Netsurion®

Integration Guide

Integrate SentinelOne With Netsurion Open XDR

Publication Date

January 4, 2024

Abstract

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

Audience

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

Table of Contents

1. Overview

SentinelOne is a next-generation endpoint security product that protects against all threat vectors. It provides unified and proactive security measures to defend the entire technology stack that keeps known and unknown malware and other bad programs from endpoints.

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

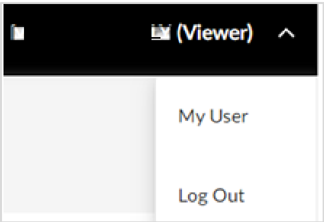
2. Prerequisites

- PowerShell version 5.0 and above must be installed.
- Admin privilege in the SentinelOne console.
- The Data Source Integrator package.

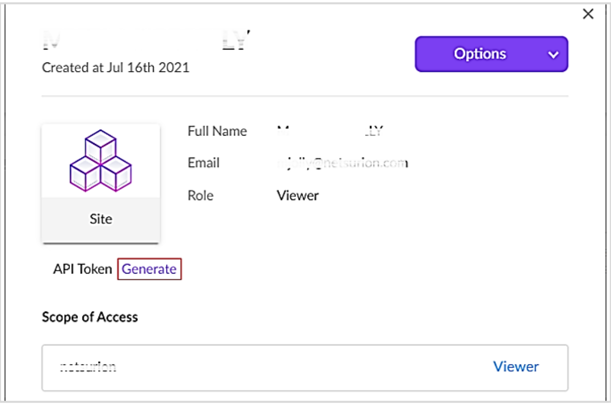
> **Note:**
>
> To get the Data Source Integrator package, contact your Netsurion Account Manager

3. Generate API Token for SentinelOne

1. Log in to **SentinelOne** Console with the viewer role.
2. Select **My User** from the **Viewer** drop-down list.



3. In the **My User** window, click the **Generate** button to generate an API Token.



Created at Jul 16th 2021

Full Name

Email

Role Viewer

API Token

Scope of Access

Viewer

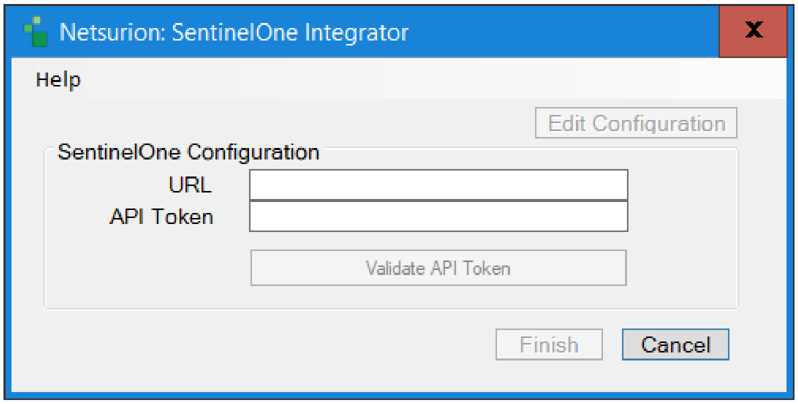
> **Note**:
>
> Make a note of the API Token for using it in subsequent steps.

4. Configuring Netsurion Open XDR SentinelOne Integrator

1. Run the **SentinelOneIntegrator.exe** file with administrator privilege.

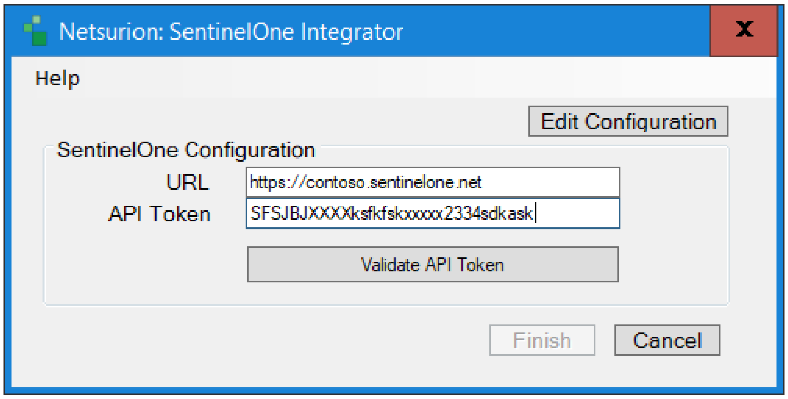
> **Note:**
>
> To get the **SentinelOneIntegrator.exe** file, contact your Netsurion Account Manager.

2. In the **Netsurion: SentinelOne Integrator** window, fill in the following fields and click **Validate API Token** to validate the given details.



- **URL**: SentinelOne console URL
- **API Token:** SentinelOne Viewer Role user token

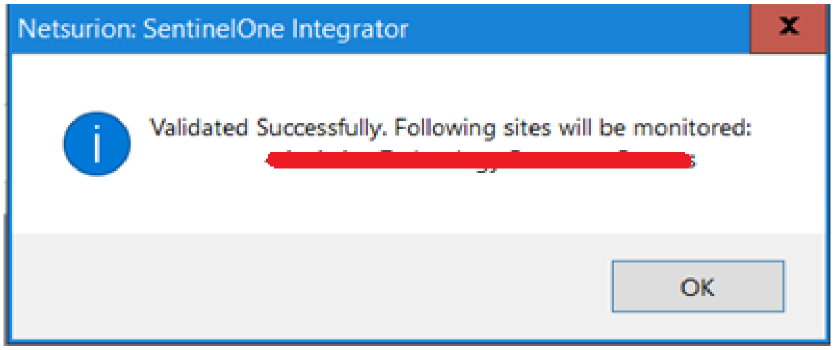
> **Note**:
>
> The **Validate API Token** button will be enabled after providing the configuration details.



URL https://contoso.sentinelone.net

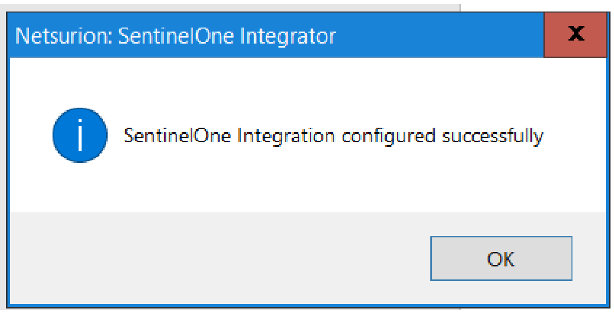
API Token SFSJBJXXXXksfkfskxxxxxx2334sdkask

3. The following message pops up after successful validation. Click **OK.**



Validated Successfully. Following sites will be monitored:
[redacted]

4. Click **Finish** to complete the configuration. The following message pops up for the successful configuration of SentinelOne integrator.



SentinelOne Integration configured successfully

5. Data Source Integrations (DSIs) 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 DSI assets for SentinelOne.

- Alerts_ SentinelOne.isalt
- Reports_ SentinelOne.etcrx
- KO_ SentinelOne.etko
- Dashboards_ SentinelOne.etwd
- Template_SentinelOne.ettd

Note

Refer to the DSI Configuration guide for the procedures to configure the above DSI assets in Netsurion Open XDR.

The following are the key assets available in this Data Source Integration.

5.1 Alerts

Name	Description
SentinelOne: Threat detected on system	Generated for any threat-related activities like new threat detected, and suspicious process dejected.
SentinelOne: USB activity on system	Generated when external devices are connected to the systems, and it is detected by the device control.
SentinelOne: Threat not mitigated	Generated for any failed threat action.

5.2 Reports

Name	Description
SentinelOne - Firewall control activities	Provides details of firewall-related activities like firewall rules applied to the traffic.
SentinelOne - Threat activity details	Provides details of threat-related activities like new threat mitigated, new threat suspicious, process marked as a threat, threat Killed by policy, etc.
SentinelOne - Device control activities	Provides details of external devices connected or disconnected and the rule applied to the event and their action.
SentinelOne - Scan activity details	Provides details of activities related to the scan.
SentinelOne - Management activity details	Provides details of activities that happened in the SentinelOne by the users.
SentinelOne - User login and logout details	Provides details of user login and logout on SentinelOne console.
SentinelOne - User management details	Provides details of user management like user added, user deleted, user, modified, etc.

5.3 Dashboard

Name	Description
SentinelOne - Threat detection by file name	Displays the data about threats detected based on file names.
SentinelOne - Threat detection by category	Displays the data about threats detected based on the category where the threat falls.
SentinelOne - Threat detection by signature	Displays the data about threats detected based on signature where it mentions threat could be in multiple forms.

SentinelOne - Threat detection by computer	Displays the data about threats detected by computers.
SentinelOne - Policy changes	Displays the data about policy changes that occurred in SentinelOne.
SentinelOne - Group management	Displays the data about group management activities of SentinelOne.
SentinelOne - User management	Displays the data about user management activities of SentinelOne.
SentinelOne - Audit activities	Displays the data about user-related changes in the SentinelOne console.

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-Support@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support