

Sending Windows Logs to Nagios Log Server 2024R2

Purpose

This document describes how to configure Windows systems to send logs to Nagios Log Server.

Target Audience

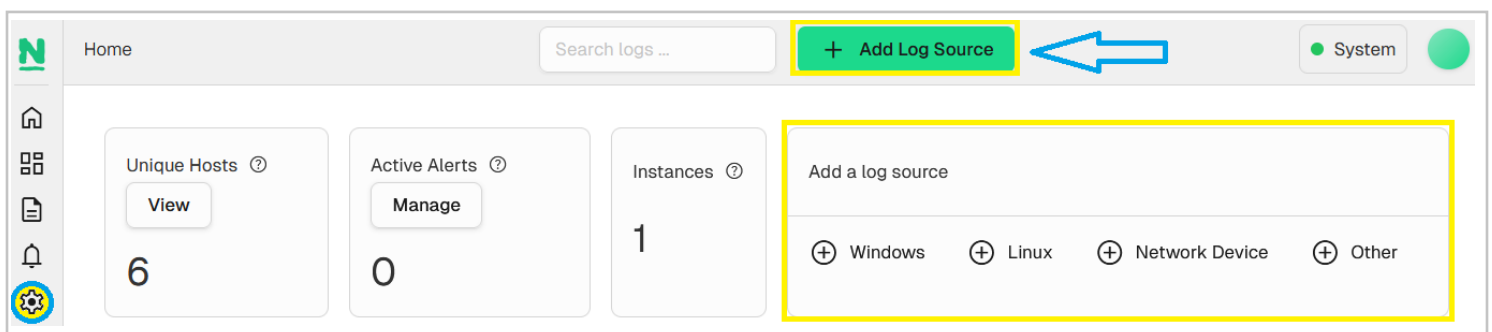
This document is intended for use by Nagios Log Server Administrators who want to receive logs from Windows sources.

Overview

To be able to receive logs from Windows, a third-party program called NXLog Community Edition (CE) is required. This documentation provides the steps to install and configure NXLog CE, and to verify that it is working.

Add A Log Source

To add a new log source, simply click the green **+Add Log Source** button at the top of each page. Alternately you can select a specific source type from the **Add a log source** section of the Home page, or navigate to **Configure -> +Add Log Source**.





Sending Windows Logs to Nagios Log Server 2024R2


Click either the **+ Windows** button on the **Home** page, or click the **Windows** button on the **Add Log Source** page:

Add Log Source


To start receiving logs, you need to set up your log source (computer, router, device, etc) and your configuration in Nagios Log Server. These guides walk you through how to do both.


 **Linux** →


 **Windows** →


 **Network Device** →

Application Logs

 **Apache Server** →

 **IIS Server** →

 **MySQL Server** →

 **MS SQL Server** →

Install NXLog CE

On the Windows source page at the top is a **Getting Started** section. There is a link here to download and install NXLog CE. Note that the installer is downloaded directly from your Nagios Log Server instance, rather than an external site:

Windows

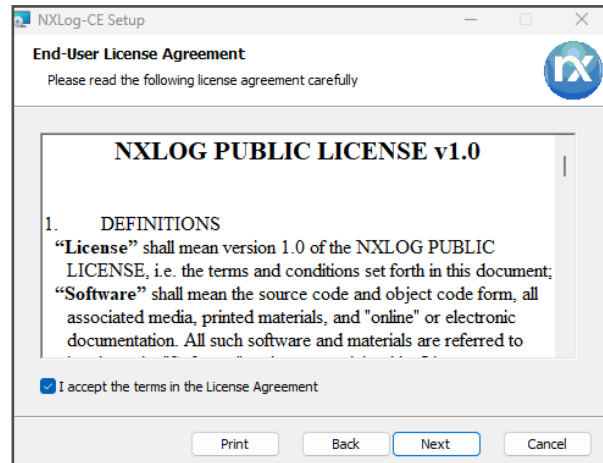
Getting Started

While there are many agents available for Windows that can send logs to Nagios Log Server, we recommend using NXLog. NXLog is an agent that will allow you to send your Windows event logs. Get started by downloading **NXLog CE** and install it on the Windows desktop or server you want to receive logs from.

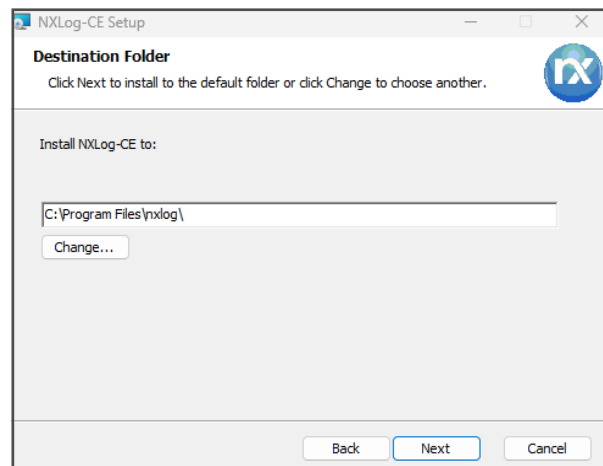
Sending Windows Logs to Nagios Log Server 2024R2

The installation steps are as follows.

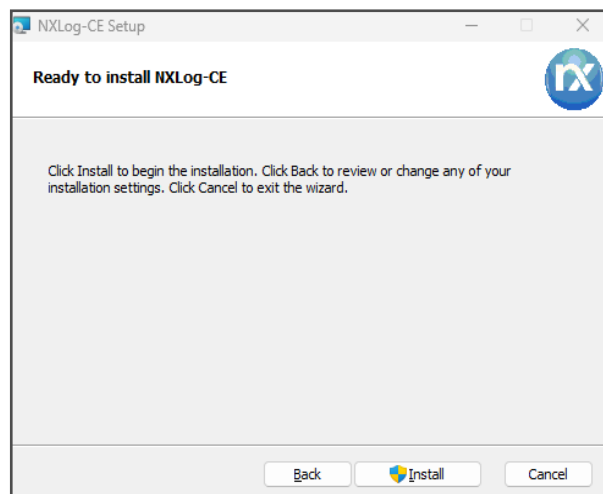
1. You will need to check the box I accept the terms in the License Agreement.



2. Next you have the option to change the install folder, or keep the default:

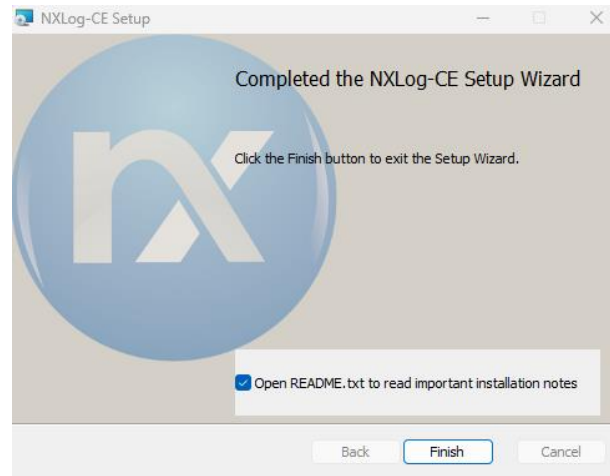


3. Click the **Install** button to complete the installation.



Sending Windows Logs to Nagios Log Server 2024R2

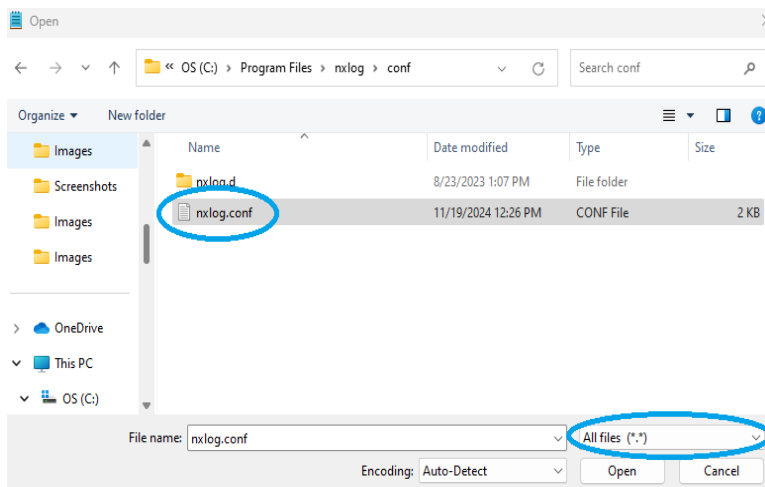
4. The installation is relatively quick and once finished you will be presented with the
5. Completed screen.



Configure NXLog CE

Now that NXLog CE is installed on your windows machine you will need to configure it. On the Nagios Log Server Windows source page there is a **Configuration Setup** section with a configuration code block that needs to be saved on your Windows machine. You can use the **Select All** icon in the top right of the code block to highlight all the code. Once you've done this **right-click** your mouse on the highlighted text and select **Copy**, this will copy the config into the clipboard.

1. Open **Notepad** on your windows machine.
2. Open the nxlog.conf file. It will be located at C:\Program Files\nxlog\conf\nxlog.conf or C:\Program Files (x86)\nxlog\conf\nxlog.conf unless you changed the install directory during install.
3. You will need to use the drop-down list on the bottom right to select **All Files (*.*)**



Sending Windows Logs to Nagios Log Server 2024R2

4. The `nxlog.conf` file will open with a default configuration that is not required. Press **CTRL + A** on your keyboard to select all and then press **DEL** on your keyboard to delete the existing contents.
5. **Right-click** your mouse on the empty `nxlog.conf` file in Notepad and select **Paste** to add the configuration required for Nagios Log Server, which you copied from the setup guide.
6. Click **File > Save** in Notepad to save these changes.
7. You can now close Notepad and proceed to the next step.

Start NXLog CE Service

The last remaining step is to start the NXLog service on the Windows machine. Open a command prompt as an administrator and execute the following command:

```
net start nxlog
```

NXLog CE will now start sending Windows logs to your Nagios Log Server. The installer also configured the service to start automatically when Windows boots.

Verify Incoming Logs

A simple way to confirm that Nagios Log Server is receiving data from the Windows server is to enter the Windows IP into the **Verify Incoming Logs** section at the bottom of the Windows setup section:

Verify Incoming Logs

Once you have configured the log sender, you should start receiving logs right away. Put in the sender's IP address to see if you are receiving logs from that IP.

IP Address

Verified. There are **14823** logs for the host **192.168.107.55**.

Another way to check is to navigate to the Dashboards page, and perform a **Query** using the **host field** and **IP Address** of your new Windows source:

```
host:<Windows Host Address>|
```

Sending Windows Logs to Nagios Log Server 2024R2

Here is an example that shows the received logs appearing in the **All Events** panel of the Nagios Log Server Search Dashboard:

The screenshot shows the Nagios Log Server Search Dashboard. The left sidebar contains navigation options like 'Query Templates' and 'Filters'. The main area displays the 'All Events' panel with a search filter 'host:192.168.107.55' and a table of log entries. The table has columns for Message, @timestamp, Host, and Type. The Host column shows '192.168.107.55' for all three entries, which are highlighted in yellow.

Message ↑↓	@timestamp ↑↓	Host ↑↓	Type ↑↓
A previous instance of the Group Policy Client Service was detected. Param...	2024-11-18T19:11:38.318959294Z	192.168.107.55	eventlog
An account was successfully logged on. Subject: Security ID: S-1-5-18 Acco...	2024-11-18T19:09:12.742359408Z	192.168.107.55	eventlog
An account was successfully logged on. Subject: Security ID: S-1-5-18 Acco...	2024-11-18T19:09:14.756114397Z	192.168.107.55	eventlog

Finishing Up

This completes the documentation on Sending Windows Logs to Nagios Log Server 2024R2. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Nagios Knowledge Base](#)

[Visit Nagios Library](#)