How-To Guide

Configure Syslog Over TLS in Netsurion Open XDR

Publication Date:

October 27, 2023

Abstract

This guide provides instructions to configure syslog over TLS to forward data from the Device or Client to Netsurion Open XDR using a Certificate.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

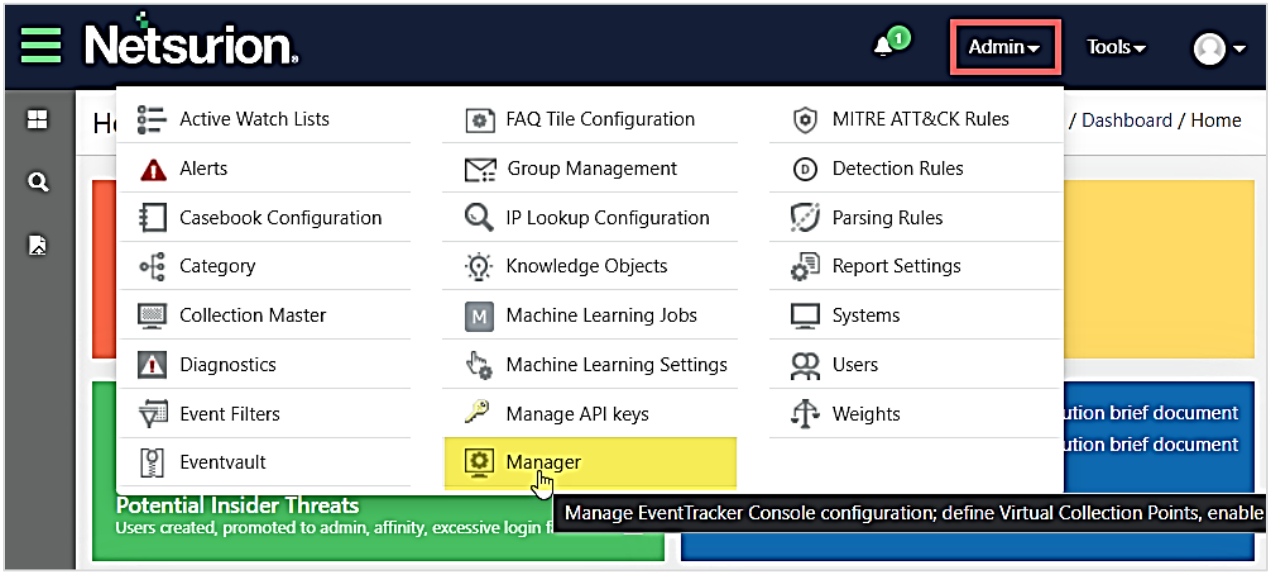
The configuration details in this guide are consistent with Netsurion Open XDR 9.3 or later.

Audience

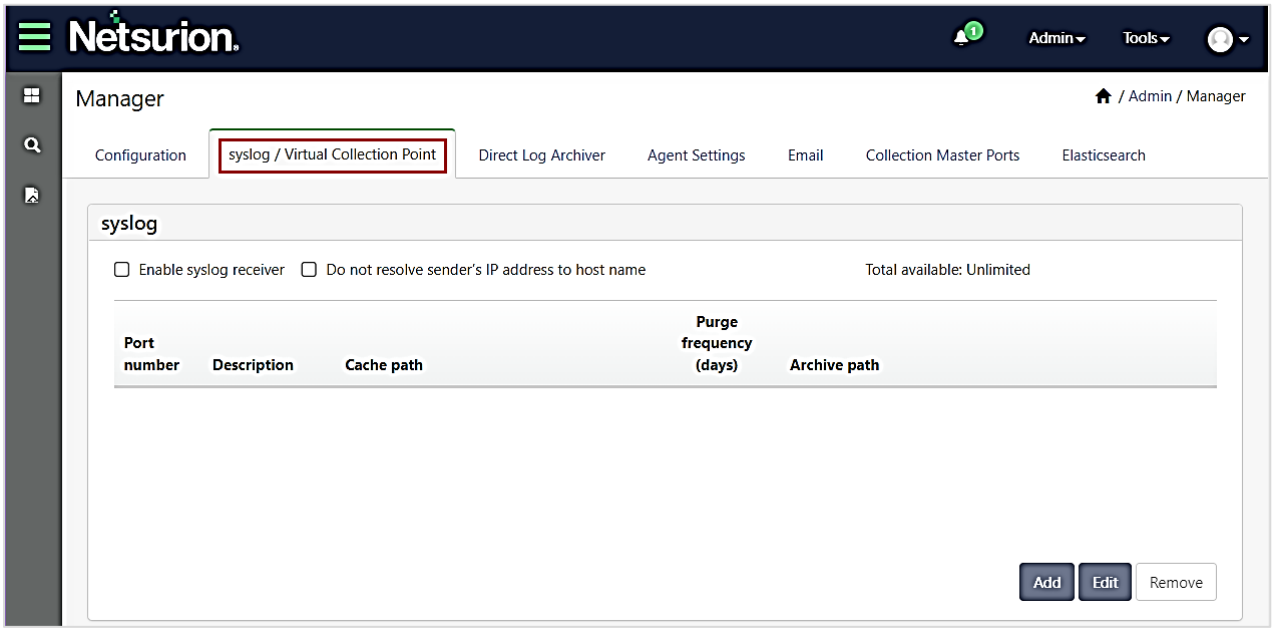
This guide is for the administrators responsible for configuring syslog over TLS using the certificate provided by Netsurion.

To configure syslog over TLS in Netsurion Open XDR,

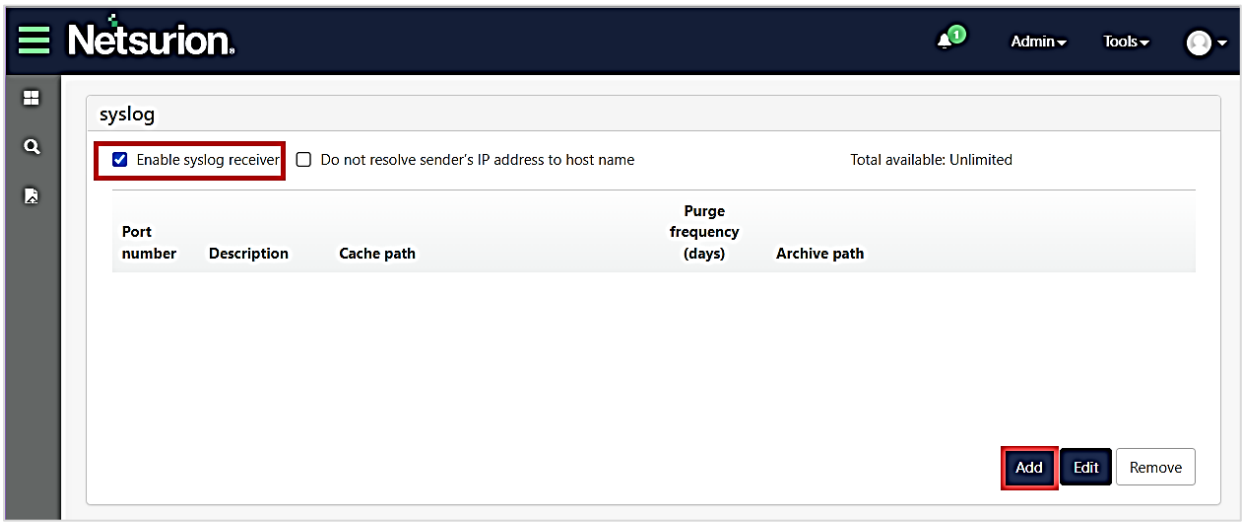
1. Log in to Netsurion Open XDR, hover over the **Admin** menu and click **Manager.**



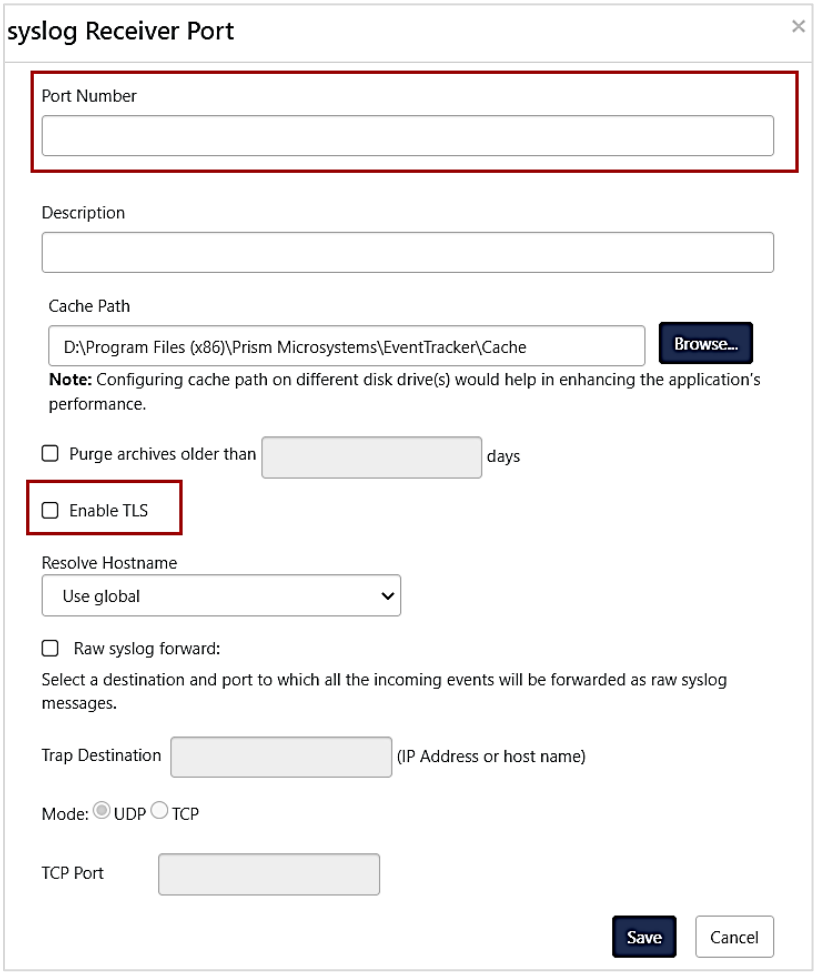
2. In the Manager interface, click the syslog/ Virtual Collection Point tab.



3. In the **syslog** pane, select the **Enable syslog receiver** check box and click **Add** to add the configuration details.



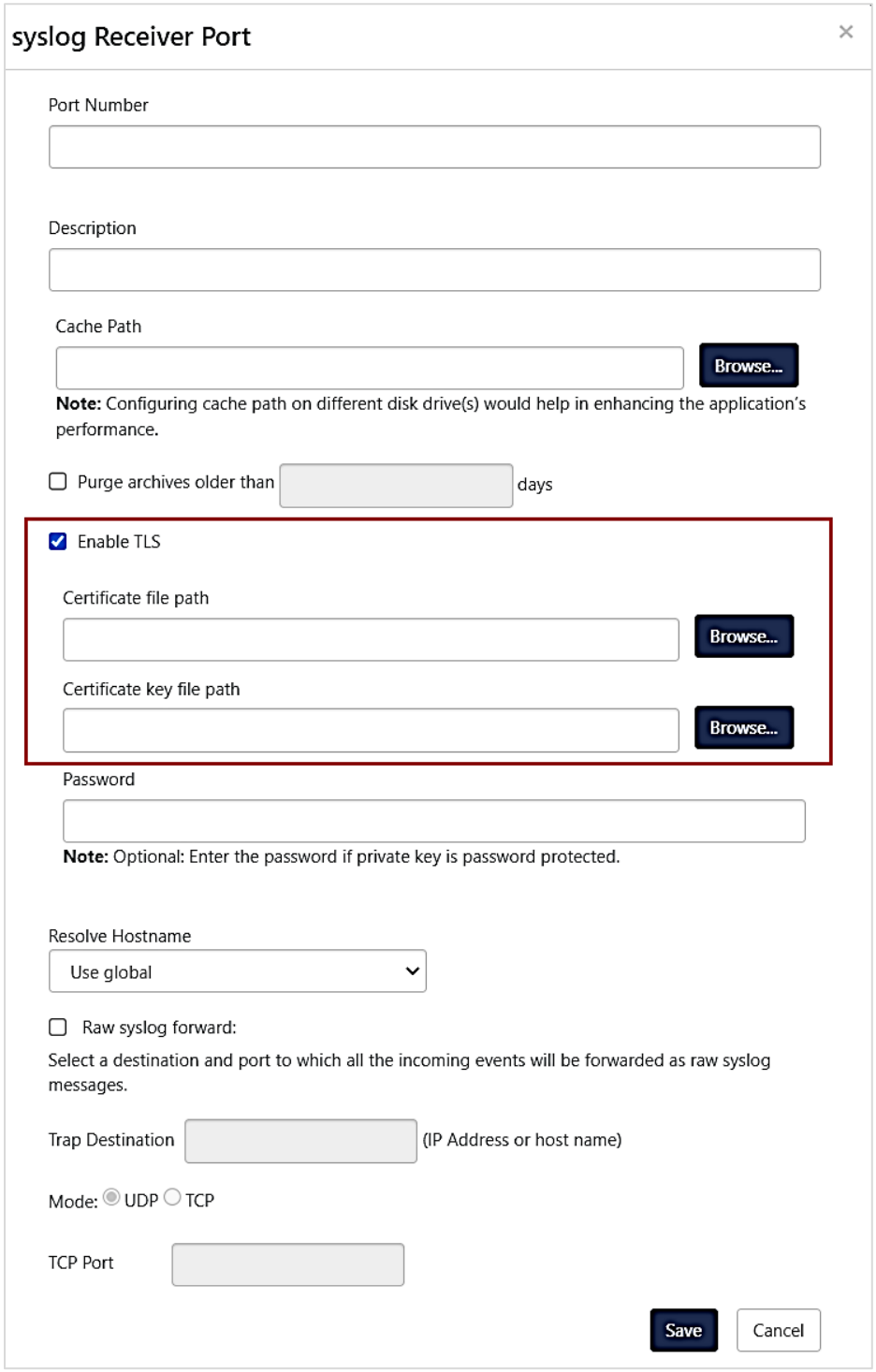
4. In the **syslog Receiver Port** window, specify the **Port Number** and then select the **Enable TLS** check box to provide the certificate information.



5. Browse and locate the appropriate **Certificate file path** and the **Certificate key file path** details.

Note:

Access the **syslogserver.cert.pem** certificate file and the **syslogserver.key.pem** certificate key file distributed with the product by navigating to the **\EventTracker\Cert** path.



6. After providing all the details, click **Save**.

If the sending device supports connecting to servers with the certificate issued by an untrusted Certificate Authority (CA, also known as "anonymous" mode), then ignore the following steps.

7. Download the CA certificate from CA certificate file.
   https://downloads.netsurion.com/Syslogover-TLS/syslogovertlsca-cert.zip

8. Add the CA certificate to the trusted CA list on the Device or Client side. Refer the Device or Client specific documentation for more details.

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