Integrate Webroot SecureAnywhere
EventTracker v9.x and above

Publication Date: June 19, 2019
Abstract

This guide helps you in configuring Webroot SecureAnywhere Business Endpoint Protection and DNS Protection with EventTracker to receive Webroot SecureAnywhere Business Endpoint Protection and DNS Protection events. In this guide, you will find the detailed procedures required for monitoring Webroot SecureAnywhere Business Endpoint Protection and DNS Protection.

NOTE:

Webroot Business Endpoint Protection and Webroot DNS Protection are two different subscriptions under Webroot SecureAnywhere. Check your subscriptions and continue with the integration accordingly.

Audience

Administrators who are assigned the task to monitor and manage Webroot SecureAnywhere Business Endpoint Protection and DNS Protection events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract .......................................................................................................................... 1  
Audience .......................................................................................................................... 1  
Overview .......................................................................................................................... 3  
Prerequisites .................................................................................................................... 3  
Obtaining Webroot SecureAnywhere Business Endpoint Protection and DNS Protection credentials .......... 3  
Integrating Webroot SecureAnywhere Business Endpoint Protection and DNS Protection to EventTracker ..... 6  

EventTracker Knowledge Pack .......................................................................................... 11  
Category ........................................................................................................................... 11  
Alerts ............................................................................................................................... 11  
Flex Reports .................................................................................................................... 11  

Importing Webroot SecureAnywhere Business Endpoint Protection and DNS Protection knowledge pack into EventTracker .................................................................................................................. 12  
Category ........................................................................................................................... 13  
Alerts ............................................................................................................................... 14  
Knowledge Object ............................................................................................................ 15  
Flex Report ....................................................................................................................... 16  
Dashboard .......................................................................................................................... 18  

Verifying Webroot SecureAnywhere Business Endpoint Protection and DNS Protection knowledge pack in EventTracker .................................................................................................................. 20  
Category ........................................................................................................................... 20  
Alerts ............................................................................................................................... 21  
Knowledge Object ............................................................................................................ 22  
Flex Report ....................................................................................................................... 23  
Sample Flex Dashboards ................................................................................................... 24
Overview

Webroot SecureAnywhere Business Endpoint Protection provides a multi-vector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never-before-seen threats that use blended strategies to deliver malicious payloads.

DNS Protection is a domain filtering service designed to provide more granular control over internet access. It extends our award-winning endpoint protection into the network to protect customers from malicious happening outside of the browser and enables category-based internet usage restrictions across the network. Configurable for the corporate, guest Wi-Fi, roaming users, and groups.

EventTracker knowledge pack for Webroot SecureAnywhere captures important and critical activities in Webroot Business Endpoint Protection and DNS Protection. Monitoring these activities is critical from a security aspect and necessary for compliance and operational reasons.

Prerequisites

- EventTracker v9.x should be installed.
- Webroot SecureAnywhere Business Endpoint Protection/DNS Protection should be installed.
- PowerShell version 5.0 and above should be installed.

Obtaining Webroot SecureAnywhere Business Endpoint Protection and DNS Protection credentials

To configure the Webroot application, you need to have the below field details available.

- Admin User Name
- Admin Password
- Client Secret
- Client ID
- Parent Keycode

1. To obtain the API details, you need to log in using the administrator account.
2. Go to the Settings tab and click new to create an API key.
3. Once the API key is created, a popup is displayed as shown below.

![Client Credential Record](image)

**Figure 1**

4. Make a note of the **Client Secret** and **Client ID**.

   **Note:** The **Client Secret** is not persisted in the console and it is your responsibility to remember the **Client Secret** and treat it as sensitive information.

5. Click on the **Account Settings** tab and choose the **Account Information** sub-tab to find the GSM code which will be given as Parent Keycode as highlighted in the below image.
NOTE: If you have configured **DNS Protection**, then make sure that the site you need to monitor has **SecureAnywhere DNS** enabled as shown below:
Integrating Webroot SecureAnywhere Business Endpoint Protection and DNS Protection to EventTracker

1. Download the WebrootIntegrator.exe on a system having EventTracker Agent.
2. Save WebrootIntegrator.exe and run the executable file “WebrootIntegrator.exe”.

3. Click on Browse and navigate to the EventTracker Agent folder and click Install.
4. This will launch the Webroot Integrator.

5. Enter the Client ID and Client Secret and Click Validate Credentials.
6. An authentication pop up window will appear asking for the administrator username and password of the GSM console, enter the same and click okay.
7. Click on **OK**.
8. If credentials are validated successfully you will receive a pop show below.

![Figure 8](image)

**Figure 8**

9. Click on **OK**.
10. Now, enter the GSM/Parent Keycode.

![Figure 10](image)

**Figure 10**
11. Select if you want to monitor all the sites or any specific sites.
   - If you wish to monitor all the sites.
     ▪ Select All Sites and click okay.
   - If you wish to monitor specific sites.
     ▪ Select Specific Sites and wait for the sites to be populated.
     ▪ Once the sites are populated select the sites you want to monitor and move them to the right panel and click Select Groups.

![Webroot Secure Anywhere Integrator](image)

**Figure 11**

12. This will get you the groups in the sites selected.
13. Select the group’s you want to monitor and move them to the right panel and OK.
14. You will get a pop up suggesting the successful integration.

![Figure 12](image)

![Figure 13](image)
Integrate Webroot SecureAnywhere EventTracker Knowledge Pack

Once logs are received into EventTracker, Alerts, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Windows.

**Category**

- **Webroot SA: Malware detection**: This category provides information related to all the malware that is detected by Webroot.
- **Webroot SA: DNS blocked traffic requests**: This category provides information related to all the blocked DNS traffic requests.

**Alerts**

- **Webroot SA: Threat detection**: This alert is generated when Webroot detects any malware or threats.

**Flex Reports**

- **Webroot SA-Malware detection**: This report provides details about any malware or threats that are detected by Webroot.

**Figure 14**

- **Webroot SA-DNS blocked traffic requests**: This report provides all the policy details that are present in the Webroot.

**Figure 15**
Integrate Webroot SecureAnywhere

Importing Webroot SecureAnywhere Business Endpoint Protection and DNS Protection knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Category
- Alerts
- Knowledge Objects
- Flex Reports

1. Launch the EventTracker Control Panel.
2. Double click Export Import Utility.

![EventTracker Control Panel](image)
3. Click the **Import** tab.

**Category**

1. Click the **Category** option, and then click the browse button.

![Image of Export Import Utility dialog box showing options and location for Category, with Import and Close buttons]

Figure 17

2. Locate **Category_Webroot.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays a success message.

![Image of Export Import Utility dialog box showing a success message: Selected category details are imported successfully.]

Figure 18

4. Click **OK**, and then click the **Close** button.
Alerts

1. Click the **Alert** option, and then click the **browse** button.

![Figure 19]

2. Locate **Alerts_Webroot.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
4. EventTracker displays a success message.

![Figure 20]

5. Click the **OK** button, and then click the **Close** button.
Knowledge Object

1. Click **Knowledge objects** under the **Admin** option in the EventTracker page.

![Figure 21](image1)

2. Click on the **Import** button as highlighted in the below image.

![Figure 22](image2)

3. Click on **Browse**.

![Figure 23](image3)
4. Locate the file named KO_Webroot.etko.
5. Now select all the checkbox and then click on the ‘Import’ option.

6. Knowledge objects are now imported successfully.

Flex Report
On EventTracker Control Panel,
1. Click Reports option and select new (etcrx) from the option.
2. Locate the file named `Reports_Webroot.etcrx` and select all the checkbox.
3. Click the **Import** button to import the reports. EventTracker displays a success message.

![Figure 28](image)

**Dashboard**

**NOTE** - Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and logon.
2. Navigate to **My Dashboard** option as shown above.
3. Click on the **Import** button as shown below.

4. Import dashboard file **Dashboard_Webroot.etwd** and checkbox the dashboards that you require and click on **Import** as shown below.
5. Import is now completed successfully.

![Selected dashlets imported successfully](image)

Figure 32

Verifying Webroot SecureAnywhere Business Endpoint Protection and DNS Protection knowledge pack in EventTracker

Category

1. Logon to EventTracker.
2. Click Admin dropdown, and then click Categories.

![EventTracker dashboard](image)

Figure 33

3. In Category Tree to view imported categories, scroll down and expand Webroot Secure Anywhere group folder to view the imported categories.
Alerts

1. Logon to EventTracker.
2. Click the Admin menu, and then click Alerts.

3. In the Search box, type 'Webroot', and then click the Go button. Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays a message box.

   ![Successfully saved configuration](image)

   **Figure 37**

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:** Specify appropriate systems in an alert configuration for better performance.

### Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.

   ![EventTracker interface](image)

   **Figure 38**

2. In the Knowledge Object tree, expand the **Webroot Business** group folder to view the imported Knowledge objects.
**Flex Report**

1. In the EventTracker web interface, click the **Reports** menu, and then select the **Report Configuration**.
2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Webroot** group folder to view the imported Webroot reports.

![Customize dashlets](image)

![Add Delete Close](image)

**Sample Flex Dashboards**

- **Webroot – Blocked DNS traffic by sites**

![Sample Flex Dashboard](image)
• **Webroot – Top DNS requests blocked category by Sitename**

![Webroot Top DNS requests blocked category by Sitename](image)

*Figure 43*

• **Webroot – Threats detected by sites**

![Webroot - Threats detected by sites](image)

*Figure 44*