

Kaseya VSA Cloud Module Assembly Version 2.0.21053.1 & above Webroot.vsaz file 1.5.20134.2 & above

Getting Started Guide

Document Version 2.0.1



Table of Contents

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



Overview

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

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

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

If you have any suggestions please contact your Webroot representative, alternatively you can post suggestions or comments in our Kaseya Partner Group community <u>here</u>.

What's New with Version 2.0

New Features

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

Enhancements

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

Prerequisites

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

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

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



Installing Webroot Kaseya VSA Cloud Module

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

To install Webroot Kaseya VSA Cloud Module:

- 1. Download the Webroot Kaseya VSA Cloud Module **Webroot.vsaz** file <u>here</u>. You can also get the latest module from Kaseya Automation Exchange under Webroot Kaseya Cloud Module.
- 2. Download the installer package to your device.



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

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



4. Click the Third Party tab.

=(Third Party	Licenses	License By Group	Role Types
P	🕑 Install 🔕 Rom	ove		
2	Tenant Name	A	oplication Name	Company Name

5. Click the Install icon.

=	Third Party	Licenses	License By Group	Role Types
---	-------------	----------	------------------	------------



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

Install Application	? • ×
Please select a .vsaz file to start the registration process	L
Manifest file name:	
1	Browse File
	Cancel Next

8. Click the **Next** button.

Install Application		90×
WEBROOT Webroot Kaseya Plugin	Webroot Inc.	
	Cancel Back	Next

9. Click the Next button.

Install Application		20×
Please enter the value for y	our custom fields.	
Custom Field	Custom Value	
Webroot	Erter Velue	
	Cancel	Back Next (m)



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

tall Application		
Agent Procedures to be installed		
Webroot Uninstall Script	~	
WR_Install_Script_6432		
WR_Mac_Install		
	*	
ServiceDesk Definitions to be installed		
There are no Service Desk Definition to be installed		
Alert Definitions to be installed		
There are no Alerts to be installed.		
	Cancel	Back Net
	Construct.	non indi

11. Click the Finish button to complete the installation.

Install Application		80×
WEBROOT	Webroot_Dev3 Webroot Inc.	
You're module is ready	to be activated?	
Click Finish to register	your module with the provider and activate it for use.	
	Cancel	Back Freish

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





Controlling Access to Webroot Settings

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

To control access to Webroot settings:

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



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



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





Г

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

Members Access	Role Type				
Set Role Access Rights					
Expand All	Collapse All				
 □ Gaster □ Anti-Malware 					

- 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

Set Role Access Rights				
Expand All		Colla	pse All]
 Root Kaseya VSA TAP Apps 				
Set Role Access Rights				? 🗆 🗙
Generation States Stat	rview loyment & Status I u ration proot Settings	Dashboard		
			Ok	Cancel



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





Getting Started and Deployment

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

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



Overview Menu

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



Organizabons 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/Organizabons", each with its own keycode



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

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

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



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



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



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

E Q Search Navigation	? Click to view Webroot plugin help	
Webroot	Overview Webroot Plugin Info	Webroot Plugin Version:
▲ Main		5
Overview		
Deployment & Status Dashboard	\sim	
 Configuration 		
Webroot Settings	WEBROOT DEPLOYMENT SMART	CW/
Alert Settings	ACTIONS VIL	
Agent Agent		

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

? Click	to view Webroot plugin h	elp	
Overview	🔅 Webroot Plugin Inf	o	Webroot Plugin VSAZ Version: (1.5)
Webroot Plu	ugin VSAZ Version	1.5	
Webroot Ka Version	seya Cloud Module	2.0.21050.2	

Plugin Version Notification

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

New Plugin Version! Click New version 1.6 to download the latest Webroot.vsaz file and upgrade from 1.5
 Click Webroot Module Information for upgrade instructions.





Admin Data Sync

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



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

? Click to view We	broot plugin hel	p		
Overview 🔅 Webr	oot Plugin Info	🛢 Admin Data Sync		
O Start New Sync	2 Refresh			
Sync Name	Admin Scope	Time	Data Results	Status
Agents	System	4/21/2020 10:44 AM	10002 out of 10002	Success
Machine Groups	System	4/21/2020 11:01 AM	11 out of 11	Success
Organizations	System	4/21/2020 11:01 AM	6 out of 6	Success

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

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

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

Search for	r machines				Ð		2 🔵 2	10000		• •
E Q Search Navigation	AGENT Sy	nc: Last Upd	late: 4/21/20	20 10:44 AM;	Admin Sco	pe: System;	Data: 100	02 agent(s);	Status: Succes	55
Webroot QA		_		Machin	2 ID	Q	<	All Groups >		~
▲ Main	🛓 Insta	<u></u>	Uninstall	C Re	fresh	Agent Com	mands 🕶			
Overview		it it 😡	j⊥ Status		Machine.	Group ID		lt	Hostname	11
Deployment & Status Dashboard		-								



Webroot Business Agent Deployment

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

Note: If you have an existing Webroot Business deployment, you can adopt already installed endpoints into the Kaseya Module. For more information, see <u>Adopting Existing Webroot Business Agents</u>.

Configuring and Obtaining a Unique Webroot Site Key

To configure:

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

≡	Q Search Navigation	Fil	ter \ Orga	/iew	าร				Service Admin: test01
<u></u>	Webroot QA	$ $ \circ	Grou	ps					
~	Main Overview	ñ	Му						
	Deployment & Status Dashboard	匬	1	Ø	Auto Install		Org/Group	17	Webroot Site Key
· ·	Configuration	Ŵ	2	Ø	~	ACME Solicit	ors		WEBR-OOT1-SITE-KEY1-1111
	Alert Settings	Ŵ	2	Ø		Global Expor	ts		WEBR-OOT2-SITE-KEY2-2222

To obtain a unique site key:

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





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

≡	Q Search Navigation	Fil	ter \ Orga	/iew	าร		Service Admin: test01								
<u>.</u>	Webroot QA	0	Grou	ps											
Ŧ	Main	~	Mv	My Webroot C Refresh											
	Overview	<u> </u>	,	TTODA											
	Deployment & Status Dashboard	ŵ	%	Ø	Auto Install	Org/Group	Webroot Site Key								
•	Configuration	Ŵ	%	Ø	~	ACME Solicitors	WEBR-OOT1-SITE-KEY1-1111								
	Alert Settings	圃	1	Ø		Global Exports WEBR-OOT2-SITE-KEY2-222									
	-														

The Webroot SecureAnywhere login page displays.

Secure Anywhere.								
Log in	Create Account							
Log in								
Email or Phone	0							
Password	Forgotten Password							
Log in								

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

Secure Anyw	Secure Anywhere.											
Dashboard Sites Ad	dmins Groups	Policies	Overrides	Alerts	Reports	Settings						
Sites	Sites											
10 Sites Accessible 10 Tota	10 Sites Accessible 10 Total											
Status 🗢	Site ≏						Devices	Site Seats ⇔				
Protected	ACME Solicitors				Ma	nage 🕞 🕞 🖓	2	5				
Protected	Corsair Inc				Ma	nage 🕞 🖙	1	5				
Protected	Global Transport	Inc			Ma	nage 🕞 🕞 🖓	0	10				



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

Secure/	Secure Anywhere.											
Dashboard Si	ites Ad	lmins	Groups	Policies	Overrides	Alerts	Reports	Settings				
Sites 10 Sites Accessib	Sites 10 Sites Accessible 10 Total											
Status ⇔		Site	<u>م</u>						Devices	Site Seats ⇔		
Protected		ACM	E Solicitors				Ма	nage ©⊽	2	5		
Protected	Protected Corsair Inc						Ма	nage ©⊽	1	5		
Protected		Glob	al Transport	Inc			Ма	nage 🕞 🖓	0	10		

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

Becur	eAnj	when	e.								
Dashboard	Sites	Admins	Groups	Policies	Overrides	Alerts	Reports	Settings			
Sites 10 Sites Acce	essible 1	0 Total									
Status ⇔		Site	<u>م</u>						Devices 👄	Site Seats	
Protected		ACM	E Solicitors				AB1	AB12-ABCD-AB12-AB12-AB12			
Protected		Cors	air Inc				Ма	nage ©v	1	5	
Protected		Glob	al Transport	Inc			Ma	nage 💿	0	10	

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



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

Filt	er View Organizations			
\bigcirc	Groups			
*	My Webroot	C	Refresh	



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

≡	Q Search Navigation	Fil	Filter View Service Admin: test01 Organizations Service Admin: test01											
<u></u>	Webroot QA	0	Groups											
~	Main	*	🕷 My Webroot 😂 Refresh											
	Overview			WODI										
	Deployment & Status Dashboard	ŵ	1	Ø	Auto Install	↓≞ Org/Group	Webroot Site Key							
· ·	Configuration	ħ	· .		~	ACME Solicitors	WEBR-OOT1-SITE-KEY1-1111							
	Webroot Settings	Ē	1			Global Exports	WEBR-OOT2-SITE-KEY2-2222							
	Alert Settings													

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

organization		
ACME Solicitors		
Vebroot Site Key		
		*
Site Key format ****_****_****	****	
Auto Install		
Enabling Auto Install will trigger iroups.	Webroot Client Installation on all agents within the selected O	rg/Group and sub

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

Edit Organization Settings	×
Organization	
ACME Solicitors	
Webroot Site Key	
WEBR-OOT1-SITE-KEY1-1111	ε
Site Key format ****_*****_*****_*****	
Auto Install	h
groups.)
Submit Cance	

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



Edit Organization Settings	×
Organization	
ACME Solicitors	
Webroot Site Key	
WEBR-OOT1-SITE-KEY1-1111	*
Site Key format ****_****_*****_****	
Auto Install Enabling Auto Install will trigger Webroot Client Installation on all agents within the selected Org/Group an groups.	d sub
Submit	incel

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

11. 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 Orgs/Groups within the Kaseya Module. We recommend a site <u>key per Organization</u>, unless you have very small organizations consisting of one or two seats.

12. If Auto Deploy has been selected within an Org/Group in Webroot Settings, the Org/Group computers will show the Auto Deploy gear icon 🔹 within the **Deployment & Status Dashboard**

					Ma	hine ID	Q		ACI	ME Solicitor	'sX	~		< No View	>	1
Webroot QA			_					_	_							
✓ Main	*	Install	•	Au	to Install 🔻	<u></u>	Uninstall	2	2	Refresh	Ag	ent Co	omma	nds 🕶		
Overview		ļt.	Jî		ļi.		ļ†				.↓†	Atter	ntion	ļ†	J1	Activ
Deployment & Status Dashboard		•		W	Status	Mach	ine.Group ID			Hostname		Requ	lirea	Infected	Policy	Inrea
 Configuration 		•	4			vrathwir	nz840.root.1010	VF	RATH	HWLNZ840.qa	local					
Webroot Settings Alert Settings		•	-	W	Installed	vrathwir a.root.1	nz849.group- 010	VF	RATH	HWLNZ849		No		No	Yes	



Auto Deploy Exclusions

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

To exclude specific Computers:

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



2. Select the Org/Group from the drop down menu

						Mac	hine ID	Q	AC	ME Solicitor	's X	~	< No View	>	
<u>v</u>	Webroot QA		_	_					_						
-	Main	*	Install	\$	Au	to Install 🔻	<u>±</u>	Uninstall	C	Refresh	Ag	ent Comma	nds 🔻		
	Overview		ļt.	11		LL.	Machi	lî		Hostnamo	↓î	Attention	.↓†	↓† Believ	Activ
	Deployment & Status Dashboard				W	Status	Wach	ne.Group ib		Hostname		Required	intected	Policy	mea
¥	Configuration		•				vrathwin	z840.root.1010	VRAT	HWLNZ840.qa	local				
	Webroot Settings Alert Settings		•				vrathwin a.root.10	iz849.group- 010	VRAT	HWLNZ849					

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

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

	Webroot QA			Apply Ex Install fo	clude/Include of Au or selected machine	tone ID s.	Q	AC	ME Solicitor:	×	~	< No View	> ~	
	Main	*	Install	•	Auto Install -	1	Uninstall	C	Refresh	Ag	ent Comm	ands 🕶		
	Overview		11	Exclu	de		ļ†.			J†	Attention	ti. Jt	.↓†	Activ
	Deployment & Status Dashboard		•	Inclu	de	Machi	ne.Group ID		Hostname		Required	Infected	Policy	Threa
-	Configuration		•	4		vrathwir	z840.root.1010	VRAT	HWLNZ840.qa.	local				
	Webroot Settings Alert Settings		•	4		vrathwir a.root.10	z849.group- 010	VRAT	HWLNZ849					



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

						Mac	hine ID:	Q	A	CME Solicitor	rs X	~	< No Viet	W > ~	
<u></u>	Webroot QA		_	_			_		_						
~	Main	*	Install	\$	Au	to Install 🔻	<u></u>	Uninstall	0	Refresh	Ag	ent Com	mands -		
	Overview		ļt.	.↓†		↓1	Mashi	11			.↓†	Attentio	001 J1	li li	Activ
	Deployment & Status Dashboard				W	Status	wachi	ne.Group ID		Hostname		Require	a Intected	Policy	Inrea
-	Configuration		•	-		8	vrathwin	iz840.root.1010	VRA	THWLNZ840.qa	a.local				
	Webroot Settings			4			vrathwin	iz849.group-	VRA	THWLNZ849					
	Alert Settings						a.root.10	010							

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

						Mad	chine ID	Q		ACI	ME Solicitor:	sX	~	< 1	No View	>	
<u></u>	Webroot QA			_					_	_							
~	Main	*	Install	•	Au	to Install 🔻	<u>+</u>	Uninstall	2	•	Refresh	Ag	ent Com	mands	s 🕶		
	Overview		ļt.	1†		ļi.	Marchi	11				J†	Attentio	D))	ţţ	J†	Activ
	Deployment & Status Dashboard		•		W	Status	wachi	ne.Group ID			Hostname		Require	ea Ir	ntected	Policy	Inrea
-	Configuration		•	4		۲	vrathwin	iz840.root.1010	VF	RATH	HWLNZ840.qa.	local					
	Webroot Settings			-	W		vrathwin	z849.group-	VF	RATH	IWLNZ849		No	٢	No	Yes	
	Alert Settings				-	Installeu	a.1001. IN	510									

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



Adopting Existing Webroot Business Agents

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

To adopt existing agents:

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



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

		ñ	My	Webroot	S	Refresh	
Search Navigation	9				_		
Webroot	^	1	Ø				Organization
WEBROOT			Ø	ACME Soli	citors		
Main 🗸 🗸 🗸		¥2		console-ul	k		
Overview		1		derbytest			
Deployment & Status Dashboard		1		mac_os			
Configuration 🔍	l.	1	Ø	myOrg			
Webroot Settings	-	1	Ø				

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

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



Deploying Webroot Agents via the Kaseya Module

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

To deploy Webroot agents:

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



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

±	Install) ±	. Un	install	c	Refresh	
)]]	11	.≞ ₩		Machine	e.Group ID	11
	•	4					
	•	4					
	•	4	•				

• 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.

<u>±</u>	Install	1	Un	install C Refresh	
	11	ļţ	11		11
			W	Machine.Group ID	
		4			
	•	4			

Viewing Installation and Dashboard Level Webroot Agent Statuses

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

1020				 2021	Martin	10			0	- A	Groups +		×.	+ R0, 1006 +		·*
	-	0	A Matters Droug D	Assessed	American Required	Estive	Expire Date	Internet	Palicy Monoped	Autors Threads	Treats Removed	Lest Suar Date	Last Seen	Kaunya Agent Refresh	P Address	Installation Dates
87	0	0			160	No.	01.jan.2018	The .	A***	6		1014.0215-Feb-2016	11.34.39.05.7+6-2016	11.37.14.05-640-2018		metallect
	0				A700	14	\$1.0pt;2218	A***	799			05 00 01 05 7 96 2010	12 20 40 00 7 40 2010	12 21 20 05-Pwb-2019		team
83	0	0			940	T	81.Jun 2018	.80	without			101710057462016	11.06.42 (0.746-2018	11.37.14 05-Feb-2010		Indated
4	•	•			- 141	44	01.Jan 2010	84	Yes			10.41.02.05.746.2016	11301405546-0016	11 38 48 35 Feb 2018		material
0.	0	•			140	-	91.Jan 2019		and the second			10 51:00-05 Feb 2016	11.36.43.05.646.2016	11373435.649.2018		make
iter	-		Lenne												10.14	

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

lcon	Description
W	Windows OS
É	Mac OS

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

*	Install	1	Uni	install 📿 Refresh		
	11	ţţ		A Machine.Group ID	Hostname	↓† Attention Required
	0	-				
	0					
	0	et.				
	0	4	Ø			A Yes
	0		•			No



Indicators in the Deployment & Status Dashboard

Red W

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

*	Install	<u>±</u>	Un	install	c	Refresh			
	11	11	11				11		1† Attention
			W		🚢 Mach	ine.Group ID		Hostname	Required
	0	4							
	0	-							
	•	et.							
	•	=(0						∆ Yes
	•	4	W						No

Warning Icon in Kaseya Agent Refresh Column

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

11 eats oved	Last 11 Scan Date	Last Seen	Kaseya Agent Refresh	IP Address	Installation Status	'
2	00:10:01 14-Mar- 2017	00:21:53 14-Mar- 2017	10:47:06 14-Mar- 2017		Installed	
0	08:00:01 14-Mar- 2017	08:02:28 14-Mar- 2017	08:42:20 14-Mar- 2017		Installed	
0	16:00:00 28-Feb- 2017	16:33:32 28-Feb- 2017	17:13:56 28-Feb- 2017		Installed	
0	02:41:00 10-Mar- 2017	02:49:09 10-Mar- 2017	04:37:07 13-Mar- 2017		Installed	



Running Webroot Agent Commands

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

To run Webroot Agent Commands:

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

	=						Machine ID Q	adoption-test	-side.lett.	~	< No Viev	N >	~
Search Navigation	9	*	Install	t	- Un	install	C Refresh Agent Co	ommands 💌					
Webroot		_					- ····						
Moin			• 11	.↓↑	W	↓≣ Status	Machine.Group ID	Hostname	Attention Required	↓† Infected	↓† Policy	Active Threats	Threats Removed
Main				-		Installed	vrathwinz585 level 01 adoption-	VRATHWI NZ585	No	No	Yes	0	1
Overview	. \	٢			W		test-side					, in the second s	
Deployment & Status Dashboard	6					Installed	vrathwlnz490.level_01.adoption-	VRATHWLNZ490	No	No	Yes	0	0
Configuration 🗸 🗸		\smile			W		test-side						
Webroot Settings	Ŧ		•				vrathwlnz580.level_01.adoption- test-side	vrathwinz580					

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

	=						Machine ID	Run a Webroot A on selected	Agent Comma machines.	nd te st-	side.lett.	~	< No Viev	N >	~
Search Navigation	9						~								
Webroot	•	*	Install	1	, Un	Install	C Refresh	Agent Com	imands 👻	2					
WEBROT			lt.	J†		17		Update Nov	N		Attention	J1	ļ†.	Active	Threats
Main 🗸		-			W	Status	Machine.	Deep Scan		ıe	Required	Infected	Policy	Threats	Removed
Overview		•	•	4	•	Installed	vrathwlnz585.lev test-side	Run Cleanu Full Scan	ıp	Z585	No	No	Yes	0	1
Deployment & Status Dashboard			-			Installed	vrathwinz490.lev	el_01.adoption-	VRATHWL	NZ490	No	No	Yes	0	0
Configuration 🗸		-			W		test-side								
Webroot Settings	Ŧ		•	-			vrathwlnz580.lev test-side	el_01.adoption-	vrathwinz58	30					



Launching Live Connect

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

To validate success:

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







Detailed Webroot Agent Status & Agent Commands

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

To generate analysis:

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



The system displays detailed Webroot Agent Information.

PROTECTION STATUS	SCAN STATUS	DETECTION STATUS	AGENT STATUS
REALTIME SHIELD ENABLED	SCHEDULED SCANS ENABLED	INFECTED NO	LAST SEEN 2:44:03 AM 10-Mar-2017
REMEDIATION ENABLED	SCHEDULE SCAN TIME 10:00	ACTIVE THREATS 0	LAST WEBROOT DATA UPDAT 10:37:34 17-Mar-2017
USB SHIELD ENABLED	LAST SCAN 02:44:03 10-Mar-2017	ATTENTION REQUIRED	ENGINE VERSION 9.0.15.50
Sidentity shield enabled	LAST SCAN COUNT 28664	THREATS REMOVED	POLICY MANAGED
WEB SHIELD ENABLED	LAST SCAN DURATION a minute	03:55:52 10-Mar-2017	10.36.16.105
PHISHING SHIELD ENABLED	SCAN COUNT	LATEST THREAT	
Soffline Shield Enabled	UAST DEFP SCAN 02:45:05 10-Mar-2017	NUM BLOCKED UNES	
	LICENSE STATUS	AGENT COMMANDS	
	DAVS REMAINING 614	Update Now	
	06:53:23 13-Nov-2018	Deep Scan Now	
		Run Cleanup Now	
		Full Scan Now	

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

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

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





Threat history information displays.

W	E DEVICE LOGS	Threat History			
#	Search	Q Search	From Date 2017-02-15	=	1 Showing 1 to 2 of 2 entries 10
			showing last 31 days		
6	Event Time	Infection	File Name		
Ŭ	1:11 13-Mar-2017				
	1:11 13-Mar-2017				

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

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



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

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



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





Integrated Alarm Parameters with Kaseya Alert Actions

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

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

≡	Q Search Navigation	Select Webroot Alerts Select the conditions for which you want to receive an alert	
	Webroot	Install Failed Edit details	
*	Main	Uninstall Failed Coll details ✓ Persistent Threat Edit details	
	Overview	Endpoint Status Failure Edit details	
	Deployment & Status Dashboard	Salect Alert Actions	
•	Configuration	Select the actions to take when an enabled alert occurs	
	Webroot Settings	Create Alarm	
	Alert Settings	Create Ticket	
£.,	Agent	Run Script after alert on the machine the alert occurred Select Agent Procedure	
1	Agent Procedures	V Clear	
AM	Anti-Malware	Send Email	
AV	Antivirus	Email recipients (Comma separate multiple addresses)	
Шð	Audit		
Ð	Backup	Apply	
0	Cloud Backup		

The following alerts can be selected:

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

To set an alert:

1. From the Webroot menu, select Alerts Settings.





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

=	Q Search Navigation	Select Webroot Alerts
_	Staron nangation	Select the conditions for which you want to receive an alert
W	Webroot	Install Failed Edit details
	Main	Uninstall Failed Edit details
		Persistent Threat EOIT details
	Overview	Endpoint Status Failure Edit details
	Deployment & Status Dashboard	Colore Alant Actions
	Configuration	Select the actions to take when an enabled alort occurs
	Webroot Settings	
	Alert Settings	Create licket
80	Agent	Run Script after alert on the machine the alert occurred
	Agein	Select Agent Procedure
10	Agent Procedures	Clear Clear
AM	Anti-Malware	Send Email
AV	Antivirus	Email recipients (Comma separate multiple addresses)
	Audit	
шq	Addit	
Ð	Backup	Apply
Ø	Cloud Backup	

3. Click on Edit details.

Select Webroot Alerts Select the conditions for which you want to receive a						
Install Failed	Edit details					
Uninstall Failed	Edit details					
 Persistent Threat 	Edit details					
Endpoint Status Failure	Edit details					



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

Edit Ale	ert Details - Persistent Threat	×
Alert re	e-arm interval	
Enable a	dditional alerts of this type from an endpoint after 4 v hours.	
Alert Te	emplate	
Customiz	te the template for the alert.	
Alarm Su	mmary / Ticket Summary / Email Subject	
Active	Threats on <id></id>	
Alarm Me	essage / Ticket Note / Email Body	
Active Latest	Threats on <id> at <ts> (UTC). Threat: <wr-lt></wr-lt></ts></id>	11
Available	template parameters	
Key	Description	
<id></id>	endpoint on which event occured	
<ts></ts>	date/time (in UTC) at which	
<wr-lt></wr-lt>	alert is sent Webroot Latest Threat seen	
'D Res	store Defaults	

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

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

≡	Q Search Navigation	Select Webroot Alerts Select the conditions for which you want to receive an alert
W	Webroot _	Install Failed Edit details
•	Main	Uninstall Failed Edit details
	Overview	Endpoint Status Failure Edit details
	Deployment & Status Dashboard	Select Alert Actions
•	Configuration	Select the actions to take when an enabled alert occurs
	Webroot Settings	Create Alarm
	Alert Settings	Create Ticket
÷.	Agent	Select Agent Procedure
1	Agent Procedures	✓ O Clear
AM	Anti-Malware	Send Email
AV	Antivirus	Email recipients (Comma separate multiple addresses)
Шð	Audit	
Ð	Backup	Apply
	Cloud Backup	

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





Setting Up Kaseya Emails and Ticketing

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

	General	Log	
Set-up lypes	🖸 Edit 📿 Test		
Server Management	Default Sender —		
Default Settings	Email:	Test @gmail.	l.com
License Manager			
Import Center			
System Log			
Logon Policy			
Outbound Email			

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

≡	Q Search Navigation	Edit				
		- Service Desk Activatio	on			
Ā	Service Desk	Activation of Service	se Desk causes Live Connect Monitoring and Alarms to integrate with service desk. These components use VSA			
•	Operations	ticketing when Service Desk is not activated. <u>More Info</u>				
	Tickets		Service Desk Activation			
	Organization Tickets					
	Tasks Associated With Tickets	Status: 🔀				
	Archived Tickets	- Service Desk Notes Co	Activate or Deactivate Service Desk and edit the color configuration across all service desks			
	Knowledge Base	Hidden Note Color:				
	Search All	System Note Color:	Activate Service Desk?			
	Deels Configuration	Task Note Color:				
_	Desk Comguration	Hidden Task Note Cold	C Color Configuration			
	Desk Definition	Normal Note Color:	Hidden Notes Color:			
*	Templates		System Notes Color:			
	Desk Templates		Task Notes Color:			
	Note Templates		Hidden Task Notes Color:			
	Massada Tamplatas		Normal Notes Color:			
	Pressage remplates					
•	Common Configuration					
	Global Settings		Save			



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

=	Q Search Navigation	🕒 New 📝 Edit 🔎 Ren	ame 🚫 Delete 🗹 Set Default 🖆 Import 🖻 Export	
_		[4 4 0 of 0 ▶ ▶]	I 100 💌	
Ă	Service Desk	Default Prefix Id	Description Editing Template	Definition Ter
•	Operations	No records found.	Add Service Desk Definition	
-	Desk Configuration			
	Desk Definition	(Service Desk Definitions determine how tickets are managed and tracked. When	
^	Templates	4	created, tickets are populated with attributes, values and requirements from a service desk definition. To help you get started quickly, new service desk definitions	
	Desk Templates	Selected: 0 Viewing: 0	are created by copying them from one of the templates, each configured to support a typical service desk business process.	·
	Note Templates	No Records Selected		
	Message Templates		Definition Template*:	
^	Common Configuration		Name#	- I
	Global Settings		Description:	
	Role Preferences		Prefix*:	_
	User Preferences		Editing Template*:	
	Incoming Email and Alarm		Desk Administrator*:	
	Procedure Variables		Show Incident Notes Pane?	
	Policies		Email:	
	Coverage Schedules			
	Holidays		Save	cel

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



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

-	O Search Navigation	Machine ID: Q Apply Machine Group: < All Groups > View: < No View > V Machine Group: All Groups > View: < No View > View
=	Search wavigation	Go to: < Select Page > ∨ ≤ > Show 10 ∨ 26 machines
4	Ticketing	Open Tickets: 130 Sort: O ascending Automatically submit on field changes Submit
	Manage Tickets	Past Due: 101 • descending Assignee: < All Assignee > <
	View Summany	Category: < All Category > <
1	view Sullimary	Status: < All Status > v
	Create/View	<pre>clastISearches> v SLATYpe: v</pre>
	Delete/Archive	Dispatch Tech < All Dispatch Tech >
	Migrate Tickets	Approval: < All Approval > V
	Configure Ticketing	Select All Mark All Read Set Field < < Select Page > V >> Merge. Change Highlight
	Notify Policy	JD Machine ID Assignee Category Status Priority SLA Type Dispatch Tech Approval Hours Worked Last Modified Date Creation Date Due Date
	Notity Policy	O Active Threats on wadmins-machook-prozool.brada-rop01 O 0.010/0 am 5 km 10, 010/0 am 5 km 1
	Access Policy	UV waaminacookingoo uuda aa a
	Assignee Policy	636 vrathwln2505.root.brada-or unassigned Application problem 🖵 Open High None No Not required 0.0 9/02:48 am 5-Jun-19 9/0
	Due Date Policy	Active Threats on wrathwinz506.root.brede-org01
	Edit Fields	G 55 wrathwinz506.root.brada-or unassigned Application problem Q Open High None No Not required 0.0 1:08:14 am 5-Jun-19 1:08:14 am 5-Jun-19 1:08:14 am 12-Jun
	Email Peader	P → V Active Threats on wadmins-matchade.prov root burdes-provided a standard or the standard
	Linar Reader	🔍 🔲 😡 Collection of data on vrathwinz505 root brade-org01 is not working
	Email Mapping	- 633 vrathwinz505.root.brada-or unassigned Application problem 😡 Open High None No Not required 0.012:02:12 am 5-Jun-19 12:02:12 am 5-Jun-19 12:02
÷	Agent	🚡 📃 🔍 Active Threats on wadmins-macbook-pro root. brada-org01
	Agent Procedures	652 wadmins-macbook-pro-root unassigned Application problem Uppen High None No Not required 0.0 4:10:39 pm 4-Jun-19 4:10:39 pm 4-Jun-19 4:10:39 pm 1-Jun
AM	Anti-Malware	Active Intension Intension Intension Intension Protocol (1) Control (1) Contro
	Antilian	🚬 🗖 🜑 Collection of data on ynsthwinz505 root. brade-org01 is not working
~	Antivirus	G30 vrathwlnz505.root.brada-or unassigned Application problem D Open High None No Not required 0.0 3:02:38 pm 4-Jun-19 3:02:38 pm 4-Jun-19 3:02:38 pm 1-Jun
Шă	Audit	Control Threats on wadmins-machook-pro: root.brade-org01
Ð	Backup	
0	Cloud Backup	628 vraftwinz506.root.brada-or unassigned Application problem 😡 Open High None No Not required 0.0 7.07.54 am 4-Jun-19 7.07.54 am 4-Jun-19 7.07.54 am 11-Jun



Disclaimer

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

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