Netsurion™ | EventTracker

How to – Configure Webroot SecureAnywhere to forward logs to EventTracker

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.

Table of Contents

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.

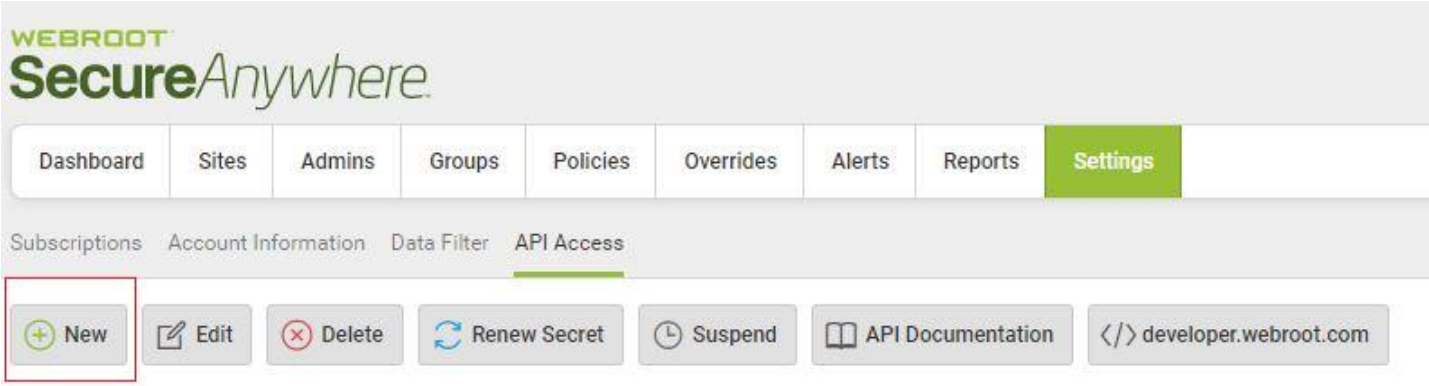

Figure 1

3. Once the API key is created, a popup is displayed as shown below.

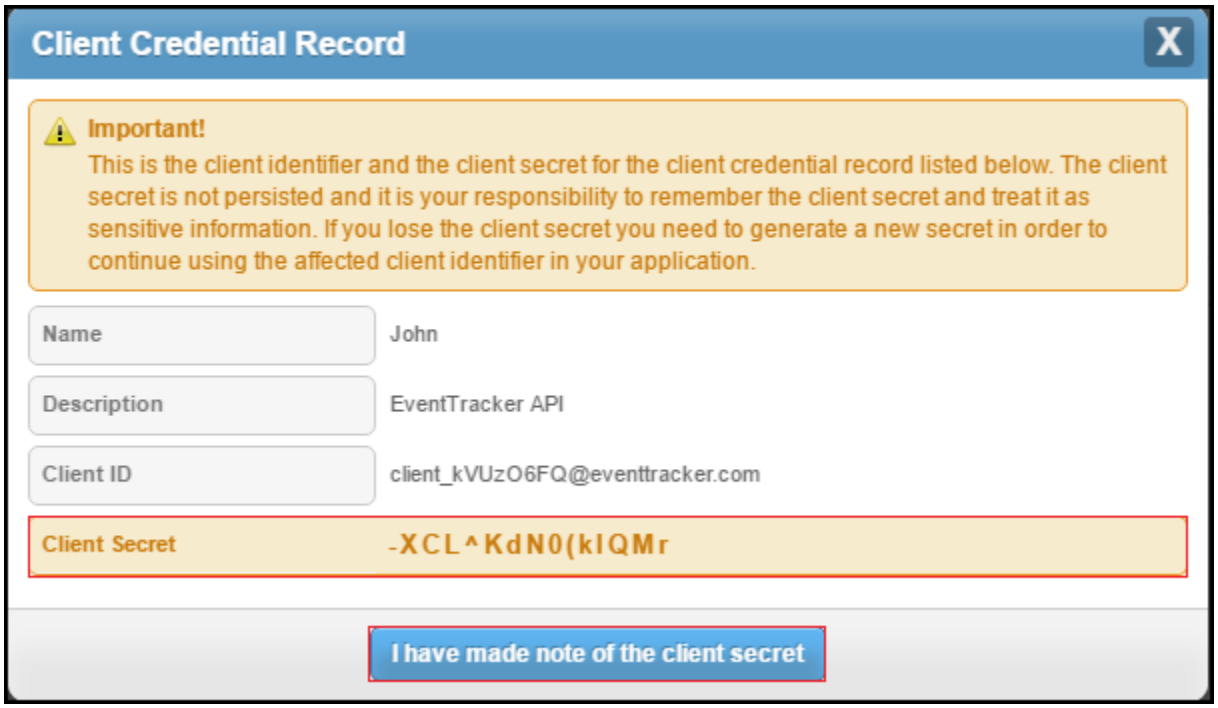

Figure 2

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.

Figure 3

NOTE: If you have configured **DNS Protection,** then make sure that the site you need to monitor has **SecureAnywhere DNS** enabled as shown below:

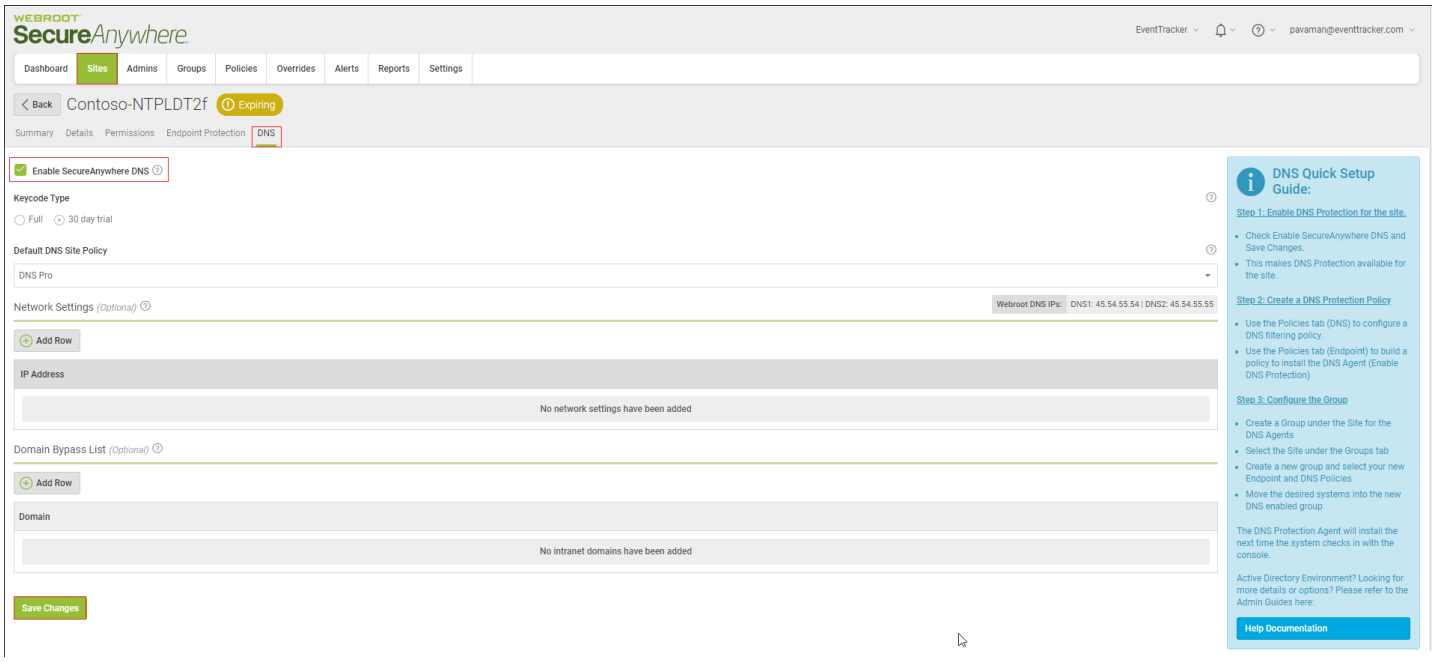

Figure 4

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".

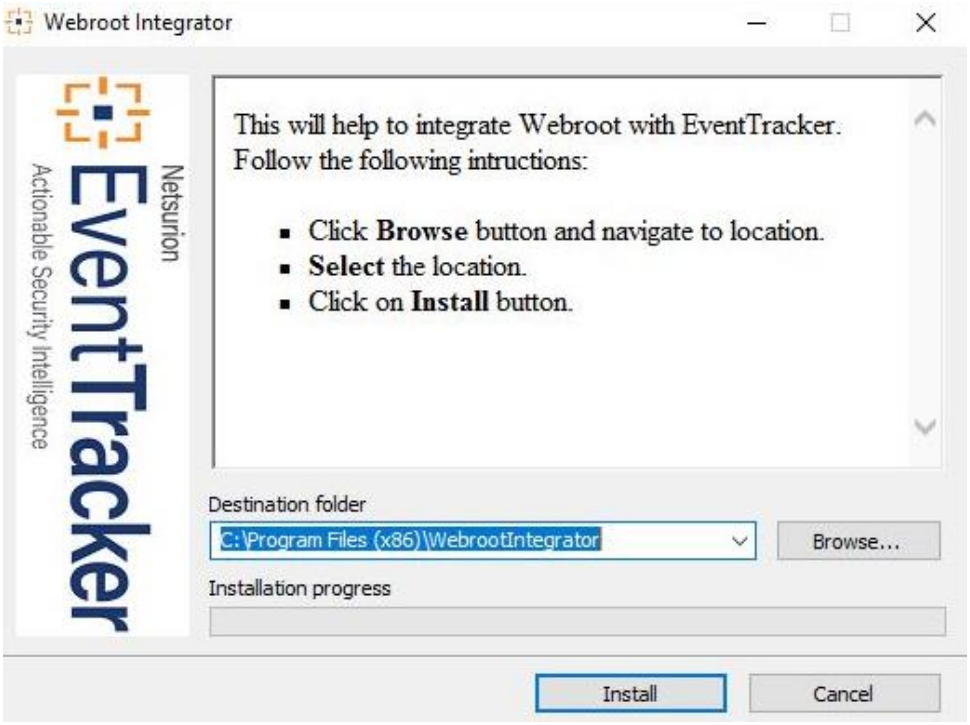

Figure 5

3. Click on **Browse** and navigate to the EventTracker Agent folder and click **Install**.

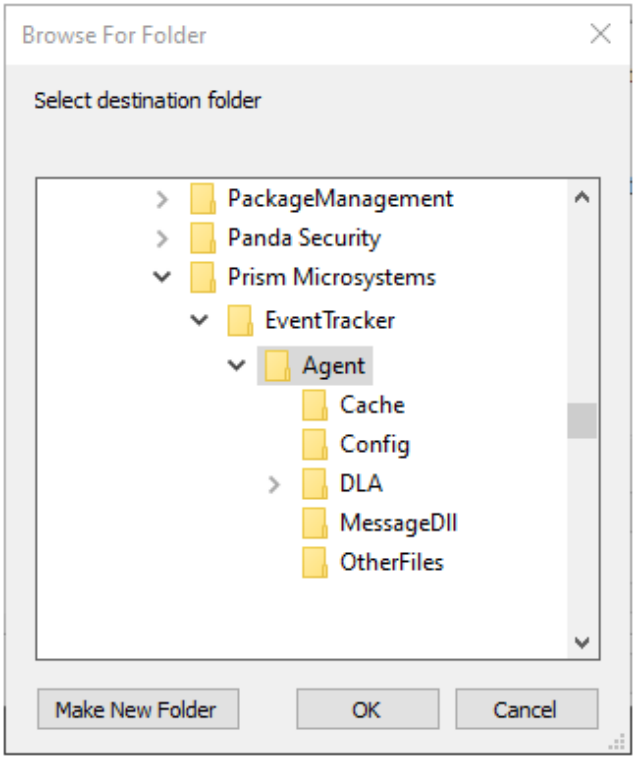

Figure 6

4. This will launch the Webroot Integrator.

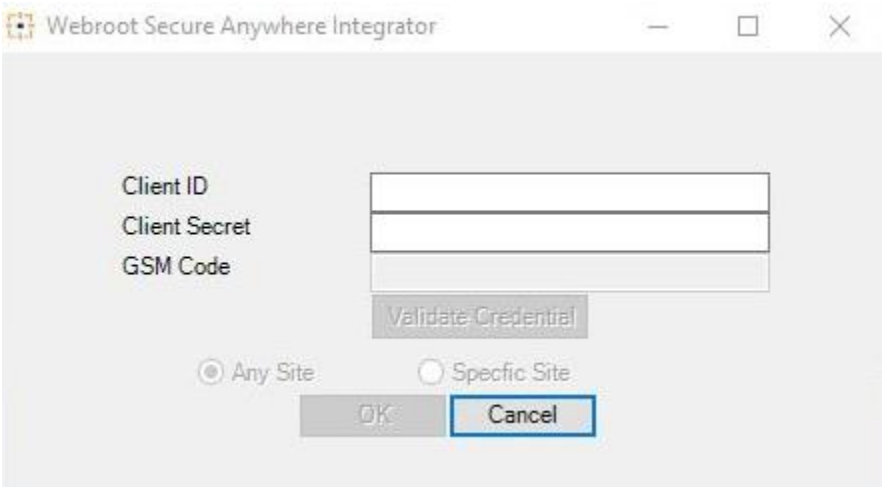

Figure 7

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.

Figure 8

7. Click on **OK**.
8. If credentials are validated successfully you will receive a pop show below.

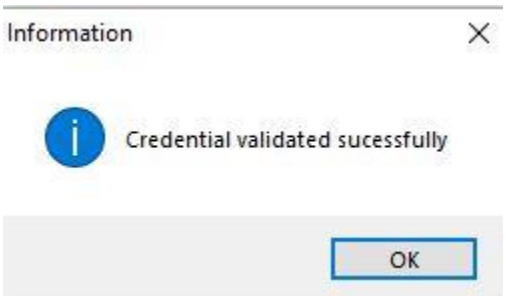

Figure 9

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

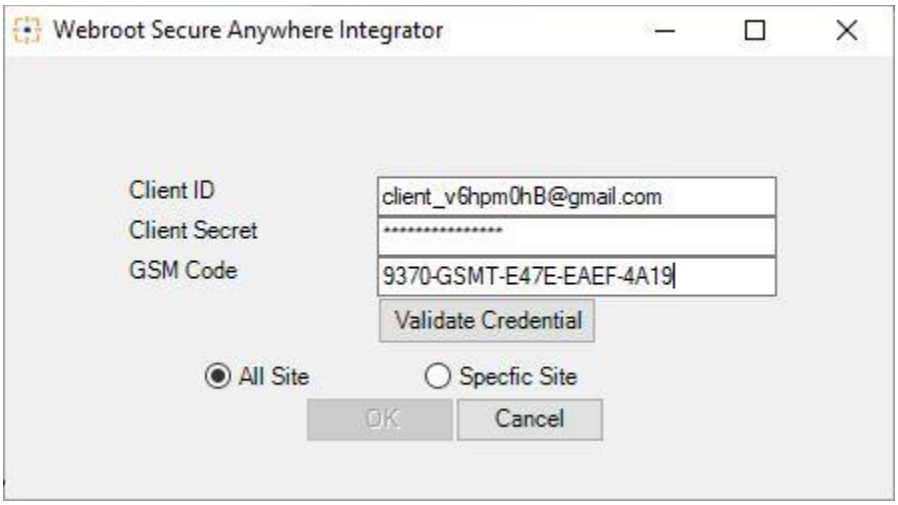

Figure 10

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.

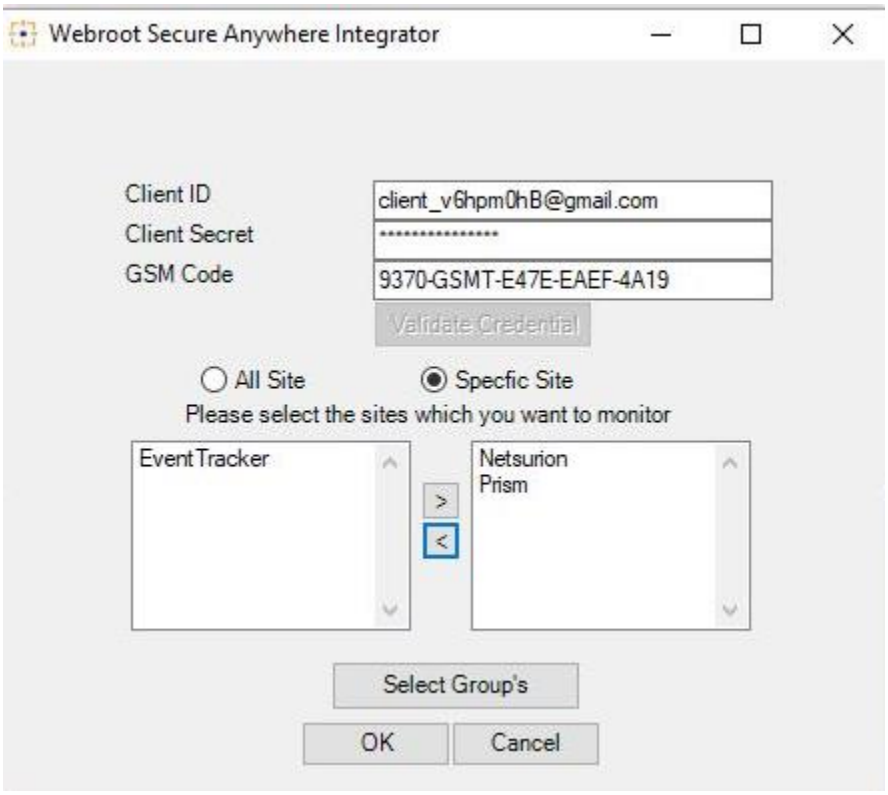

Figure 11

12. This will get you the groups in the sites selected.

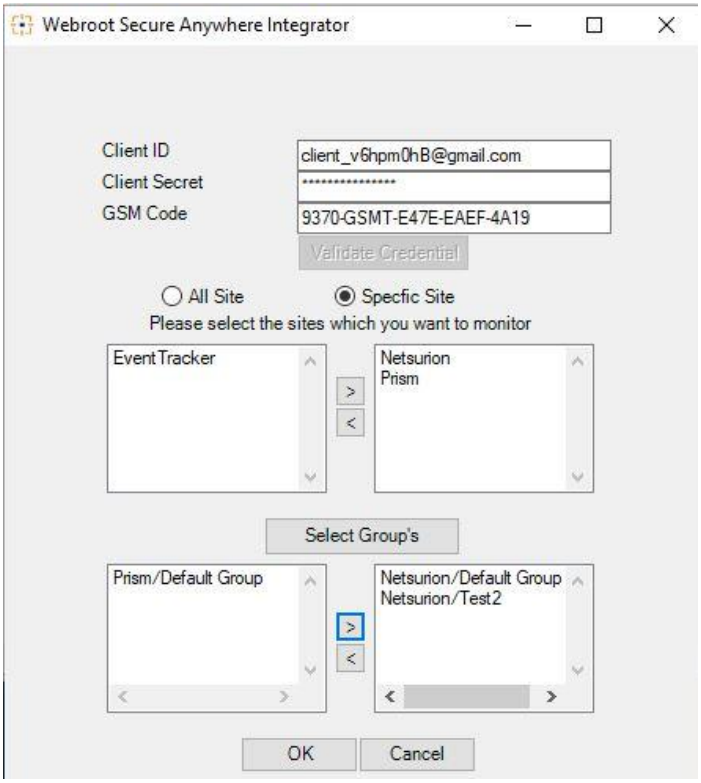

Figure 12

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.

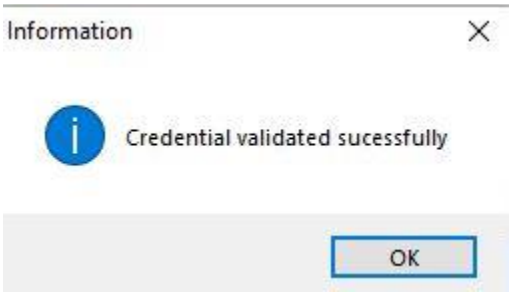

Figure 13