



How To Guide

Uninstall Webroot SecureAnywhere Integrator

Publication Date:

June 20, 2023

Abstract

This guide provides instructions to uninstall the legacy Webroot SecureAnywhere integrator from Netsurion Open XDR platform.

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 uninstalling the Webroot SecureAnywhere integrator and its logs from Netsurion Open XDR.

Table of Contents

1	Overview	4
2	Prerequisite	4
3	Uninstalling the Integration of Legacy Webroot SecureAnywhere	4
3.1	Uninstalling the Legacy Webroot SecureAnywhere Integrator	4
3.2	Deleting the Existing Data Source Integration	5
3.2.1	Category	5
3.2.2	Alerts	6
3.2.3	Reports	7
3.2.4	Knowledge object	8
3.2.5	Dashboards	10

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 Prerequisite

- Legacy version of the Webroot SecureAnywhere integrator is installed and configured.

3 Uninstalling the Integration of Legacy Webroot SecureAnywhere

3.1 Uninstalling the Legacy Webroot SecureAnywhere Integrator

Perform the below steps to delete the legacy Webroot SecureAnywhere Integrator from Netsurion Open XDR.

1. In the Task Scheduler, delete the tasks named **EventTracker - Webroot AV Events** and **EventTracker - Webroot DNS Events** where the legacy Integrator was running.
 - i. Go to **Start** and open **Task Scheduler**.

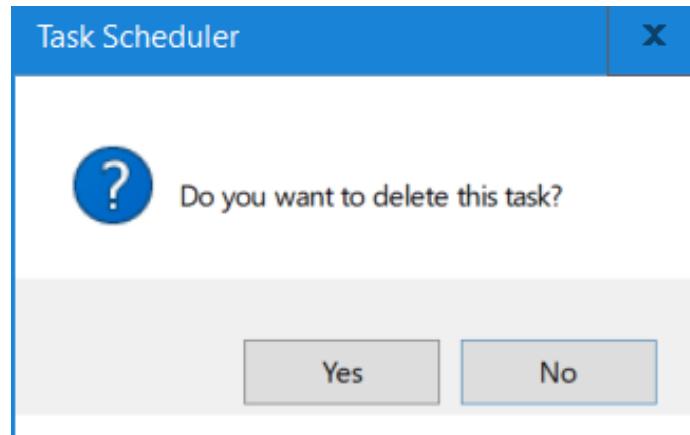
The following sample image displays the Webroot scheduler created with legacy Integration.

Name	Status	Triggers
Adobe Acrobat Update Task	Ready	Multiple triggers defined
EventTracker - Webroot AV Events	Ready	At 05:51 PM every day - After triggered, repeat every 5 minutes indefinitely.
EventTracker - Webroot DNS Events	Ready	At 05:51 PM every day - After triggered, repeat every 1 hour indefinitely.

- ii. Right-click the **EventTracker - Webroot AV Events** and **EventTracker - Webroot DNS Events** tasks and click **Delete**.

Name	Status	Triggers
Adobe Acrobat Update Task	Ready	Multiple triggers defined
EventTracker - Webroot AV Events	Ready	At 05:51 PM every day - After triggered, repeat every 5 minutes indefinitely.
EventTracker - Webroot DNS Events	Ready	At 05:51 PM every day - After triggered, repeat every 1 hour indefinitely.
FreshserviceAgentUpdater	Ready	Multiple triggers defined
GoogleUpdateTaskMachineCore[EAC5DD8F]	44D9DD1)	Multiple triggers defined
GoogleUpdateTaskMachineUA(624CAB00-8	083A0)	At 03:08 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.
MicrosoftEdgeUpdateTaskMachineCore[B2]	DF5880...	Ready

- iii. Click **Yes** to confirm the deletion of the **EventTracker - Webroot AV Events** and **EventTracker - Webroot DNS Events** tasks.



The **EventTracker - Webroot AV Events** and **EventTracker - Webroot DNS Events** tasks will be successfully deleted from the task scheduler.

Note:

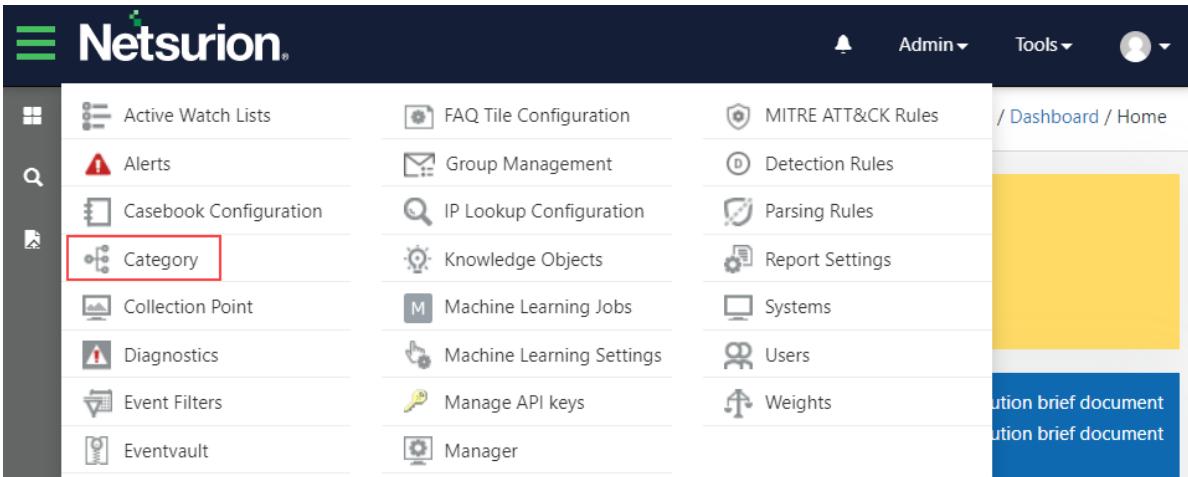
After deleting the task ensure to delete the **Webroot** folder from the integrator path.

3.2 Deleting the Existing Data Source Integration

Perform the following steps to delete the existing Data Source Integration from Netsurion Open XDR.

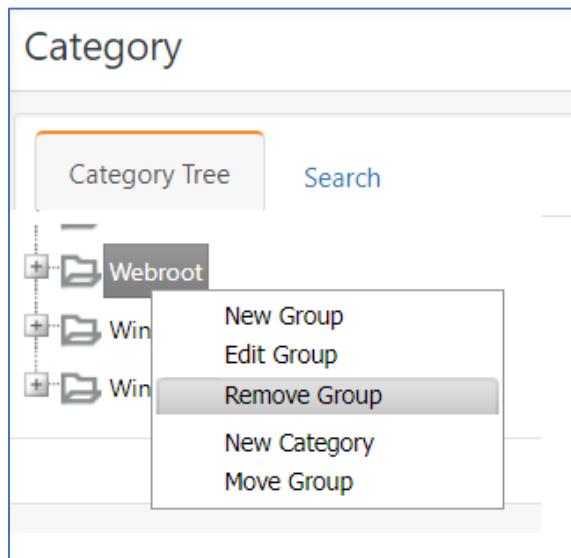
3.2.1 Category

1. In Netsurion Open XDR, hover over the **Admin** menu and click **Category**.



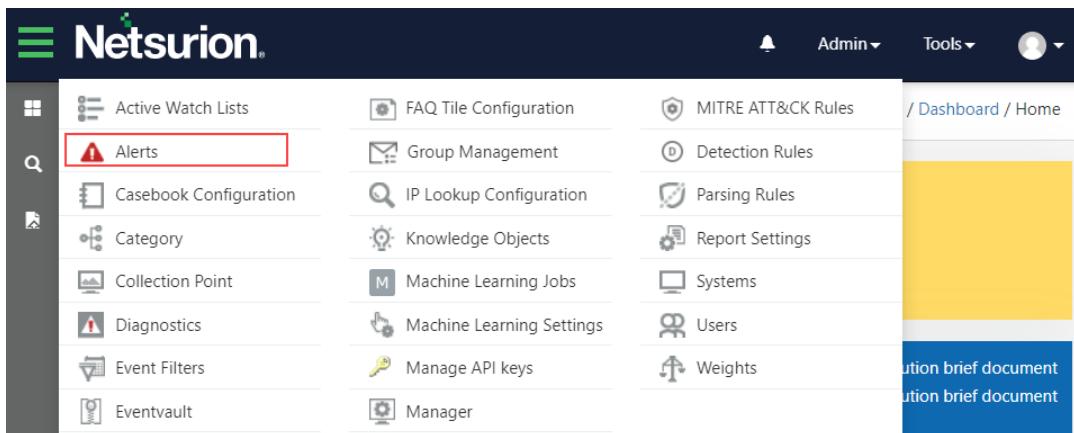
The screenshot shows the Netsurion Open XDR Admin interface. The left sidebar has a 'Category' item highlighted with a red box. The main content area lists various configuration options: Active Watch Lists, FAQ Tile Configuration, MITRE ATT&CK Rules, Alerts, Group Management, Detection Rules, Casebook Configuration, IP Lookup Configuration, Parsing Rules, Collection Point, Knowledge Objects, Report Settings, Diagnostics, Machine Learning Jobs, Systems, Event Filters, Machine Learning Settings, Users, Eventvault, Manage API keys, and Manager. The URL in the top right is /Dashboard / Home.

2. In the **Category** interface, under the **Category Tree** tab, right-click the **Webroot** group folder and click **Remove Group** to delete the existing Webroot category.



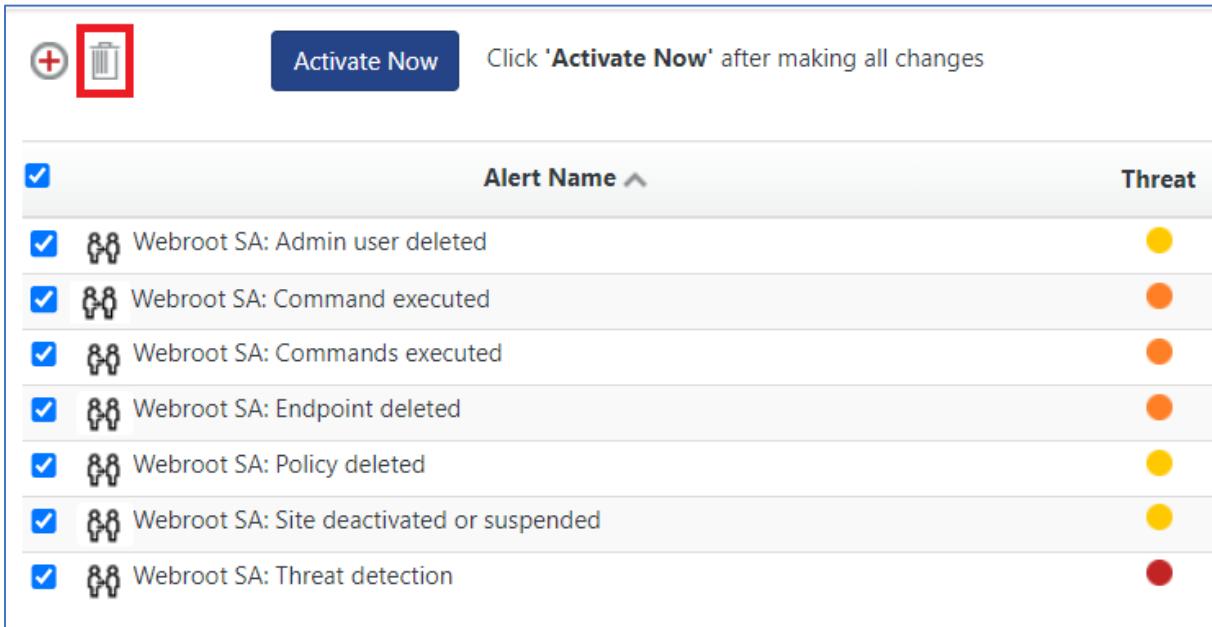
3.2.2 Alerts

1. In **Netsurion Open XDR**, hover over the **Admin** menu and click **Alerts**.



2. In the **Alerts** interface, type **Webroot** in the **Search** field and click the **Search** button.
3. The **Alerts** interface will display all the imported **Webroot** alerts.

4. Click the Select All check box to select all the **Webroot** alerts as shown below and click the **Delete** icon to delete all the existing alerts.



Activate Now Click 'Activate Now' after making all changes

Alert Name	Threat
Webroot SA: Admin user deleted	Yellow
Webroot SA: Command executed	Orange
Webroot SA: Commands executed	Orange
Webroot SA: Endpoint deleted	Orange
Webroot SA: Policy deleted	Yellow
Webroot SA: Site deactivated or suspended	Yellow
Webroot SA: Threat detection	Red

3.2.3 Reports

1. In **Netsurion Open XDR**, go to **Reports > Report Configuration**.



My Dashboard / Dashboard

Report Configuration

Report Dashboard

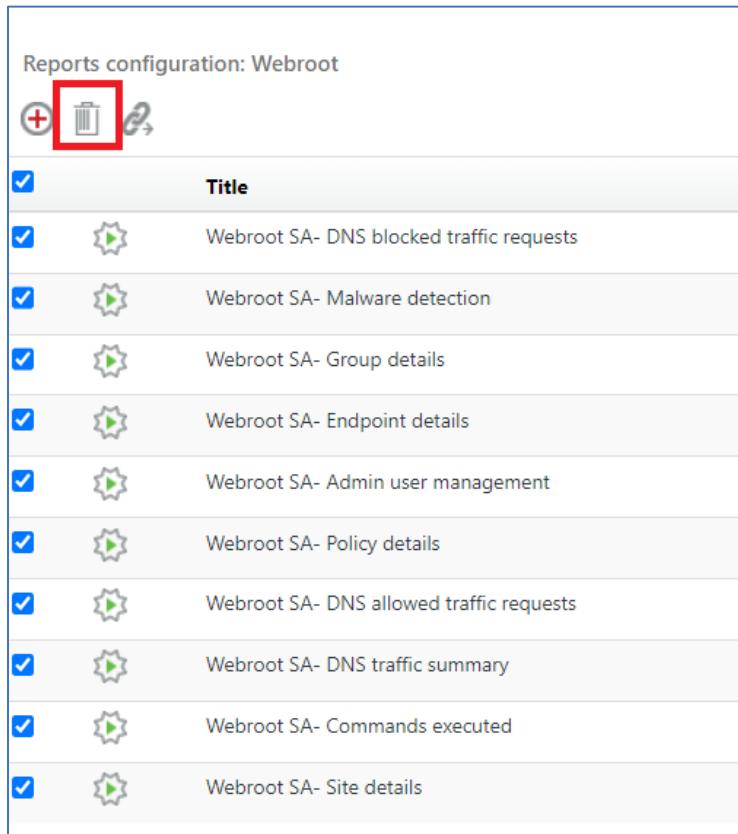
Explorer

Windows-New Schedule...

2. In the **Reports Configuration** interface, select the **Defined** option.

3. In the search field, type **Webroot** and click **Search** to search for the Webroot files.

4. Click the **Select All** check box to select all the **Webroot** reports and click the **Delete** icon to delete all the existing reports.

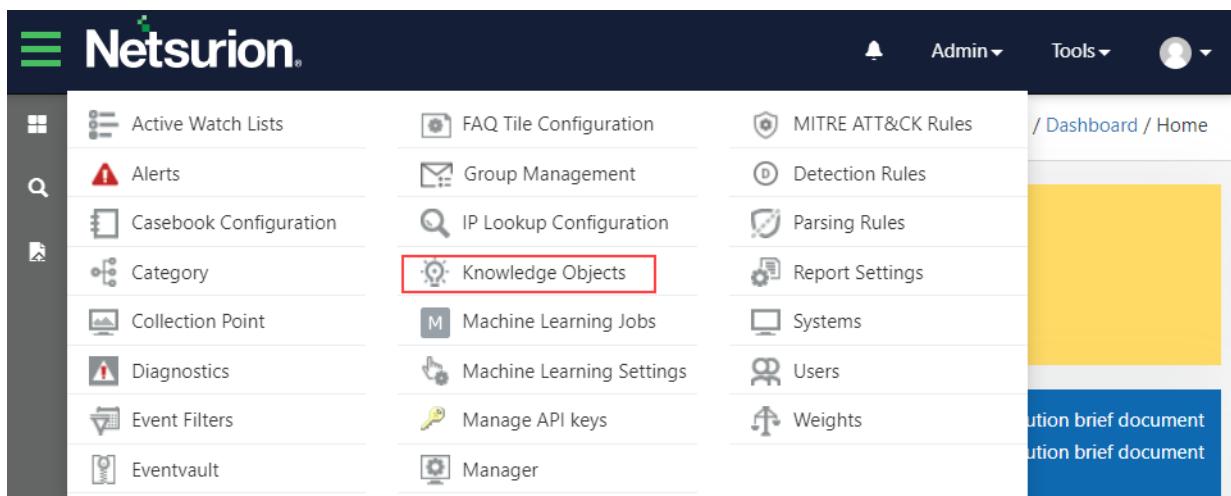


Reports configuration: Webroot

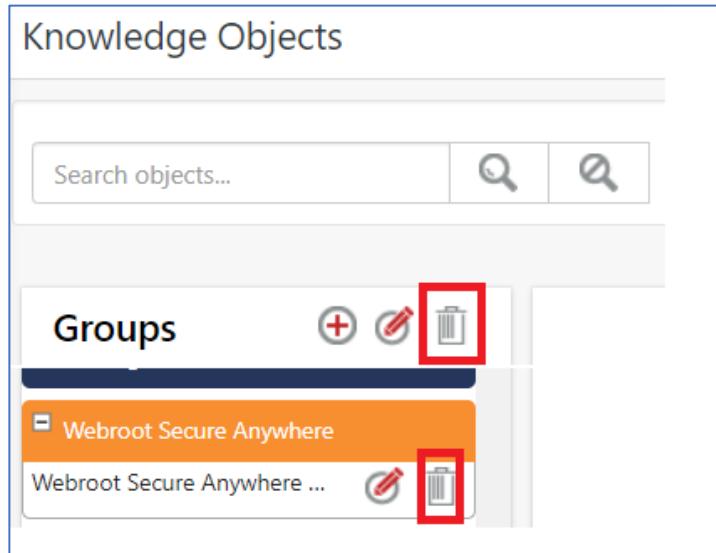
<input checked="" type="checkbox"/>	Title
<input checked="" type="checkbox"/>	Webroot SA- DNS blocked traffic requests
<input checked="" type="checkbox"/>	Webroot SA- Malware detection
<input checked="" type="checkbox"/>	Webroot SA- Group details
<input checked="" type="checkbox"/>	Webroot SA- Endpoint details
<input checked="" type="checkbox"/>	Webroot SA- Admin user management
<input checked="" type="checkbox"/>	Webroot SA- Policy details
<input checked="" type="checkbox"/>	Webroot SA- DNS allowed traffic requests
<input checked="" type="checkbox"/>	Webroot SA- DNS traffic summary
<input checked="" type="checkbox"/>	Webroot SA- Commands executed
<input checked="" type="checkbox"/>	Webroot SA- Site details

3.2.4 Knowledge object

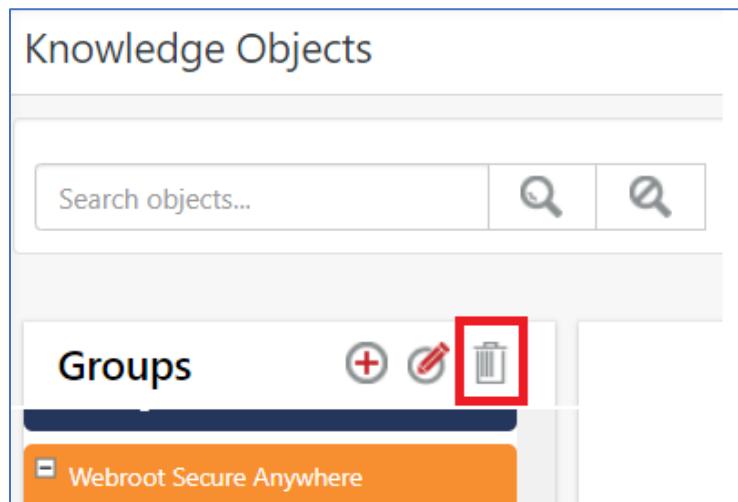
1. In **Netsurion Open XDR**, hover over the **Admin** menu and click **Knowledge Objects**.



2. In the **Knowledge Object** interface, under **Groups** tree, click the **Webroot Secure Anywhere** group and click the **Delete** icon to delete all existing Webroot SecureAnywhere KO files.

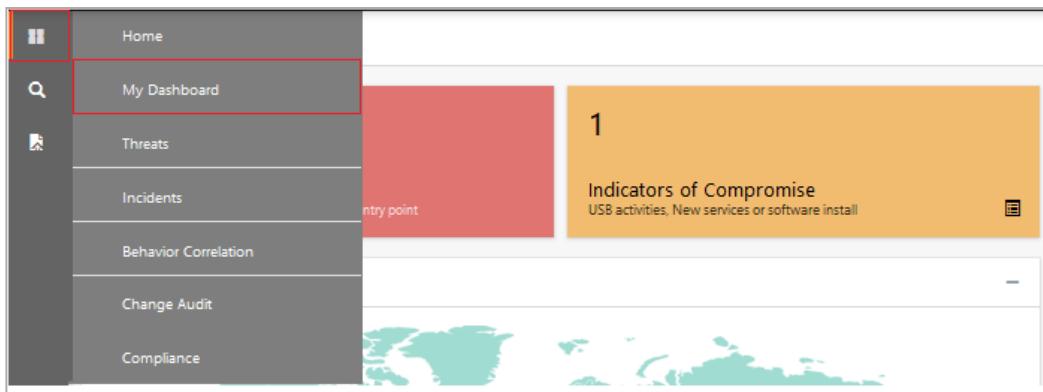


3. In the **Knowledge Object** interface, click the **Webroot SecureAnywhere** group and click the **Delete** icon to delete existing Webroot SecureAnywhere KO group.

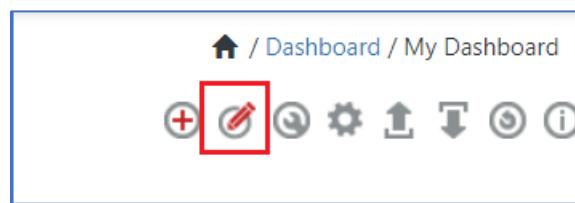


3.2.5 Dashboards

1. Log in to **Netsurion Open XDR** and go to **Dashboard > My Dashboard**.



2. In the **My Dashboard** interface, click the **Edit** button, and then click **Delete** to delete all the existing dashlets.

A screenshot of the 'Edit Dashboard' interface. At the top, there is a breadcrumb navigation: Home / Dashboard / My Dashboard. Below the navigation, there is a row of icons: a plus sign, a pencil (highlighted with a red box), a circular arrow, a gear, an upward arrow, a downward arrow, a circular arrow, and an information icon. The main area is titled 'Edit Dashboard'. It contains two sections: 'Title' with the value 'Webroot SecureAnywhere' and 'Description' with the value 'Webroot SecureAnywhere'. At the bottom right, there are three buttons: 'Save' (blue), 'Delete' (highlighted with a red box), and 'Cancel'.

About Netsurion

Netsurion® 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 www.netsurion.com.

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>