WEBROOT®

Info Center Reporter Version 1.0 Getting Started Guide

Document Version 1.2.8

Table of Contents

Overview

The Webroot Kaseya Info Center Reporter is designed to increase Webroot reporting inside the Kaseya Info Center. The tool will only work with the Kaseya On-Premise VSA, while using the Webroot Kaseya On-Premise Module.

The Kaseya Info Center offers powerful reporting including scheduled reports, customized templates, and customized graphing tools.

The Webroot Info Center Reporter is designed to bring data points from the Webroot Module into the Info Center allowing reports to be generated using the Machine Filters. It's intuitive to use, 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 version 9.5 and up.

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

Prerequisites

- This guide.
- All of the following:
  - RDP and Administrator access to the On-Premise VSA host server
  - Webroot On-Premise Module
  - Kaseya On-Premise VSA
  - Webroot GSM account

    Note: If you are a first-time Webroot user, please complete your GSM account setup before going any further. For more information, see Creating Webroot Accounts.
- The latest installation files are available here.

Report Parts

This is a list of the Report Parts from the Webroot On-Premise Module. This data will be joined with the Kaseya On-Premise VSA Data allowing reports to be generated using the Machine Filters within Info Center Reports.

Client Status

This report part will include data in the Webroot.ClientStatus database table. It will be combined with the Kaseya agent data. Below is the Column description of the Webroot Client Status Data Set.

Name	Description
Active Threats	Current count of active threats
agentGuid	A globally unique identifier for a Machine Id.Group Id account and its corresponding agent
Attention Required	Attention is required on endpoint. Usually triggered after 24-36 hours of persistent threat
Blocked URLs	Number of blocked URLs
Computer Name	Name of the Computer
Current User	Current User that is logged onto the machine
Days Remaining	Days before license expires
Expiration Date	Webroot Client expiration date
Firewall Enabled	Is Firewall enabled
Group Name	Name of the agents org and group
ID Shield Enabled	Is ID Shield enabled
Infected?	Is currently infected
Internal IP	Internal IP Address
Is Expired	Is the Webroot Client license expired
Just Infected	Was just infected, set to 1 until next scan cycle.
Last Deep Scan	Last deep scan date time
Last Deep Scan Duration	Last deep scan duration in seconds
Last Logged On User	Last Logged On User on the machine
Last Scan	Last Scan date time
Last Scan Count	Count of last scans
Last Scan Duration	Last Scan time in seconds
Latest Threat	Description of latest threat
Machine Id	Machine Id used throughout the system
Offline Shield Enabled	Is Offline Shield enabled
Operating System	Operating System of the agent
OS Information	OS Information including Edition/Build/Service Pack
Phishing Shield Enabled	Is Phishing Shield enabled
Protection Enabled	Is protection enabled
Remediation Enabled	Is Remediation enabled
Reverse Group Name	Name of the agents org and group in reverse order
Root Kit Shield Enabled	Is Root Kit Shield enabled
Scan Count	Total count of scans
Scheduled Scan Time	Time schedule scan to run
Scheduled Scans Enabled	Is Scheduled Scans enabled
Threat Blocked	Current threat blocked
Threats Removed	Count of threats removed
Update Time	Timestamp of when Webroot Client last updated
USB Shield Enabled	Is USB Shield enabled
Version	Version of Webroot Client
Web Threat Shield	Is Web Threat Shield enabled

Threat Info

This report part will include data in the Webroot.ThreatHistory database table. It will be combined with the Kaseya agent data. Below is the Column description of the Webroot Threat Info Data Set.

Name	Description
agentGuid	A globally unique identifier for a Machine Id.Group Id account and its corresponding agent
Computer Name	Name of the Computer
Current User	Current User that is logged onto the machine
Event Date	Date and time of infection
File Name	File Name
Group Name	Name of the agents org and group
Infection	Infection description
Last Logged On User	Last Logged On User on the machine
Machine Id	Machine Id used throughout the system
Operating System	Operating System of the agent
OS Information	OS Information including Edition/Build/Service Pack
Reverse Group Name	Name of the agents org and group in reverse order

Name Value Parts

The following name value parts will include data from Webroot.ThreatHistory, Webroot.Clients, and Webroot.ClientStatus database tables. Each will provide and example of how to do an aggregation of data to display within a custom report. Click and edit the parts to see the SQL used to join the tables to get the results.

1. **Webroot – Active Threats**: Count the number of active threats on the selected agents.
2. **Webroot – Active Threats Removed:** Count of threats removed from selected agents.
3. **Webroot – Managed Agent Count**: Count of machines with Webroot Client installed.
4. **Webroot – unmanaged Agent Count:** Count of machines without Webroot Client installed.

Database Definitions

Database Column	Definition
Webroot.Clients.StatusId	• -2: Invalid Site Key Assigned • -1: No Site Key Assigned • 0: Not installed • 1: Installing • 2: Installed • 3: Install Failed • 4: Uninstall Failed • 5: Uninstalling • 11: Uninstalled • 12: Data Failure

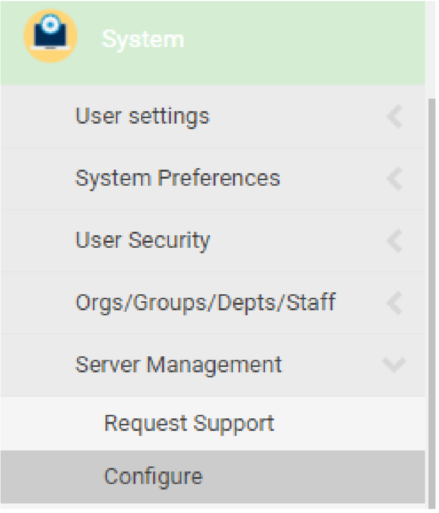
Installation

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

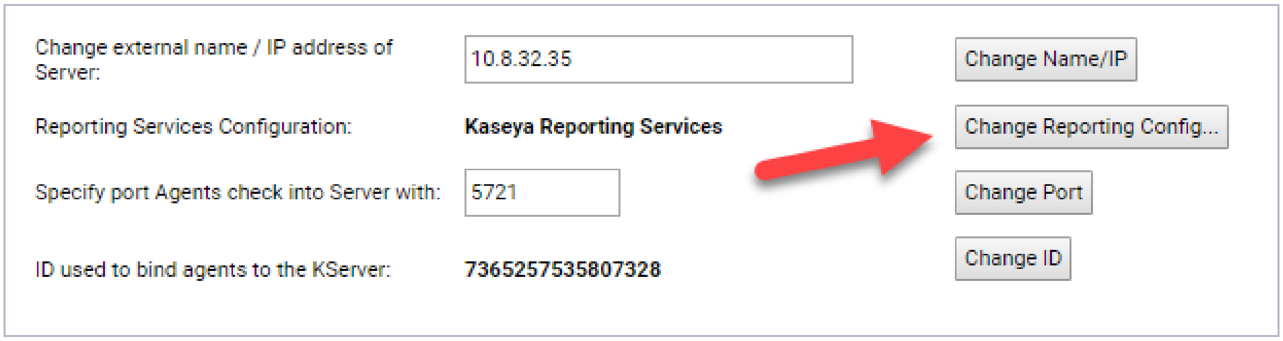
To install Webroot Kaseya Info Center Reporter:

1. Download the Webroot Info Center Reporter here. You can also get the latest module from Kaseya AutomationExchange under Webroot Kaseya Info Center Reporter.
2. Move the Zip file to your Kaseya On-Prem Server.

   NOTE: Please ensure the downloaded file is named **Webroot-InfoCenterReports.V1.0.zip**
3. From your VSA host machine navigate to: C:\Kaseya\xml\Reporting\Custom\DataSetRegistration\1.
4. Extract and Copy the files from Webroot-InfoCenterReports.zip to C:\Kaseya\xml\Reporting\Custom\DataSetRegistration\1
   a. Webroot-ActiveThreatCount.xml
   b. Webroot-ClientStatus.xml
   c. Webroot-ManagedAgentsCount.xml
   d. Webroot-ThreatInfo.xml
   e. Webroot-ThreatsRemovedCount.xml
   f. Webroot-unManagedAgentsCount.xml
   g. **DO NOT COPY Webroot-ExecSummary.xml at this time**
5. Please navigate to your On-Prem VSA
6. Within Kaseya VSA navigate to **System - Server Management - Configure**.



7. Scroll to the bottom of this page and click **Change Reporting Config**



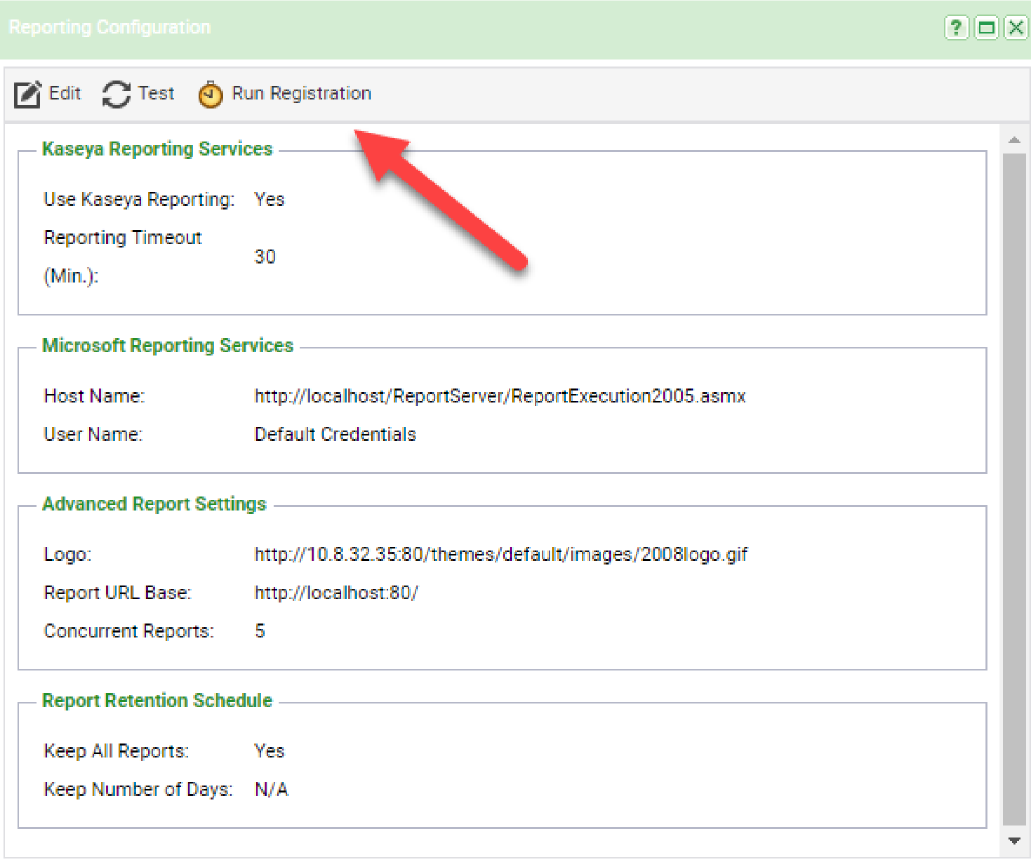
Change external name / IP address of Server: 10.8.32.35

Reporting Services Configuration: **Kaseya Reporting Services**

Specify port Agents check into Server with: 5721

ID used to bind agents to the KServer: **7365257535807328**

8. Click the **Run Registration**



Reporting Configuration

Kaseya Reporting Services

Use Kaseya Reporting: Yes

Reporting Timeout (Min.): 30

Microsoft Reporting Services

Host Name: http://localhost/ReportServer/ReportExecution2005.asmx

User Name: Default Credentials

Advanced Report Settings

Logo: http://10.8.32.35:80/themes/default/images/2008logo.gif

Report URL Base: http://localhost:80/

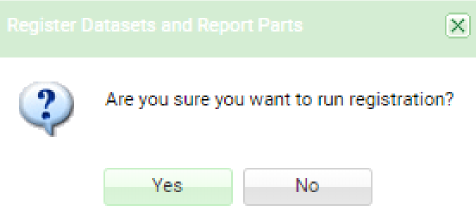
Concurrent Reports: 5

Report Retention Schedule

Keep All Reports: Yes

Keep Number of Days: N/A

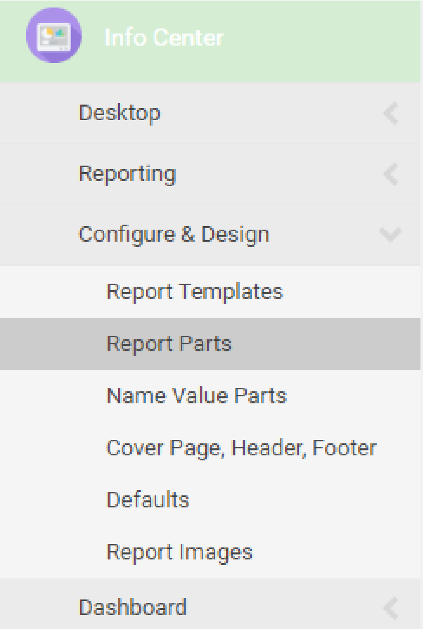
9. Click the **Yes**.

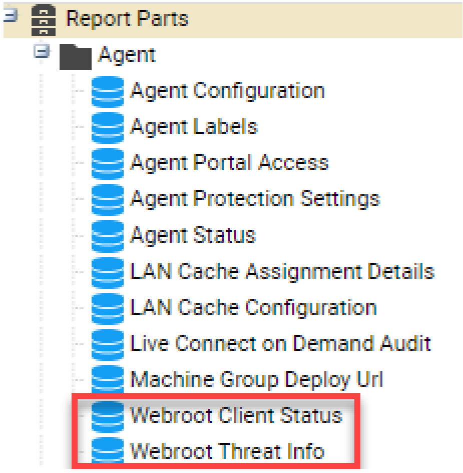


Register Datasets and Report Parts

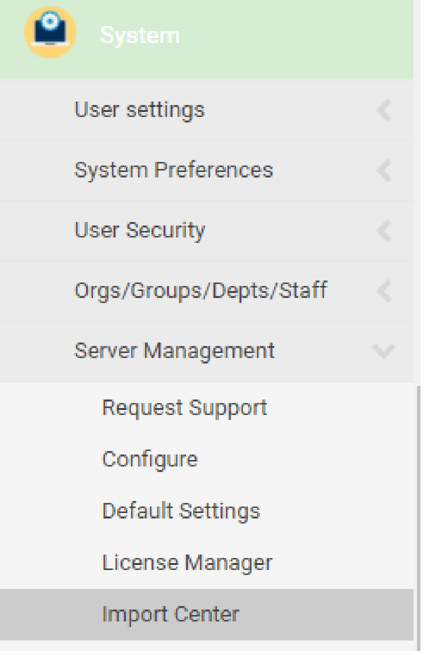
Are you sure you want to run registration?

10. Within the Kaseya VSA Navigate to **Info Center - Configure & Design - Report Parts**. You should see the two Webroot Report Parts under the Agents folder.

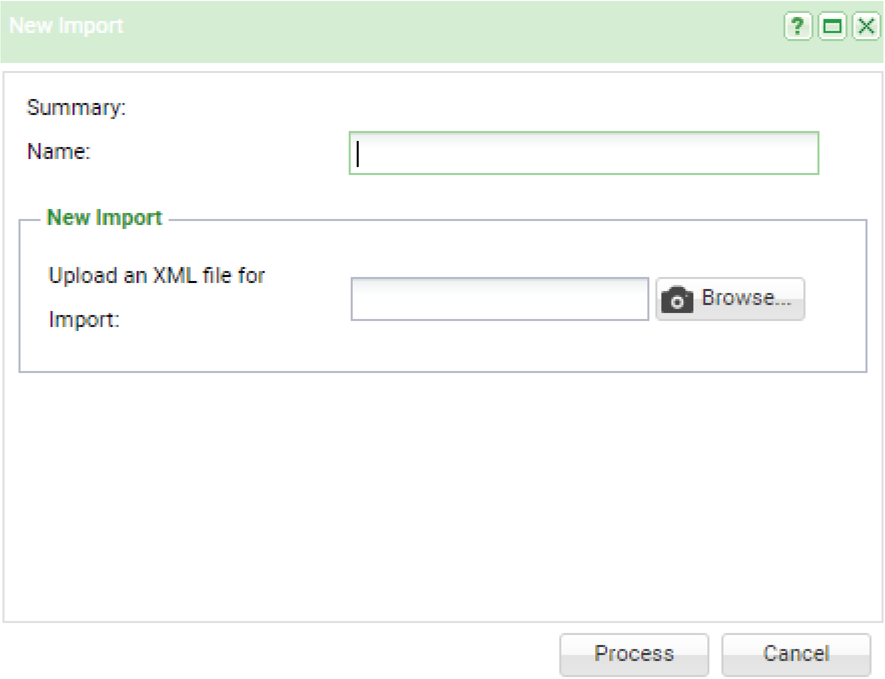




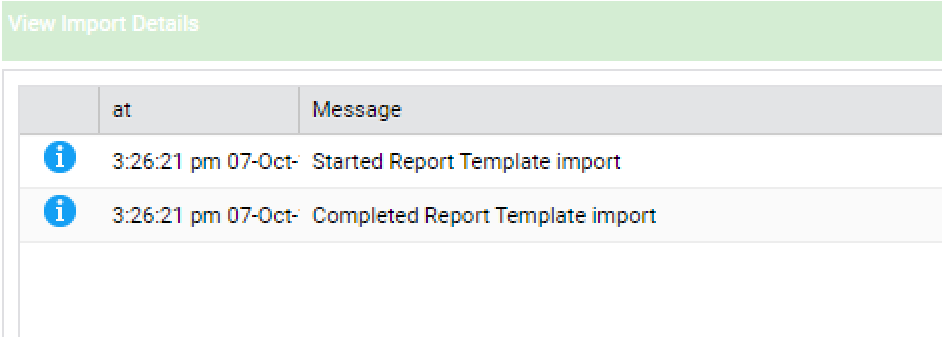
11. From the Kaseya VSA Navigate to **System - Server Management - Import Center**



12. Select **New Import**.

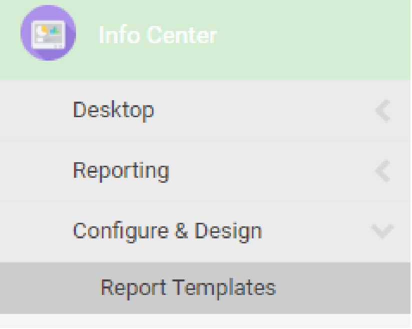


13. Name the new import "**Webroot Executive Summary**".
14. Then **Browse** to the file Webroot-ExecSummary.xml.
15. Click the **Process** button.
16. Once completed it will display in the Imports Grid. Click **View Import Details** to make sure it worked.

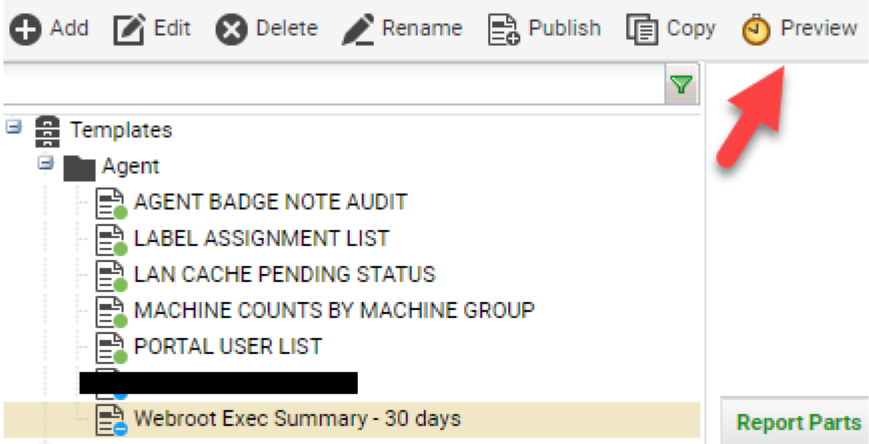

View Import Details

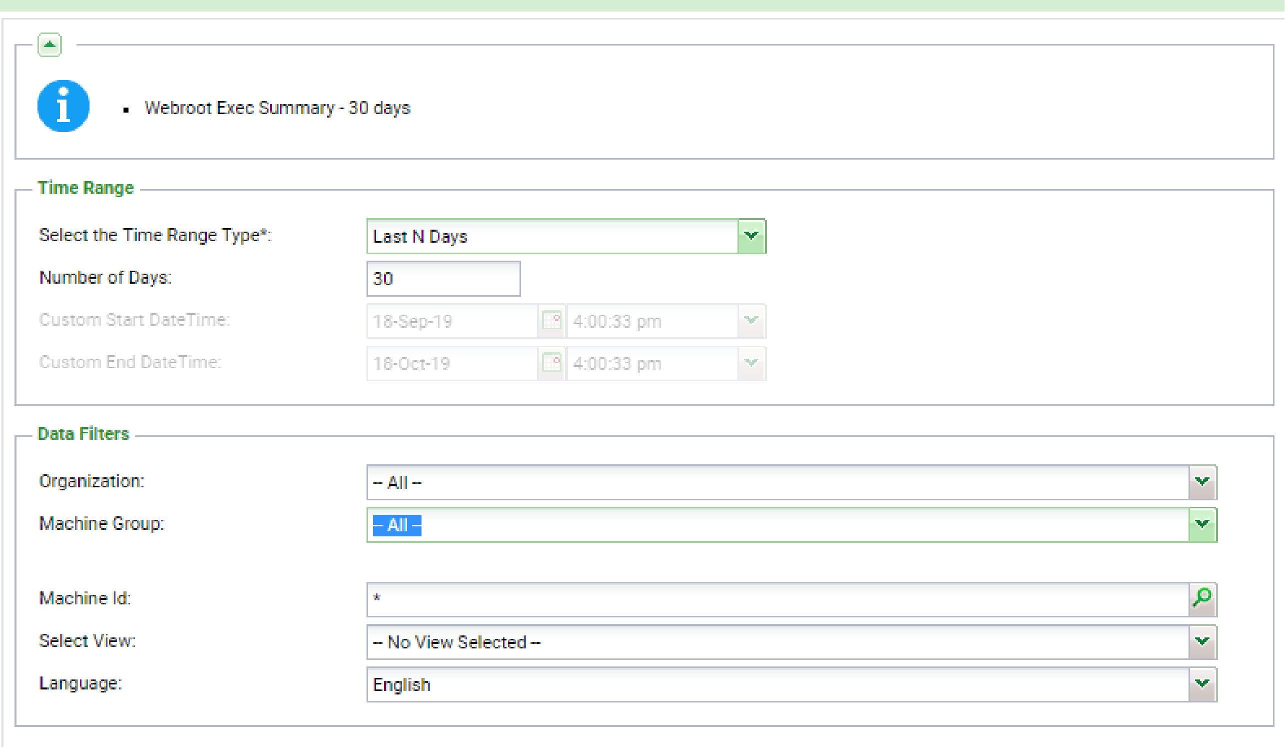
	at	Message
ℹ	3:26:21 pm 07-Oct-	Started Report Template import
ℹ	3:26:21 pm 07-Oct-	Completed Report Template import

17. Close this window then navigate to **Info Center - Configure & Design - Report Templates**.



18. Under Agent folder you will find **Webroot Exec Summary**.
19. Select the **report** and click the **Preview** button.





- Webroot Exec Summary - 30 days

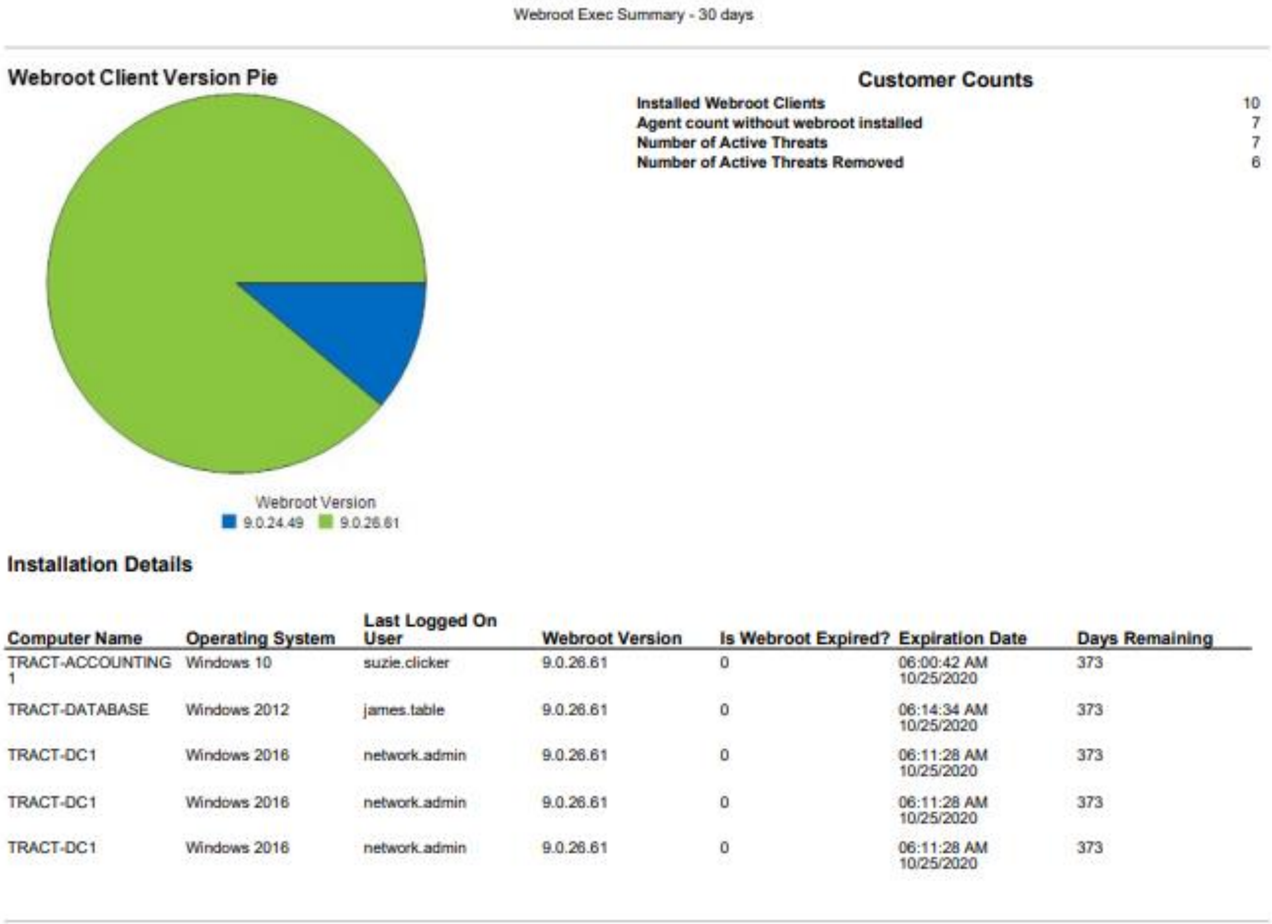
Time Range

Select the Time Range Type*:	Last N Days
Number of Days:	30
Custom Start DateTime:	18-Sep-19 4:00:33 pm
Custom End DateTime:	18-Oct-19 4:00:33 pm

Data Filters

Organization:	-- All --
Machine Group:	-- All --
Machine Id:	*
Select View:	-- No View Selected --
Language:	English

20. Report is generated for all orgs, groups, and last 30 days of threats. Example below.



Webroot Exec Summary - 30 days

Webroot Client Version Pie

Customer Counts

Installed Webroot Clients	10
Agent count without webroot installed	7
Number of Active Threats	7
Number of Active Threats Removed	6

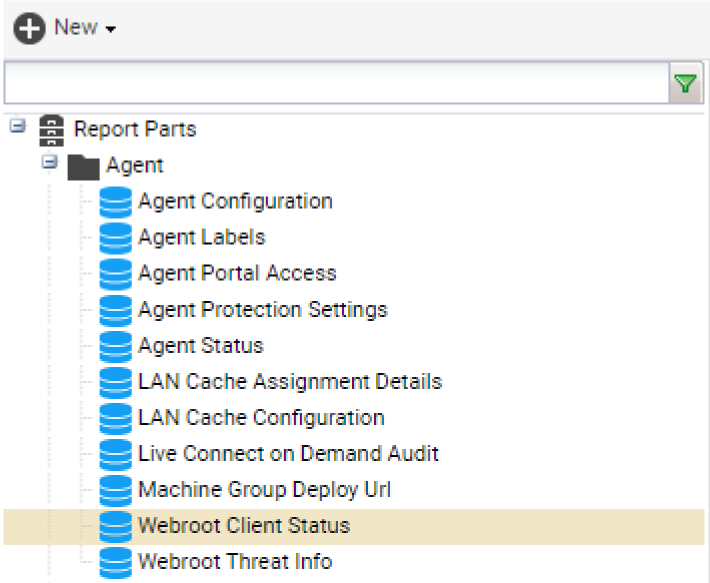
Installation Details

Computer Name	Operating System	Last Logged On User	Webroot Version	Is Webroot Expired?	Expiration Date	Days Remaining
TRACT-ACCOUNTING1	Windows 10	suzie.clicker	9.0.26.61	0	06:00:42 AM 10/25/2020	373
TRACT-DATABASE	Windows 2012	james.table	9.0.26.61	0	06:14:34 AM 10/25/2020	373
TRACT-DC1	Windows 2016	network.admin	9.0.26.61	0	06:11:28 AM 10/25/2020	373
TRACT-DC1	Windows 2016	network.admin	9.0.26.61	0	06:11:28 AM 10/25/2020	373
TRACT-DC1	Windows 2016	network.admin	9.0.26.61	0	06:11:28 AM 10/25/2020	373

Report Generation

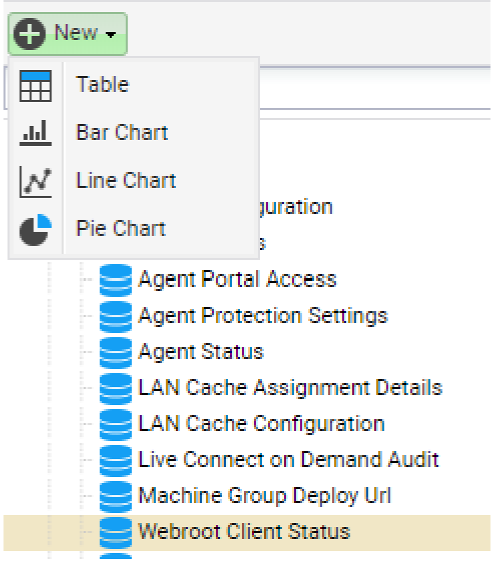
Administrators can create reports many ways. Please review the Kaseya Documentation on Custom Reports. Below are some examples of how to create your own custom reports with Webroot data.

1. Navigate to Info Center – Configure & Design – Report Parts
2. Under Report Parts – Agent. Listed you see Webroot Client Status – Webroot Threat Info



From this screen you can create new tables, bar charts, line charts or pie charts. As an example:

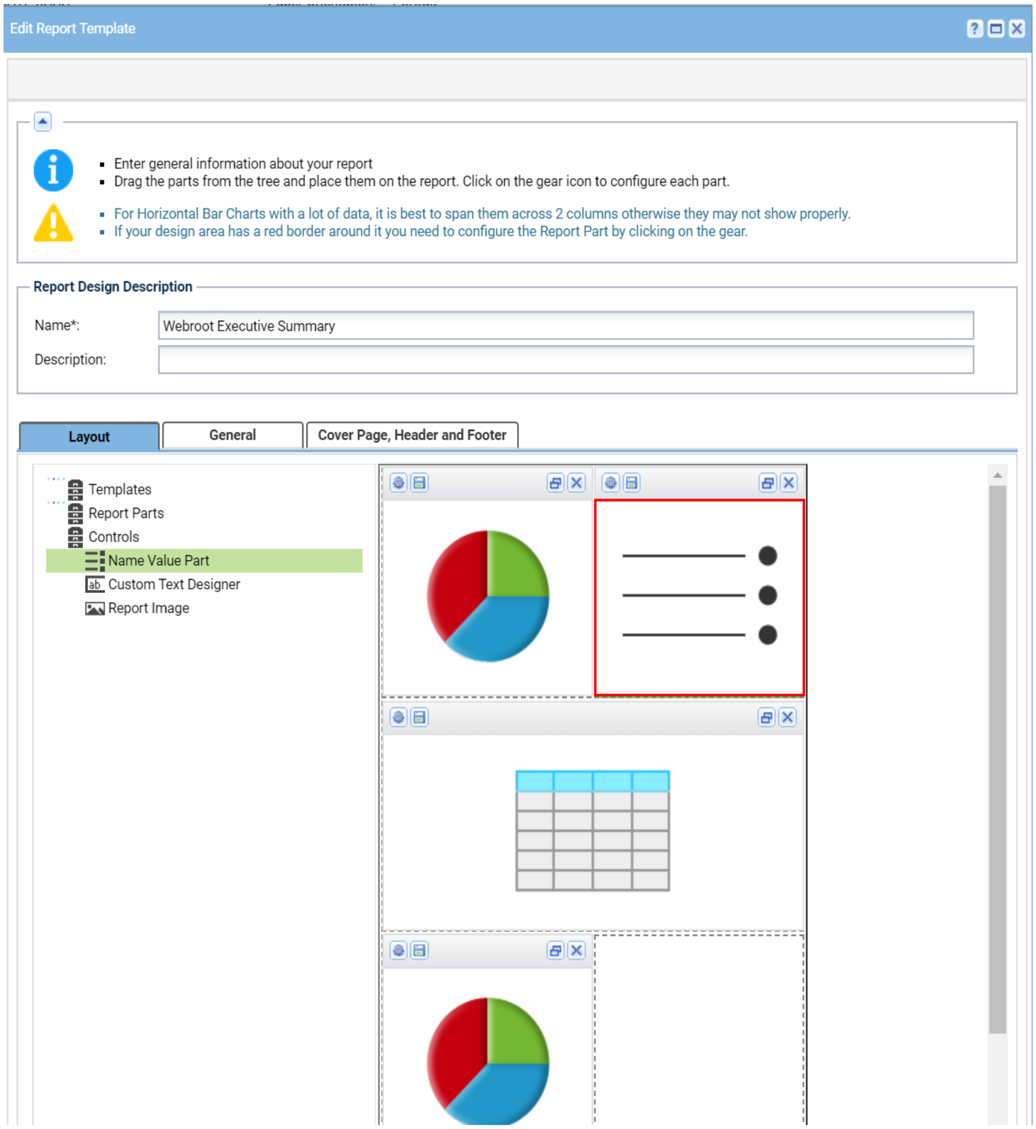
3. Click Webroot Client Status
4. Then **New**



5. Pick the type you would like to create using the tables that have been imported

Adding parts to the Webroot Executive Summary Report. As an example, the following will add the "Customer Counts Part" to the existing Webroot Executive Summary Template:

1. Click Edit of the Webroot Executive Summary and add a Name Value Part by dragging it into the layout section. Once you have dropped it into a section the report should look like the following:



Edit Report Template

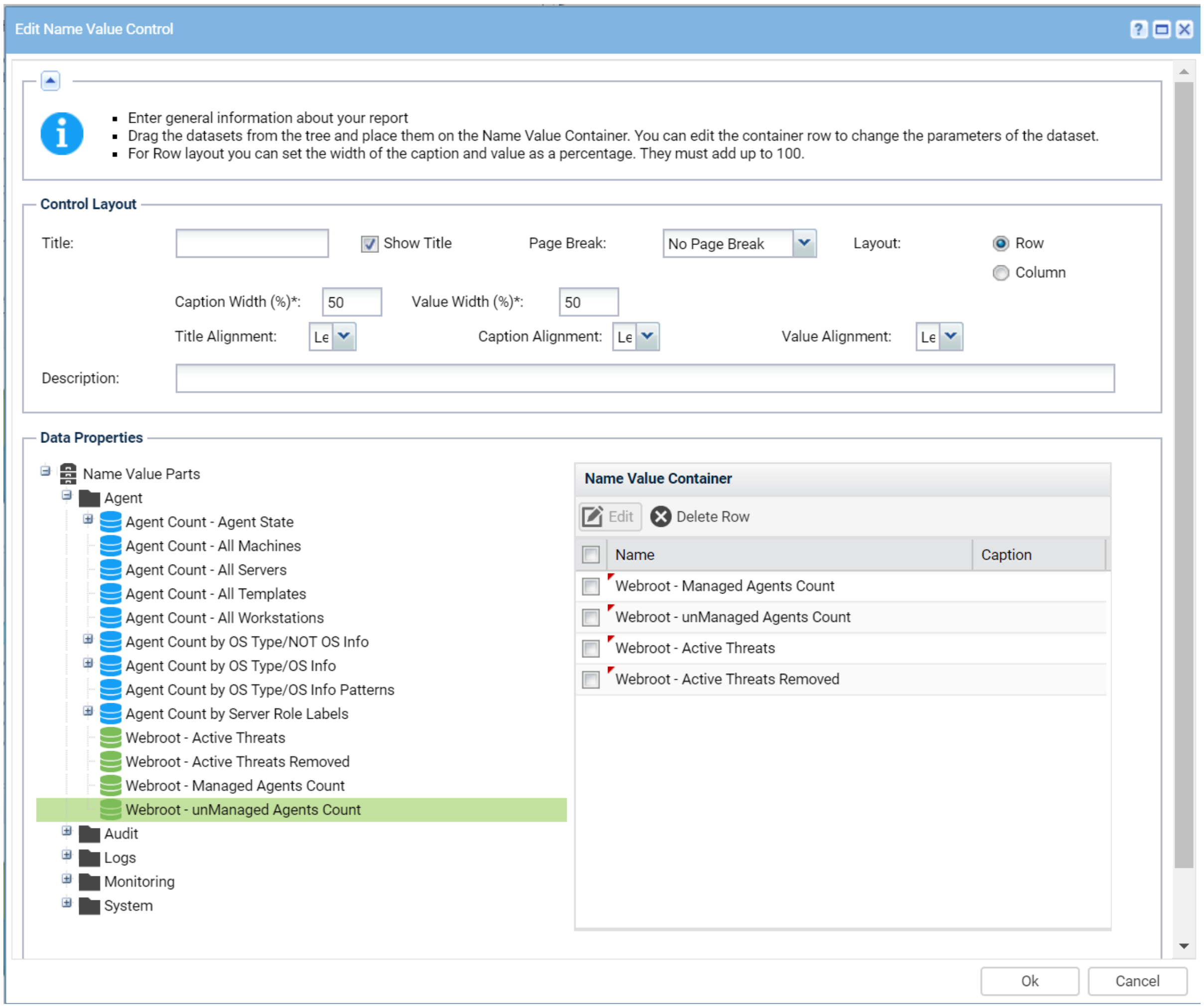
- Enter general information about your report
- Drag the parts from the tree and place them on the report. Click on the gear icon to configure each part.
- For Horizontal Bar Charts with a lot of data, it is best to span them across 2 columns otherwise they may not show properly.
- If your design area has a red border around it you need to configure the Report Part by clicking on the gear.

Report Design Description

Name*: Webroot Executive Summary

Description:

2. Next select the new part and click the gear icon in the toolbar to make changes to the content. Expand the agent folder and select each **Webroot Name Value Part** and drag into the **Name Value Container** and order.



Edit Name Value Control

- Enter general information about your report
- Drag the datasets from the tree and place them on the Name Value Container. You can edit the container row to change the parameters of the dataset.
- For Row layout you can set the width of the caption and value as a percentage. They must add up to 100.

Control Layout

Title: ☑ Show Title Page Break: No Page Break Layout: ● Row ○ Column

Caption Width (%)*: 50 Value Width (%)*: 50

Title Alignment: Le Caption Alignment: Le Value Alignment: Le

Description:

Data Properties

- Name Value Parts
  - Agent
    - Agent Count - Agent State
    - Agent Count - All Machines
    - Agent Count - All Servers
    - Agent Count - All Templates
    - Agent Count - All Workstations
    - Agent Count by OS Type/NOT OS Info
    - Agent Count by OS Type/OS Info
    - Agent Count by OS Type/OS Info Patterns
    - Agent Count by Server Role Labels
    - Webroot - Active Threats
    - Webroot - Active Threats Removed
    - Webroot - Managed Agents Count
    - Webroot - unManaged Agents Count
  - Audit
  - Logs
  - Monitoring
  - System

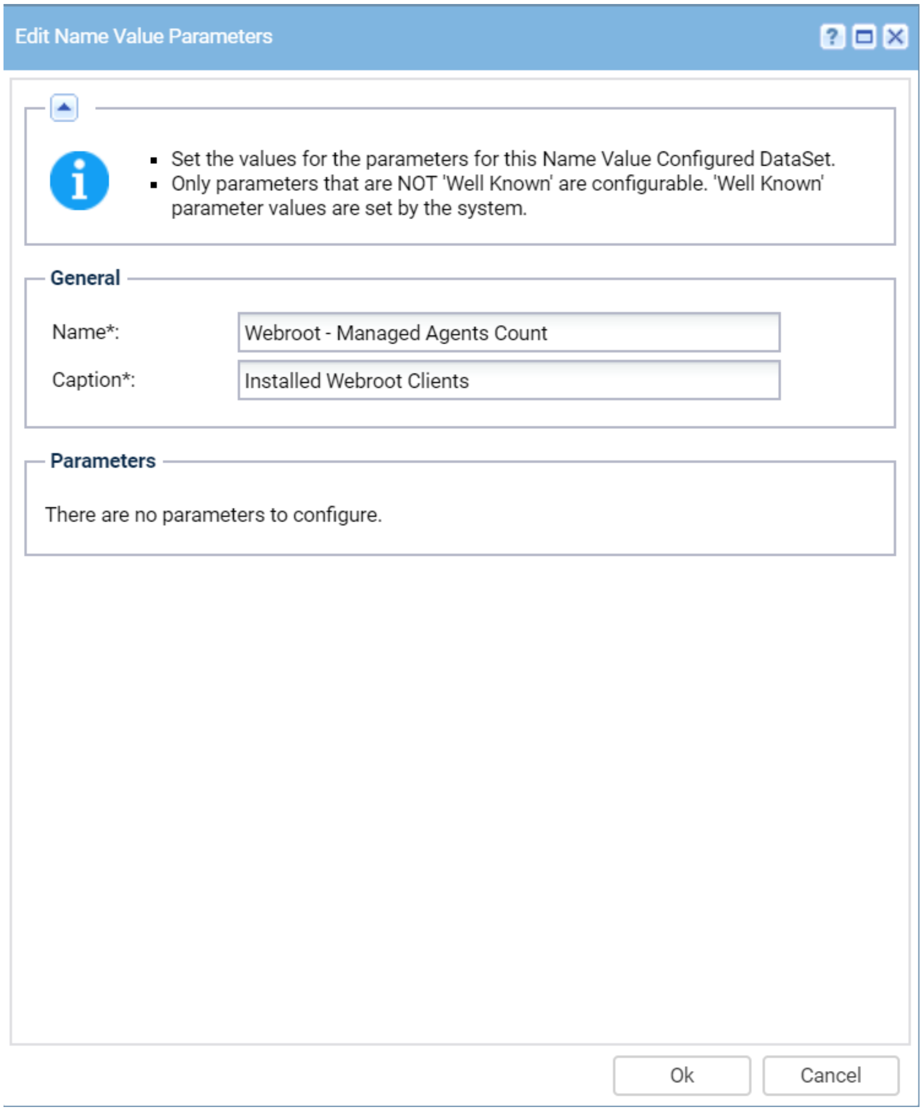
Name Value Container

Edit ⊗ Delete Row

□	Name	Caption
□	Webroot - Managed Agents Count	
□	Webroot - unManaged Agents Count	
□	Webroot - Active Threats	
□	Webroot - Active Threats Removed	

Ok Cancel

3. Click and edit each part within the container and give them an appropriate caption and Click "OK" to save each change:



- Set the values for the parameters for this Name Value Configured DataSet.
- Only parameters that are NOT 'Well Known' are configurable. 'Well Known' parameter values are set by the system.

General

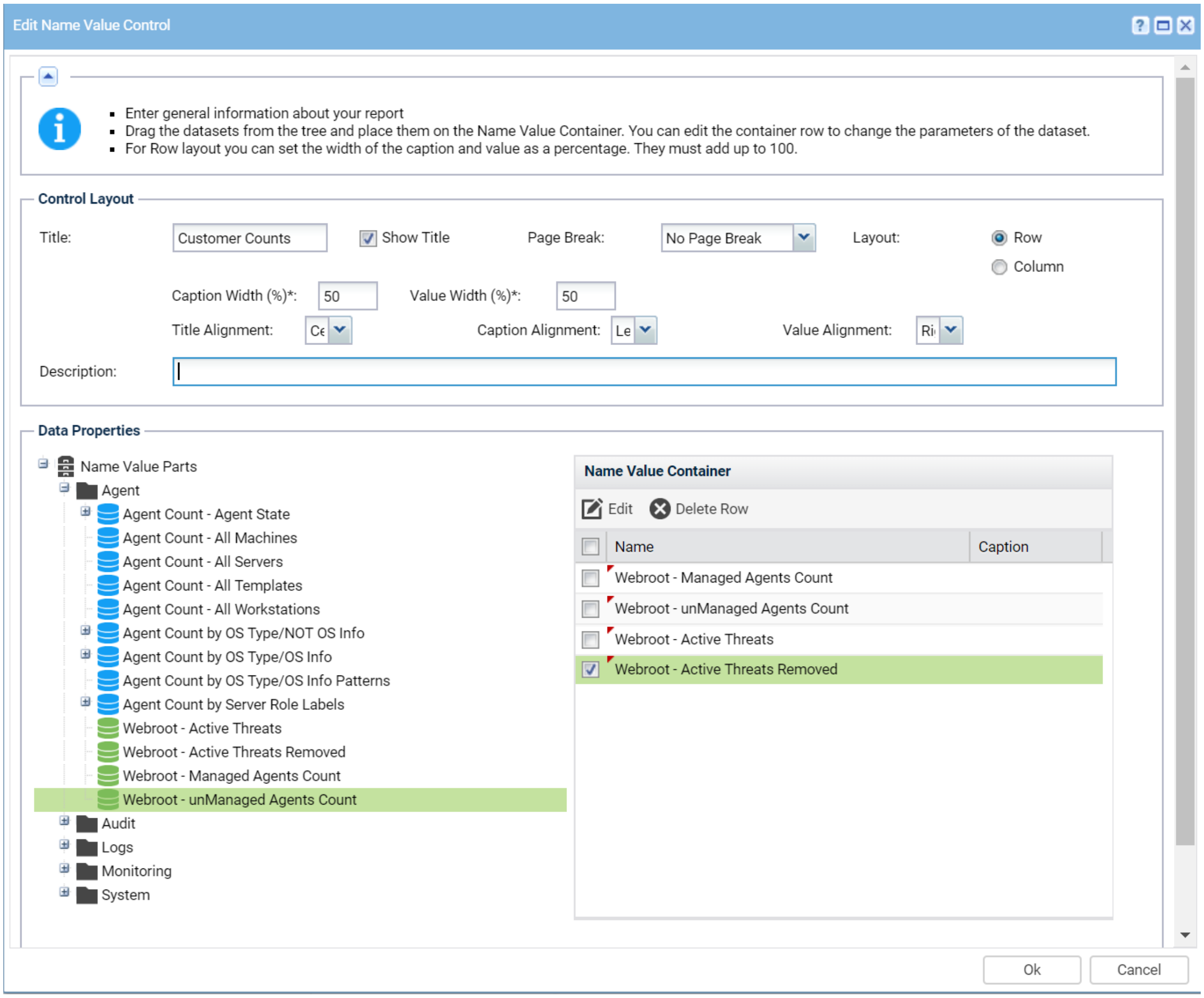
Name*: Webroot - Managed Agents Count

Caption*: Installed Webroot Clients

Parameters

There are no parameters to configure.

4. Finally update the Title and alignment and click **OK** to and **Save** the template.



Edit Name Value Control

- Enter general information about your report
- Drag the datasets from the tree and place them on the Name Value Container. You can edit the container row to change the parameters of the dataset.
- For Row layout you can set the width of the caption and value as a percentage. They must add up to 100.

Control Layout

Title: Customer Counts ☑ Show Title Page Break: No Page Break Layout: ● Row ○ Column

Caption Width (%)*: 50 Value Width (%)*: 50

Title Alignment: Ce Caption Alignment: Le Value Alignment: Ri

Description:

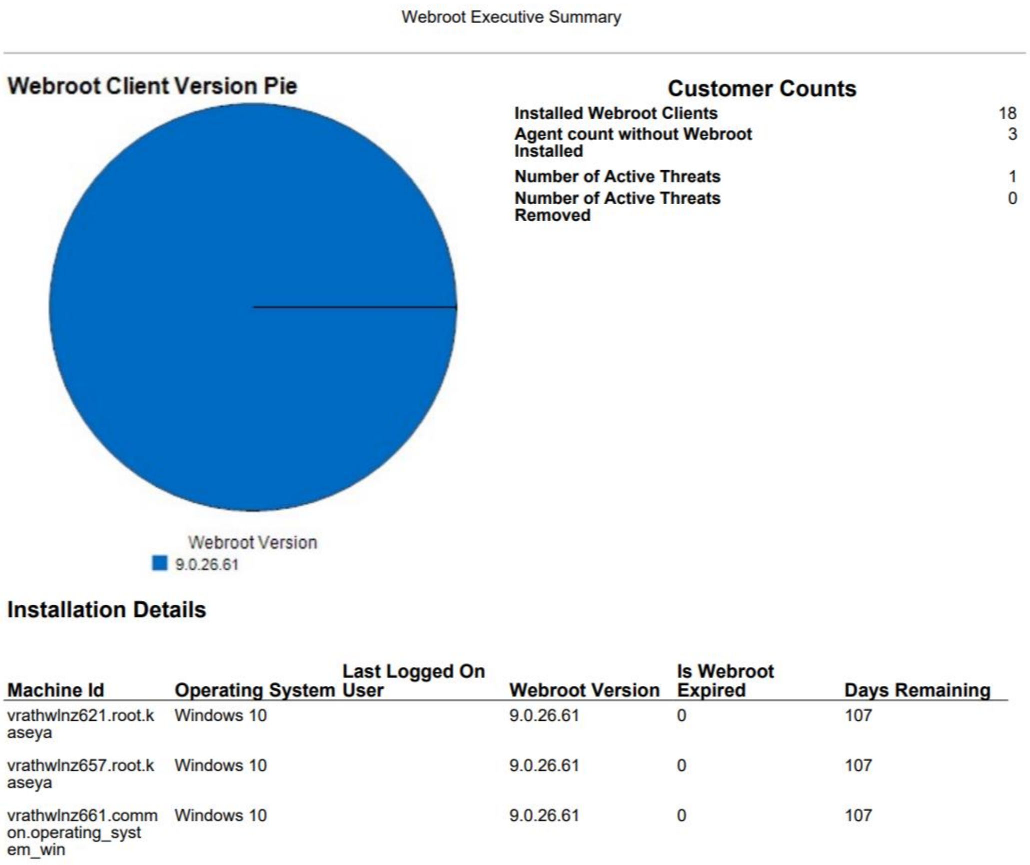
Data Properties

Name Value Parts
Agent
Agent Count - Agent State
Agent Count - All Machines
Agent Count - All Servers
Agent Count - All Templates
Agent Count - All Workstations
Agent Count by OS Type/NOT OS Info
Agent Count by OS Type/OS Info
Agent Count by OS Type/OS Info Patterns
Agent Count by Server Role Labels
Webroot - Active Threats
Webroot - Active Threats Removed
Webroot - Managed Agents Count
Webroot - unManaged Agents Count
Audit
Logs
Monitoring
System

Name Value Container

☐	Name	Caption
☐	Webroot - Managed Agents Count	
☐	Webroot - unManaged Agents Count	
☐	Webroot - Active Threats	
☑	Webroot - Active Threats Removed	

5. Run the preview of the template and the new part will be displayed:



Webroot Executive Summary

Webroot Client Version Pie

Customer Counts

Installed Webroot Clients	18
Agent count without Webroot Installed	3
Number of Active Threats	1
Number of Active Threats Removed	0

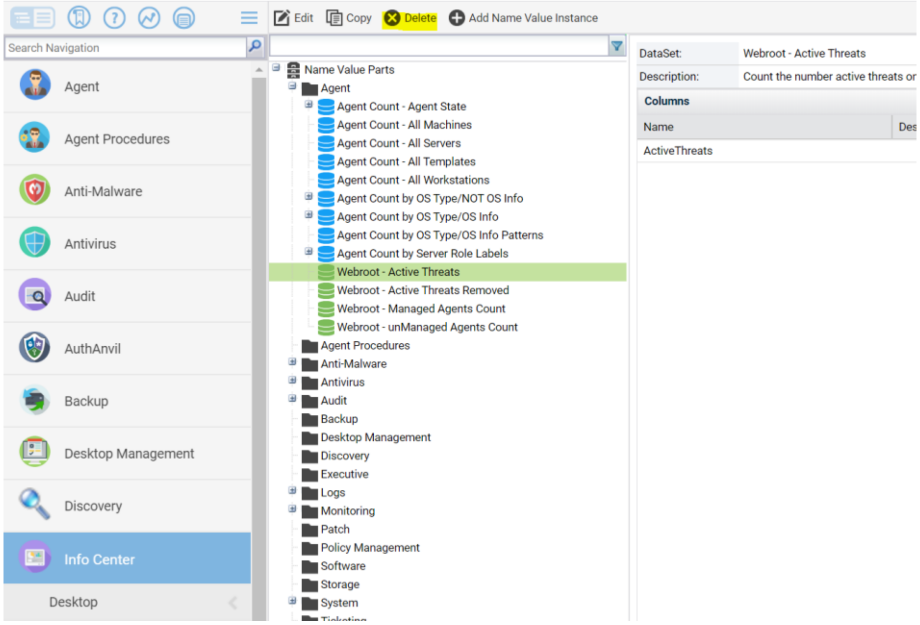
Installation Details

Machine Id	Operating System	Last Logged On User	Webroot Version	Is Webroot Expired	Days Remaining
vrathwlnz621.root.kaseya	Windows 10		9.0.26.61	0	107
vrathwlnz657.root.kaseya	Windows 10		9.0.26.61	0	107
vrathwlnz661.common.operating_system_win	Windows 10		9.0.26.61	0	107

Uninstall

If you need to uninstall the Webroot template please follow these steps:

1. Select the Webroot named value parts and click **Delete** on the top menu bar. This will remove the configuration and the files from your server.


Edit
Copy
Delete
Add Name Value Instance
Search Navigation
Agent
Agent Procedures
Anti-Malware
Antivirus
Audit
AuthAnvil
Backup
Desktop Management
Discovery
Info Center
Desktop
Name Value Parts
Agent
Agent Count - Agent State
Agent Count - All Machines
Agent Count - All Servers
Agent Count - All Templates
Agent Count - All Workstations
Agent Count by OS Type/NOT OS Info
Agent Count by OS Type/OS Info
Agent Count by OS Type/OS Info Patterns
Agent Count by Server Role Labels
Webroot - Active Threats
Webroot - Active Threats Removed
Webroot - Managed Agents Count
Webroot - unManaged Agents Count
Agent Procedures
Anti-Malware
Antivirus
Audit
Backup
Desktop Management
Discovery
Executive
Logs
Monitoring
Patch
Policy Management
Software
Storage
System

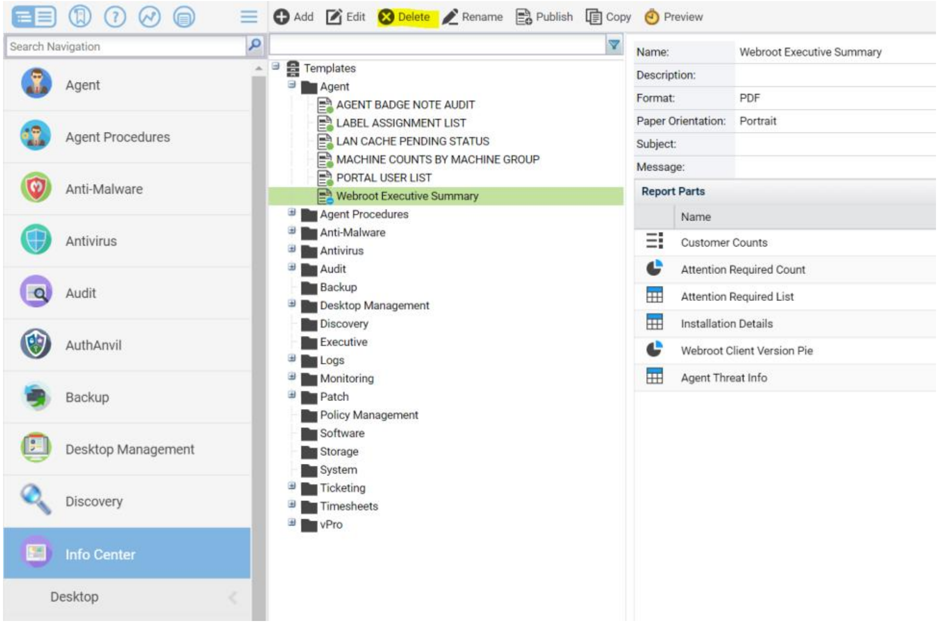
DataSet: Webroot - Active Threats

Description: Count the number active threats or

Columns

Name	Des
ActiveThreats	

2. Select the report template “Webroot Executive Summary”, then click delete.



Name: Webroot Executive Summary

Description:

Format: PDF

Paper Orientation: Portrait

Subject:

Message:

Report Parts

Name
Customer Counts
Attention Required Count
Attention Required List
Installation Details
Webroot Client Version Pie
Agent Threat Info

3. As of Kaseya v9.4 the ability to delete Report Parts is not available. Leaving the Webroot Report Parts does not negatively impact your Kaseya Info Center implementation.

Disclaimer

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

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