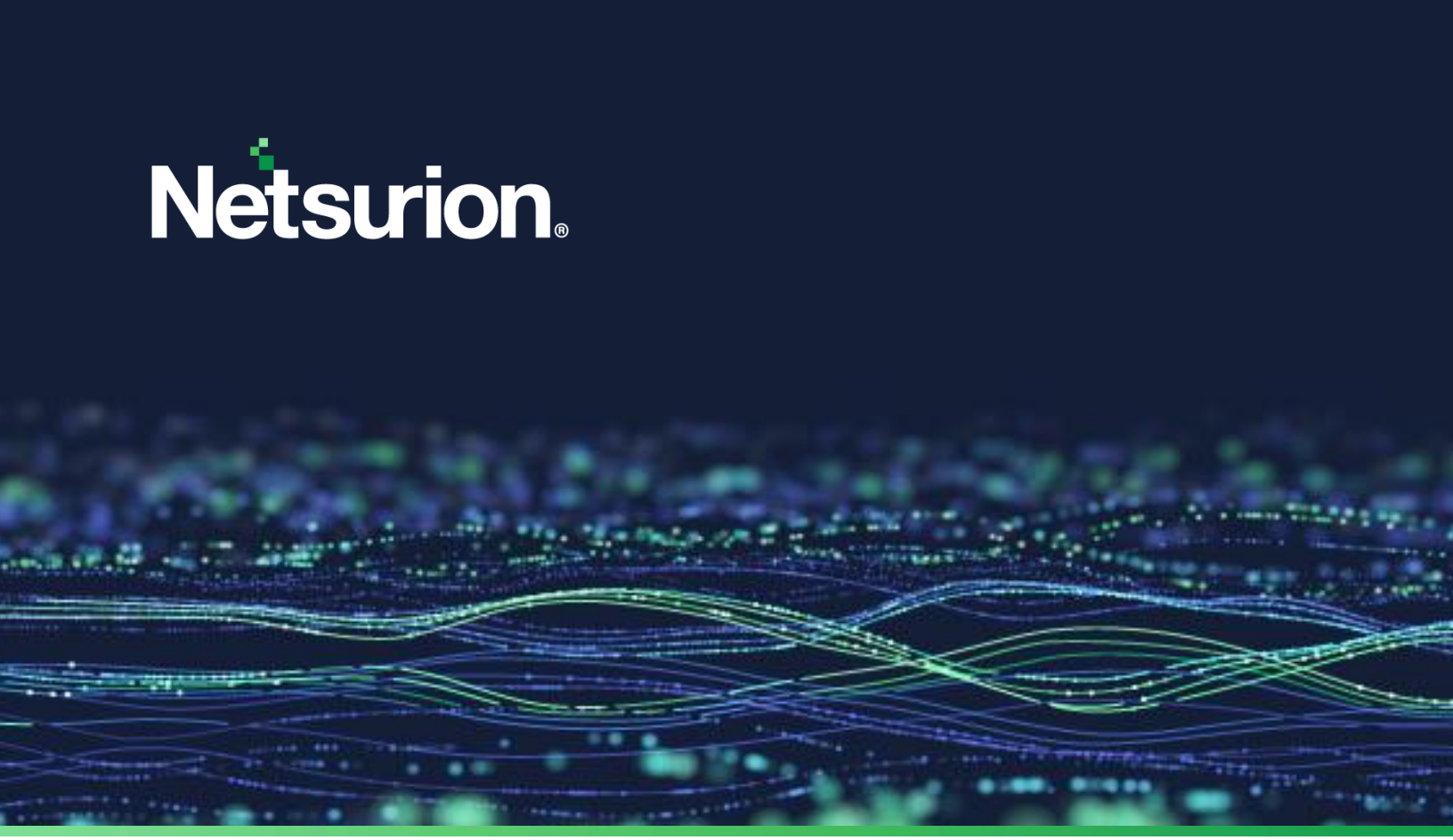


How-To Guide

Integrate Trend Micro Deep Security with Netsurion Open XDR

Publication Date

September 14, 2023

Abstract

This guide provides instructions to configure and integrate Trend Micro Deep Security 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 Trend Micro Deep Security 9.5 and above, and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Trend Micro Deep Security in Netsurion Open XDR.

Table of Contents

1 Overview

Trend Micro Deep Security delivers a comprehensive security platform optimized for virtual and cloud environments. Its extensive security capabilities include anti-malware with web reputation, host-based firewall, intrusion detection and prevention (IDS/IPS), integrity monitoring, and log inspection.

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

2 Prerequisites

- Administrator access to Trend Micro Deep Security Manager (**DSM**) console.
- The Data Source Integration package.

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

3 Integrating Trend Micro Deep Security with Netsurion Open XDR

3.1 Deep Security Manager Server Configuration

Perform the following procedure to configure the DSM server.

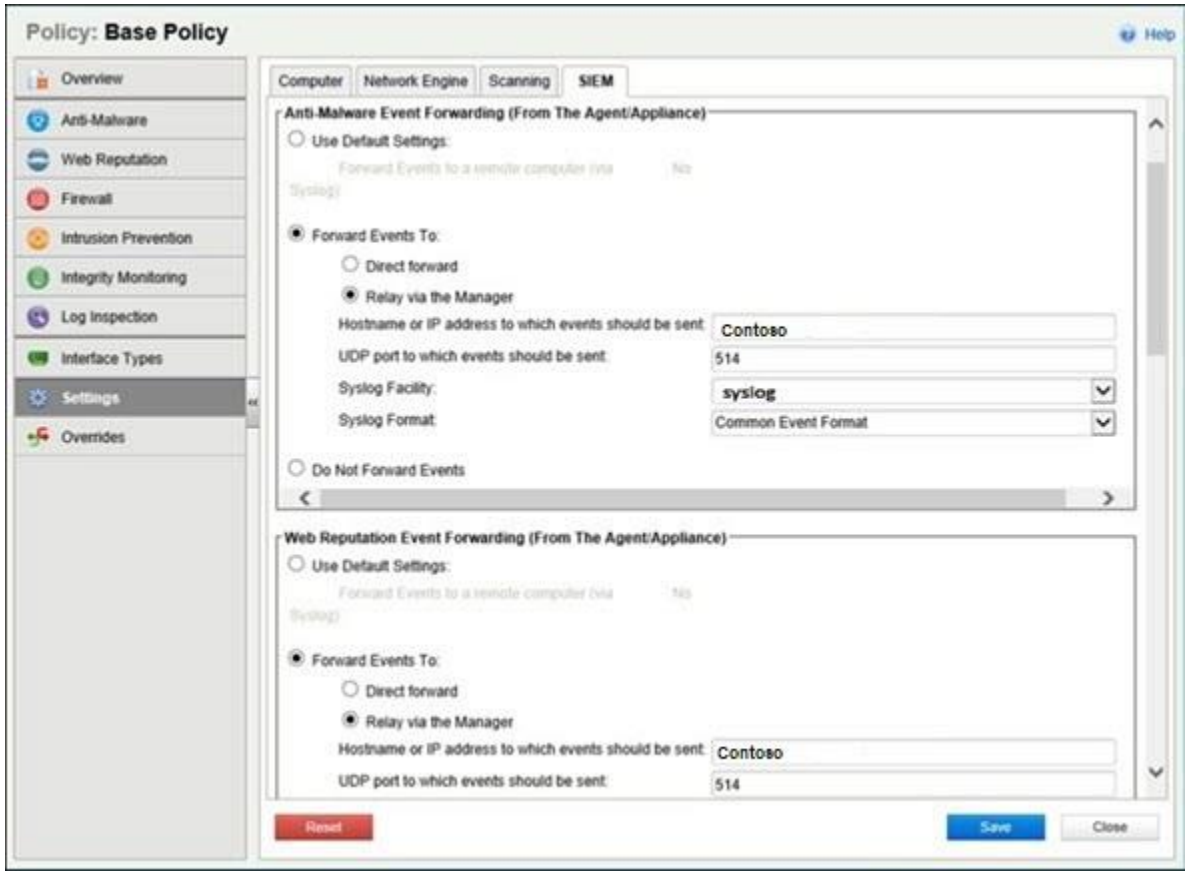
1. Log in to the DSM console and go to **Administration** > **System Settings** > **SIEM**.

2. In the **SIEM** > **System Event Notification** section, provide the following details and click **Save**.
    - Select **Forward System Events to a remote computer** check box to allow the DSM manager to send logs to Netsurion Open XDR.
    - **Hostname or IP to which events should be sent**: Specify the Netsurion Open XDR machine **FQDN** (recommended) or **IP address**. Specify the **UDP Port**. For example, 514.
    - **Syslog Facility: UDP Port to which events should be sent:** Select syslog facility as **syslog.**
    - **Syslog Format**: Specify the **syslog format** as Common Event Format (CEF).

3.2 Deep Security Manager Policy Configuration

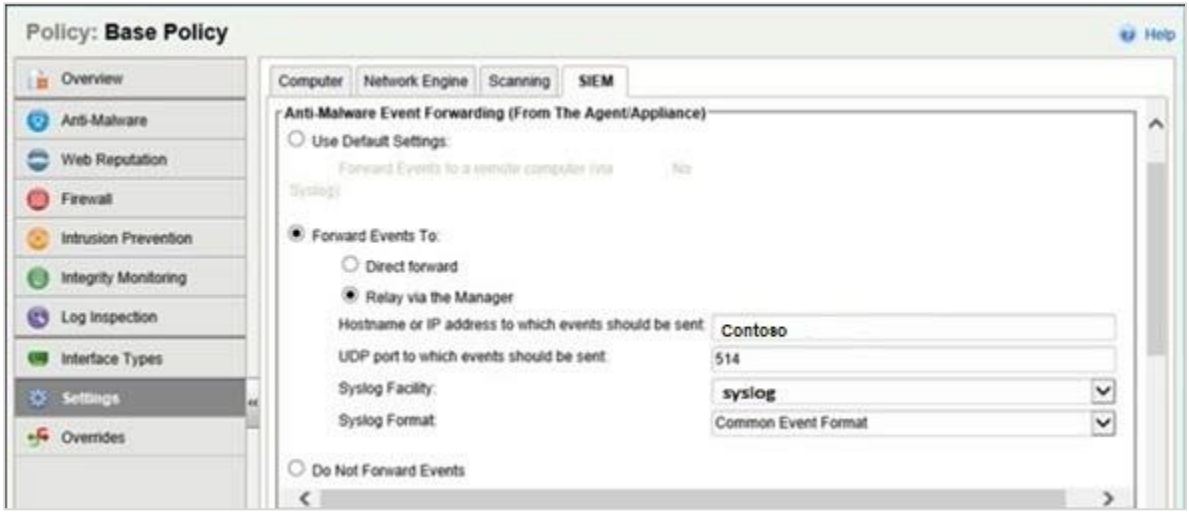
Add the syslog source to your policy configuration and set the integration details at the top (root/ base) policy as follows.

1. In the **DSM** console, go to **Policies** > **Settings** > **SIEM**.



2. In the **SIEM** > **Anti-Malware Event Forwarding** section, choose the **Forward Events To:** and **Relay via the Manager** options, and provide the manager details.

   - **Hostname or IP to which events should be sent**: Specify the **Netsurion Open XDR FQDN (recommended) or IP address**.
   - **UDP Port to which events should be sent:** Specify the UDP port. For example: 514.
   - **Syslog Facility**: Select syslog facility as **syslog** from the drop-down list.
   - **Syslog Format**: Specify the syslog format as **Common Event Format (CEF)**.



3. In the **SIEM** > **Web Reputation Event Forwarding** section, choose the **Forward Events To:** and **Relay via the Manager** options, and provide the manager details.

   - **Hostname or IP to which events should be sent:** Specify the **Netsurion Open XDR FQDN (recommended) or IP address**.
   - **UDP Port to which events should be sent:** Specify the UDP port. For example: 514.
   - **Syslog Facility**: Select syslog facility as **syslog** from the drop-down list.
   - **Syslog Format**: Specify the syslog format as **Common Event Format (CEF)**.

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

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 Trend Micro Deep Security

- Categories_Trend Micro Deep Security.iscat
- Alerts_Trend Micro Deep Security.isalt
- Reports_Trend Micro Deep Security.etcrx
- KO_Trend Micro Deep Security.etko
- Dashboards_Trend Micro Deep Security.etwd
- Token_Trend Micro Deep Security.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
Trend Micro Deep Security: Action taken on malware	Generated whenever Trend Micro Deep Security has acted on a potentially malicious file.
Trend Micro Deep Security: Administrator authentication failed	Generated when Trend Micro user authentication has failed for the user.
Trend Micro Deep Security: Anti-malware action failed	Generated when Trend Micro Deep Security failed to act on a potentially malicious file.
Trend Micro Deep Security: Duplicate computer detected	Generated whenever Trend Micro Deep Security has detected a duplicate computer.
Trend Micro Deep Security: Intrusion prevention detected	Generated when an intrusion prevention event has occurred related to Trend Micro Deep Security.
Trend Micro Deep Security: Malicious URL detected	Generated when a request related to the device has been marked as suspicious due to some reason.
Trend Micro Deep Security: No action taken on malware	Generated when Trend Micro Deep Security acted on a potentially malicious file.

4.2 Reports

Name	Description
Trend Micro Deep Security - User management	Provides all details related to activities concerning User management in Trend Micro Deep Security.
Trend Micro Deep Security - Active directory activity	Provides all details related to active directory activities in Trend Micro Deep Security.
Trend Micro Deep Security - File integrity monitoring	Provides all details related to the file integrity monitoring in Trend Micro Deep Security.
Trend Micro Deep Security - Antimalware activity	Provides all details related to the antimalware activities in Trend Micro Deep Security.
Trend Micro Deep Security - Firewall activity	Provides all details related to activities concerning firewall activities in Trend Micro Deep Security.
Trend Micro Deep Security - Intrusion prevention	Provides all details related to the intrusion prevention in Trend Micro Deep Security.
Trend Micro Deep Security - User authentication failed	Provides all details related to user authentication failed in Trend Micro Deep Security.
Trend Micro Deep Security - User logon activity	Provides all details related to user logon activities in Trend Micro Deep Security.
Trend Micro Deep Security - System logs	Provides all details related to activities concerning system logs in Trend Micro Deep Security.
Trend Micro Deep Security - Computer management	Provides all details related to activities concerning computer management in Trend Micro Deep Security.
Trend Micro Deep Security - Policy management	Provides all details related to policy management in Trend Micro Deep Security.
Trend Micro Deep Security - Roles management	Provides all details related to roles management in Trend Micro Deep Security.
Trend Micro Deep Security - Group management	Provides all details related to group management in Trend Micro Deep Security.

4.3 Dashboards

Name	Description
Trend Micro Deep Security - User authentication failed	Displays all details about user authentication failed activities.
Trend Micro Deep Security - Successful user login by IP address	Displays all details about successful user login by IP address.
Trend Micro Deep Security - Malicious hashes by threat names	Displays all details about malicious hashes by threat names.
Trend Micro Deep Security - Suspicious file paths by threat name	Displays all details about suspicious file paths by threat name.
Trend Micro Deep Security - Intrusion detected on destination IP	Displays all details about intrusion detected on destination IP.
Trend Micro Deep Security - Computer management	Displays all details about computer management.
Trend Micro Deep Security - Policy management	Displays all details about policy management.

4.4 Saved Searches

Name	Description
Trend Micro Deep Security - User management	Provides all details related to activities concerning User management in Trend Micro Deep Security.
Trend Micro Deep Security - Active directory activity	Provides all details related to active directory activities in Trend Micro Deep Security.
Trend Micro Deep Security - File integrity monitoring	Provides all details related to the file integrity monitoring in Trend Micro Deep Security.
Trend Micro Deep Security - Antimalware activity	Provides all details related to the antimalware activities in Trend Micro Deep Security.
Trend Micro Deep Security - Firewall activity	Provides all details related to activities concerning firewall activities in Trend Micro Deep Security.
Trend Micro Deep Security - Intrusion prevention	Provides all details related to the intrusion prevention in Trend Micro Deep Security.
Trend Micro Deep Security - User authentication failed	Provides all details related to user authentication failed in Trend Micro Deep Security.
Trend Micro Deep Security - User logon activity	Provides all details related to user logon activities in Trend Micro Deep Security.

Trend Micro Deep Security - Computer management	Provides all details related to activities concerning computer management in Trend Micro Deep Security.
Trend Micro Deep Security - Policy management	Provides all details related to policy management in Trend Micro Deep Security.
Trend Micro Deep Security - Roles management	Provides all details related to roles management in Trend Micro Deep Security.
Trend Micro Deep Security - Group management	Provides all details related to group management in Trend Micro Deep Security.
Trend Micro Deep Security - System logs	Provides all details related to activities concerning system logs in Trend Micro Deep Security.

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