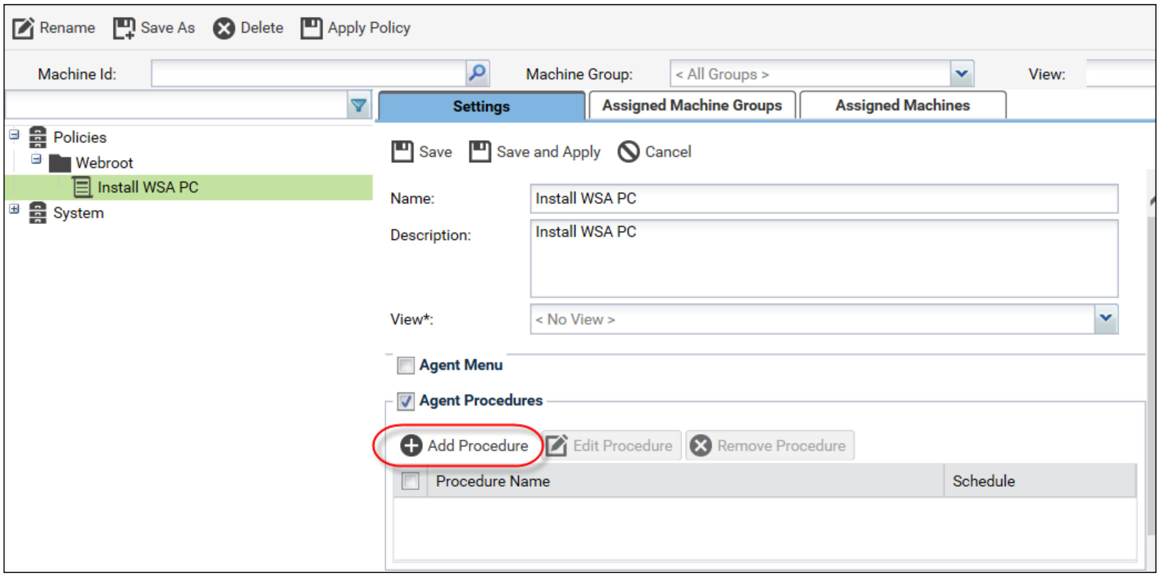
Description: Install WSA PC

View*: < No View >

☐ Agent Menu

☑ Agent Procedures

10. Click the **Add Procedure** button.



Name: Install WSA PC

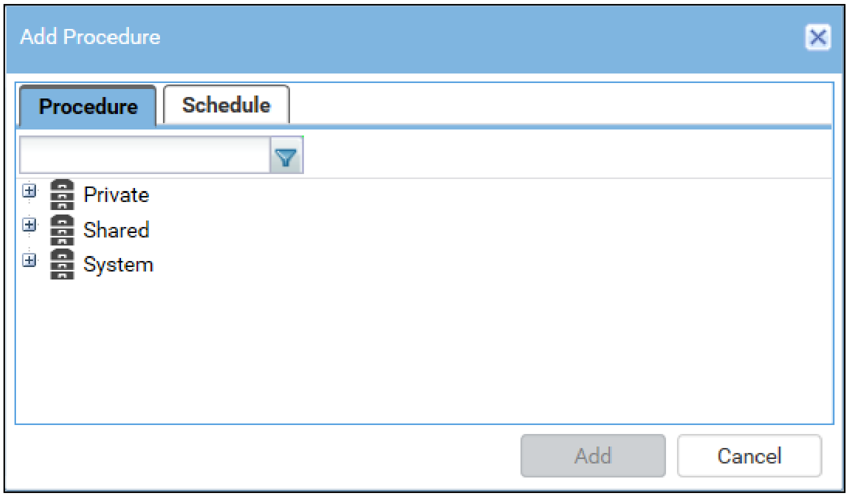
Description: Install WSA PC

View*: < No View >

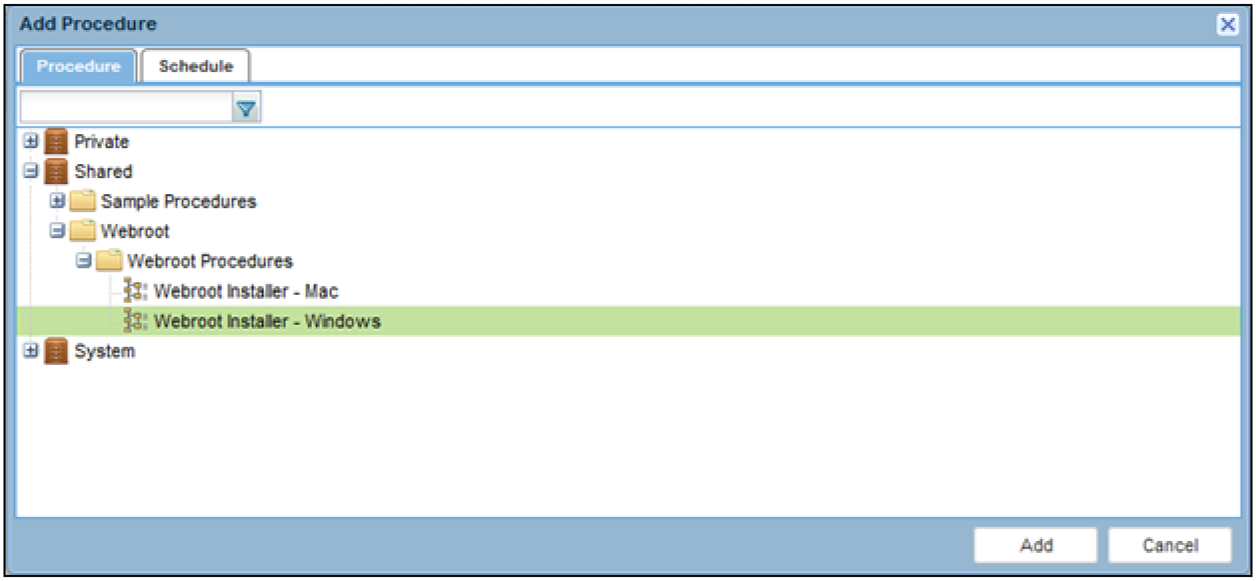
☐ Agent Menu

☑ Agent Procedures

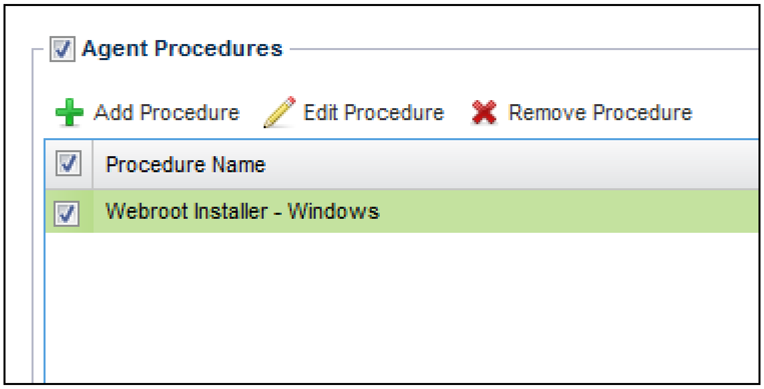
The Add Procedure window displays.



11. Open the tree by selecting **Shared** > **Webroot** > **Webroot Procedures**.



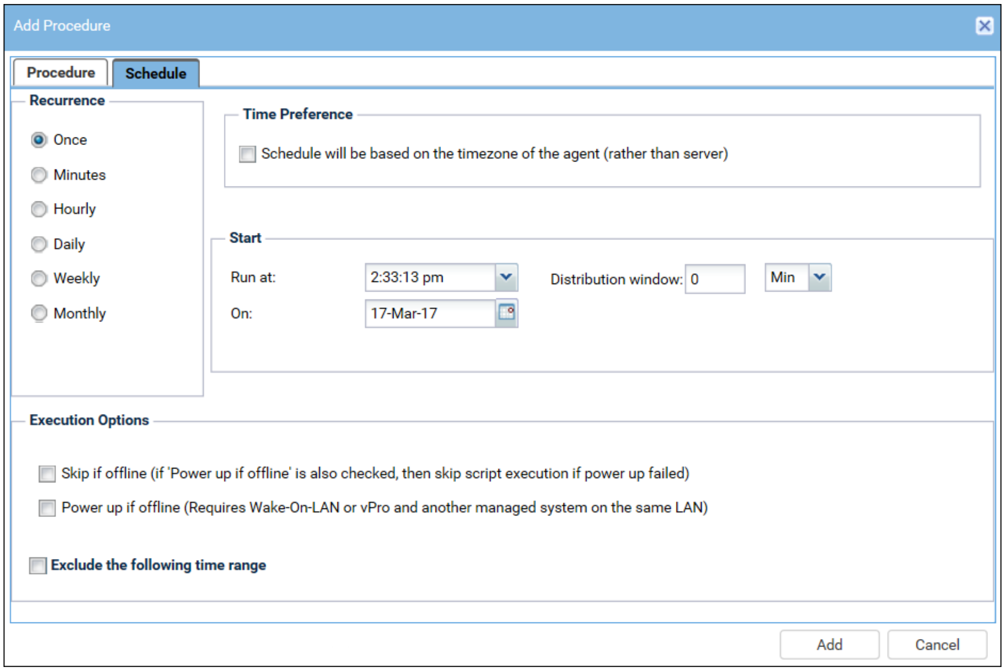
12. Select the **Agent Procedure** you just added.



☑ Agent Procedures

☑	Procedure Name
☑	Webroot Installer - Windows

13. Click the **Schedule** tab to display the Schedule area. Update any of the options, as needed.



Recurrence

● Once
○ Minutes
○ Hourly
○ Daily
○ Weekly
○ Monthly

Time Preference

☐ Schedule will be based on the timezone of the agent (rather than server)

Start

Run at: 2:33:13 pm

Distribution window: 0 Min

On: 17-Mar-17

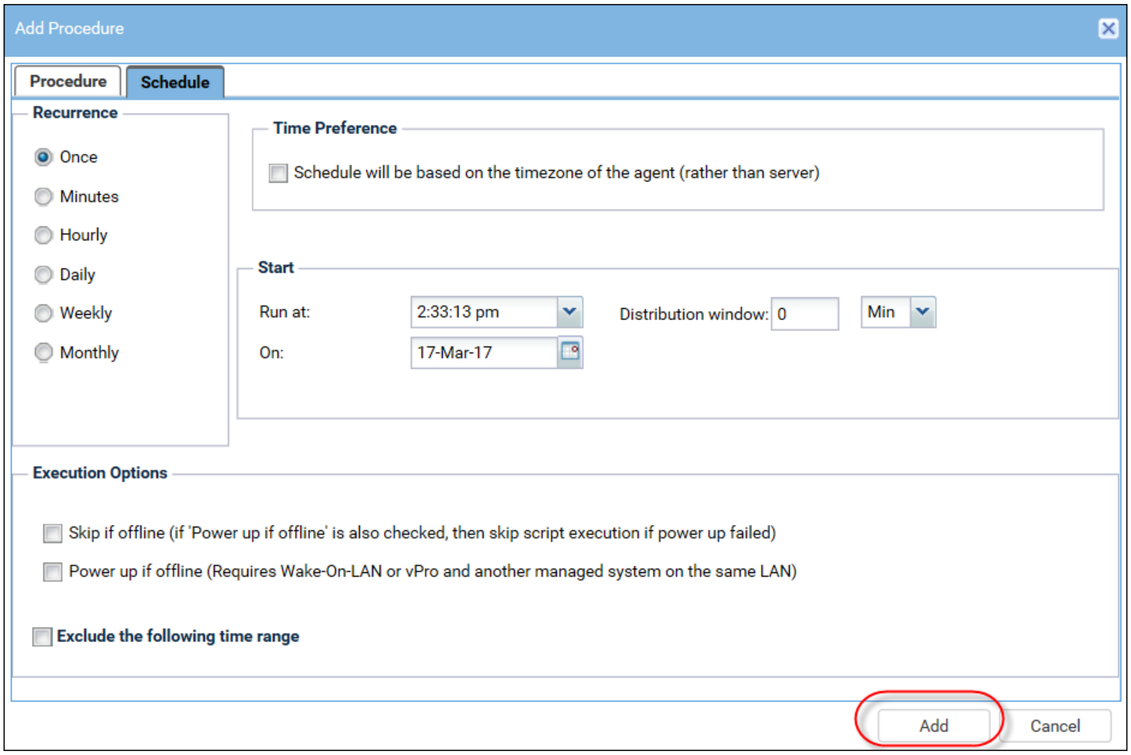
Execution Options

☐ Skip if offline (if 'Power up if offline' is also checked, then skip script execution if power up failed)

☐ Power up if offline (Requires Wake-On-LAN or vPro and another managed system on the same LAN)

☐ Exclude the following time range

14. When you're done, click the **Add** button.



Recurrence

- ● Once
- ○ Minutes
- ○ Hourly
- ○ Daily
- ○ Weekly
- ○ Monthly

Time Preference

□ Schedule will be based on the timezone of the agent (rather than server)

Start

Run at: 2:33:13 pm

On: 17-Mar-17

Distribution window: 0 Min

Execution Options

□ Skip if offline (if 'Power up if offline' is also checked, then skip script execution if power up failed)

□ Power up if offline (Requires Wake-On-LAN or vPro and another managed system on the same LAN)

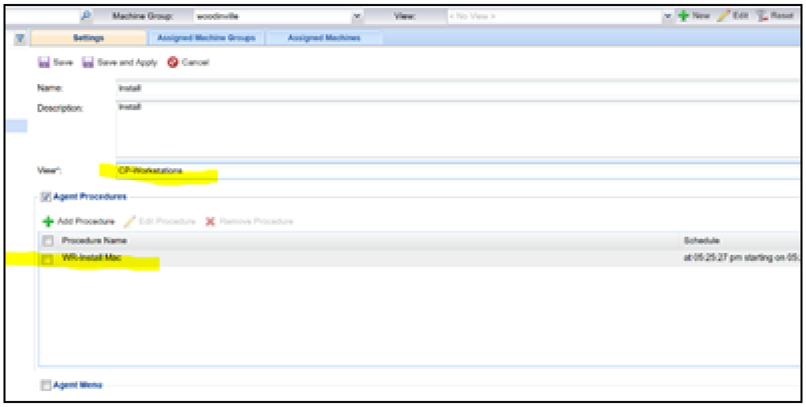
□ **Exclude the following time range**

Part Four - Applying Policies

You can apply a policy one time or globally to an organization or group.

Applying Policies Once

1. With Kaseya Policy, you can create the ability to run an agent procedure on a schedule or only run once.
   - To install, they will want to have it run once.
   - If a new machine shows up in the group you select, it will run this agent procedure. The example below shows a a view selected to filter for only specific machines.



Machine Group: woodinville

View: < No View >

Name: install

Description: install

View*: CP-Workstations

☑ Agent Procedures

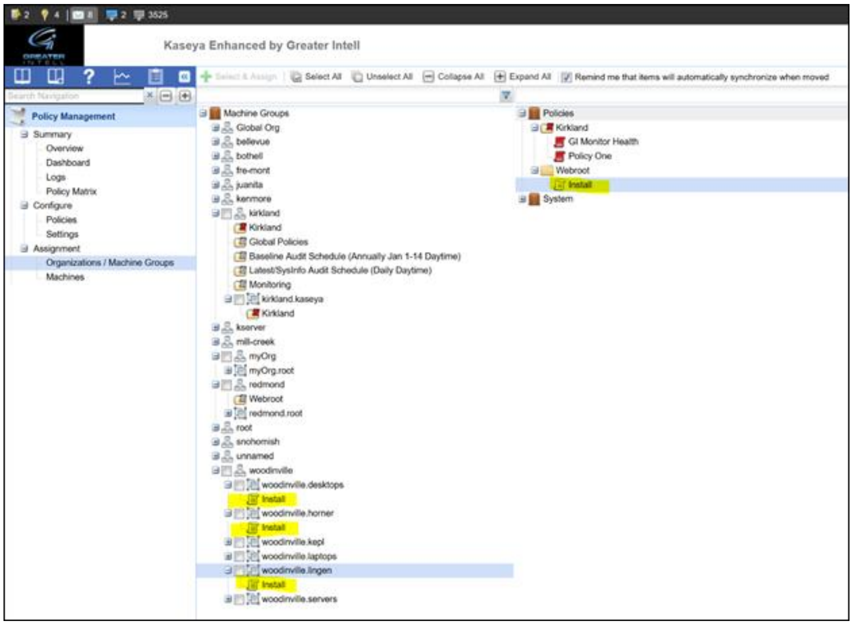
Procedure Name	Schedule
WR-install Mac	at 05:25:27 pm starting on 05

□ Agent Menu

Applying Policies Globally

1. Once you have created the policy, from the main menu, select **Policy Management** > **Assignment** > **Organizations / Machine Groups**.
2. Drop that folder or policy into the tree where you want it applied.

   For example, I only want the policy to run within a few groups



New Features in Version 2 - Summary

Org/Group Site Key

Added the capability to Webroot Settings to assign Site Key by Org and top level Groups.

- Added ability to view settings by Groups or Organizations.
- Added sorting to key columns on the setting grid.
- If API is turned on, the Site Key selection will be done using a drop-down menu. No copy and paste needed.

Auto Install

Added the ability to select a Org/Group to auto install all agents.

- Added the Auto Install checkbox to Settings page. This allows customers to automatically install Webroot on endpoints within that container.
- New background task added, which fires once an hour and looks through all the orgs/groups that are configured to auto install. If there are any new endpoints, the install agent procedure will be scheduled to run on those endpoints.

Mac Install

Added support for Mac endpoints.

- Added new agent procedures to install webroot on Mac endpoints.
- Added new agent procedures to uninstall webroot on Mac endpoints.
- Added new icon to Deployment Page, displaying whether Mac or Windows machine.
- Updated Deployment grid to display status of Mac.
- Updated endpoint dashboard to show status values that apply to Mac only.
- Added icon to endpoint dashboard showing OS type.
- Added new mac consumer for installation, this will handle the install state and consuming of the install log to track failures.
- Added new mac consumer for uninstallation.
- Added new mac consumer for status, if API is turned off pull data from plist file on machine and save to the database.
- If the API is off, add Mac endpoint status consumption to hourly process.
- If the API is on, Mac endpoint status should be the same as the Windows endpoints by just pulling from Unity API.

Unity API

Added Unity API to replace the consumption from registry and plist files on the endpoints. Also selecting existing sites from a drop down for assigning them to Organizations and Groups is now available.

- Added session management of API credentials.
- Added infrastructure to make web calls to the Unity API.
- Added the ability to turn on/off API settings. If turned off, then run the v1.0 process of pulling from the registry and plist files on the endpoints.
- Added new API Settings page, admin entering creds, configuration and testing.
- Store API Credentials in DB encrypted.

- Added new background task that will run every 15 minutes to get all the changed endpoints for all the site keys managed.
- Made all the API settings and processes Tennant-aware for Kaseya Saas.
- Created data consumers for JSON data coming back from API Status calls.
- Added API call to get status of one endpoint.
- Added API call to test credentials and status of API configuration.

Update Configuration Info

Add plugin info to overview page for support.

- Added new tab to overview page called Webroot Plugin Info.
- Added Label showing plugin current version.
- Within the plugin info tab include labels:
  - Version
  - Clients Installed
  - API Enable

Uninstalling the Kaseya Plugin

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

Note: After uninstalling Kaseya module V2, extra clean-up steps are required if you wish 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. Please report document omissions or issues to your Webroot representative.

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