How-To Guide

Integrate Carbon Black Cloud Endpoint Standard with Netsurion Open XDR

Publication Date

August 30, 2023

Abstract

This guide provides instructions to configure and integrate Carbon Black Cloud Endpoint Standard with Netsurion Open XDR to retrieve its logs via API 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 Carbon Black Cloud Endpoint Standard and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Carbon Black Cloud Endpoint Standard in Netsurion Open XDR.

Table of Contents

1 Overview 4

2 Prerequisites 4

3 Integrating CB Cloud Endpoint Standard with Netsurion Open XDR 5

3.1 Collecting API Details from Carbon Black Cloud 5

3.1.1 Creating RBAC Permissions for API 5

3.1.2 Collecting API ID and KEY 5

3.1.3 Collecting API Hostname and Organization Key 6

3.2 Configuring Netsurion CB Cloud Endpoint Standard Integrator 6

4 Data Source Integration (DSI) in Netsurion Open XDR 10

4.1 Alerts 10

4.2 Reports 10

4.3 Dashboards 11

4.4 Saved Searches 12

1 Overview

Carbon Black Cloud Endpoint Standard (formerly called CB Defense) is a Next-Generation Antivirus (NGAV), and Endpoint Detection and Response (EDR) solution that protects against the full spectrum of modern cyber-attacks. Next-Generation Anti-Virus (NGAV) uses machine learning and behavioural models to analyze endpoint activity and uncover malicious behaviour to stop all types of attacks before they reach critical systems.

Netsurion Open XDR manages logs retrieved from Carbon Black Cloud Endpoint Standard. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Carbon Black Cloud Endpoint Standard.

2 Prerequisites

- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on host system/ server to run PowerShell.
- Admin access to Carbon Black Cloud console.
- The Data Source Integration package.

Note

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

IMPORTANT

From integrator version 2.x.x onwards, the system name will be changed. Following is an example for the system name format.

`<OrganizationName>-CB_EndPoint_Standard@<ComputerName>~<GroupName>`

By default, the CB Cloud Endpoint Standard reputation type TRUSTED_WHITE_LIST logs are excluded by Netsurion Open XDR.

Note

Reputation types can be included or excluded in the **Filter.json** located in **\CB Defense\Data\Filter.json**.

Note

Refer to the How-To-Upgrade-Carbon-Black-Cloud-Endpoint-Standard-Netsurion document to upgrade the CB Cloud Endpoint Standard integrator from v1.0.0 to v2.0.0. Do not adhere to Sections 3 if you opt to upgrade the integrator.

3 Integrating CB Cloud Endpoint Standard with Netsurion Open XDR

The following procedure facilitates configuring Netsurion Open XDR to receive specific events related to email traffic and events related to links clicked through using CB Endpoint Standard enriched_events REST API.

3.1 Collecting API Details from Carbon Black Cloud

The following details are required to configure CB Cloud Endpoint Standard integrator.

- API Key
- API Secret
- API Host
- Organization Name (Org Name)
- Organization Key (Org Key)

3.1.1 Creating RBAC Permissions for API

Before creating the API Key, it is required to create the **Custom** Access Level.

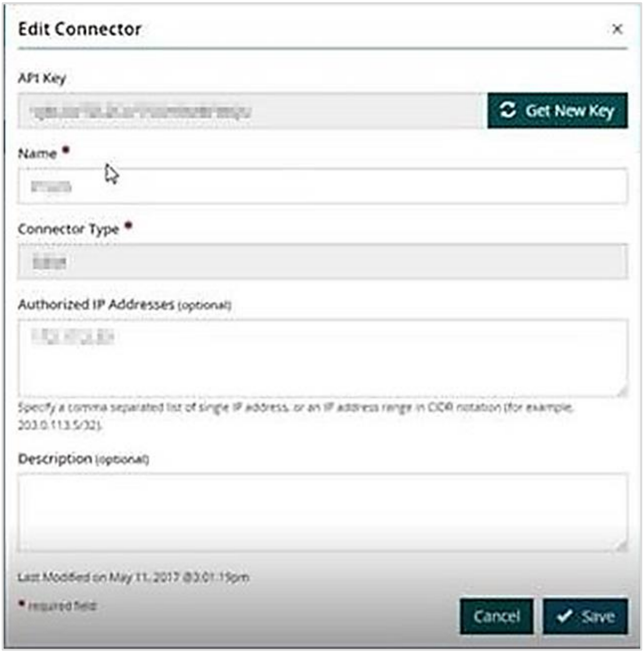
1. Log in to the **Carbon Black Cloud** console using admin access.
2. Go to **Settings** > **API Access** > **Access Levels** set the following permissions.

   For category **Search > Events > "org.search.events"** specify **CREATE** permission to start a job and **READ** permission to get results.

   NOTATION: `Category: Search > Permission: org.search.events`

3.1.2 Collecting API ID and KEY

1. In the Carbon Black Cloud console, go to **Settings** > **API Access** > **API Keys**.



Edit Connector

API Key

Name *

Connector Type *

Authorized IP Addresses (optional)

Specify a comma separated list of single IP address, or an IP address range in CIDR notation (for example, 203.0.113.5/32).

Description (optional)

Last Modified on May 11, 2017 @3:01:15pm

* required field

2. In the **Connector** section, define a new connector and note down its **API ID** and **API SECRET.**

   Note:

   Use an appropriate name for the connector

3. Set the Access Level Type to **Custom**, then select the **Access Level** created in the previous step.

   Note:

   Leave the **Authorized IP address** blank.

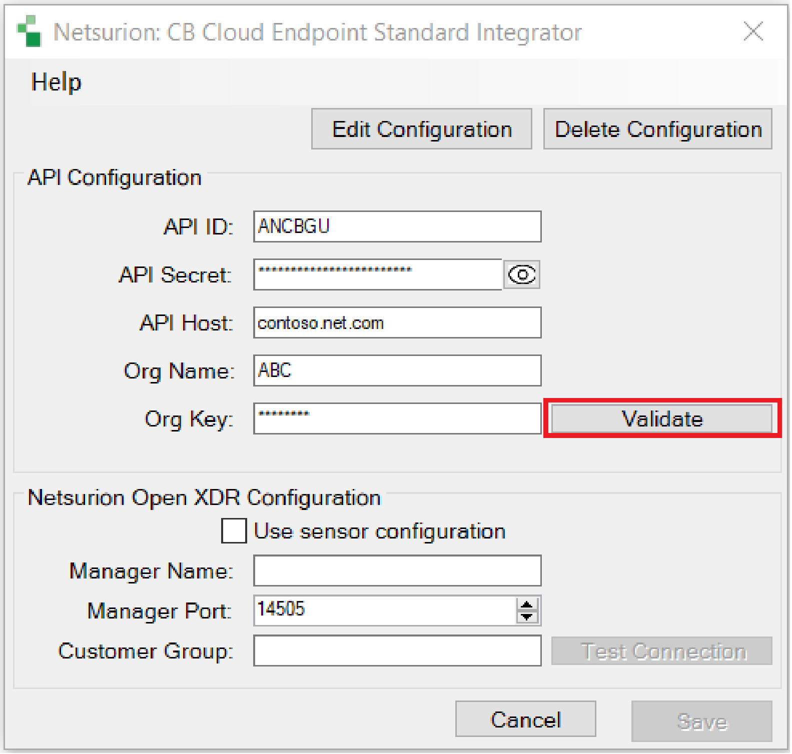
3.1.3 Collecting API Hostname and Organization Key

The following is the URL of the Carbon Black Cloud console (Dashboard URL) - **defense-eap01.conferdeploy.net**. The organization key (**Org_Key**) is located in the Carbon Black Cloud console.

- Log in to Carbon Black Cloud console and go to **Settings** > **API Access**.
- It is an 8-digit alpha-numeric value. For example, ABCD1234.

3.2 Configuring Netsurion CB Cloud Endpoint Standard Integrator

1. After receiving the executable application, right-click the file and click **Run as Administrator**.
2. In the Integrator window, specify the appropriate details for API Key, API Secret, API Host, Organization Name, and Organization Key and click the **Validate** button to verify the credentials.



Netsurion: CB Cloud Endpoint Standard Integrator

API Configuration

API ID: ANCBGU

API Secret: ************************

API Host: contoso.net.com

Org Name: ABC

Org Key: ********

Netsurion Open XDR Configuration

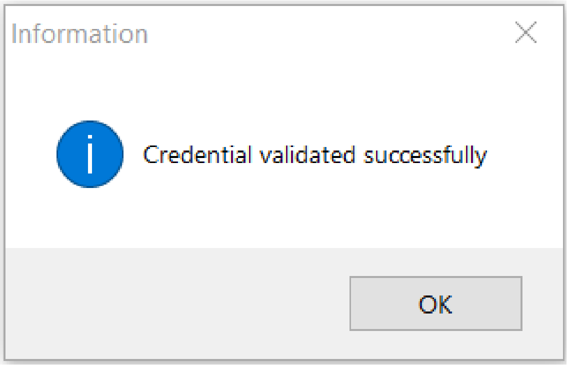
□ Use sensor configuration

Manager Name:

Manager Port: 14505

Customer Group:

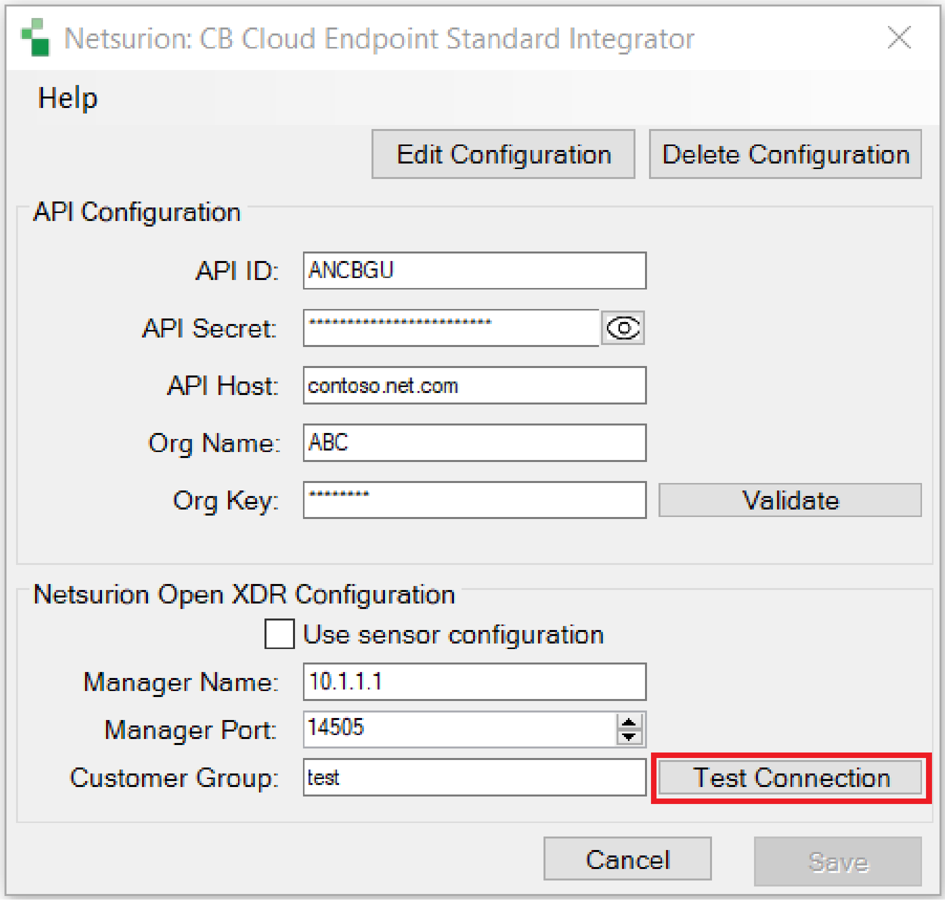
If the configuration is validated successfully, an Information window pops-up stating **“Credential validated successfully”**.



Credential validated successfully

3. In the CB Cloud Endpoint Standard Integrator > Netsurion Open XDR Configuration section, provide the appropriate details.

   a. You may either specify the details for **Manager Name**, **Manager Port**, and click **Test Connection** to validate the details.



API Configuration

API ID: ANCBGU

API Secret: ************************

API Host: contoso.net.com

Org Name: ABC

Org Key: ********

Netsurion Open XDR Configuration

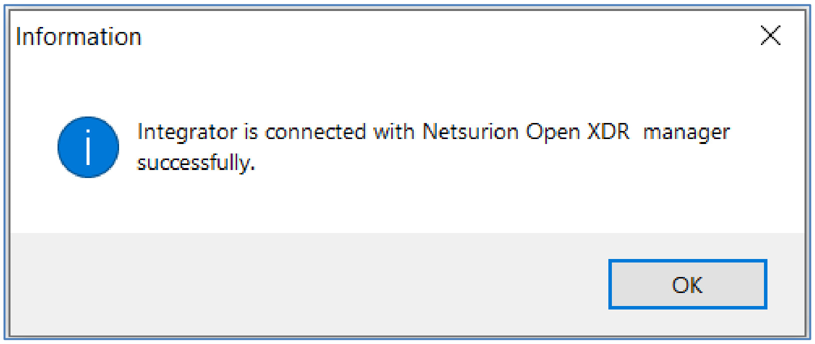
□ Use sensor configuration

Manager Name: 10.1.1.1

Manager Port: 14505

Customer Group: test

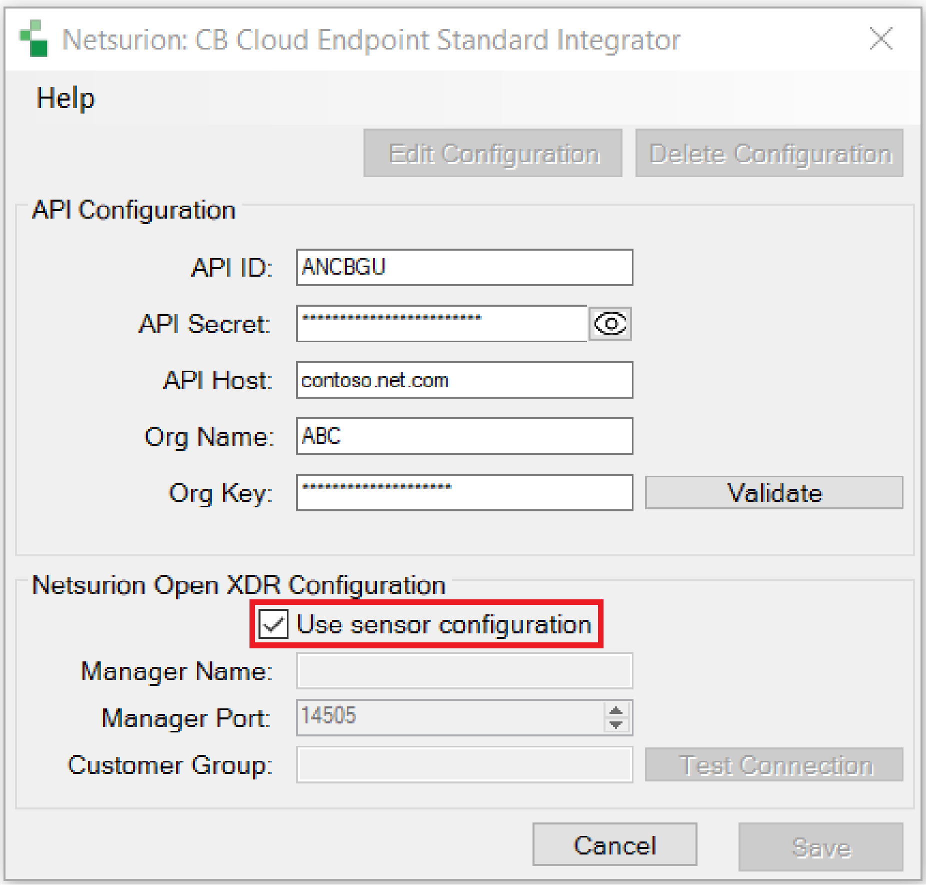
If the connection is validated successfully, an Information window pops-up stating '***Integrator is connected with Netsurion Open XDR manager successfully***'.



Information

Integrator is connected with Netsurion Open XDR manager successfully.

b. Otherwise, select the **Use sensor configuration** checkbox if you want to use the sensor configuration and the Netsurion Open XDR sensor is installed in the system.



Netsurion: CB Cloud Endpoint Standard Integrator

API Configuration

API ID: ANCBGU

API Secret: ************************

API Host: contoso.net.com

Org Name: ABC

Org Key: ********************

Netsurion Open XDR Configuration

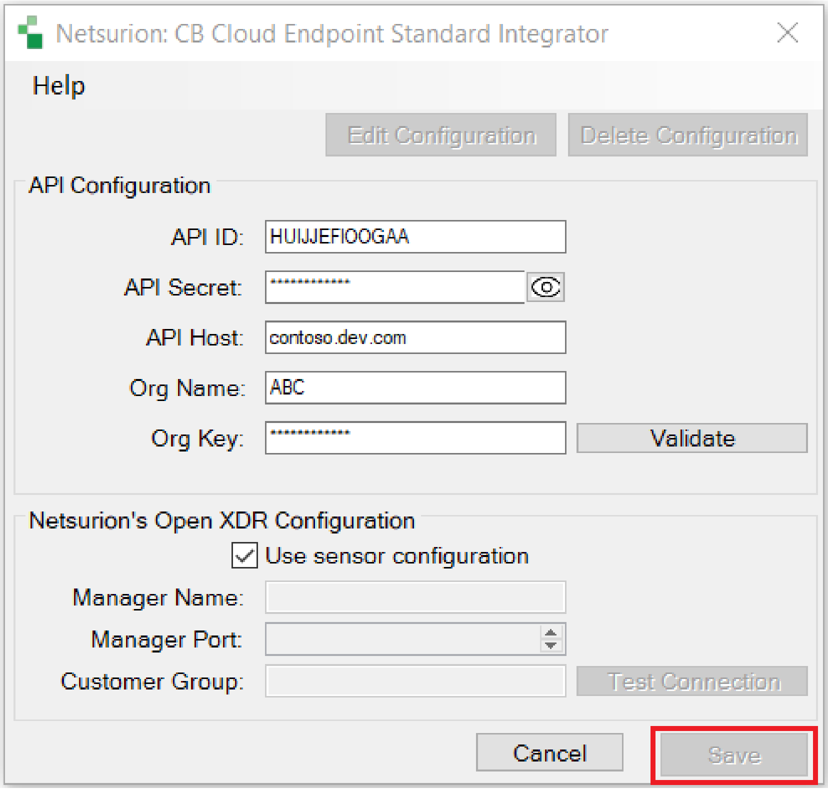
☑ Use sensor configuration

Manager Name:

Manager Port: 14505

Customer Group:

4. After providing the appropriate details, click **Save**.



API Configuration

API ID: HUIJJEFIOOGAA

API Secret: *************

API Host: contoso.dev.com

Org Name: ABC

Org Key: *************

Netsurion's Open XDR Configuration

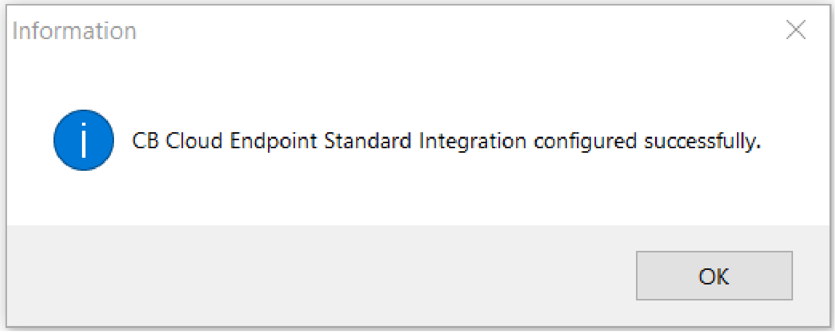
☑ Use sensor configuration

Manager Name:

Manager Port:

Customer Group:

The integrator validates the details, and saves the configuration, resulting in the successful integration of CB Cloud Endpoint Standard with Netsurion Open XDR.



CB Cloud Endpoint Standard Integration configured successfully.

4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integrations package contains the following files for CB Cloud Endpoint Standard.

- Categories_ CB Defense.iscat
- Alerts_ CB Defense.isalt
- Reports_ CB Defense.etcrx
- KO_ CB Defense.etko
- Dashboards_ CB Defense.etwd

Note

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

4.1 Alerts

Name	Description
CB Defense: Threat detected	Generated for events which are flagged as INJECT_CODE, or a source of malicious behaviour.
CB Defense: Policy action enforced	Generated for the events that are flagged as POLICY_ACTION, which occurs when a user performs certain activities like create policy, delete policy, modify policy, and more.

4.2 Reports

Name	Description
CB Defense - Threat detection	Provides information about threats detected. This includes information like device timestamp, device name, device OS, OS version, device installed by, process command line, process name, process reputation, SHA256, MITRE TTP (if applicable).
CB Defense - Policy action	Provides information about policies changed by users. This includes information like device timestamp, device policy, enrichment status, Sha256, process name, process reputation, MITRE TTP (if applicable).

Name	Description
CB Defense - Network activity	Provides information about network traffic details. This includes information like device timestamp, remote IP address, remote port number, peer geo location, process name, process reputation, MITRE TTP (if applicable).
CB Defense - Application access	Provides information about the applications accessed by users. This includes information like device timestamp, child process name, child process reputation, parentprocess name, parent process reputation, process name, process reputation, MITRE TTP (if applicable).
CB Defense - File and Registry access	Provides information about the file and registry changes made by users. This includes information like device timestamp, file name, file hash, file path, process name, process reputation, MITRE TTP (if applicable).
CB Defense - Data access	Provides information about data accessed by users. This includes information like device timestamp, device name, device OS, OS version, process name, process reputation, MITRE TTP (if applicable).

4.3 Dashboards

Name	Description
CB Defense - Enriched event types	Displays all the enriched event types captured by CB Defense.
CB Defense - Device locations	Displays all the device locations captured by CB Defense.
CB Defense - Device names	Displays all the device names captured by CB Defense.
CB Defense - MITRE ATT&CK by event types	Displays all the MITRE ATT&CK by event types.
CB Defense - Top child processes	Displays all the top child processes captured by CB Defense.
CB Defense - Top parent processes	Displays all the top parent processes captured by CB Defense.

4.4 Saved Searches

Name	Description
CB Defense - Threat detection	Provides users to filter and view the logs that are specific to INJECT_CODE, foe events that are flagged as INJECT_CODE, or found to be asource of malicious behaviour.
CB Defense - Policy action	Provides users to filter and view the logs that are specific to policy control activities such as create policy, remove policy, modify policy, etc.
CB Defense - Application access	Provides users to filter and view the logs that are specific to application access activity, such as CREATE_PROCESS or SYSTEM_API_CALL.
CB Defense - Data access	Provides users to filter and view the logs that are specific to DATA_ACCESS activity by a user.
CB Defense - File and registry access	Provides users to filter and viewthe logs that are specific to file creation and registry access, such as REGISTRY_ACCESS or FILE_CREATE.
CB Defense - Network activity	Provides users to filter and view the logs that are specific to network activity, which includes the connection details established to a remote IP.

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