



**Integration Guide** 

# Integrate Webroot SecureAnywhere with Netsurion Open XDR

**Publication Date** June 20, 2023

© Copyright Netsurion. All Rights Reserved.



# Abstract

This guide provides instructions to configure and integrate Webroot SecureAnywhere with Netsurion Open XDR to retrieve its logs via API integration and forward them to Netsurion Open XDR.

#### Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

# Scope

The configuration details in this guide are consistent with Webroot SecureAnywhere and Netsurion Open XDR 9.3 or later.

# Audience

This guide is for the administrators responsible for configuring and monitoring Webroot SecureAnywhere in Netsurion Open XDR.



# Table of Contents

1	Ove	4	
2	Pre	4	
3	Inte	egrating Webroot SecureAnywhere with Netsurion Open XDR	4
4	Dat	14	
4	4.1	Alerts	14
4	4.2	Reports	14
4	4.3	Dashboards	
4	4.4	Saved Searches	



## 1 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.

Netsurion Open XDR manages logs retrieved from Webroot SecureAnywhere. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Webroot Business Endpoint Protection and DNS Protection.

## 2 Prerequisites

- Webroot SecureAnywhere Business Endpoint Protection/DNS Protection must be installed.
- PowerShell version 5.0 and above must be installed.
- The Data Source Integration package.

#### Note

To get the Data Source Integration package, contact your Netsurion Account Manager

Existing legacy version of the Webroot integrator must be uninstalled.

#### Note

Refer to the <u>How to Uninstall</u> guide to uninstall the Webroot Integrator.

## 3 Integrating Webroot SecureAnywhere with Netsurion Open XDR

- **1.** To configure the Webroot application, it is required to obtain the following field details.
  - Admin Username
  - Admin Password
  - Client Secret
  - Client ID
  - Parent Keycode
- 2. To obtain the API details, log in to <u>Webroot</u> using the administrator account.



3. Go to the Settings tab and click NEW to create the API key.



	Management Console CE 23.1
<b>O</b>	Subscriptions Account Information Data Filter Web Block Page Settings Unity API Access
∷⊟ Sites List	New Edit Delete Renew Secret Suspend API Documentation Developer.Webroot.Com

4. In the Create New interface, provide the API Name and Description, and then click Next.

CREATE NEW CLIENT CREDENTIAL		(i)
1	2	3
Name * 😧		
Description * @		
Please remember that you are solely Webroot's service is subject to the We Webroot. You, or anyone using your c when using this service, including all a	responsible for any actions taken us ebroot SecureAnywhere Business So redentials, must at all times comply applicable data protection, privacy la	ing your credentials and use of lution Agreement between you and with all applicable laws and regulations aws and regulations.
The Unity API is currently provided for data types over time. In the event, We included as part of the Unity API, thes API service and you will have the optic	r free, and Webroot reserves the rig ebroot does charge a fee for certain se chargeable API types and data typ on to purchase access to it.	ht to add or remove certain API types or API types and data types currently es will be included as part of a new paid
Click here to view Webroot SecureAny	where Business Solution Agreemen	ıt
Cancel		Next



5. In the subsequent window, select the Integration with SIEM provider option from the drop-down list and click Next.

CREATE NEW CLIENT CREDENTIAL					
<b>2</b> 3					
<b>Do you plan to use the event notification AP!?</b> Notification API allows you to subscribe to a set of events on different domain levels, and receive related notifications in near real-time (for example WebThreatShield.UrlAction or Endpoint.FileDetection).					
Yes					
O No					
How do you plan to use Unity API?					
Integration with SIEM provider					
Please provide the SIEM provider name \star					
Netsurion's open XDR platform					
Cancel Previous Next					

6. After providing the necessary information, click **Save** to save the API details.

CREATE NEW CLIENT CREDENTIAL	
	3
If you have any suggestions regarding the Unity API, please enter them he	re.
Cancel	Previous Save

#### Note:

Make a note of the Client Secret as it will only be visible only for the first time and will not be continued in the console.



7. To renew the Client Secret, select the appropriate API site (If multiple APIs created) and click **Renew** Secret to get new client secret.

Management Console CE 23.1						
Subscriptions Account Info	rmation Data Filter Web	b Block Page Settings Unity A	IPI Access			
New Edit Delete	Renew Secret Suspend	API Documentation Devel	oper.Webroot.Com			
NAME	DESCRIPTION	CLIENT ID	STATUS	NOTIFICATION API		
			Active	Enabled		

8. In the Webroot console, go to **admin** to give **admin** permission for the required sites to monitor as displayed below.

ADMIN:			Delete Admin
Details Site Permissions			
SITE PERMISSIONS 23 Results			٩
SITE \$	○ admin ≑		O NO ACCESS 🗢
<u> </u>	O Admin	O View Only	No Access
	Admin	O View Only	O No Access

The GSM code data will be available in Admin tab.

**9.** To know the GSM code, go to the **admin** tab and select **Account information** sub-tab to find the GSM code which will be available as Parent Keycode as highlighted in the following image.

Management Console CE 23.1							
Subscriptions	Account Information	Data Filter	Web Block Page Settings	Unity API Access			
ACCOUNT DETAIL	S						
Site / Company N	ame		· · · · ·	Rename			
Company Address	5						
Contact Email							
Contact Phone							
Parent Keycode			A This keycode should	d not be used for installation. Please use the correct site			
				1000 devices purchased - 286 days remaining)			
			Renew / Upgrade				



**10.** If you have configured DNS Protection, then make sure that the site you require to monitor has the SecureAnywhere DNS Protection value as **ON**.

Summary	Details	Admin Permissions	Endpoint Protection	DNS Protection
				▲ Settings cannot be changed for non-active sites
DNS Protection: Off 🕜				

**11.** After completing the API and site permission configurations, run the integrator package **Integrator\_Webroot.exe**.

📲 Netsurion: Webroot Secure	eAnywhere Integrator			×
Help				
	Edit Configuration		Delete Con	figuration
API Configuration				
Client ID:				
Client Secret:		$\odot$		
GSM Code:				
User Name:			Validate and	Configure
Netsurion Open XDR Configura	tion			
🗖 U:	se sensor configuration			
Manager Name:				
Manager Port: 1	4505	÷	Test Con	nection
		Cance	el	Save

Г



 In the Webroot SecureAnywhere Integrator window > API Configuration section, enter the details for Client ID, Client Secret, and GSM code, and then click Validate and Configure to validate and configure the credentials.

lelp				
	Edit Configura	tion	Delete Configurat	ion
PI Configuration				
Client ID:	-			
Client Secret:		0		
GSM Code:	and the second			
User Name:	-		Validate and Config	jure
etsurion Open XDR Configuration	n			
Use :	sensor configuration			
Manager Name:				
Manager Port: 145	05	÷	Test Connection	
Manager Name. Manager Port: 145	05	÷	Test Connection	

**13.** Windows PowerShell credential is required to validate the APIs. Provide the Webroot admin credentials and click **OK** to validate.

Windows PowerShell credential request. ? ×						
<b>R</b>				A		
Please provide the ad GSM console	min use	ername a	and passv	word of \	Nebroot	
<u>U</u> ser name:	😰				×	
Password:						
		(	Ж	Car	ncel	

If the configuration is validated successfully, an Information window pops-up stating *Credential validated successfully*.





14. In the subsequent window, select the required organizations to monitor and click Next.

#### Note:

It may take few seconds to get the below window as validation may take time.

Netsurion: Webroot Secure	Anywhere Integra	tor	
Note: Maximum limit is 5 or	rganizations.		
Select organization			
V			^
			~
	Back	Next	

**15.** Then, enter the Group details for each selected site and click **Finish** to complete the site configuration.

Netsurion: Webroot SecureAnywhere Integrator

F	Provide group name	for each orga	nization	
cognizant		CO		
1.00		V		
			Back	Finish





**16.** In the **Netsurion: Weboot SecureAnywhere Integrator** > **Netsurion Open XDR Configuration** section, either provide the Manager details to send the logs to a specific Netsurion Open XDR manager or use the sensor configuration.

#### To provide the Manager details:

• Specify the Manager Name and Manager Port and click Test Connection to validate the details.

Netsurion: Webroot Secure	Anywhere Integrator			
Help				
	Edit Configuration		Delete Configuration	
API Configuration				
Client ID:				
Client Secret:		0		
GSM Code:				
User Name:	and the second second		Validate and Configure	
letsurion Open XDR Configurati	on			
□ Use	sensor configuration			
Manager Name:				
Manager Port: 14	505	3	Test Connection	
		Cancel	Save	



If the connection is validated successfully, an Information window pops-up stating *Integrator is connected with the Netsurion Open XDR manager successfully*.

Webroot Integration	×
Integrator is connected with Netsurion Open XDR manager successfully.	
(OK	

To use the Sensor configuration:

• Select the **Use sensor configuration** check box if you want to use the sensor configuration where the Netsurion Open XDR sensor is already installed in the system.

Netsurion: Webroot Secure	Anywhere Integrator		>
Help			
	Edit Configuration	Dele	ete Configuration
API Configuration			
Client ID:	a the second of	1	
Client Secret: .		2	
GSM Code:			
User Name: i	a second second second	Valida	ate and Configure
Netsurion Open XDR Configuration	on		
Vse	e sensor configuration		
Manager Name:			
Manager Port: 14	505	Te	st Connection
		Cancel	Save



1/. After providing the required details, click <b>Save</b> to save the configura	ation.
---	--------

guration
guration
onfigure
ection

The integrator validates the details, retrieves the organization's information, and saves the configuration, resulting in the successful integration of Webroot SecureAnywhere with Netsurion Open XDR.





## 4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the DSIs in Netsurion Open XDR.

The Data Source Integrations package contains the following files for Webroot SecureAnywhere.

- Categories\_Webroot SecureAnywhere.iscat
- Alerts\_Webroot SecureAnywhere.isalt
- Reports\_Webroot SecureAnywhere.etcrx
- KO\_Webroot SecureAnywhere.etko
- Dashboards\_Webroot SecureAnywhere.etwd

#### Note

Refer the <u>How To Configure DSI</u> guide for the procedures to configure the above DSIs in Netsurion Open XDR.

## **Data Source Integrations Details**

## 4.1 Alerts

Name	Description
Webroot SA: Threat detection	Generated whenever the threat is detected on endpoint.
Webroot SA: Command executed	Generated whenever the command has been executed on endpoint.

## 4.2 Reports

Name	Description
Webroot SA - Malware detection	Provides the details about any malware or threats that are detected by Webroot.
Webroot SA - DNS blocked traffic requests	Provides the details of the contents that are being accessed by users who are blacklisted or blocked by Webroot.
Webroot SA - DNS allowed traffic requests	Provides the details of the contents that are being accessed by users who are whitelisted or allowed by Webroot.
Webroot SA - DNS traffic summary	Provides the details about DNS traffic summary of all endpoints monitored by Webroot.



Name	Description
Webroot SA - Commands executed	Provides the details about commands which are executed by user on endpoint.

## 4.3 Dashboards

Name	Description
Webroot SA - Threat detected by hostname	Displays the data about threats detected by hostname.
Webroot SA - Threat detected by signature	Displays the data about threats detected by signature.
Webroot SA - Blocked DNS request by sitename	Displays the data about blocked DNS requests by site name.
Webroot SA - Web requests blocked by country	Displays the location of web request blocked by Webroot.
Webroot SA - Malware group by username	Displays the data of malware by username.

## 4.4 Saved Searches

Name	Description
Webroot SA - Malware Detection	Provides the details about any malware or threats that are detected by Webroot.
Webroot SA - DNS blocked traffic requests	Provides the details of the contents that are being accessed by users who are blacklisted or blocked by Webroot.
Webroot SA - DNS allowed traffic requests	Provides the details of the contents that are being accessed by users who are whitelisted or allowed by Webroot.
Webroot SA - DNS Traffic Summary	Provides the details about DNS traffic summary of all endpoints monitored by Webroot.
Webroot SA - Commands Executed	Provides the details about commands which are executed by user on endpoint.



## **About Netsurion**

Netsurion<sup>®</sup> delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at <u>www.netsurion.com</u>.

## **Contact Us**

#### **Corporate Headquarters**

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

#### **Contact Numbers**

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support