



How-To Guide

Configure Syslog Over TLS in Netsurion Open XDR

Publication Date:

October 27, 2023

© Copyright Netsurion. All Rights Reserved.



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.

≡	Netsurion.		▲ 1 Admin •	Tools 🗸 🌍 🗸
1 Q	H Image: Active Watch Lists Alerts Image: Casebook Configuration Image: Category Image: Collection Master Image: Diagnostics Image: Event Filters Image: Event Vault	 FAQ Tile Configuration Group Management IP Lookup Configuration Knowledge Objects Machine Learning Jobs Machine Learning Settings Manage API keys 	 MITRE ATT&CK Rules Detection Rules Parsing Rules Report Settings Systems Users Weights 	/ Dashboard / Home
	Potential Insider Threats Users created, promoted to admin, affinity,	excessive login f	Console configuration; define Virtual	Collection Points, enable

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

≡	Netsurio	on.				A 0	Admin -	Tools -	•
	Manager						1	🕈 / Admin /	Manager
۹	Configuration	syslog / Virtual Collection Point	Direct Log Archiver	Agent Settings	Email	Collection Master Ports	Elastic	search	
	syslog								
	Enable sy	slog receiver 🔲 Do not resolve send	der's IP address to host na	me		Total available: Unlimited			
	Port number	Description Cache path		Purge frequency (days)	Archive	path			
						[Add E	dit Remo	ve



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

≡	Netsurion.			A D	Admin -	Tools 🗸	•
•	syslog						
۹	Enable syslog receiver Do not resolve sender's IP address to host name	e	Total avai	lable: Unlim	ited		
R.		Purge					
	number Description Cache path	(days)	Archive path				
					Add E	dit Remo	ve

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

Port Number			
Description			
Cache Path			
D:\Program Files (x86)\Prisr	Microsystems\EventTra	acker\Cache	Browse
Note: Configuring cache path performance.	on different disk drive(s) would help in enhancing the	application's
D Purge archives older than		days	
Enable TLS			
Resolve Hostname			
Use global	~		
Raw syslog forward:			
Select a destination and port to messages.	which all the incoming	events will be forwarded as ra	w syslog
Trap Destination	(IP Ad	dress or host name)	
Mode: 🖲 UDP 🔿 TCP			
TCP Port			
		Save	Cancel

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.

Port Number					
Description					
Cache Path					
					Browse
Note: Configur performance.	ing cache path	on different dis	k drive(s) wo	uld help in enhancin	g the application's
Purge archiv	es older than			days	
Enable TLS					
Certificate file	path				
	-				Browse
Certificate key	file path				
					Browse
Password					
Nete: Option:	l. Entor the pa	soword if private	kov is possu	and protocted	
Note. Optiona	al. Enter the pa	ssword in private	e key is passw	ord protected.	
Resolve Hostnar	ne				
Use global			~		
Raw syslog	forward:				
Select a destinat messages.	tion and port to	o which all the ir	ncoming ever	nts will be forwarded	as raw syslog
Trap Destinatior	1		(IP Address	or host name)	
Mode: 🖲 UDP 🤇	TCP				

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 <u>www.netsurion.com</u>.

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