

**Installation Guide** 

# **Netsurion Open XDR 9.4**

**Publication Date** 

September 22, 2023

© Copyright Netsurion. All Rights Reserved.



# Abstract

This guide facilitates the procedures to install and configure Netsurion Open XDR 9.4 and helps to verify the expected functionality of all its components.

Netsurion Open XDR is a reliable, policy-driven SIEM solution that further monitors and manages critical events generated by Windows Operating System, Solaris BSM, Unix (SYSLOG), SYSLOG-NG and SNMP devices. Netsurion Open XDR is an Enterprise-Grade solution for managing IT security, log management, and auditing user activity that provides real-time alerts, secure warehousing, and flexible reporting.

### Note:

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

# Audience

This guide is for Netsurion Open XDR users and Network/ System administrators responsible for installing and configuring Netsurion Open XDR 9.4.



### **Table of Contents**

1	I	ntro	roduction	5
2	S	Syst	tem Requirements	5
	2.1		Hardware Requirements	5
	2.2		Software Requirements	6
3	I	nsta	talling Netsurion Open XDR	7
	3.1		Pre-installing Instructions for Local Account and Active Directory Authentication	7
	3.2		Installing the Netsurion Open XDR Manager	8
	3.3		Pre-install Checklist for the Netsurion Open XDR Manager	8
	3	3.3.1	1 IIS Settings	9
	3	3.3.2	2 User Permission on SQL Server	9
	3.4		Installing the Netsurion Open XDR Manager - Custom	10
	3	3.4.1	1 Netsurion Open XDR Preinstall Check	12
	3	3.4.2	2 The Netsurion Open XDR 9.4 Setup Wizard	23
	3	3.4.3	3 Configuring Netsurion Open XDR 9.4	34
	3.5		Installing the Netsurion Open XDR Manager – Standard or Collection Point Evaluation Version	35
4	0	Dep	oloying the Netsurion Open XDR Windows Sensor	37
	4.1		Pre-install Instructions for Windows Sensor	37
	4.2		Pre-install checklist for Windows Sensor	38
	4.3		Different methods to install the Netsurion Open XDR Sensors	38
	4.4 fea	ture	Deploying the Netsurion Open XDR Windows Sensor via System Manager for Sensor Based Systems ( ed)	(full 39
	4.5		Configuring the Netsurion Open XDR Windows Sensors	47
	4.6		Configuring Sensor-less collection via System Manager (limited features)	48
	4.7		Deploying the Netsurion Open XDR Windows Sensor - Microsoft Windows 10 and above	54
	4	1.7.1	1 Prerequisites for Windows Sensor – Microsoft Windows 10 and above	54
	4	1.7.2	2 Installing / Uninstalling Microsoft Windows 10 and above Sensor	55
5	S	Sens	isor Deployment	. 55
6	S	Secu	uring Netsurion Open XDR	. 55
7	ι	Jnir	installing the Netsurion Open XDR Windows Sensor	. 55
	7.1		Uninstalling via Control Panel	55
	7.2		Uninstalling via System Manager	56
		1	installing Notsurian Anon YDP	FO



9	Ро	rts in Netsurion Open XDR	. 60
10	I	URL or Domain Accessed by Netsurion Open XDR	.61
11		Troubleshooting	.62
1	1.1	Known Issues while installing Netsurion Open XDR 9.4	. 62
1	1.2	Frequently Asked Questions	. 63



# 1 Introduction

Today, the concern for security has rapidly increased among leading-edge entities and requires technologydriven, tenable solutions to work in a secure environment. Netsurion Open XDR, our Managed Threat Protection platform, efficiently conducts vulnerabilities, prevents malware attacks, detects skeptical behavior, and promptly acknowledges suspicious anomalies. This installation guide helps you to install our product effortlessly.

To familiarize with the various product features, follow our web site, <u>Threat Protection Platform</u> in the brochure of this package.

# 2 System Requirements

For optimal performance, the following are the hardware and software requirements to host **Netsurion Open XDR**.

#### Note

Ensure the update of the latest service packs of all Microsoft Windows.

### 2.1 Hardware Requirements

The **minimum hardware configuration** required to install and smoothly run Netsurion Open XDR.

### IMPORTANT

Netsurion Open XDR 9.4 installation is supported on 64-bit Operating System only.

CPU		2.80 GHz and above, 8 Core or equivalent
RAM		16GB
חחו	SSD	200 GB for application and search cache
нии	Non - SSD	100 GB for storing archives (varies as per data retention needs)

### Note

Recommended to have two Partitions in Disk 1 (SSD); Partition 1 for Operating System and Partition 2 for Netsurion Open XDR and search cache. The Archives are stored in a NON-SSD disk (for example, Disk 2).



# 2.2 Software Requirements

### The Netsurion Open XDR console

Microsoft Windows Platforms	64-bit
Server 2022	Supported
Server 2019	Supported
SQL server	64-bit
SQL Server 2019	Supported
onsole Components	
Microsoft .NET Framework	< 4.8 and above.
• Elastic Search 7.10.2.	
• Update of the latest servic	e packs of all Microsof

### The Netsurion Open XDR sensor

Microsoft Windows Platforms	32-bit	64-bit
Server 2022	Not Applicable	Supported
Server 2019	Not Applicable	Supported
Server 2016	Not Applicable	Supported
Server 2012 R2	Not Applicable	Supported
Windows 11	Not Applicable	Supported
Windows 10	Supported	Supported

### **Sensor Components**

• Microsoft .NET Framework 3.5 and above.

#### Note:

Versions other than those listed above are not supported.



#### Web Browsers:

- Microsoft Edge Browser latest.
- Firefox Browser latest.
- Google Chrome latest.

#### Note:

Installing **Elasticsearch 7.10.2** will automatically install the compatible OpenJDK version 15.0.1. **TLS-1.2** should be enabled for Netsurion Open XDR 9.4 Installation and all other protocols must be disabled.

#### Note:

Recommended not to install Netsurion Open XDR on a Domain Controller and to run the Netsurion Open XDR console on a dedicated Microsoft Windows Server.

### 3 Installing Netsurion Open XDR

### 3.1 Pre-installing Instructions for Local Account and Active Directory Authentication

Netsurion Open XDR users will be authenticated locally or against the Microsoft Windows Active Directory. You can also configure the same via Netsurion Open XDR pre-installer and this entire process is automated.

#### Note:

To configure via Pre-Installer, refer to <u>Procedure to Install the Netsurion Open XDR Manager</u> and to configure manually, refer to <u>How To Create Local Account And Active Directory Authentication</u> guide to create Local User or Active Directory User and Group Accounts.

#### IMPORTANT

Recommended users to refer the <u>Install and Customize IIS Web Server v9x guide</u> prior installing Netsurion Open XDR 9.4.



### 3.2 Installing the Netsurion Open XDR Manager

Run Netsurion Open XDR 9.4 installation package. During the installation, the application prompts to provide the path of the digital certificate. The certificate is validated against the latest CRL. Installation proceeds only if the certificate is found to be valid.

### Note:

The installation procedure is identical for all Operating System(s).

### 3.3 Pre-install Checklist for the Netsurion Open XDR Manager

The pre-install checklist describes the specific settings, permissions, and privileges that are required for installing the Netsurion Open XDR Manager. Read the checklist before installing the application to avoid installation failure.

	The update of the latest service packs of all Microsoft Windows.
	User is a member of the 'Local Administrators' group
	MSI package installation is allowed
ENSURE	User has 'Logon As Service' rights
	User has 'Logon As Batch job' rights
	Network Discovery is enabled
	<b>System cryptography</b> : Use of FIPS 140 compliant cryptographic algorithms, with encryption, and hashing and signing algorithms disabled.
	The user has permission on 'Application install directory' (Folders and sub folders).
VERIFY IF	The user has created the service permission on the target system (SCM- Service Control Manager).
	The user has Read/Write permission on the Microsoft Windows registry.



### 3.3.1 IIS Settings

For the Microsoft Windows Operating System, ensure to configure the IIS Settings details in the Application Pools as follows.

×	(General)		
	.NET CLR Version	v4.0	
	Enable 32-Bit Applications	True	
	Managed Pipeline Mode	Classic	
	Name	Classic .NET AppPool	
	Queue Length	1000	
	Start Mode	OnDemand	
~	CPU		
	Limit (percent)	0	
	Limit Action	NoAction	
	Limit Interval (minutes)	5	
	Processor Affinity Enabled	False	
	Processor Affinity Mask	4294967295	
	Processor Affinity Mask (64-bit	c 4294967295	
~	Process Model		
>	Generate Process Model Event	L.	
	Identity	NetworkService	
	Idle Time-out (minutes)	20	
	Idle Time-out Action	Terminate	
	Load User Profile	False	
	Maximum Worker Processes	1	
	Ping Enabled	True	
	Ding Maximum Recoonce Time	00	

### Note:

For details to configure the above settings, refer to Install and Customize IIS Web Server Guide.

### 3.3.2 User Permission on SQL Server

Users installing Netsurion Open XDR must have sysadmin privilege on the respective SQL Server 2019.

- In the SQL Server 2019, verify that the sysadmin privilege has been granted to **NT AUTHORITY\SYSTEM**.
- If the SQL Server 2019 is used by the customer, then the SQL service in the service control manager must be changed from 'NT Service\MSSQL\$SQLEXPRESS' to 'Network Service'.



### 3.4 Installing the Netsurion Open XDR Manager - Custom

Perform the following procedure to install Netsurion Open XDR. If you are launching Netsurion Open XDR for the first time, then run the executable program and proceed.

### Note:

If the previous version of the Netsurion Open XDR is already installed, refer the <u>Upgrade Guide</u> for detailed instructions.

- 1. Run the Netsurion Open XDR 9.4 set-up file via Run as Administrator.
- 2. Netsurion Open XDR prompts to install the .NET Framework 4.8 to proceed with the installation. Click **Yes** to install.

### Note:

The .NET 4.8 is enabled by default for Microsoft Windows 2019/2022. If it is not available, Netsurion Open XDR verifies and installs in the Pre-install check window.

EventTracker	$\times$
EventTracker 9.4 requires .NET Framework 4.8. Click Yes to Install, No to Quit	
[ <u>Y</u> es]] <u>N</u> o	

The following is the sample representation of the Micorsoft .Net Framework Dowload and Installation progress details.

Microsoft .NET Framework	
Download progress:	0
Downloading Windows10.0-KB4486153-x64.cab	
Installation progress:	0
Installing necessary components for .NET Framework	
	Cancel



After the .net framework 4.8 installation is complete, Netsurion Open XDR pops-up a message window stating, *A reboot is required to continue with installtion*.

3. Click **OK** to reboot and re-run Netsurion Open XDR setup.



After the reboot, it is required to re-run Netsurion Open XDR 9.4 set-up file via Run as Administrator.The following pop-up window appears, if the system does not contain the latest Windows updates.



The Installation process involves the following procedures,

- Preinstallation checks
- Netsurion Open XDR 9.4 Setup Program
- Configuring Netsurion Open XDR 9.4

### 3.4.1 Netsurion Open XDR Preinstall Check

- EventTracker Pre-Install Check Netsurion. Welcome to EventTracker Pre-Install check Welcome License PREDICT Hardware Summary Install Type Prerequisite 24 Install Define User Group Define User Summary This application helps the Administrators to validate their environment and assess if it is ready for Event Tracker installation. Checks hardware for minimum requirements Checks for network connectivity Checks prerequisites and offers to install them Checks for configuration of users and offers them to create the configuration Both on screen and text reports are provided which can help for further troubleshooting Quit Next >
- EventTracker Pre-Install Check

2. In the License section, (read the agreement,) click Accept to acknowledge and proceed with the process.

	Netsurion.	
	License Agreement	-
Welcome	Please read the following license agreement carefully.	
Hardware Summary	NETSURION LLC END USER SOFTWARE AND HARDWARE LICENSE AGREEMENT	٦
Install Type Prerequisite	NOTICE – THIS END USER LICENSE AGREEMENT ("EULA" OR "AGREEMENT") IS A LEGAL DOCUMENT BETWEEN NETSURION LLC. ("NETSURION" OR "LICENSOR") AND THE LEGAL ENTITY THAT ACQUIRED THE NETSURION SOFTWARE AND/OR HARDWARE FOR USE BY AN END USER ("YOU", "YOUR", "CUSTOMER" AND "LICENSEE").	
Install Define User Group Define User Summary	READ THIS BEFORE INSTALLING, USING OR OTHERWISE ACCESSING NETSURION'S PROPRIETARY HARDWARE OR SOFTWARE, INCLUDING SOFTWARE AS A SERVICE ("SaaS"), TRIAL OR EVALUATION AND ACCOMPANYING DOCUMENTATION THIS EULA GOVERNS YOUR USE OF THE NETSURION HARDWARE (HARDWARE'), ANY SOFTWARE THAT IS INCLUDED IN THE HARDWARE AND ANY STANDALONE SOFTWARE THAT IS PROVIDED WITHOUT HARDWARE FOR USE ON YOUR HARDWARE, INCLUDING VIRTUAL MACHINE ("VM") SOFTWARE OR ENDPOINT SOLUTIONS (ENDPOINT") (COLLECTIVELY, "SOFTWARE"), ANY SOFTWARE AS A SERVICE, AND OTHER SUBSCRIPTION-BASED SERVICES.	
	THE SOFTWARE IS COPYRIGHTED AND IS LICENSED, NOT SOLD, TO YOU BY NETSURION. BY CLICKING ON THE "ACCEPT" OR "I AGREE" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, CREATING AN ORCHESTRATOR ACCOUNT, USING OR OTHERWISE ACCESSING THE SOFTWARE OR SERVICES, INDICATES THAT YOU HAVE READ, UNDERSTAND, ACCEPT, AGREE TO BE BOUND BY THE TERMS AND CONDITIONS, AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THE LEGAL ENTITY IF AT ANY TIME YOU DO NOT ACCEPT THESE TERMS, YOU MUST IMMEDIATELY DELETE THE SOFTWARE, AND CEASE USING OR ACCESSING THE SOFTWARE AND/OR HARDWARE.	
	IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND SUCH LEGAL ENTITY TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IN SUCH EVENT WOLF AND "YOUR" AS USED IN THIS AGREEMENT DECED TO SUCH ENTITY. IS AT ANY TIME	

**1.** The Netsurion Open XDR console launches the Pre-Install Check window. Click **Next** to continue with the process.



**3.** In the **Hardware Summary** section, it may take a few seconds to fetch the hardware details and a processing icon appears during the data collection process. Click **Next** to proceed.

EventTracker Pre-Install Check						
	Netsurion.					
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group Define User Summary	Machine Name IP Address MAC Address Processor RAM Network Connectivity OS Version Disk space	UT 1988, AQUITO UT 1988, AQUITO UT 1971 - H Tomat UT 1971 UT 1				
Quit		< Back	Next >			

4. In the Install Type section, choose the approriate installation setup type from the listed options, Standard or Collection Point or Custom, and then click Next.

#### Note:

By default, the **Standard** option is selected and you may select the required option.

EventTracker Pre-Install	Check	3
		Netsurion.
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group Define User Summary	Please select a setup type Standard Collection Point Custom E	Select this option for on premise installation Default program features will be installed A 21 day evaluation license is installed (can be upgraded), Event Tracker will be installed as a Standard Console. Local User Group "Event Tracker" will be created. Local User "Event Tracker Admin" will be created and must be used to login to Event Tracker. Select this option for Event Tracker Cloud Default program features will be installed A 21 day evaluation license is installed (can be upgraded) Event Tracker will be installed as a Collection Point. Local User "Event Tracker" will be created and must be used to login to Event Tracker. Choose program features and location. Recommended for advanced users.
Quit	•	< Back Next >



5. In the **Prerequisite** section, click **Next** to proceed with the installation of the softwares that are not installed.

Note:

The **Prerequisite** section lists all of the required softwares, as well as their status (Installed or Not Installed) adjacent to it.

entTracker Pre-Install Check					
	Prerequisites that a	re needed:			
Welcome License Hardware Summany	N	Microsoft .NET Framework (4.8.03761)	Installed		
Install Type	Microsoft	IIS (Version 10.0)	Installed		
Install		Windows Installer (5.0)	Installed		
Define User Group		SQL ODBC Driver (12.2.5543.11)	Installed		
Summary	$\geq$	PowerShell (5.1.17763.1)	Installed		
	😽 elastic	Elasticsearch (7.10.2)	Not Installed		
	SQL Server	Microsoft SQL Server 2019 Express Edition (15.)	Not installed		
Quit	1	< Back	Next >		

If the SQL Server is running with multiple instances, click the Browse appropriate instance.

button to select the

EventTracker Pre-Insta	II Check
	Netsurion.
Welcome	Prerequisites that are needed:
License	EventTracker Pre-Install Check
Hardware Summary Install Type	SQL Install Directory C:\Program Files\Microsoft SQL Server
Prerequisite Install Define User Group	Event Tracker0 Not Installed
Define User Summary	
	ок
	Velastic Elasticsearch (7.10.2)
	Microsoft SQL Server 2019 Express Edition (15.) Not Installed
Quit	< Back Next >



6. In the **Install** section, click **Next** to proceed with the installation of the requisite softwares.

ventTracker Pre-Install Check ×				
	Netsurion.			
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group Define User Summary	Installing : Elasticsearch Note: In case the installer prompts for a restart/reboot of the system, please do so. Failing to do so, might make the system unusable. Once that is done please run this setup again. View Details			
Quit	< Back Next >			

- 7. In the **Define User Group** section, choose the required option to create a user group in local machine or in Active Directory, and then click **Next**.
  - Creating a user group in Local Machine
  - Creating a user group in Active Directory

ventTracker Pre-Install Check				
	Netsurion.			
Welcome License Hardware Summary Install Type Prerequisite Install <b>Define User Group</b> Define User Summary	Congratulations! This system can host Event Tracker, if you want to install proceed, else Quit. A report has been generated at : C:\EventTracker-Preinstall-Check_005056B0AB7D.log A user group is required. The purpose of which is to manage Event Tracker. That group can be created in local machine or in Active Directory Please choose: Local Machine Active Directory			
Quit	< Back Skip Next	>		



#### Note:

While creating a group and/or user, the user should be part of the administrator's group in the local machine. The user should have "Logon as Batch' and "Logon as Service' rights granted.

a. If choosing the Local Machine option, click Next and in the You have selected to use local machine window, choose either the <u>Create User Group EventTracker</u> or <u>Select existing User Group</u> option, and then click Next.

EventTracker Pre-Instal	Check
	Netsurion.
Welcome License Hardware Summary Install Type Prerequisite Install <b>Define User Group</b> Define User Summary	We recommend user group "Event Tracker" or you can use an existing User Group  () Create User Group EventTracker () Select existing User Group (User should be a domain administrator)
Quit	< Back Next >

#### Note:

When creating a group, suggested to use the group name as **EventTracker**, though Netsurion Open XDR works with any group name. In case this group name does not exist then it is necessary choose the **Create User Group EventTracker** option else choose the **Select Existing** Group option.



 If choosing the Create User Group EventTracker option, then click Next and specify a unique name in Group Name field, and then click Next.

EventTracker Pre-Install	Check		
		Netsurion.	
Welcome License Hardware Summary Install Type Prerequisite Install <b>Define User Group</b> Define User Summary	Members of this I	ser Group can acess Event Tracker	]
Quit		< Back	Next >

 Otherwise, if choosing the Select existing User Group option, then select the required group name from the available list, and click Next.

	Netsurion.	
Welcome License Hardware Summary Install Type Prerequisite	We recommend user group "EventTracker" or you can use an existing User Group O Create User Group EventTracker  Select existing User Group (User should be a domain administrator)	
Install <b>Define User Group</b> Define User Summary	Access Control Assistance Operators Administrators Backup Operators Certificate Service DCOM Access Cryptographic Operators Device Owners Distributed COM Users Event Log Readers Event Tracker Guests Hyper-V Administrators	Í
Quit	IIS_IUSRS Network Configuration Operators Performance Log Users Performance Monitor Users Power Users	Next >



b. Alternatively, if choosing the Active Directory option, then click Next and in the You have selected Active Directory domain window, choose either <u>Create User Group EventTracker</u> or <u>Select existing</u> <u>User Group</u> option, and then click Next.

#### Note:

The administrator should have sufficient privileges on the active directory to create a user group.

ventifacker Pre-instal	Netsurion.	
Welcome License Hardware Summary Install Type Prerequisite Install <b>Define User Group</b> Define User Summary	We recommend user group "Event Tracker" or you can use an existing User Group Create User Group Event Tracker Select existing User Group (User should be a domain administrator)	Find Group     Find     Find     Wildcard ['] can be used [e.g., ev']     This can take time in large installations
Quit	< Back	Next >

#### Note:

When creating a group, suggested to use the group name as **EventTracker**, though Netsurion Open XDR works with any group name. In case this group name does not exist then it is necessary to choose the **Create User Group EventTracker** option else choose the **Select Existing Group** option.



 If choosing the Create User Group EventTracker option, then click Next and specify a unique name in Group Name field, and then click Next.

EventTracker Pre-Install	Check		×
		Netsurion.	
Welcome License Hardware Summary Install Type Prerequisite Install <b>Define User Group</b> Define User Summary	Members of this Use	r Group can acess EventTracker	
Quit		< Back	Next >

Contact the administrator if an error message occurs stating **Access Denied** as shown in the below image. This error occurs in the case if you do not have sufficient permissions to create a user group in the Active Directory.





• If choosing the **Select existing User Group** option, then select the required group name from the available list, and then click **Next**.

EventTracker Pre-Instal	I Check		×
	Netsurion.		
Welcome License Hardware Summary Install Type Prerequisite	We recommend user group "Event Tracker" or you can use an existing User Group Create User Group Event Tracker  Select existing User Group (User should be a domain administrator)	○ Find Group	
Install <b>Define User Group</b> Define User Summary	EventTracker		~
Quit	< Back		Next >

 In the Define User Group section, choose either <u>Create EventTrackerAdmin</u> or <u>Select exisiting User</u> or <u>Find User</u> to find the user.

Welcome       Userse         License       Logon as a Batch job permission         Hardware Summary       Added to Administrator Group         Install Type       Install         Prerequisite       Create EventTrackerAdmin         Install       Define User         Summary       Summary			Netsurion.		
	Welcome License Hardware Summary Install Type Prerequisite Install Define User Group <b>Define User</b> Summary	We recommend you to create "Ever Note: This user will be granted : . Logon as a Batch job per . Logon as a Service perm . Added to Administrator's ( . Added to Event Tracker ( Create Event TrackerAdmin	nt Tracker" administrator or you can use mission Group Group O Select existing User	an existing user. Selected domain is NTPL.LC	)CAL



If choosing Create EventTrackerAdmin, then click Next and in the This User will manage EventTracker window, under User Details, provide the appropriate user credentails and then click Next.

EventTracker Pre-Install	II Check	×
	This User will manage Event Tracker	
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group <b>Define User</b> Summary	Note: This user will be granted          Logon as Batch right         Logon as Service right.         Added to Administrator's Group         Added to Event Tracker Group         User Details         User Name:         Event TrackerAdmin         Password:         Confirm Password:	
Quit	< Back Skip Next	>

If choosing the Select existing User option, then select the appropriate user name from the available list, and then select Next.

Netsurion.				
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group	We recommend you to create "Event Tracker" administrator or you can use an existing user. Selected domain is NTPL.LOCAL Note: This user will be granted : . Logon as a Batch job permission . Logon as a Service permission . Added to Administrator's Group . Added to Event Tracker Group O Create Event TrackerAdmin  Select existing User  Find User			
Define User Summary	Colout Vastemate Nataragen Naskinstrian Japakume Kund Ehen Noter Kuna Noter Tuske Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster Stutte Vaster			



 The following message pops-up if the selected user name is not a EventTracker Administrator. Click Yes to proceed.



If choosing the **Find User** option, then in the **text** field, provide the appropriate user name, and then click **Find**.

#### Note:

A wildcard can also be entered.

EventTracker Pre-Install Check

	Netsurion.	
Welcome License Hardware Summary Install Type	We recommend you to create "EventTracker" administrator or you can Note: This user will be granted : . Logon as a Batch job permission . Logon as a Service permission . Added to Administrator's Group . Added to EventTracker Group O Create EventTrackerAdmin O Select existing User	use an existing user. Selected domain is NTPL.LOCAL Image: Selected domain is NTPL.LOCAL
Prerequisite Install Define User Group		sid* Find . Wildcard (*) can be used (e.g., ev*). This can take time in large installations
Define User Summary	sid F	
Quit	Skip	< Back Next >



9. In the Summary section, verify all the details and click Install to proceed with the Installation process.

Note:

If required click the **Browse** button to modify the **EventTracker Archive Drive** or the **Program Drive** location.

Netsurion.				
Welcome	EventTracker Archive Drive	D:\Program Files (x86)\Prism Microsystems\EventTracker\Archives		
icense	EventTracker Program Drive	C:\Program Files (x86)\Prism Microsystems\		
ardware Summary	Elasticsearch Data Drive	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache		
stall Type	Elasticsearch	Elasticsearch [7.10.2](Installed)		
rerequisite	Network Adapters	172 28 5 43-000004 /5 Wh		
istali	Operating System Version	Microsoft Windows Server 2019 Datacenter		
enne User Gummary	Hard Disk Summary	C: Total 69 GB, Free 24 GB D: Total 99 GB, Free 99 GB E: Total 9 GB, Free 9 GB	~ ~	
	Event Tracker User Group	G Event Tracker Testing		
	Event Tracker Administrator User	00 1001140		
	Internet Information Services	IIS[Version 10.0] (Installed)		
	Microsoft SQL Server	Microsoft SQL Server 2019 Express Edition(Installed)		
	Please check : [C:\EventTracker-	Preinstall-Check_005056A757F9.log] for more details.		

### 3.4.2 The Netsurion Open XDR 9.4 Setup Wizard

When Installing, Netsurion Open XDR displays the EventTracker - InstallShield Wizard.

Netsurion.	
© Copyright 2022 Netsurion. All Rights Reserved.	
	EventTracker - InstallShield Wizard
	EventTracker Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
	Extracting: EventTracker.msi
	Activate Windows Go to Settings to activate Windows.



 In EventTracker - InstallShield Welcome window, click Next to proceed with Netsurion Open XDR setup process.



2. In Select a Certificate File window, click Browse and locate the appropriate certificate file (the file with .cer extension), and then click Next.

#### Note:

If the user has selected **Custom** option in EventTracker Pre Install Check, then the installer prompts to add the certificate file.

🛃 EventTracker 9.4			×
Select a Certificate File Please provide a certificate file		Nets	urion.
C:\Users\dgowda\Documents\EventTr	acker1612835148.cer		Browse
InstallShield			
	< Back	Next >	Cancel



3. In Select Components window, select the required component details and click Next.

EventTracker 9.4 Select Components Select EventTracker components from the options below.	Netsurion.
Click on an icon in the list below to change how a feature	is installed. Feature Description Complete framework capable of log management, change audit.
nstall to: C:\Program Files (x86)\Prism Microsystems\ stallShield	Change
Help Space < Back	K Next > Cancel

Components	Description
EventTracker Console	Select this component to install the manager console on the target computer.
Change Audit	Optional component. Installing this component enables you to monitor and manage change over the enterprise. The sensor component will also be installed along with the Manager Console. You can also deploy the sensor to the monitored computers using System Manager after installing the Manager Console.
Trap Tracker	Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.



Спск	То
Change	Select a different destination folder to install the setup.
	Eolder name: C:\Program Files (x86)\Prism Microsystems\ InstallShield
Help	Select Component conventions.         Image: Select Components The Components The Components The Components The Components The Component Selectively instal Selective Component Selectively instal Selective Component Selectively instal Selective Component Selectively instal Selective Component Selective Componen



	EventTracker 9.4 Disk Space Requirement The disk space required selected features.	s for the installation of the	Net	surion.
Space	Volume	Disk Size 99GB	Available 68GB	Required 1462MB
	The highlighted volumes du You can remove files from select different destination	o not have enough disk space ava the highlighted volumes, choose t drives.	ilable for the curren to install fewer featu	tly selected features. ures onto local drives, or

- 4. In Select EventTracker Console Type window, choose the appropriate Console Type and click Next to proceed.
  - **a. Standard Console** option is suitable for flat network topologies, where all the monitored nodes report directly to one (or redundant) Netsurion Open XDR console.

EventTracker 9.4	×
Select EventTracker Console Type	Netsurion.
	EventTracker Console Types: Standard Collection Point Collection Master Standard Best for flat network topologies where all monitored nodes report directly to one (or redundant) EventTracker Console
InstallShield	< Back Next > Cancel



**b. Collection Point** is applicable for hierarchical network topologies, where the monitored nodes report to a local Netsurion Open XDR console which in turn replicates its event log archive to a Collection Master.

🔀 EventTracker 9.4	×
Select EventTracker Console Type	Netsurion.
	EventTracker Console Types:
	Standard
	Collection Point
	O Collection Master
	Collection Point
	Used in hierarchical network topologies where monitored nodes report to a local EventTracker Console which in turn replicates its event log archive to a Collection Master.
InstallShield	
	< Back Next > Cancel

If choosing the Collection Point option, then click Next and in the Configure Collection Point site window, specify the Site name, and then click Next.

#### Note:

The following special characters  $\ / : * ? " < > | ; , ' ~ []$  are not applicable while specifying the site or the group name

EventTracker 9.4			×
Configure Collection	n Point site	Nets	rion.
Collection Point det	ails		
Site name:	ETTVMBLR22019-2		
	A friendly name for this I	eventTracker installation server	
stallShield			
	< E	ack Next >	Cancel



The Wizard pops up the following message if the site or group name includes inapplicable special characters.



The setup wizard navigates to the Configure Collection Master window for Collection Point – Collection Master setup.

 Here, provide either the Collection Master details or select the Skip check box, and then click Next.

<b>B</b>			×
Configure Collection Master		Nets	urion.
Collection Master details			
Provide the Collection Ma Collection Point will report	aster name (e.g., cm3.contoso rt to	o.com) or IP Address to	which this
Collection Master:	VMBLR22019-3		Skip
InstallShield			
	< Back	Next >	Cancel



c. Collection Master is applicable for hierarchical network topologies where collection points replicate their event log archives to a Collection Master.

🕼 EventTracker 9.4	×
Select EventTracker Console Type	Netsurion.
InstallShield	EventTracker Console Types: Standard Collection Point Collection Master Collection Master Used in hierarchical network topologies where Collection Points replicate their event log archives to a Collection Master.
	< Back Next > Cancel

• If choosing the **Collection Master** option, then click **Next**.

In the **Select Components** window, if the **Change Audit** component is also selected, then the InstallShield Wizard navigates to the **Change Audit SnapShot** window.



5. In the **Change Audit SnapShot** window, keep either the default folder location or click **Change** to browse the required store location, and then click **Next**.

EventTracker 9.4	_		
Change Audit SnapShot		Nets	urion.
Change Audit can use a different To use the default folder, click N	t folder to store SnapShot d	ata	
C:\Program Files (x86)\Prism M	licrosystems\WCWindows\S	napShots	Change
llShield			
	< Back	Next >	Cancel

#### Note:

The Change Audit snapshot store location can be changed only during fresh install and if snapshots are not retained during uninstall. In case of an upgrade, if the change audit snapshots are retained during product un-installation, then the snapshot store location path cannot be changed.

EventTracker 9.4 Select Components Select EventTracker components from the options below.	Netsurion.
Click on an icon in the list below to change how a feature	is installed. Feature Description Complete framework capable of log management, change audit.
Install to: C:\Program Files (x86)\Prism Microsystems\ nstallShield	Change
Help Space < Back	Cancel



6. The **Ready to Install the Program screen** provides the summary of the details, the installation path, console type, and the selected features. Verify and click **Install** to install the selected components.

EventTracker 9.4		
Ready to install the Program The wizard is ready to begin installation		Netsurion
Click Install to begin the installation.		
Installation Path: C:\Program Files (x86)\Prism Microsystems Console Type: Collection Master	51	
EventTracker Change Audit TrapTracker		
To review or change settings,click Back. Cano	cel exits the wiza	rd.
	< Back	Install Cancel

InstallShield Wizard installs the selected components.

Streamline Compliance Management	Netscrion. Netscrion		
		xe.	
			Activate Windows Cancel Go to Settings to activate Windows.



**7.** In the **Installation is finished** window, select the required option details and click **Finish** to conclude the installation process.

EventTra	cker 9.4			×
EventTra	cker installation is finished		Nets	urion.
Options				
	Import existing event log er	ntries.		
	Event logs from this machine	will be imported.		
	Add a shortcut to the deskt	op.		
	Add EventTracker Control Pa	nel to the desktop.		
$\checkmark$	Add EventTracker Diagnosti	cs as a startup p	rogram.	
	Helps to notify problems about	ut EventTracker if a	ny.	
The Ins	tallShield Wizard has successfull	y installed EventTra	cker. Click Finish to	exit the wizard.
tallShield _	2			
		< <u>B</u> ack	<u>F</u> inish	Cancel

**a.** Select the **Import existing event log entries** option if you require to import the Netsurion Open XDR event logs.

The progress of importing the logs will be displayed through the command prompt window.



- **b.** Select the **Add a shortcut to the desktop** option to add the shortcuts to the Netsurion Open XDR application on the desktop.
- c. The Add EventTracker diagnostics as a startup program option is selected by default to notify the Netsurion Open XDR issues (if any).



### 3.4.3 Configuring Netsurion Open XDR 9.4

After the InstallShield Wizard is complete, it navigates to the EventTracker :: Configuration.

1. In the EventTracker :: Configuration interface, specify the User Credentials, User Authentication and EventTracker Group, and then click OK to login.

#### Note:

Though the username/authentication provided in the EventTracker Preinstall Check reflects in this interface, the user still has the option to override it.

EventTracker :: Configuration	×
Netsurion.	
User Credentials	User Authentication
User Name NTPL	<ul> <li>Local Account</li> </ul>
Password	<ul> <li>Active Directory</li> </ul>
EventTracker Group	Database Authentication
Note: For "Active Directory" authentication enter user name and pa domain user and for "Local Account" authentication enter loc name and password. User must be administrator on this sys	OK Cancel assword of a cal system user tem. Refer <u>install quide</u> .

#### Note:

The Netsurion Open XDR services run under this account. By default, this user is assigned the 'EventTracker Administrator' role and can log in to Netsurion Open XDR.

User Credentials		Specify the valid user credentials in the User Name and Password fields.
User	Local Account	Authentication will be done locally on the computer where Netsurion Open XDR is installed
Authentication	Active Directory	Authentication will be done in the Active Directory.



EventTracker Group	Specify the EventTracker group name

2. The following EventTracker Configuration message box pops-up after successfully validating the user credentials. Click OK.



#### Note:

If the password is changed for the above-configured user, it is mandatory to re-run the **EventTracker :: Configuration** with the updated password.

#### Note:

You can also access EventTracker :: Configuration via Start > All Programs > Prism Microsystems > EventTracker > EventTracker Configuration.

### 3.5 Installing the Netsurion Open XDR Manager – Standard or Collection Point Evaluation Version

If Standard or Collection Point is selected, then,

- The archive path is the drive with the maximum free space.
- Local machine authentication is used.
- Group created as 'EventTracker'.
- Username is 'EventTrackerAdmin'.
- This user is local machine admin.
- This user is given 'Logon as batch user' rights, and 'Logon as Service' rights.
- Only express versions of IIS and SQL can be used.



To install Netsurion Open XDR 21-day trial for Standard or Collection Point.

- 1. Run the Netsurion Open XDR 9.4 installation package via Run as Administrator.
- 2. Netsurion Open XDR launches the Pre-Install Check window. Click Next to continue with the process.



**3.** In the **Hardware Summary** section, it may take a few seconds to fetch the hardware details and a processing icon appears during the data collection process. Click **Next** to proceed.

211408.00010 12.000 2000.0000 2000.000 2000.000 2000.000 2000.00000000	
	171.000.00000 172.0000 177.0000 177.00000 177.00000 177.00000 177.00000 177.000000 177.0000000000



4. In the **Install Type** section, choose either the **Standard** or **Collection Point** option, and then click **Next**.

EventTracker Pre-Install	Check	Netsurion.
Welcome License Hardware Summary Install Type Prerequisite Install Define User Group Define User Summary	Please select a setup ty      Standard      Collection Point      Custom      Custom	<ul> <li>pe:</li> <li>Select this option for on premise installation Default program features will be installed</li> <li>A 21 day evaluation license is installed (can be upgraded).</li> <li>Event Tracker will be installed as a Standard Console.</li> <li>Local User Group "Event Tracker" will be created.</li> <li>Local User "Event Tracker Cloud Default program features will be installed (can be upgraded).</li> <li>Select this option for Event Tracker Cloud Default program features will be installed</li> <li>A 21 day evaluation license is installed (can be upgraded)</li> <li>Event Tracker will be installed as a Collection Point.</li> <li>Local User "Event TrackerAmin" will be created and must be used to login to Event Tracker.</li> <li>Cocal User "Event TrackerAmin" will be created and must be used to login to Event Tracker.</li> <li>Local User "Event Tracker" will be installed (can be upgraded)</li> <li>Event Tracker will be installed as a Collection Point.</li> <li>Local User "Event TrackerAmin" will be created and must be used to login to Event Tracker.</li> <li>Choose program features and location. Recommended for advanced users.</li> <li>A valid license certificate is required during installation.</li> </ul>
Quit		< Back Next >

To proceed with the further installation, refer to the ETLM-Install Guide.

#### Note:

After logging in to Netsurion Open XDR, some of the components will not be available as this is a trial version.

In Collection Point installation, components like Trap Tracker, Reports are omitted.

# **4 Deploying the Netsurion Open XDR Windows Sensor**

### 4.1 Pre-install Instructions for Windows Sensor

- You must have Local Admin privileges on the remote systems where you want to remotely install the Sensors.
- You can also install **Sensors** with Local Admin privileges.
- Ensure that the systems you are selecting to monitor are accessible through the network, have disks that are shared for the Admin, and have disk space up to 90MB that can be used by the Sensor.
- If the remote system is accessed through a VPN with slow line speed, the installation may take time and it is recommended that you schedule your activities accordingly.
- To monitor a system that supports syslog messages (for example, Unix, Linux, and Cisco, etc.) configure that specific system to forward the syslog messages to the Netsurion Open XDR Manager.



### 4.2 Pre-install checklist for Windows Sensor

The following settings, permissions, and privileges are necessary when deploying the Netsurion Open XDR sensor to ensure safe and smooth sensor installation.

	User is a member of the 'Local Administrators' group
	MSI package installation is allowed
ENCLIDE	User has 'Logon As Service' rights
ENSORE	Network Discovery is enabled
	File sharing is allowed
	Access this computer from the network
	The user has permission on 'Application install directory' (Folders and sub folders).
VERIFY	The user must create service permission on the target system(SCM- service control manager)
	The user has Read/Write permission on the Microsoft windows registry.
	The user has permission to Admin share(C\$) of Target systems and C\$ should be accessible from the Netsurion Open XDR Manager.

### 4.3 Different methods to install the Netsurion Open XDR Sensors

There are two methods to deploy the Netsurion Open XDR Sensors,

- Using the **System Manager** which is as part of Netsurion Open XDR. From this **System Manager**, the Netsurion Open XDR Sensors can be deployed to all systems.
- Using the Manual Sensor Installation package for all systems.

### Note:

If the Auto agent update is enabled on the console, all the reporting sensors are automatically upgraded to latest version.



## 4.4 Deploying the Netsurion Open XDR Windows Sensor via System Manager for Sensor Based Systems (full featured)

The installation procedure is identical for all the supported Microsoft Windows Operating Systems.

- 1. Log in to Netsurion Open XDR with the appropriate user credentials.
- 2. In Netsurion Open XDR, hover over the Admin and click Systems.

This interface displays the list of systems that are members of all the trusted domains including the operating system type, asset value, port number, and managed system status through which the Sensor communicates with the Netsurion Open XDR Receiver.

#### Note:

Make sure **Auto Discover** is in ON state to view the list of systems. If it is not in ON state then the interface displays only the Netsurion Open XDR Manager details.

Systems							A / Admin / Syste
2 Non Reporting Systems Systems nut reporting once the last 24 Neuro	O Request Status Status of entropy requests		8 Manager	Menger		3 64-bar ti 12-bar ti 12-bar ti bentTracker Sensor Version Arcon by court	
Groups	Systems						
Create Group Delete Group	Request Status Non Reporting Systems Search Computers System	Report Auto Discover	Sourcetype	o			
<b>200000</b>	All Domain Computers					@	Managedt 7
Seach Groups	Spiles.	Q			25	Computer	V
All Groups O	< 1 df1 > 60						
Ortautt O	Computer	Type	Purt	EventTracker version	Ounge audit versio	n Asset value	
Domain Controllers	CT RIA-DA	2008 R2	14	-		Undefined	0
beenster 0	N3 <sup>TTEUTER38-DOCUMENTATION</sup>	Win 7	54 1	9.0 - Build 18	**	Lów	0
Name Contract O	R*MI M	2016	14	5.2 - Build 8	9.2 - Build 8	Serious	0
Volters O	RU-MU-MUKA	2016	54 1	-		Serious	0
Win 7 and Server 2008 Above O	Se <sup>KSN</sup> ICSVDLA	Unknown	54 i	-	-	Undefined	0
We XP and Server 2003	Se <sup>MQ</sup> ISOLDLA	Unknown	54 )		-	Undefined	0
	ter	2008 R2	54	-	-	Undefined	0

3. In the Systems interface, select the required group or system to install the sensor.

#### Note:

Refer <u>Installing Sensors for a Group</u> section to install the sensors for a group or the <u>Installing Sensor for</u> a <u>System</u> section to install the sensor for a system, and then proceed with the next step.

### • Installing Sensors for a Group

a. In the Systems interface, from the All Groups pane, click the required domain or the group name, and then click the gear 🌣 icon and select Install agent/Start poll from the drop-down list.



Systems							•	r / Admin / Syste
2 Non Reporting Systems Systems not reporting since the last 24 hours	O Rr St.	equest Status atus of various sensor requests		8 Managed Managed/U	Managed I vs Unmanaged Inmanaged system count	3 EventTracker S Version by count	90 - Buile 18 9.1 - Buile 19 92 - Buile 8 ensor Version	
< Groups	Systems							
Create Group Delete Group	Details Edit	Non Reporting Systems	Search Computers System R	eport Auto Disc	cover Source type C		Q ,	Managed: 7
All D E F N T V W	Install agent/Start poll Uninstall agent/Stop poll Upgrade agent		Q			Page size	Sort by columns	~
All Groups Default	Restart agent service Agent service status Query for agent version	of 1 > GO	Type	Port	EventTracker version	Change audit version	Asset value	
Domain Controllers	Remove agent components		Unknown	50"	9.1 - Build 19		Undefined	ö
EventTracker	Delete systems		2008 R2	59	**		Undefined	Ö
Firewall Devices	Manage asset value	DOCUMENTATION	Win 7	50	9.0 - Build 18		Low	\$
Network Devices	Query for agent update info		2016	50	9.2 - Build 8	9.2 - Build 8	Serious	<b>\$</b>
TOONS	R 5- 11 LA		2016	50			Serious	\$
vmware	S so iV- LA		Unknown	50			Undefined	\$
win / and server 2008 Above	S SO OF DL	A	Unknown	50			Undefined	\$
(Ctrl)	ti jsc ile- LA		2008 R2	50			Undefined	\$

### b. In the Install agent/Start poll window, the following three options are available,

Install agent/Start poll					×
Select systems and agent type					
All systems in the selected group     Take systems from text file     Browse					
(One system per line)					
Agent Type 🔲 EventTracker 🗌 Change Audit					
O Specific systems in the selected group					
	Cancel	Back	Next	Advanced	Install

### c. Choose the appropriate option and select the required **Agent Type** to upgrade the sensors.

Options	Description
All systems in the selected group	• Click this option to upgrade all the sensors available in the selected group.



Options	Description
Take systems from the text file	<ul> <li>Browse for the text file holding sensor system names for which you require to upgrade. The text file should contain one system name per line.</li> <li>If you desire to select this option, then create the text file to select the sensor system names.</li> </ul>
Agent Type	<ul><li>Select the appropriate sensor type to upgrade.</li><li>EventTracker</li><li>Change Audit</li></ul>
Specific systems in the selected group	Out of all the sensor systems available in the group, select a specific sensor system(s) to upgrade.

- d. After selecting the appropriate details click **Next** to proceed.
- Installing Sensor for a System
- a. In the Systems interface, from the Computer list, click the gear icon (located corresponding to the remote system's name) for which you require to install the sensor, and then click Install agent/Start poll from the drop-down list.

Systems										🕈 / Admin,	/ Syste
2 Non Reporting Systems Systems not reporting since the last 24 hours	9	8 Request Stats Status of verious	Failed 2 Noise 2 Success Second Pailor	9 	anaged v	si Unin Is Unimai nanaged sj	anaged 1 naged steen count		3 EventTracke Version by cour	10-1848-19 1-1-1848-19 1-2-1848-19 1-1-1	
Groups		Systems									
Create Group Delete Group		Request Status	Non Reporting Systems	Search Computers	System	Report	Auto Discover	Source type	C		
		Default - Default	Group							Dutville	-
Search Groups	Q					0	Page size		Sort	v rstall agent/Start poll	1
All Groups Default	0	Type here_	of 1 > 60			Q	25		Y C0	Manage asset value Upgrade agent Remove agent components	
Domain Controllers EventTracker	0	Computer		Type	Port	Even	Tracker version	Chan	ge audit version	Restart agent service	
Firewall Devices	0	ND DU		2008 R2 Win 7	4 2	 9.0 - 8	uild 18			Query for agent version	00
NTPL TOONS	0	nsc IV-E A nsc ON EA		Unknown Unknown	45	••				Enable syslog relay Disable syslog relay	00
WriWare Win 7 and Server 2008 Above	0	itjs le-[ A		2008 R2	4 5			**		Undefined	0
Win XP and Server 2003	0										7044



**b.** In the **Install Agent/Start poll** window, select the required sensor type (EventTracker or Change Audit) check box, and then click **Next**.

elect system to be monitored.			
Name	EventTracker	☑ Change Audit	
NTT LUTULING ~ DOCU N			
	Colort "Next" to proceed		
	select Next to proceed.		
		Cancel Back Next Advar	nced Inst

Next, choose the required EventTracker Agent Type that is, either the Agent based (Full Featured) option or the Agent-less (limited feature)\* option.

Install agent/Start poll						×
EventTracker Agent type						
<ul> <li>Agent based (Full featured)</li> </ul>						
Install default Remedial Action EXEs on this system 1						
Deploy WinSCP						
Poll every 15 minutes	ccount is preferred.					
Log file monitoring	Guaranteed Event Deli	ivery				
System monitoring (CPU,Disk,Memory)	Process monitoring (C	PU,Memory	)			
Network connection monitoring	Application monitoring	g				
Software Install/Uninstall	Service monitoring					
		Cancel	Back	Next	Advanced	Install



Agent based (Full featured)					
Install default Remedial Action EXEs on this system	<b>Remedial Actions</b> are scripts or executable files that can be launched at either the sensor or the manager side, in response to events.				
	If this option is enabled, predefined scripts are placed in the EventTracker\Agent\Script folder at the manager side. These may be installed at the Sensor side also, during deployment via the <b>System</b> manager.				
Deploy WinSCP	Provides an option to install WinSCP components to remote machines while deploying Sensor(s).				
Agentless (limited feature)					
Poll Every	By default, the frequency is set to 15 min to receive events from the remote Sensor system. You can change the poll frequency as per the requirement.				

If the **EventTracker Agent type** is selected as 'Agent based (Full Featured)', then remedial actions EXEs can be installed on the system.

- **d.** Select the **Install default Remedial Action EXEs on this system** check box if you require to install remedial action scripts.
- e. The following message window pops-up to confirm to enable this feature. Review and either click **OK** to proceed or click **Cancel** if you do not require to install the remedial action EXEs, and then click **Next**.



### Note:

'Install default Remedial Action EXEs on this system' option is available for 'Agent based (Full featured)' installation.



The **Install agent/Start poll** interface displays the default client installation path on the remote computer.

all agent/Start poll		
Installation path	%ProgramFiles%\Prism Microsystems	
Note: Installation path	on the remote machine	
Create "Program M	enu" shortcuts 🕦	
Account	(ex.mydomain\administrator)	
Password		
Confirm Password		
Selected systems	Change Audit : NTPLDTBLR38~DOCUMENTATION	
	Select 'Install' to proceed.	
	Cancel Back Next Advanced	1

- Specify the required location details in the Installation path field to install the Sensor in a different drive apart from the default one.
- Select the Create 'Program Menu' shortcuts check box to create shortcuts.
- Specify the valid **Account** name and **Password** and click **Next**.

The Sensor is installed on the selected machine with the default 'etaconfig.ini' configuration.

**f.** To set a more specific configuration, click **Advanced**.

Install agent/Start poll					×
Apply configuration					
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify the file. You can also select 'Default' and configure later.					
Default     Custom config     Select File					
	Cancel	Back	Next	Advanced	Install



g. Choose the Custom config option to select a custom configuration file.

#### Note:

The **Default** option is selected by default to apply the manager side 'Sensor configuration' settings (etaconfig.ini).

The custom configuration will provide the templates you created in Sensor configuration along with two more predefined templates.

etaconfig_Servers.ini	This predefined template contains the ideal server configurations which can be applied to the selected sensor system.
etaconfig_Workstations.ini	This predefined template contains the ideal workstation configurations which can be applied to the selected sensor system. This option disables the 'Offline event sending' option.

Install agent/Start poll		×
Apply configuration		
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify the file. You can also select 'Default' and configure later.		
O Default  Custom config Select File etaconfig.ini etaconfig_Servers.ini etaconfig_Workstations.ini		
	Cancel Back Next Advanced Inst	all

#### Note:

In case if you choose the Custom config option (and selected either **etaconfig\_Servers.ini**, **etaconfig\_Workstations.ini**) then configure the Manager.



4. After providing the required details, click Install.

A message window pops-up stating 'Install in progress. Check the Request status screen for updates.'



5. Click OK and go to Systems > Request Status interface to view the installation status.

Request Status							×
Application All	- Status All	∽ Sort b	Date V				
Purge all status olde	er than					Purge 1	C
Date	Group/System	Ву	Agent	Туре	Status	Description	^
Nov 26 07:37:21 PM		: 'R	Change Audit	Install agent	New	In progress.	
Nov 26 07:07:01 PM	ntpldthlr1C2	Harsha D	N/A	Search computers	Success	Search was successful.	
							Close

Select	То
Application	Sort the <b>Request Status</b> results by the application installed. Available options are EventTracker and Change Audit.
Status	Sort the <b>Request Status</b> results by the status of the application installed. Available options are All, New, Success, and Failed.
Sort by	Sort the <b>Request Status</b> results by <b>Date</b> of the application installed /on which <b>System</b> it is installed / <b>Type</b> of activity performed/ <b>Status</b> of the application.
Purge all status	Remove the older Request Status details from the list.



Select	То
older than	
Export	Export the 'System Status' into Excel format

6. Click **Refresh** C to view the latest progress status or reopen the **Request Status** dialog box to see the updated status.

### 4.5 Configuring the Netsurion Open XDR Windows Sensors

All configurations for the sensor(s) are set by default during installation. Perform the following steps if you require to change the default configuration settings.

1. Log in to the Netsurion Open XDR Control Panel.





2. Double-click EventTracker Agent Configuration and configure the sensor according to the requirement.

EventTracker Agent Configuration
ile Help
Select Systems
Agent based system
Apply the following settings to specified Agents
dan serie de tientieure
Manager destinations.
Log Backup Performance Network Connections
Logfile Monitor   File Transfer   syslog FTP server   Application Control
Managers   Event Filters   System Monitor   Monitor Processes   Services
Windows Manager(s)
Manager Name Port Mode Encrypt
A <u>d</u> d <u>E</u> dit <u>B</u> emove
syslog Manager(s)
Manager Name Port Mode Encrypt
Add Edit Remove Message Options
Gave Close

# 4.6 Configuring Sensor-less collection via System Manager (limited features)

If installing the Netsurion Open XDR Windows Sensor is not feasible or desirable, then Netsurion Open XDR can be set up to subscribe or poll remote computers' event logs over the network to collect new event log entries.

Pros

• No sensor to deploy – Simple product deployment and trivial effort during planning, deployment, and upgrade.

Cons

- Increased network traffic Depending on the polling cycle or level of event generation that is chosen, network load is greater.
- Greater dependency and more critical points of failure The Console becomes critical since it is polling target machines. Network choke points can impact performance.



- Limited to operation within a domain The Console and target machine must be in the same domain so that domain privileges are preserved.
- Performance monitoring, Log file Monitoring, System Monitoring, Network Connection Monitoring, Software Install / Uninstall, Guaranteed Event Delivery, Process Monitoring, Application Monitoring, Service Monitoring, Software install/removal monitoring, Host-based intrusion detection, Monitoring external log files – The specified feature will not be available.
- Non-domain topologies not supported This feature is only available when the Console and target machine are in the same Windows domain.

### Adding Systems for Sensor-less monitoring

This feature facilitates you to add systems from where you require to collect events periodically. The resource (CPU/memory/disk) usage, log file monitoring, and other Sensor-required features are disabled, in the Sensor-less monitoring systems. Additionally, the service account of the local Sensor should have administrative privileges on all the systems that are added for collecting events.

#### Note:

In Microsoft Windows Firewall, ensure that the Remote Event Log Management is added in the filter exception list, or else it will not connect to the target system.

1. In the System manager interface, select the gear sicon of the system in which you require to install the sensor and then click Install agent/ Start poll from the drop-down list.

Systems				Admin / S	systems
0	0	2 <sub>Mar</sub>	aged 2	1 9.0 Build 8	
Non Reporting System Non Reporting System Since Last 24 hour	Installation status Installation(job) status	Managed v/s defau Variation between manag	lt ed and default	Version Total version count	
< Groups	Systems				
Create Group Delete Group	Request Status Non Reporting Systems Sea	rch Computers System Report A	auto Discover		
All Groups Ö	TOONS - Enterprise Domain			Managed: 2	^
Default 🔅		Q	Page size 25	✓ Sort by Name ✓	
Domain Controllers	Computer	Type Port	EventTracker Version	Change Audit Version Asset value	
EventTracker	SX SERVE	2003		High 🗘	μ
Firewall Devices	5X N10VI 01	Win 10			μ.
Network Devices	SYL N2K11 12W B	2012 R2		Details	i l
SIEM1 🔅		2016		Install agent/Start poll	e i
SUPPORT 🔅		2010		Manage asset value	
Test 🔅	SX INZKLE IMU	2016		Remove agent components	-
TOONS	SXI N2K8F VM	2008 K2			-
VmWare 🔅	SXI N2K8F IVM.	2008 R2		Delete system	÷
970	SXIvvaN7VM	2016		High 🛱	k



- 2. In the Install Agent/Start poll window, select the EventTracker check box to install the Netsurion Open XDR Sensor (Agent-less) and click Next.
  - a. Check the Change Audit option to install Change Audit Sensor (Only for Sensor-based option)

stall agent/Start poll						
Select system to be monitored.						
Name	□ EventTracker		☑ Change	e Audit		
	Select "Next" to proceed.					
		Cancel	Back	Next	Advanced	Insta

- 3. In the EventTracker Agent Type window, choose the Agent-less (limited feature)\* option.
- **4. Poll Every** Select the time frequency during which you want to get the events. By default, the frequency is set to 15 min to receive events from the remote Sensor system.

Install age	nt/Start poll		×
EventT O Agent Ir Ø D	racker Agent based (Full feature astall default Reme reploy WinSCP	type d) dial Action EXEs on this system 🛈	
Agent Poll every	-less (limited featu 15 minutes	'e) *	
Provide The fol	30 minutes 1 hour 2 hour	ficient privilege to collect events remotely. A domain account is preferred. not be applicable for agent-less agent(s):	
Log file System	3 hour	Guaranteed Event Delivery )isk,Memory) Process monitoring (CPU,Memory)	
Netwo Softwa	5 hour 6 hour	toring Application monitoring Service monitoring	
	7 hour 8 hour 9 hour	Cancel Back Next Advanced Insta	all
	10 hour 11 hour		



5. Netsurion Open XDR displays the Install agent/Start poll dialog box with the default client Installation path on the remote computer. Specify the appropriate details and click Install.

Install agent/Start poll		×
Installation path	%ProgramFiles%\Prism Microsystems	^
Note: Installation path on	n the remote machine	
Create "Program Men	nu" shortcuts (j)	
Account	toons\karen (ex.mydomain\administrator)	
Password	••••••	
Confirm Password	•••••	
Selected systems	EventTracker [Agent-less] : ESXWIN2K16VM02	
	Select 'Install' to proceed.	
	Cancel Back Next Advanced	Install 🗸

Field	Description
Account	Specify the valid username and password in Account, Password and Confirm Password fields respectively.
Selected Systems	This field displays the selected system list.

The sensor is installed on the selected machine with the default 'etaconfig.ini' configuration.

6. To set a more specific configuration, click Advanced.

istall agent/Start poll	
Apply configuration	
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify the file. You can also select 'Default' and configure later.	
Default     Custom config     Select     File	
	Cancel Back Next Advanced Insta



7. Choose the **Custom config** option to select a custom configuration file.

#### Note:

The **Default** option is selected by default to apply the manager side 'Sensor configuration' settings (etaconfig.ini).

The custom configuration will provide the templates you created in Sensor configuration along with two more predefined templates.

etaconfig_Servers.ini	This predefined template contains the ideal server configurations which can be applied to the selected sensor system.
etaconfig_Workstations.ini	This predefined template contains the ideal workstation configurations which can be applied to the selected sensor system. This option disables the 'Offline event sending' option.

Apply configuration		
After events are collected, they are proce To apply a predefined configuration, sele You can also select 'Default' and configu	essed at the Manager. Ect 'Custom' and specify the file. re later.	
O Default	File etaconfig.ini etaconfig_Servers.ini	
	etaconiig_workstations.ini	

7. After providing the required details, click Install.

A message window pops-up stating 'Install in progress. Check the Request status screen for updates.'

Install in progress. Check the Request status scree	n for updates.
[	ОК



8. Click OK and go to Systems > Request Status interface to view the installation status.

equest Status							
Application All	<ul> <li>Status All</li> </ul>	~ Sort	by Date ~	]			
Purge all status olde	r than					Purge 1	C
Date	Group/System	Ву	Agent	Туре	Status	Description	
lov 26 07:37:21 PM		R	Change Audit	Install agent	New	In progress.	
lov 26 07:07:01 PM	PhalathletC2	Harsha D	N/A	Search computers	Success	s Search was successful.	

Select	То
Application	Sort the <b>Request Status</b> results by the application installed. Available options are EventTracker and Change Audit.
Status	Sort the <b>Request Status</b> results by the status of the application installed. Available options are All, New, Success, and Failed.
Sort by	Sort the <b>Request Status</b> results by <b>Date</b> of the application installed /on which <b>System</b> it is installed / <b>Type</b> of activity performed/ <b>Status</b> of the application.
Purge all status older than	Remove the older Request Status details from the list.
Export	Export the 'System Status' into Excel format

- 9. Click **Refresh** <sup>C</sup> to view the latest progress status or reopen the **Request Status** dialog box to see the updated status.
- **10.** Then, go to the Netsurion Open XDR Control Panel, double-click the EventTracker Agent Configuration.



Only limited feature tabs are available as shown in the figure below:

📮 EventTracker Agent Configuration	×
File Help	
Select Systems  Agent based system  Apply the following settings to specified Agents	
Manager destinations:	
ETT-MBL/C2016-2	
Log Backup   Performance   Network Connections Logfile Monitor   File Transfer   syslog FTP server   Application Contr Managers   Event Filters   System Monitor   Monitor Processes   Servic	ol es
Windows Manager(s)	1
Manager Name Port Mode Encrypt	
Add Edit Remove	
syslog Manager(s)	
Manager Name Port Mode Encrypt	
Add Edit Remove Message Options	
Save Dose	

# 4.7 Deploying the Netsurion Open XDR Windows Sensor - Microsoft Windows 10 and above

### 4.7.1 Prerequisites for Windows Sensor – Microsoft Windows 10 and above

Before deploying the Sensor, perform the following mandatory settings on Windows 10 or later system(s).

- By default, the Startup Type of Remote Registry is manual. Modify the **Startup Type** as Automatic and start the service.
- Enable File and Printer Sharing.
- Turn on and enable Network Discovery.
- To configure Sensor remotely, add port no 14506 TCP to Firewall Exceptions.
- The user must be domain administrator, member of domain admin, or must be added to the local administrator group where the Sensor must be deployed.



### 4.7.2 Installing / Uninstalling Microsoft Windows 10 and above Sensor

The installation and the uninstallation procedure for Windows 8.1 and above Sensor are identical to the procedures for other Windows Sensors. No other additional configuration settings are required.

# 5 Sensor Deployment

To install the Netsurion Open XDR Sensor and Change Audit Sensor, refer <u>EventTracker Agent Deployment –</u> <u>User Manual</u>.

# 6 Securing Netsurion Open XDR

To secure Netsurion Open XDR, refer EventTracker Hardening Guide and <u>OWASP Complaint EventTracker</u> <u>Guide</u>.

# 7 Uninstalling the Netsurion Open XDR Windows Sensor

There are different methods to uninstall the Netsurion Open XDR Windows Sensor.

- Uninstalling via Control Panel.
- Uninstalling via System Manager.

### 7.1 Uninstalling via Control Panel

Perform the following procedure to uninstall the Netsurion Open XDR Windows Sensor via Control Panel.

- 1. Go to Start > Control Panel > Programs and Features.
- 2. In the Uninstall or change a program, search, and right-click Netsurion Sensor, and then click Uninstall to uninstall the Netsurion Open XDR Windows Sensor.
- 3. A message window pops up to permit and confirm the process. Click Yes to confirm.

User Account Control	×
Do you want to allow this app to make changes to your device?	
msi.	
Verified publisher: Netsurion LLC File origin: Hard drive on this computer	
Show more details	
Yes No	



**4.** Another message window pops-up to proceed with the uninstallation process. Click **OK** to update the setup and proceed with the uninstallation.



5. Netsurion Open XDR pops up a message window stating whether to retain the Sensor configuration settings. Click either Yes to retain or No to rule out as per the requirement.

Netsurion		×
?	Do you wish to retain Sensor configuration settings?	
	Yes No	

Thus, by carrying out the specified procedure, the Netsurion Open XDR sensor will be successfully uninstalled.

### 7.2 Uninstalling via System Manager

Perform the following procedure to uninstall the Netsurion Open XDR Windows Sensor via System Manager.

- 1. Log in to Netsurion Open XDR, hover over Admin and click Systems to go to the Systems Manager interface.
- 2. In the Systems interface, select the required group or system to uninstall the sensor.



3. Then, click the gear icon of the group or system and then click Uninstall agent/ Stop poll from the drop-down list.

	Systems												<b>†</b> /	Admin / Systems
đ R	2 Non Reporting Systems Systems not reporting since the last 24 hours		9 Request Status of v	Failed New Success Status arious sensor requests	2	9 Managed/U	ur I vs Unma nmanaged s	Managed managed managed strength of the second seco	1	8	3 EventTracke Version by cour	9.0 - 8u 9.1 - 8u 9.2 - 8 r Sensor V t	id 18 id 19 id 8 fersion	
	< Groups		Systems											
	Create Group Delete Group	Details	Request Status	Non Reporting Systems	Search Computers	System Repor	t Auto I	Discover	Source type	C				
		Edit Move syst	ems	uters							Page size		Sort by columns	naged: 7
	Search Groups	Install age Uninstall a	nt/Start poll gent/Stop poll		Q,						25	~	Computer	~
	All Groups	Upgrade a Restart ag	igent ent service	of 1 🔰 GO										
	Default	Agent sen	vice status		Type	Port	Event	Tracker v	rsion	Ch	ange audit version		Asset value	
	Domain Controllers	Query for	agent version		Unknow	vn ' 0	i 9.1 -	Build 19			-		Undefined	\$
	EventTracker	Remove a	gent components		2008 R	2 9	2						Undefined	\$
	Firewall Devices	Delete sys	tems		Win 10								Undefined	\$
	Network Devices	Manage a	sset value	0	Win 7	. 0	i 9.0 -	Build 18					Low	\$
	TOONS	Query for	agent update info		2016	. 0	9.2 -	Build 8		9.2	- Build 8		Serious	\$
	VmWare	0	DACE VALLE DI A		2016	. 0	i						Serious	\$
	Win 7 and Server 2008 Above	0	Seneor(CSV-DLA		Unknow	vn 0	i						Undefined	\$
	Win XP and Server 2003	0			Unknow	vn 0	;						Undefined	\$
			t		2008 R	20							Undefined	\$

4. In the Uninstall agent/ Stop poll window, choose the required function from the available option, and click Next.

Uninstall Remote agent(s)/Stop poll		×
Select systems and agent type		
All systems in the selected group		
<ul> <li>○ Take systems from text file</li> <li>Browse</li> <li>(One system per line)</li> <li>Agent Type □ EventTracker □ Change Audit</li> </ul>		
O Specific systems in the selected group		
Ca	ncel Back Next Uninsta	all



5. Select the required EventTracker, Change Audit options and then click Next.

nstall Remote agent(s)/St	top poll						
Select system to be	monitored.						
Name	EventTracker		Change Audit 📋				
LUNTERALIZEVTITIVA	V						
		Select "Next" to proceed.					
			Cancel	Back	Next	Advanced	Install

### 6. Specify the valid credentials and then click Uninstall.

Uninstall Remote agent(s)/Stop poll						×
Account	()					
Password						
Confirm Password						
EventTracker: CVM/ND/46/M00						
Select 'Uninstall' to proceed.						
			Cancel	Back	Next	Uninstall



# 8 Uninstalling Netsurion Open XDR

Perform the following procedure to uninstall Netsurion Open XDR via Control Panel.

- 1. Go to Start > All Programs > Control Panel and click Add or Remove Programs.
- 2. In the Add or Remove Programs, search, and right-click EventTracker, and then click Uninstall to uninstall Netsurion Open XDR.

Name		Publisher	Installed On	Size	Version
📻 Azure Data Studio		Microsoft Corporation	7/19/2022	567 MB	1.36.2
Browser for SQL Server 2019	)	Microsoft Corporation	1/12/2023	11.0 MB	15.0.2000.5
늘 EventTracker		Netsurion LLC	1/12/2023	684 MB	9.4
O Google Chrome	Uninstall	Google LLC	1/11/2023		109.0.5414.75
IIS URL Rewrite Module 2		Microsoft Corporation	1/12/2023	1.80 MB	7.2.1952
Microsoft Access database engine 2010 (English)		Microsoft Corporation	1/12/2023	110 MB	14.0.7015.1000
聞Microsoft Help Viewer 2.3		Microsoft Corporation	1/12/2023	12.1 MB	2.3.28307

3. A message window pops up to confirm the uninstallation. Click Yes to confirm.

Programs and Features				
Are you sure you want to uninstall EventTracke	er?			
□ In the future, do not show me this dialog box	Yes	No		

4. Netsurion Open XDR pops up a message window stating reboot the system to complete the setup. Click **OK** to proceed.





5. In the Uninstall EventTracker Enterprise window, select the required configuration files check boxes to retain the **Configuration, Reports, Elastic Data and Snapshots** files and click **OK**.

ŝ,	Uninstall EventTracker Enterprise	$\times$
?	Please select the files which you wish to retain and o	dick "Ok"
	Configuration	
	Retains all the related configuration files	
	Configuration, Reports and Data	
	Retains Archives, Elasticsearch Data, published reports and all the related configuration files	Î.
	Keep Snapshots	
	Snapshots collected in Change Audit	
	Ok	

# 9 Ports in Netsurion Open XDR

Netsurion Open XDR Module	Port(s)
Netsurion Open XDR Sensor	14506/TCP
Windows Receiver	14505(TCP/UDP) - Optional and multiple VCP's can be configured
Syslog Receiver	514(UDP/TCP) can be configured to any number of ports
Collection Master	14507/TCP - Optional and can be configured to any TCP port
Correlation Receiver	14509/TCP
EventTracker – Change Audit Sensor	14502 (TCP) - To transfer snapshot between client and Server. 14508 (TCP) - Used for real-time comparison of any system with the golden snapshot located at the server.
License Server	14503/TCP
EventTracker Active WatchList	14504

### Note:

In case the user creates multiple Virtual Collection Points, ensure the port used does not contradict with the Default ports used.



# **10** URL or Domain Accessed by Netsurion Open XDR

URL/Domain	Port/Protocol/Direction	Purpose		
*.eventtracker.com	442/TCD/Outbourd	Download the VDD platform undates and DSI		
*.netsurion.com	443/102/000000000	Download the XDR platform updates and DSI		
threatcenter.netsurion.com	442/TCD/Outle out d	Neter wise Thread Contain		
threatcenter.eventtracker.com	443/TCP/Outbound	Netsurion Threat Center		
nsrl.eventtracker.com	9120/TCP/Outbound	Netsurion NSRL server (Hash IOC Lookup)		
certificates.eventtracker.com	443/TCP/Outbound	Netsurion Licensing server		
ipinfo.io	443/TCP/Outbound	Load the map in Machine Learning dashboard		
geolite.maxmind.com	80/TCP/Outbound	Download the Geolocation details in the Attackers Dashboard		
maps.google.com	443/TCP/Outbound	Load the map in the Attackers Dashboard		
virustotal.com	443/TCP/Outbound	IOC lookup from Application Control		
hybrid-analysis.com	443/TCP/Outbound	IOC lookup from Application Control		
whois.domaintools.com	443/TCP/Outbound	IOC lookup from Threat Dashboard		
exchange.xforce.ibmcloud.com				
api.xforce.ibmcloud.com	443/TCP/Outbound	IOC lookup from Threat Dashboard		
xforce-api.mybluemix.net				
rules.emergingthreats.net	443/TCP/Outbound	IOC lookup from Threat Dashboard		
otx.alienvault.com	443/TCP/Outbound	IOC lookup from Threat Dashboard		
ipvoid.com	80/TCP/Outbound	IOC lookup from Threat Dashboard		
senderbase.org		IOC lockup from Threat Dark harrid		
talosintelligence.com	443/ ICP/Outdound	IOC IOOKUP ITOM I MEAL DASNDOARD		
app.recordedfuture.com	443/TCP/Outbound	IOC lookup from Threat Dashboard		



# 11 Troubleshooting

### 11.1 Known Issues while installing Netsurion Open XDR 9.4

The following issues are related to Netsurion Open XDR 9.4 Pre-Installer only.

1. After the admin (A) completes the pre-installation tasks, the user (B) continues to complete the installation on the same system and encounters the following message.



#### Solution

This issue arises when two users alternate while installing the application. As a result,

- make sure the admin user who started the installation finishes installing the application.
- make sure that the logged in user and the system user have the sysadmin privileges on the SQL instance.

#### Note

Refer to User Permission on MS SQL Server for detailed instructions on granting sysadmin privilege.



2. Steps to follow for the below error message.



### Solution

Click **OK** and proceed with the installation.

### 11.2 Frequently Asked Questions

Query	User unable to login to Netsurion Open XDR.			
Cause	Issue with querying Active Directory to authenticate the user			
Solution	<ul> <li>Perform the following steps.</li> <li>1. Go to the <install_path>\EventTrackerWeb\Bin folder.</install_path></li> <li>2. Run the executable "ActiveDirectoryAuthenticationTypes.exe" file.</li> <li>3. Select the following flags and click Apply.</li> <li>Delegation, Secure and Signing (in the section "Use the below flags to authenticate while logging in from Web GUI)</li> <li>Negotiate, Signing and Sealing (in the section "Use the below flags to authenticate while using "EventTracker Configuration" or "Update Users List" utility)</li> <li>4. Then, re-run the EventTracker Configuration utility.</li> </ul>			

Query	User unable to login to Netsurion Open XDR		
Cause	Identity impersonation		
Solution	<ul> <li>Perform the following steps.</li> <li>1. Verify if the "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Prism Microsystems\EventTracker\ASPNET_SETREG" registry hive has values (such as, Impersonate, username, and password) present in it.</li> <li>2. If not, then run the following command by launching the Microsoft Windows Command Prompt via "Run as administrator".</li> <li>Go to <install_path>\EventTrackerWeb\Bin directory.</install_path></li> </ul>		



<ul> <li>Run aspnet_setreg.exe -k:"SOFTWARE\\Prism Microsystems\\EventTracker\\Temp" -u:"username" -p:"password".</li> </ul>
Note:
Replace "username" and "password" with either domain or local admin credentials.
<b>3.</b> Then, re-run the EventTracker Configuration utility.

Query	How to modify Netsurion Open XDR webserver port				
Scenario	If Netsurion Open XDR installation is using IIS, follow the steps to use port 80:				
Solution	<text><list-item><list-item><list-item><list-item></list-item></list-item></list-item></list-item></text>				
	The binding "*:80:" is assigned to another site. If you assign the same binding to this site, you will only be able to start one of the sites. Are you sure that you want to add this duplicate binding? Yes No				



If the issue occurs with Shortcut message stating *Cannot apply changes to this Internet Shortcut,* 



- 6. Then copy the path...\Prism
   Microsystems\EventTrackerWeb\EventTrackerWeb.url to a different location.
   Modify and update the file in the ...\Prism
   Microsystems\EventTrackerWeb\EventTrackerWeb.url.
- 7. Next, stop the **Default Web Site** and start the **EventTracker** site as illustrated in the following image.



Then, go to...\Prism Microsystems\EventTrackerWeb and right-click
 EventTrackerWeb.url (Internet Shortcut) and click Properties, and then modify the URL as illustrated in the following image.

EventTrackerWeb Properties			>		
General Web	Document	Security	Details	Previous Versions	
Event Tracker Web					
URL:	http://lo	calhost/Lo	ogin.asp	¢	
Shortcut key:	None				



Query	Prerequisites for displaying the Attacks Dashboard.		
Required	Access needs to be provided for these websites.		
Solution	Attackers Dashboard feature uses the following websites: <ul> <li>maps.google.com</li> <li>lpvoid.com</li> <li>IBM XFE</li> </ul>		



### **About Netsurion**

Netsurion<sup>®</sup> delivers an adaptive managed security solution that integrates our Netsurion Open XDR 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@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support