



**Installation Guide** 

# Install Netsurion Open XDR Without an Internet Connection

Publication Date March 06, 2024

© Copyright Netsurion. All Rights Reserved.



### Abstract

This guide provides instructions to install Netsurion Open XDR 9.4 without an internet connection.

#### 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 9.4 or later.

#### Audience

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



# Table of Contents

1	Overview	.4
2	Prerequisites	.4
3	Installing Internet Information Service (IIS)	.4
4	Installing SQL ODBC Driver	.5
5	Installing Elasticsearch	.6
6	Installing SQL Server 2019 Express	.8
7	Installing Netsurion Open XDR 9.4	.9



#### 1 Overview

This guide provides a step-by-step procedure for installing Netsurion Open XDR in a system without an internet connection.

## 2 Prerequisites

- Internet Information Service (IIS)
- SQL ODBC Driver
- Elasticsearch 7.10.2
- SQL Server 2019 Express
- Updated Windows Operating System

## 3 Installing Internet Information Service (IIS)

IIS is generally available on Windows Server 2019 and above. If it is not available, follow the below steps to install it.

- 1. Open the command prompt and run as an Administrator.
- 2. Type / Copy-paste the following command in the command prompt and press the Enter key.

```
dism.exe /online /enable-feature /all /featurename:IIS-WebServerRole
/featurename:IIS-WebServer /featurename:IIS-
IIS6ManagementCompatibility /featurename:IIS-ManagementConsole
/featurename:IIS-ManagementService /featurename:IIS-
ApplicationDevelopment /featurename:IIS-ISAPIExtensions
/featurename:IIS-ISAPIFilter /featurename:IIS-ApplicationInit
/featurename:IIS-ServerSideIncludes /featurename:IIS-
NetFxExtensibility /featurename:IIS-NetFxExtensibility45
/featurename:IIS-ASP /featurename:IIS-NetFxExtensibility45
/featurename:IIS-Security /featurename:IIS-IPSecurity
/featurename:IIS-URLAuthorization /featurename:IIS-Performance
/featurename:IIS-HttpCompressionStatic /featurename:IIS-
HttpCompressionDynamic /featurename:IIS-Metabase /featurename:IIS-
WMICompatibility /featurename:IIS-LegacyScripts /featurename:IIS-
LegacySnapIn
```





3. After successful installation, restart the system.

### 4 Installing SQL ODBC Driver

Download the **SQL ODBC Driver** file from the system with an internet connection and transfer it to the system in which Netsurion Open XDR is being installed through any storage device like USB. <u>https://downloads.netsurion.com/ETBuildFiles/msodbcsql\_v11.msi</u>

Once the .msi file is downloaded, perform the following steps:

- 1. Run the .msi file, and the ODBC SQL server setup screen appears. Click Next.
- 2. In the next step, accept the terms and conditions and click Next.
- 3. In the Feature Selection window, Client Components will be enabled, and ODBC for SQL server SDK will be disabled by default.
- 4. Click the drop-down icon and enable **ODBC for SQL server SDK**. Click the **Next** button.



Microsoft ODBC Driver 11 for SQL Server Setup	)	×
Feature Selection		
Select the program features you would like to install.		
Click an icon in the following list to change how a feat	ature is installed.	
	Feature description	
ODBC Driver for SQL Server SDK	ODBC Driver for SQL Serve	er
To shell a king on all		
Installation path		
	Browse	
	Disk Cost	
	Disk Costin	
< Back	Next > Cancel	

- 5. Click **Install** to proceed with the installation.
- 6. Click **Back** to review or modify the settings. Click **Cancel** to exit the setup.

#### 5 Installing Elasticsearch

Download **Elasticsearch version 7.10.2 (zip package)** from the system with an internet connection and transfer it to the system in which Netsurion Open XDR is being installed through any storage device like USB. <u>https://downloads.netsurion.com/ETBuildFiles/elasticsearch/Elasticsearch-7.10.2.zip</u> Once Elasticsearch is downloaded, perform the following steps:

- 1. Extract it and copy it to X:\Program Files\Elasticsearch-7.10.2.
- 2. Create the following registry string values in the following path:

#### "HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Prism Microsystems\EventTracker\Manager"

- a. EsInstallPath (string) with value X:\Program Files\Elasticsearch-7.10.2
- b. EsVersion (string) with value 7.10.2
- c. OpenJDKInstallPath (string) with value X:\Program Files\Elasticsearch-7.10.2\jdk
- d. **OpenJDKVersion** (string) with value **15.0.1**.



Registry Editor			-		×	
File Edit View Favorites Help						
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Prism Microsystems\EventTracker\Manager						
Computer\HKEY_LOCAL_MACHINE\SOI Microsoft ODBC ODBC ODBC Partner Policies Policies Setup VMware, Inc. WWW6432Node	IVARE/WOW6432Nod Name (Default) (Def	eVPnsm Microsystems Type REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	Levent Iracker\Manager Data (value not set) C\Program Files\Elasticsearch-7.10.2 7.10.2 C\Program Files\Elasticsearch-7.10.2\jdk 15.0.1			
<ul> <li>Apache Software Founda</li> <li>Clients</li> <li>Description</li> <li>dotnet</li> <li>Google</li> <li>Intel</li> <li>JavaSoft</li> <li>ODBC</li> <li>Policies</li> <li>Prism Microsystems</li> <li>EventTracker</li> <li>Manager</li> <li>RegisteredApplications</li> <li>SAP BusinessObjects</li> <li>SNIA</li> </ul>						
< SYSTEM <						

3. Set the JDK environment variable path as mentioned below:

🤰 System							- 0	×
← → ~ ↑ 🎐 > Cont	trol Panel > System and Security > System					~ <sup>(1)</sup>	Search Control Panel	م ر
Control Panel Home	System Properties ×							?
Device Manager	Computer Name Hardware Advanced Remote							
<ul> <li>Remote settings</li> <li>Advanced system settings</li> </ul>	You must be logged on as an Administrator to make most of these changes. Performance Visual effects, processor scheduling, memory usage, and visual memory Settings	Environment Variables			×	W	indows Server* 2019	
	User Ptofiles Desktop settings related to your sign in Settings	User variables for dgowda Variable Path TEMP	Value C\Users\dgowda\AppData\Local\M C\Users\dgowda\AppData\Local\Te	ficrosoft\Window	/sApps;			
	Stahup and Recovery System statup, system failure, and debugging information Settings.	TMP	C:\Users\dgowda\AppData\Local\Te	emp			(Change	settings
	Environment Variables		New	Edit	Delete			
	OK Cancel Apply	System variables						
	Product ID: 00429-70000-00000-AA889	Variable ComSpec DriverData JAVA_HOME NUMBER_OF_PROCESSORS OS Path PATHEXT	Value C.\Windows\System32\cmd.exe C.\Windows\System32\DriverDiv C.\Program Files\Elasticsearch-7.10, 8 Windows\yrt C.\Windows\ystem32.C.\Windows\yrt C.\Windows\ystem32.C.\Windows\yrt New_	erData 2\jdk C:\Windows\Syste 5E:WSF:WSH:MS Edit_	em32\Wb C		SActivate 1	Vindows
See also Security and Maintenance			[	ОК	Cancel			

- 4. Run CMD as an Admin and execute X\Program Files\Elasticsearch-7.10.2\bin\elasticsearch-service.bat with parameter Install, then Start.
- 5. The Elasticservice starts running if it is installed successfully. The services can be validated by typing services.msc in the **Run** command window.
- 6. The **elasticsearch.yml** file must include the below commands at the end:

```
path.data: C:\Program Files (x86)\Prism
Microsystems\EventTracker\Cache
```



```
cluster.name: EventTracker
node.name: Node1
indices.query.bool.max clause count: 5120
cluster.routing.allocation.disk.threshold enabled: true
cluster.routing.allocation.disk.watermark.flood stage: 5gb
cluster.routing.allocation.disk.watermark.low: 15gb
cluster.routing.allocation.disk.watermark.high: 10gb
searchquard.disabled: true
searchquard.enterprise modules enabled: false
searchquard.ssl.transport.pemcert filepath: esnode.pem
searchquard.ssl.transport.pemkey filepath: esnode.key.pem
searchguard.ssl.transport.pemkey password:
d2f8725dc0b72b3fa38bc3727aadb8b4
searchquard.ssl.transport.pemtrustedcas filepath: Root-CACert.pem
searchguard.ssl.transport.enforce hostname verification: false
searchquard.ssl.transport.resolve hostname: false
searchguard.ssl.http.enabled: true
searchguard.ssl.http.pemcert filepath: esnode.pem
searchquard.ssl.http.pemkey filepath: esnode.key.pem
searchquard.ssl.http.pemkey password:
d2f8725dc0b72b3fa38bc3727aadb8b4
searchguard.ssl.http.pemtrustedcas filepath: Root-CACert.pem
searchquard.nodes dn:
- CN=ETESnode
searchquard.authcz.admin dn:
- CN=ETESadmin
#signals.enabled: false
```

7. Restart the core elastic service i.e. Elasticsearch 7.10.2 (elasticsearch-service-x64).

### 6 Installing SQL Server 2019 Express

Download **SQL Server 2019 Express** from the system with an internet connection and transfer it to the system in which Netsurion Open XDR is being installed through any storage device like USB. <u>https://downloads.netsurion.com/ETBuildFiles/SQLEXPR\_x64\_ENU\_2019.exe</u>

Select the custom option and proceed with the installation.

While installing SQL Server 2019 Express, under **Server Configuration**, change the **Account name** to **Network service** as shown in the below figure.



Server Configuration							
Specify the service accounts ar	nd collation configuration.						
Install Rules	Service Accounts Collation						
Feature Selection							
Feature Rules	Microsoft recommends that you use a separate account for each SQL Server service.						
Instance Configuration	Service Account Name Password		Startup Typ	e			
2				Automatic	~		
Server Configuration	SQL Server Database Engine	NT Service\MSSQL\$SQL		Automatic	-		
Server Configuration Database Engine Configuration	SQL Server Database Engine SQL Server Browser	NT Service\MSSQL\$SQL NT AUTHORITY\LOCAL		Disabled	~		
Server Configuration Database Engine Configuration Feature Configuration Rules	SQL Server Database Engine SQL Server Browser	NT Service\MSSQLSSQL NT AUTHORITY\LOCAL		Disabled	~		
Server Configuration Database Engine Configuration Feature Configuration Rules Installation Progress	SQL Server Database Engine SQL Server Browser	NT Service\MSSQL\$SQL NT AUTHORITY\LOCAL tenance Task privilege to SQL Ser	ver Database En	Disabled gine Service	~		
Server Configuration Database Engine Configuration Feature Configuration Rules Installation Progress Complete	SQL Server Database Engine SQL Server Browser Grant Perform Volume Main This privilege enables instant	NT Service\MSSQLSSQL NT AUTHORITY\LOCAL tenance Task privilege to SQL Ser t file initialization by avoiding zero	ver Database En oing of data pag	gine Service ges. This may lea	d		
Server Configuration Database Engine Configuration Feature Configuration Rules Installation Progress Complete	SQL Server Database Engine SQL Server Browser Grant Perform Volume Main This privilege enables instant to information disclosure by	NT Service\MSSQL\$SQL NT AUTHORITY\LOCAL tenance Task privilege to SQL Ser t file initialization by avoiding zero allowing deleted content to be ac	ver Database En ping of data pag ccessed.	gine Service ges. This may lea	d		

## 7 Installing Netsurion Open XDR 9.4

After installing the prerequisites, download Netsurion Open XDR 9.4 install files from the system with an internet connection and transfer it to the system in which Netsurion Open XDR is to be installed through any storage device like USB.

Refer the Netsurion Open XDR 9.4 Installation Guide from the below link for the step-by-step instructions. https://www.netsurion.com/assets/content/uploads/files/support-docs/Installation-Guide-Netsurion-v9-4.pdf

Download the latest **EventTrackerCA.crl** from the following link and replace it in the mentioned path: **Install path\Prism Microsystems** 

http://certificates.eventtracker.com/certenroll/EventTrackerCA.crl



#### **About Netsurion**

Netsurion<sup>®</sup> 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	C@Netsurion.com
Managed XDR Enterprise MSPs SOC	C-MSP@Netsurion.com
Managed XDR Essentials Esse	entials@Netsurion.com
Software-Only Customers Soft	ware-Support@Netsurion.com

https://www.netsurion.com/support