**Installation Guide**

# Install Netsurion Open XDR Without an Internet Connection

**Publication Date**

March 06, 2024

## 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

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-ASPNET /featurename:IIS-ASPNET45
/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.
https://downloads.netsurion.com/ETBuildFiles/msodbcsql_v11.msi

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.

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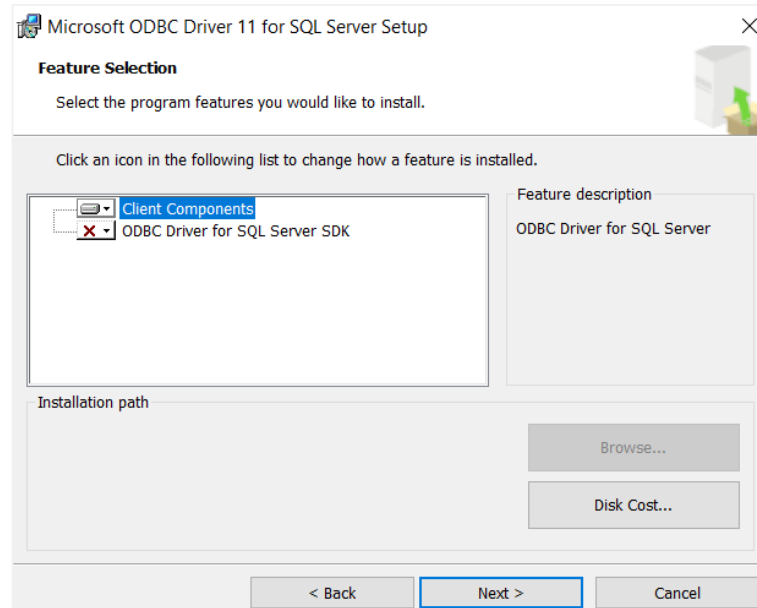
5. Click **Install** to proceed with the installation.
6. Click **Back** to review or modify the settings. Click **Cancel** to exit the setup.
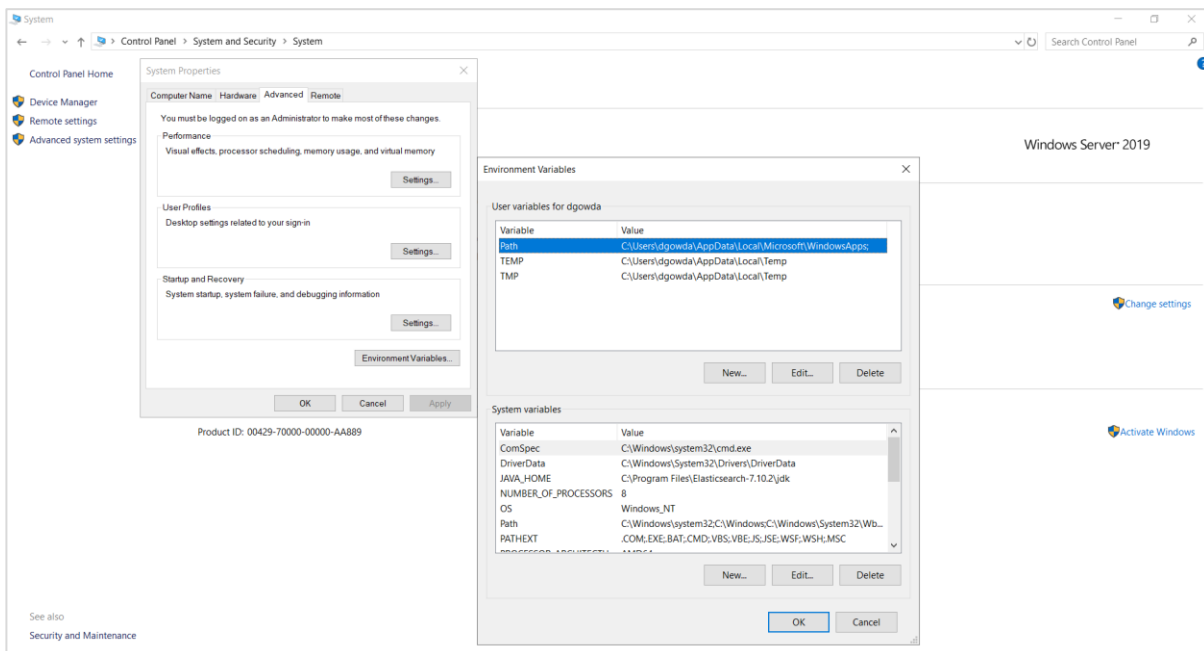
# 5 Installing Elasticsearch

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.
https://downloads.netsurion.com/ETBuildFiles/elasticsearch/Elasticsearch-7.10.2.zip
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.**
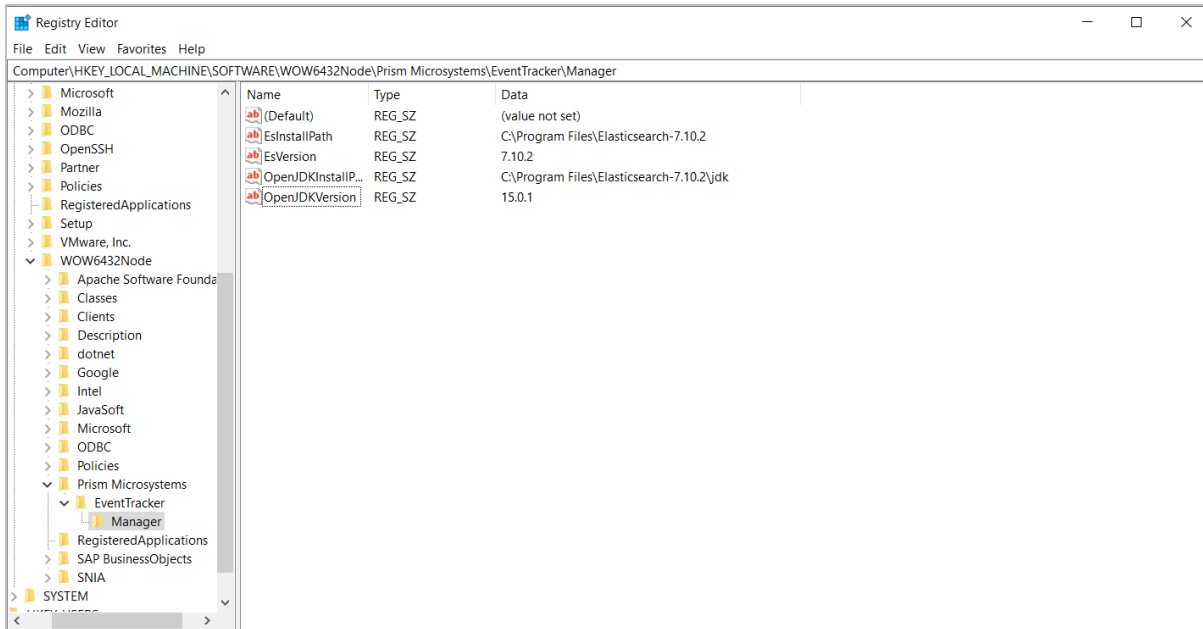
3. Set the JDK environment variable path as mentioned below:



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
searchguard.disabled: true
searchguard.enterprise_modules_enabled: false
searchguard.ssl.transport.pemcert_filepath: esnode.pem
searchguard.ssl.transport.pemkey_filepath: esnode.key.pem
searchguard.ssl.transport.pemkey_password:
d2f8725dc0b72b3fa38bc3727aadb8b4
searchguard.ssl.transport.pemtrustedcas_filepath: Root-CACert.pem
searchguard.ssl.transport.enforce_hostname_verification: false
searchguard.ssl.transport.resolve_hostname: false
searchguard.ssl.http.enabled: true
searchguard.ssl.http.pemcert_filepath: esnode.pem
searchguard.ssl.http.pemkey_filepath: esnode.key.pem
searchguard.ssl.http.pemkey_password:
d2f8725dc0b72b3fa38bc3727aadb8b4
searchguard.ssl.http.pemtrustedcas_filepath: Root-CACert.pem
searchguard.nodes_dn:
- CN=ETESnode
searchguard.authcz.admin_dn:
- CN=ETESadmin
#signals.enabled: false
```

7. Restart the core elastic service i.e. **Elasticsearch 7.10.2 (elasticsearch-service-x64).**
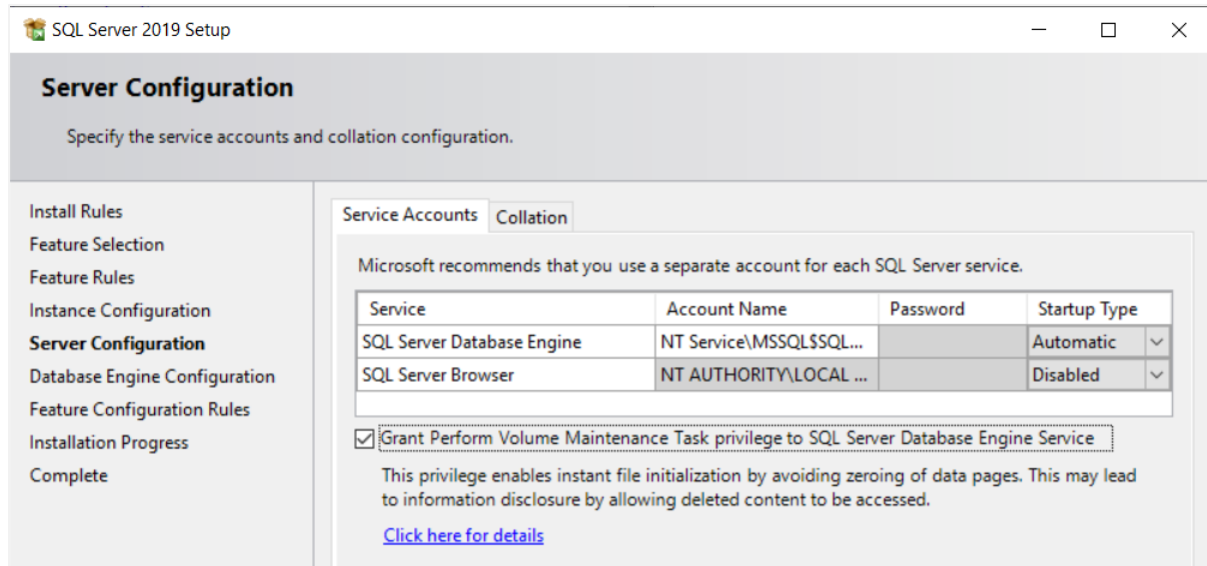
# 6 Installing SQL Server 2019 Express

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.
https://downloads.netsurion.com/ETBuildFiles/SQLEXPR_x64_ENU_2019.exe

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.

# 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® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

## Contact Us

### Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

### Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

| | |
|---|---|
| Managed XDR Enterprise Customers | SOC@Netsurion.com |
| Managed XDR Enterprise MSPs | SOC-MSP@Netsurion.com |
| Managed XDR Essentials | Essentials@Netsurion.com |
| Software-Only Customers | Software-Support@Netsurion.com |

https://www.netsurion.com/support