How-To Guide

Integrate SonicWall SMA with Netsurion Open XDR

Publication Date

August 09, 2023

Abstract

This guide provides instructions to configure and integrate SonicWall SMA with Netsurion Open XDR to retrieve its logs via Syslog Integration 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 SonicWall SMA and Netsurion Open XDR 9.3 or later.

Audience

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

Table of Contents

1 Overview

SonicWall SMA (Secure Mobile Access) is a unified secure access gateway that enables organizations to provide access to any application, anytime, from anywhere and any devices, including managed and unmanaged.

Netsurion Open XDR manages logs retrieved from SonicWall SMA. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in SonicWall SMA. This DSI supports all SonicWall SMA 100 series devices which includes SMA 200/210, SMA 400/410, SMA 500v.

2 Prerequisites

- SonicWall SMA 100 series appliance with administrator access.
- Port **514** (UDP) must be set to OPEN and must be dedicated for SYSLOG communication only.
- Must have the subscription enabled for **Web Application Firewall (WAF)** service in the respective SonicWall SMA device.

  IMPORTANT

  If this **Web Application Firewall (WAF)** service is not enabled, then the following DSI assets will not be reflected.

  - **Dashboard:** SonicWall SMA - Web application firewall events.
  - **Report:** SonicWall SMA - Web application firewall events
  - **Saved Search:** SonicWall SMA - Web application firewall events.
- The Data Source Integration package.

  Note

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

3 Integrating SonicWall SMA with Netsurion Open XDR

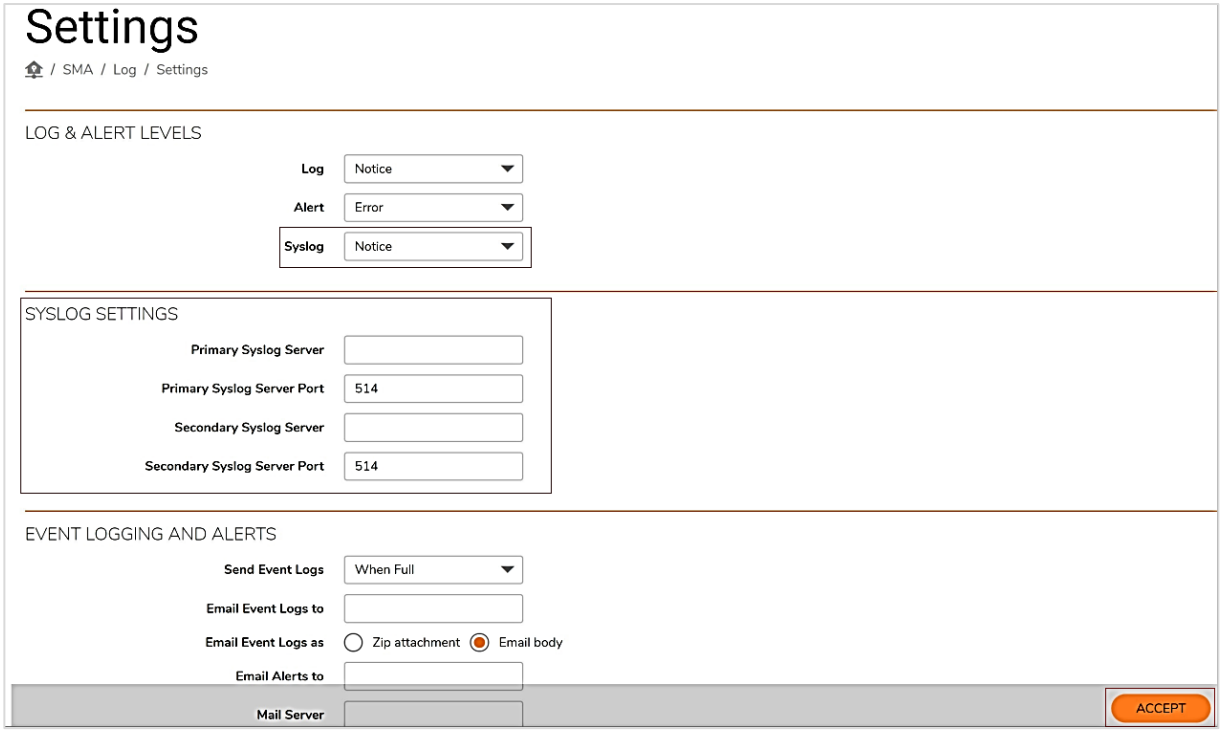
Integrate SonicWall SMA to Netsurion Open XDR via syslog by using the syslog service available in the SonicWall SMA GUI console.

Note

The following syslog integration steps and DSI components will support all SonicWall SMA 100 series devices which includes SMA 200/210, SMA 400/410, SMA 500v with firmware v10.2.1.x.

3.1 Configuring the SYSLOG Settings

1. Log in to the **SonicWall SMA** web console and go to **Log** > **Settings** to configure and transmit the log from SonicWall SMA device to Netsurion Open XDR server.



2. In the **LOG & ALERT LEVELS** section, from the **Syslog** drop-down list, select the required option (such as, emergency, alert, critical, error, warning, notice, info, and debug).

> **Note**
>
> Recommended selecting **Notice** to get all the relevant logs that have the notice priority level and above as per SonicWall.

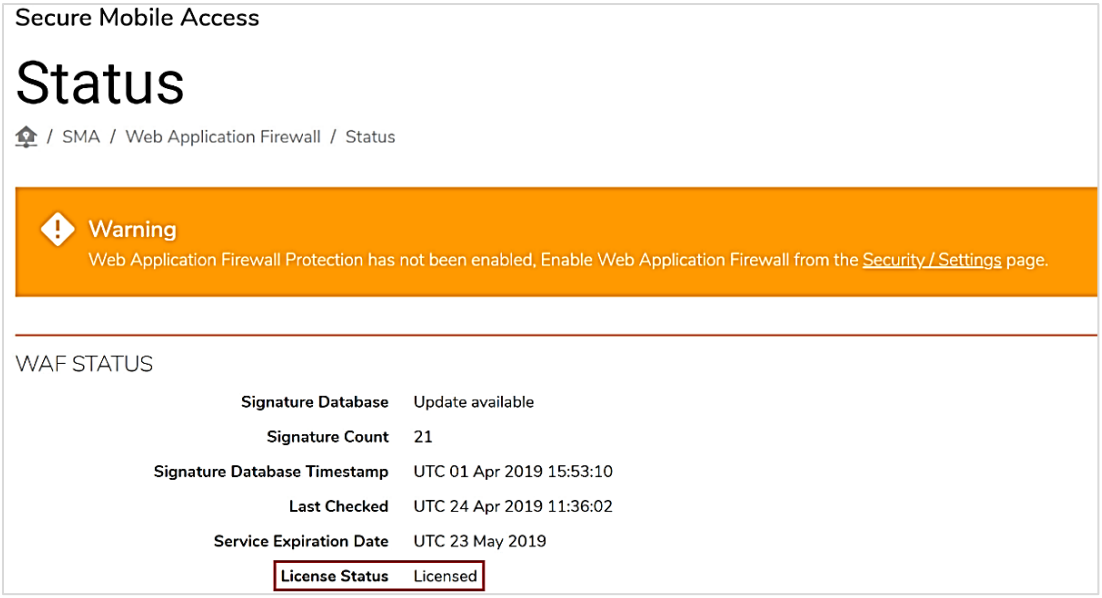
3. In the **SYSLOG SETTINGS** section, provide the following details for Netsurion Open XDR.
   - In the **Primary Syslog Server** field, enter the **IP Address** or **FQDN** (recommended to provide FQDN).
   - In the **Primary Syslog Server Port** field, enter **514**.

> **Note**
>
> If the primary syslog server is already defined, kindly provide the specified configuration details in the Secondary Syslog Server. Port **514 (UDP)** must be set to open for communication with Netsurion Open XDR (IP/ FQDN.).

4. After providing the details, click **ACCEPT** to update and save the changes.

3.2 Verifying the Web Application Firewall Service Status

Log in to the **SonicWall SMA** web console and navigate to **Web Application Firewall** > **Status** to verify the status of WAF service.



4 Data Source Integration (DSI) in Netsurion Open XDR

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

The Data Source Integration package contains the following files for **SonicWall SMA**.

- Categories_SonicWall SMA.iscat
- Alerts_SonicWall SMA.isalt
- Reports_SonicWall SMA.etcrx
- KO_SonicWall SMA.etko
- Dashboards_SonicWall SMA.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
SonicWall SMA: Anomalous authentication detected	Generated when a potential anomalous authentication is detected by SonicWall SMA.
SonicWall SMA: Suspicious event detected	Generated when a suspicious activity is detected by SonicWall SMA.

4.2 Reports

Name	Description
SonicWall SMA - Web application firewall events	Provides details about all the Web Application Firewall (WAF) events detected by SonicWall SMA device.
SonicWall SMA - VPN client events	Provides details about the VPN client events detected by SonicWall SMA device.
SonicWall SMA - Authentication and authorization events	Provides details about the authentication and authorization related events detected by SonicWall SMA device.
SonicWall SMA - Device management events	Provides details about the device management events detected by SonicWall SMA device.

4.3 Dashboards

Name	Description
SonicWall SMA - Login failed events by user	Displays events related to users failed login attempts.
SonicWall SMA - Web application firewall events	Displays events related to Web Application Firewall (WAF).
SonicWall SMA - Login and logout successful events by user.	Displays events for a user successfully login and logout.
SonicWall SMA - Source IP by geo location.	Displays the geo location of the source IP address.

4.4 Saved Searches

Name	Description
SonicWall SMA - Web application firewall events	Provides details about all the Web Application Firewall (WAF) events detected by the SonicWall SMA device
SonicWall SMA - VPN client events	Provides details on the events that the SonicWall SMA device's VPN client has triggered.
SonicWall SMA - Authentication and authorization events	Provides details about the authentication and authorization related events detected by the SonicWall SMA device.
SonicWall SMA - Device management events	Provides details about the device management events detected by the SonicWall SMA device.

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