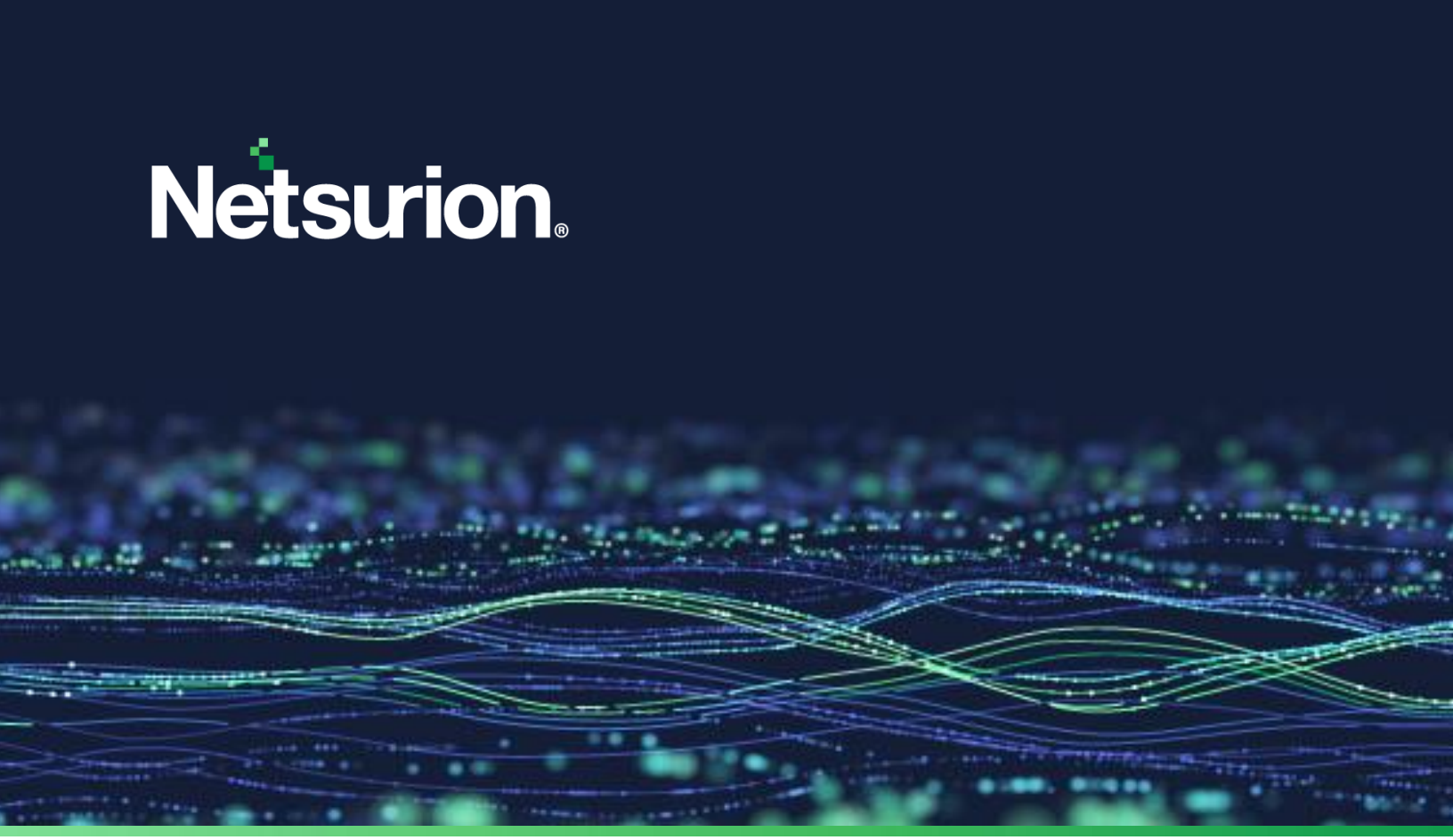


How-To Guide

Integrate Sophos Central with Netsurion Open XDR

Publication Date

August 16, 2023

Abstract

This guide provides instructions to configure and integrate Sophos Central with Netsurion Open XDR to retrieve its logs via syslog 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 Sophos Central and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Sophos Central in Netsurion Open XDR.

Table of Contents

1 Overview

Sophos Central is a unified platform for security management and an element of Sophos' synchronized security strategy to enable multiple security products to work together seamlessly with simpler management and better security.

Netsurion Open XDR manages logs retrieved from Sophos Central. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Sophos Central.

2 Prerequisites

- Must have Python application v3.6 or above. (Recommended the latest version.)
- Sophos Central Management console Administrator access.
- The Data Source Integration package.

Note

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

3 Integrating Sophos Central with Netsurion Open XDR

IMPORTANT:

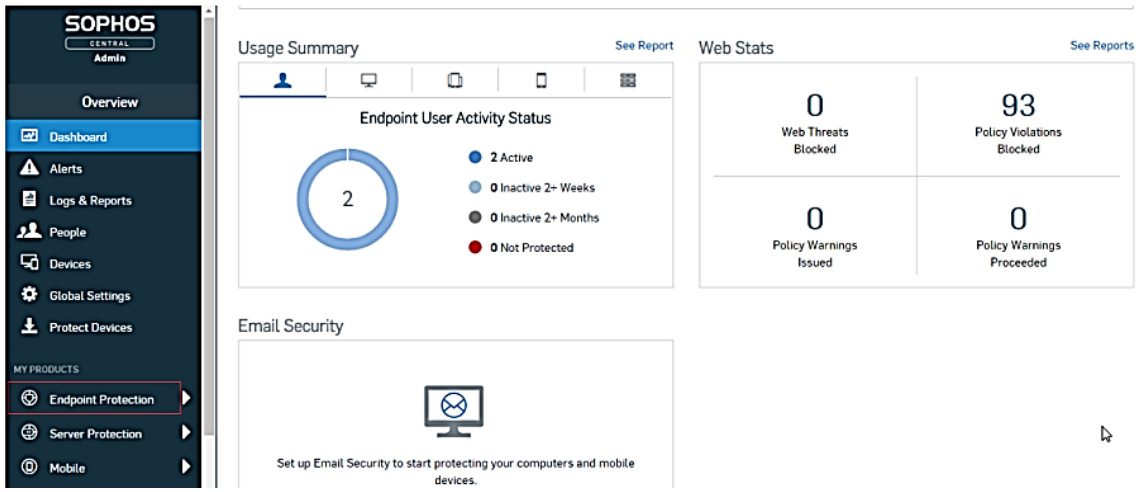
The specified integration script details are provided by Sophos Central and Netsurion does not have any accountability to the script. For any integration-related troubleshooting, recommended to contact the Sophos support team.

3.1 Integration Prerequisites

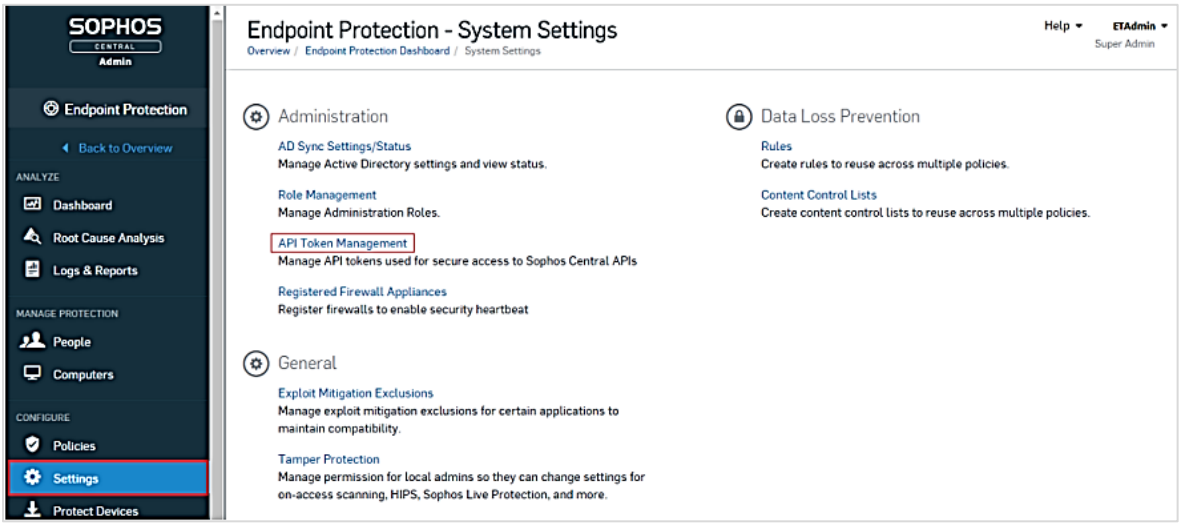
Sophos Central is integrated to Netsurion Open XDR via syslog with the help of Sophos Central API using Python. The following are the two prerequisites that must be verified and acquired before running the Python script.

3.1.1 Sophos Central API Configuration

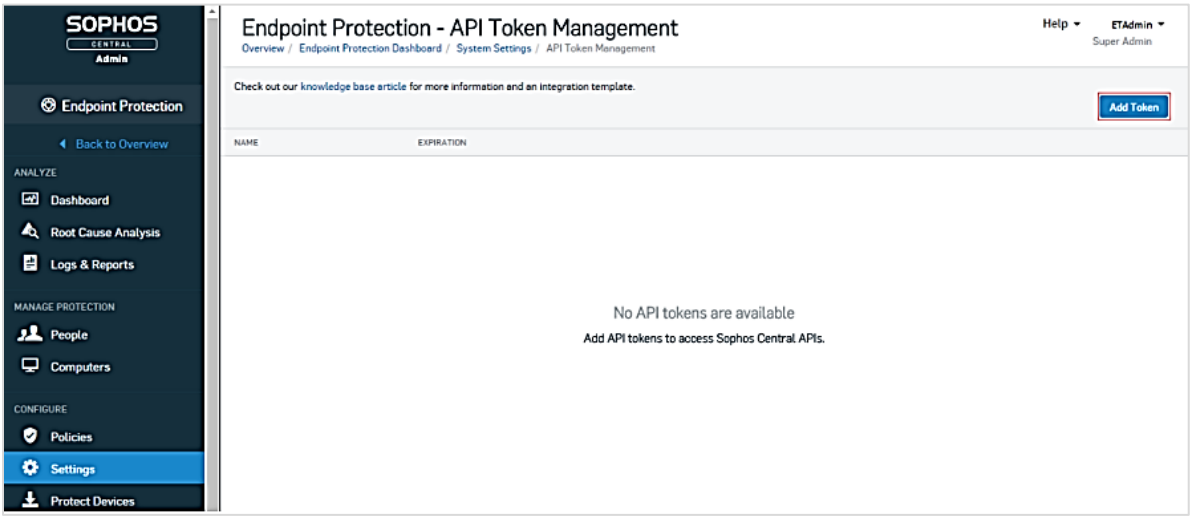
1. Log in to [Sophos Central] and go to **Endpoint Protection**.



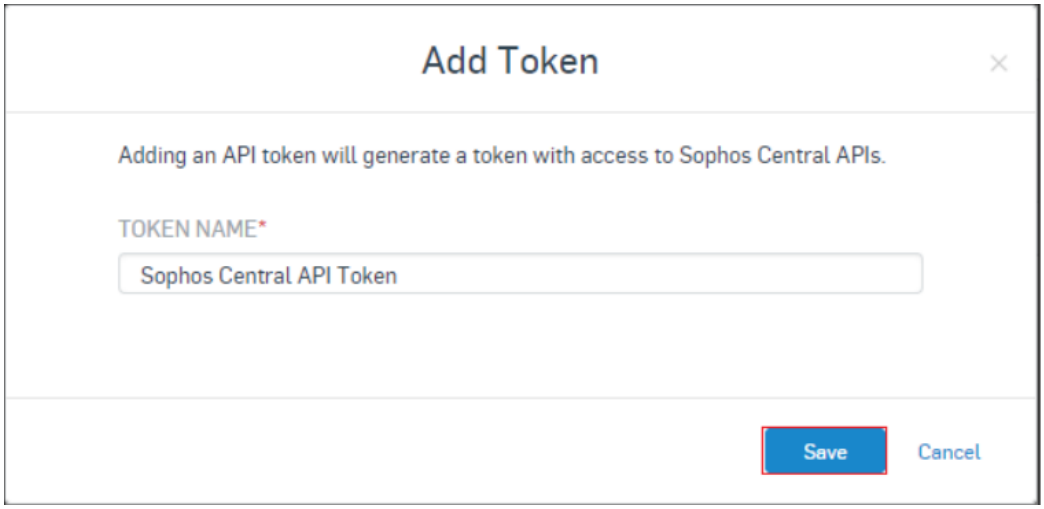
2. On the left panel, under the **Configure** section, click **Settings** and then click **API Token Management**.



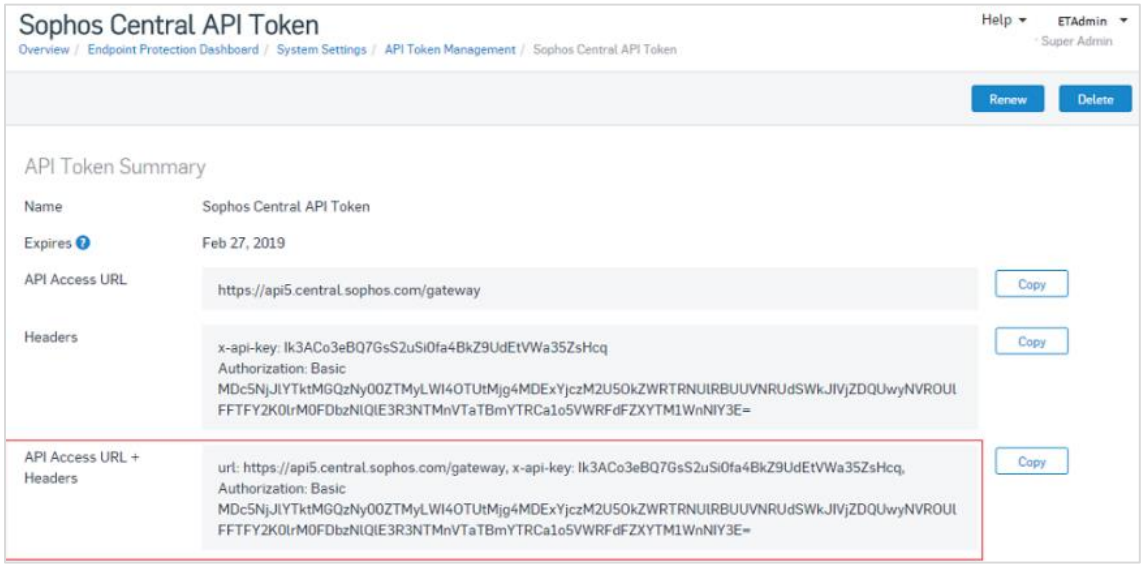
3. If there is no existing API token configured, then click **Add Token**.



4. A window pops up to add the token details. Provide the **Token Name** and click **Save**.

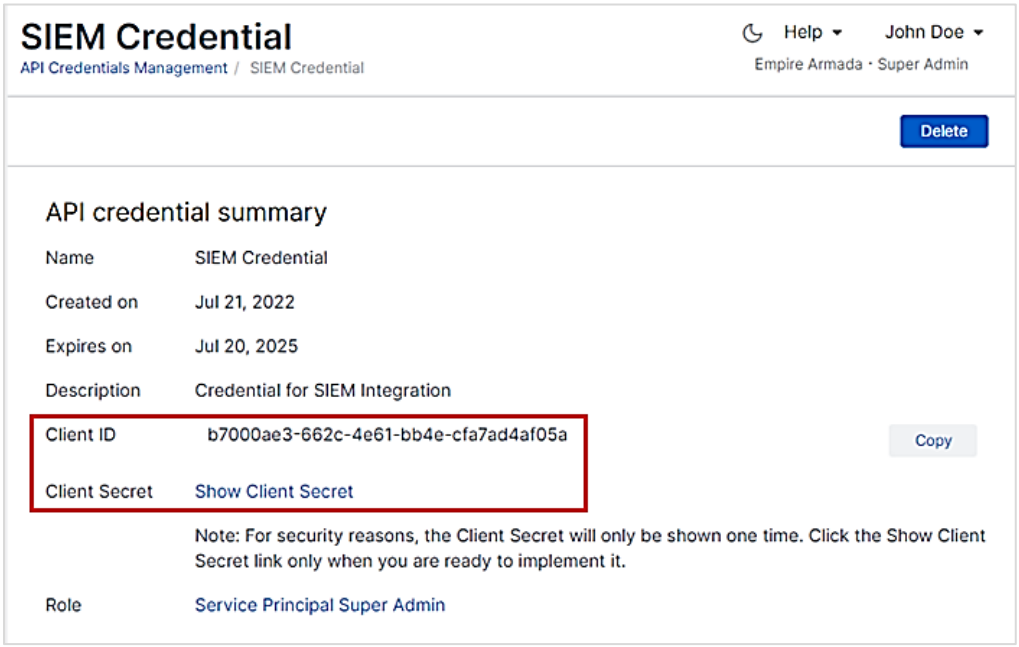


5. Once saved, you will the **API key**. Make a note of the **API Access URL + Headers** which will be used later in the **Python script** for authentication purposes.



Perform the following procedure to generate the API Client Secret and ID.

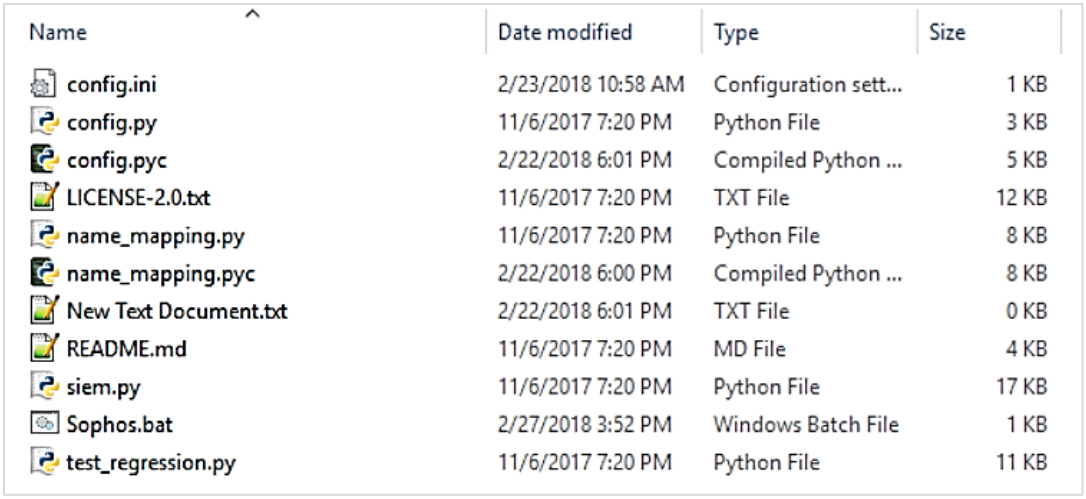
- In Sophos Central Admin, go to **Global Settings** > **API Credentials Management** to access event and alert data via the API.
- To create a new token, click **Add Credential** from the top-right corner of the screen.
- Provide the **Credential name** and appropriate role, add an optional description, and then click **Add**. The **API credential Summary** for this credential will be displayed.
- Click **Show Client Secret** to show **Client Secret.**



3.1.2 Configuring the Sophos Central Integrator Package

To get the Sophos Central Data Source Integrator, contact your account manager.

1. The Integrator package will be obtained in a zip format. Extract the folder to get the following files as shown in the image.



Name	Date modified	Type	Size
config.ini	2/23/2018 10:58 AM	Configuration sett...	1 KB
config.py	11/6/2017 7:20 PM	Python File	3 KB
config.pyc	2/22/2018 6:01 PM	Compiled Python ...	5 KB
LICENSE-2.0.txt	11/6/2017 7:20 PM	TXT File	12 KB
name_mapping.py	11/6/2017 7:20 PM	Python File	8 KB
name_mapping.pyc	2/22/2018 6:00 PM	Compiled Python ...	8 KB
New Text Document.txt	2/22/2018 6:01 PM	TXT File	0 KB
README.md	11/6/2017 7:20 PM	MD File	4 KB
siem.py	11/6/2017 7:20 PM	Python File	17 KB
Sophos.bat	2/27/2018 3:52 PM	Windows Batch File	1 KB
test_regression.py	11/6/2017 7:20 PM	Python File	11 KB

2. In the extracted folder, double click the **config.ini** file to open.

```
[login]
# API Access URL + Headers
# API token setup steps: https://community.sophos.com/kb/en-us/125169
token_info = <Copy API Access URL + Headers block from Sophos Central here>


# Client ID and Client Secret for Partners, Organizations and Tenants
# <Copy Client ID and Client Secret from Sophos Central here>
client_id =
client_secret =
# Customer tenant Id
tenant_id =

# Host URL for Oauth token
auth_url = https://id.sophos.com/api/v2/oauth2/token

# whoami API host url
api_host = api.central.sophos.com

# format can be json, cef or keyvalue
format = json

# filename can be syslog, stdout, any custom filename
filename = result.txt

# endpoint can be event, alert or all
endpoint = event

# syslog properties
# for remote address use <remoteServerIp>:<port>, for e.g. 192.1.2.3:514
# for linux local systems use /dev/log
# for MAC OSX use /var/run/syslog
# append_nul will append null at the end of log message if set to true
address = /var/run/syslog
facility = daemon
socktype = udp
append_nul = false
```

3. In the config.ini file modify the details for **token_info**, **format**, **filename**, **endpoint**, **address**, **facility**, and **socktype** with the appropriate data as specified in the following image.

   - **token_info** = Please replace this value with the **API Access URL + Headers** that is generated by you as show above.
   - **format** = keyvalue is retained by default.
   - **filename** = syslog is retained by default.
   - **endpoint** = all is retained by default.
   - **address** = enter the Netsurion Open XDR Platform manager IP address with port 514 which is default
   - **facility** = daemon is retained by default.
   - **socktype** = udp is retained by default (514 UDP port)
   - **client_id** = copy Client ID from Sophos Central
   - **client_secret** = copy client Secret from Sophos Central

4. Save the file after modifying the details.

5. Next, create a batch file **Sophos.bat** in the same location where the integrator exists and click **Edit** to add the following details.

6. Provide the **path** (in the highlighted location as shown in the below image) where the location of the **python.exe** is present along with **siem.py**

   Note:

   Path varies as per the configuration.

```
C:
cd "%~dp0"
C:\Users\etadmin\AppData\Local\Programs\Python\Python311\python.exe "siem.py"
```

The following is the reference to find python.exe.

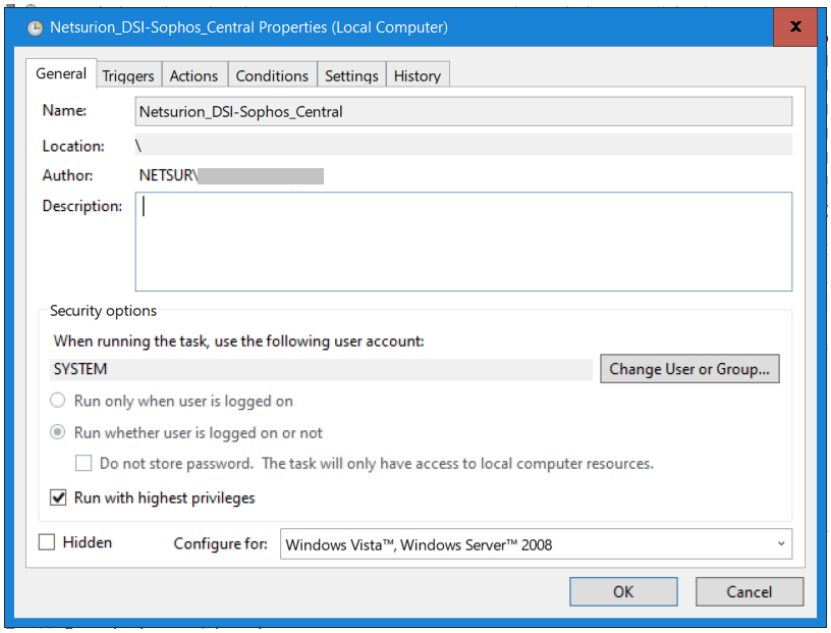
```
C:\Users\[redacted]>where python.exe
C:\Users\[redacted]\AppData\Local\Programs\Python\Python311\python.exe
```

7. Save the file to update the configuration.

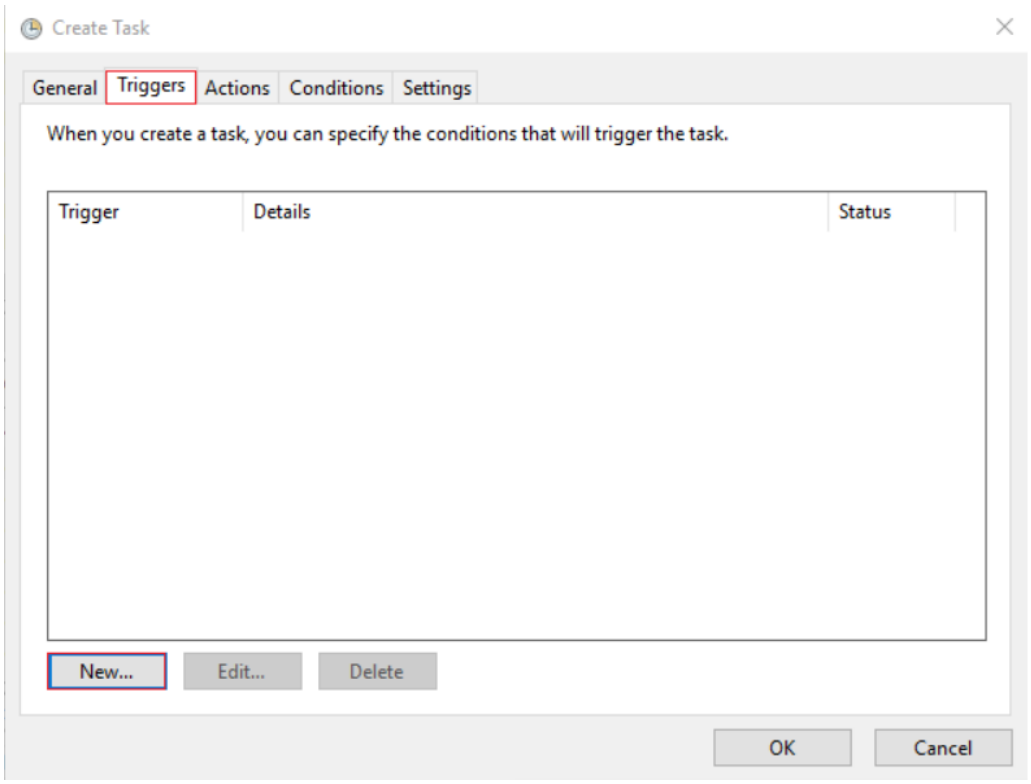
3.1.3 Scheduling the Integrator Script

For the script to fetch the syslog events from Sophos Central on timely basis, a task needs to be scheduled so that the task runs either on hourly, daily, or weekly basis to forward the syslog events to Netsurion Open XDR.

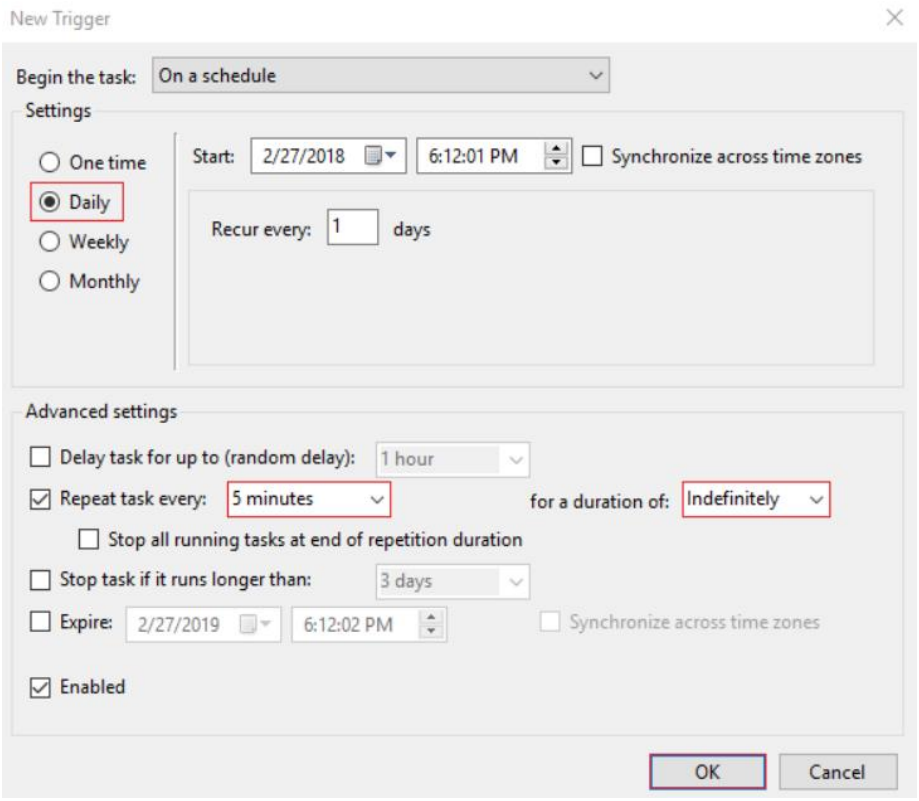
1. Open **Task Scheduler** and click **Create Task**.
2. In the subsequent window, go to the **General** tab and provide the **Name**, **Description** and select the appropriate check box as displayed in the below image.



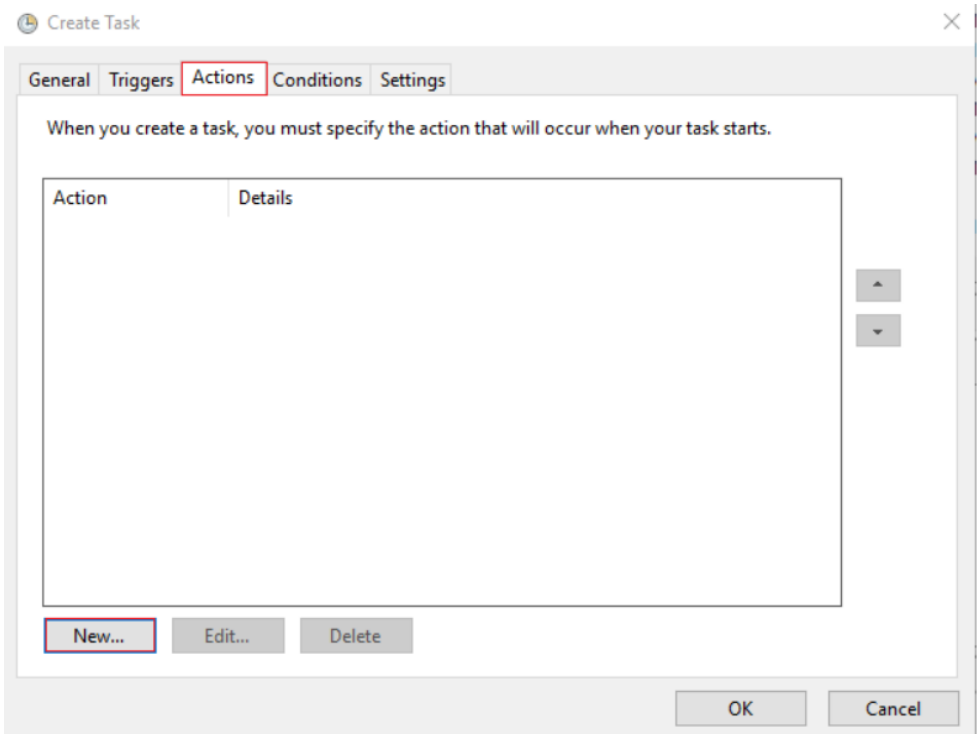
3. Next, go to the **Triggers** tab and click **New**.



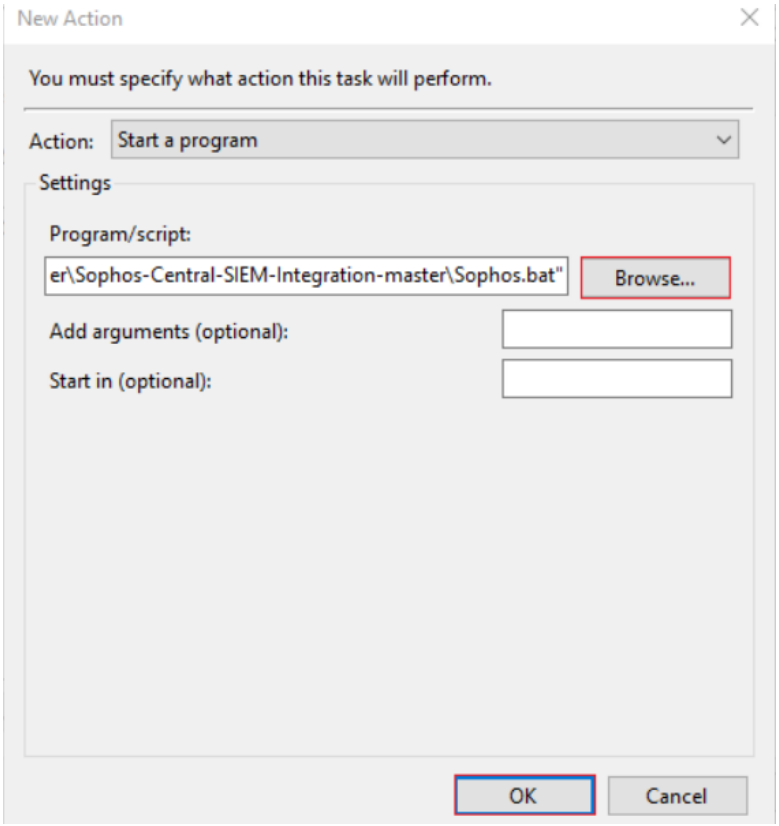
4. In the **New Trigger** window, replicate the same configurations as shown in the following image and click **OK**.



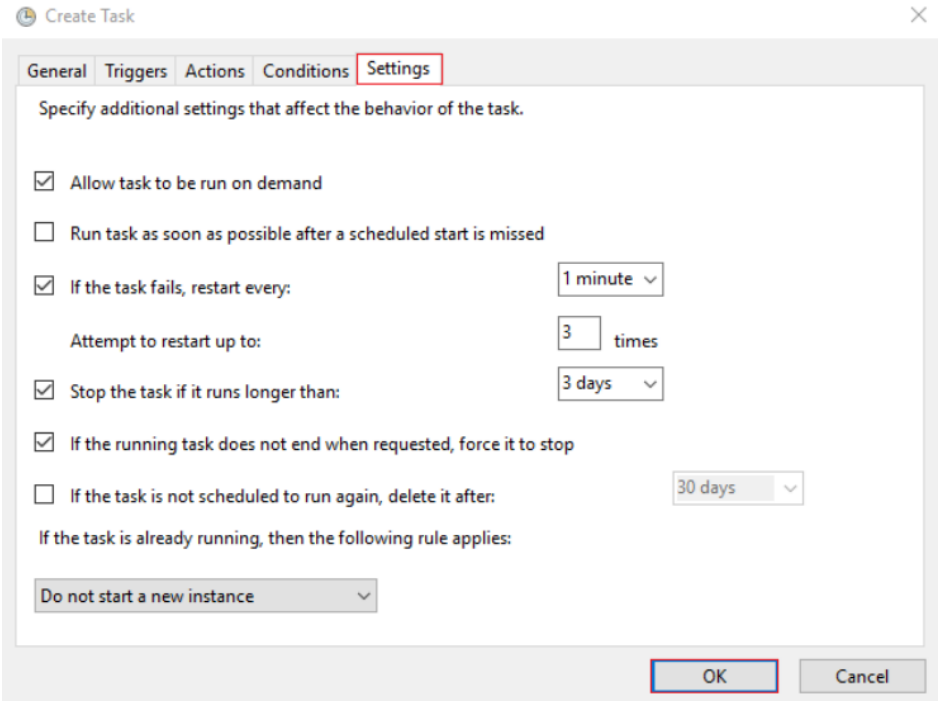
5. Then, go to the **Action** tab and click **New**.



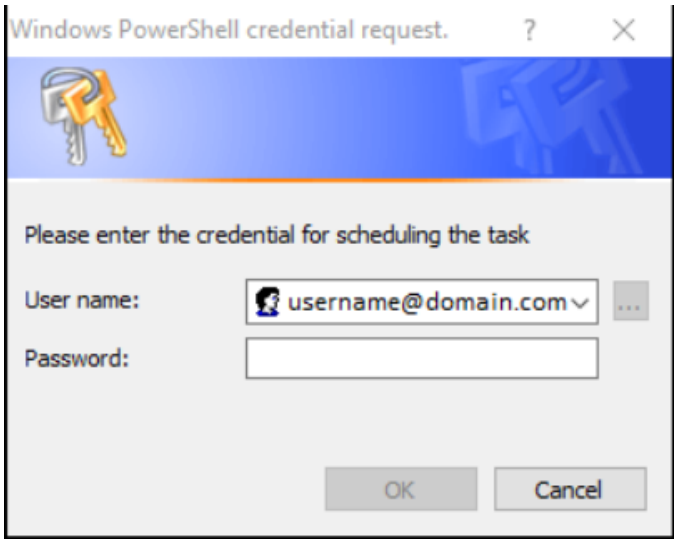
6. In the **New Action** window, choose the **Start a program** option from the **Action** drop-down list**.**
7. Then, click **Browse** to locate the path of the **Sophos.bat** file and click **OK**.



8. Next, go to the **Settings** tab, and replicate the same configurations as shown in the following image and click **OK**.



An authentication window pops-up requesting the Username and password as shown in the following image.



9. Provide your **Administrator System Username** and **Password** to proceed with the Task Scheduling.

The Task is now created, and it runs periodically to execute the script and sends the logs to **Netsurion Open XDR**.

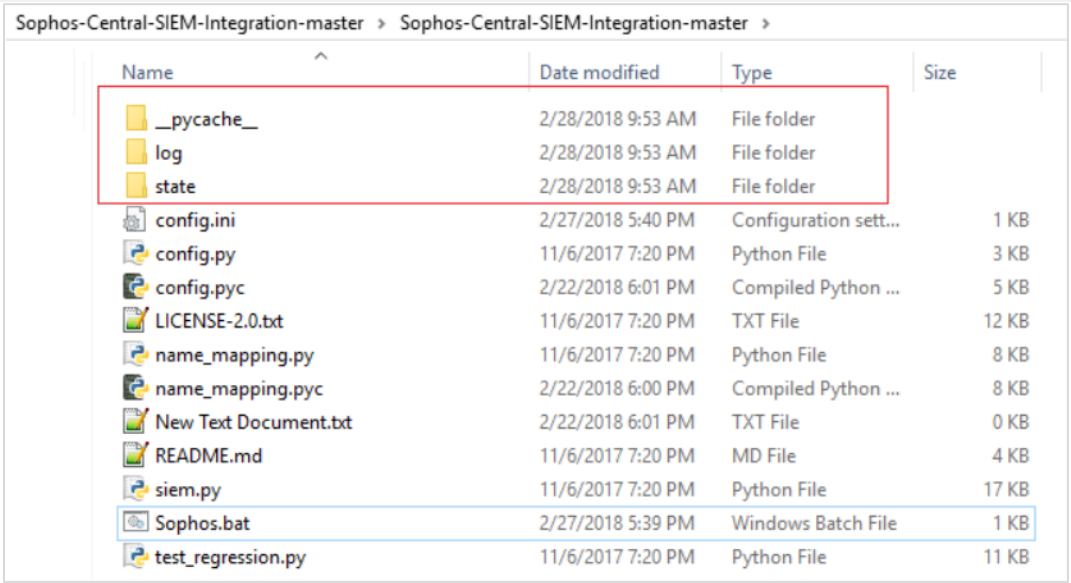
3.2 Verify Sophos Central Integration in Netsurion Open XDR.

Verify the Execution Status of Python Script.

Once the task starts running, three folders (__pycache__, log and state) will be created in the same path where the Sophos.bat file is present as shown in the following image.

Note:

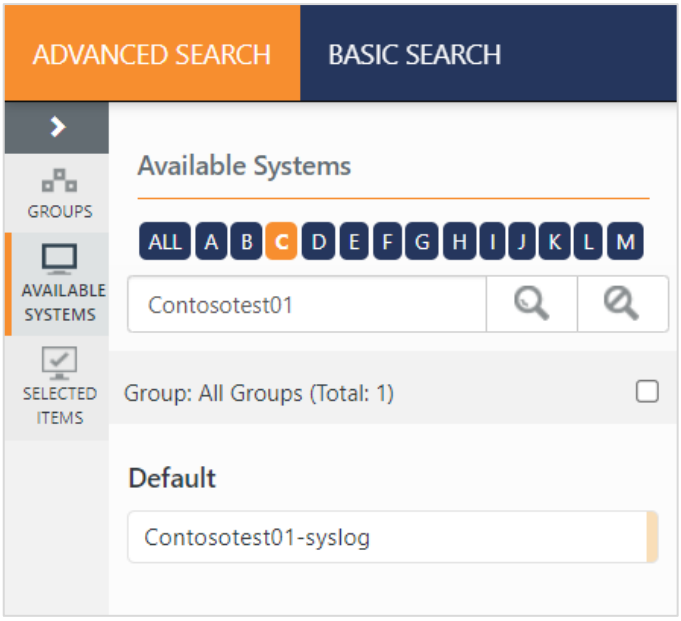
If the folders are not created, then it indicates that the script was not executed successfully.

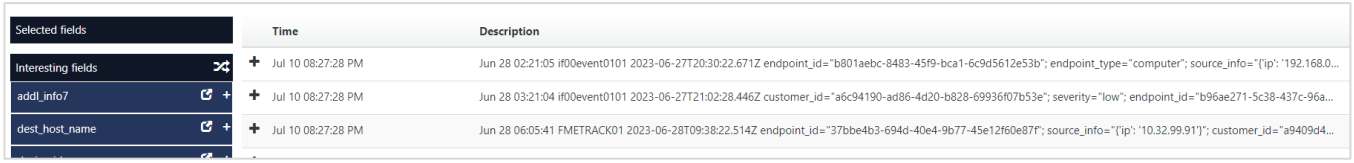


Verify the Logs are Forwarded via Syslog to Netsurion Open XDR.

1. Login to **Netsurion Open XDR** and click **Search**.
2. In the left pane, a system will be added with the name same as that of your system hostname followed by syslog (for example, **hostname-syslog**) as shown in the below image.

Example: If Hostname is **Contosotest01**; then the System added in the console would be **Contosotest01-syslog**.





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 **Sophos Central**.

- Categories_Sophos Central.iscat
- Alerts_Sophos Central.isalt
- Reports_Sophos Central.etcrx
- KO_Sophos Central.etko
- Dashboards_Sophos Central.etwd
- Templates_Sophos Central.ettd

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
Sophos Central: PUA detected	Generated when a Potentially Unwanted Application (PUA) is detected.
Sophos Central: Threat detected	Generated when a suspicious file is detected.

4.2 Reports

Name	Description
Sophos Central - Web filter and application control events	Provides details about web and application control related events detected by Sophos Central.
Sophos Central - PUA and threat events	Provides details about Potentially Unwanted Applications (PUA) and malware related events detected by Sophos Central.
Sophos Central - DLP events	Provides details on Data Loss Prevention (DLP) events detected by Sophos Central.
Sophos Central - Update and user events	Provides details about user and update related events detected by Sophos Central.
Sophos Central - Peripheral related events	Provides details about modification related events detected for peripherals by Sophos Central.

4.3 Dashboards

Name	Description
Sophos Central - DLP events detected	Displays information related to Data Loss Prevention (DLP) events detected.
Sophos Central - PUA and threat detected	Displays information related to threat events categorized as Malware and PUA.
Sophos Central - Events overview	Displays an overview on different type of events detected.
Sophos Central - Action taken by log severity	Displays event types as per severity defined.
Sophos Central - DLP events detected	Displays information related to Data Loss Prevention (DLP) events detected.

4.4 Saved Searches

Name	Description
Sophos Central - DLP events	Provides details about Data Loss Protection (DLP) related events detected by Sophos Central
Sophos Central - PUA and threat events	Provides details about Potentially Unwanted Application (PUA) and malware related events detected by Sophos Central.
Sophos Central - Policy disabled	Provides details on policy modification events detected by Sophos Central.
Sophos Central - Web filter and application control events	Provides details about web and application control related events detected by Sophos Central.
Sophos Central - Windows firewall blocked	Provides details on Windows firewall blocked events detected by Sophos Central.
Sophos Central - Peripheral related events	Provides details about modification related events detected for peripherals by Sophos Central.
Sophos Central - Update and user events	Provides details about user and update related events detected by Sophos Central.

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