



Purpose

This document describes how to configure Windows 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 a Windows machine.

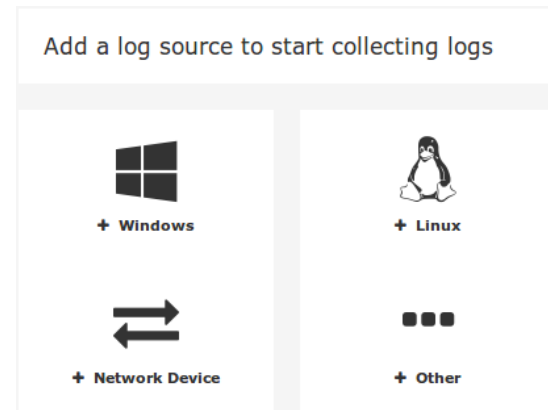
Overview

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.

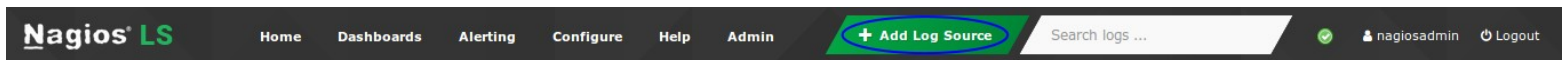
Add A Log Source

When you log in to Nagios Log Server you are presented with the Home page. In the bottom left of the page there are buttons to start sending logs to Nagios Log Server.

Multiple types of sources can be used, this documentation will be using a Windows log source as an example. Click on the **+ Windows** button.

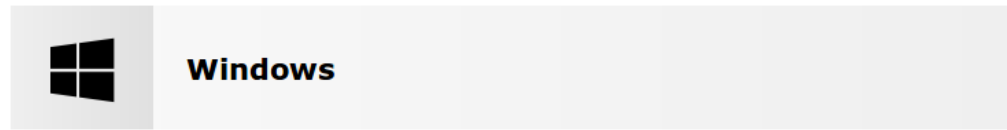


Alternatively you can click the **+ Add Log Source** button on the navigation bar. This will take you to the Add Log Source page where you can click on the **Windows** button.



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, the installer is downloaded from your Nagios Log Server instance.



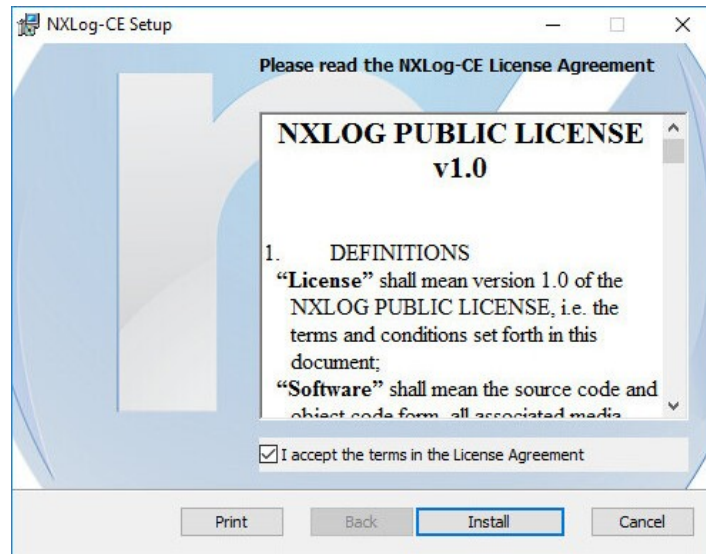
Getting Started

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.

The installation steps are as follows.

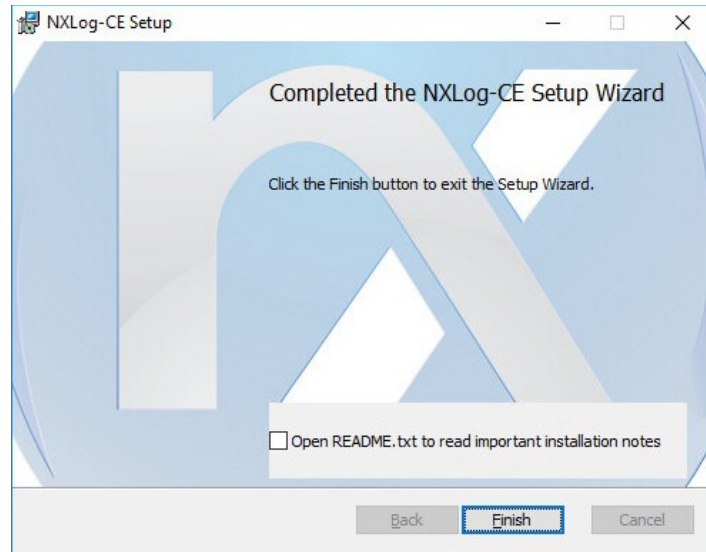
You will need to check the box **I accept the terms in the License Agreement**.

Click the **Install** button.



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

Click the **Finish** button to complete the install.



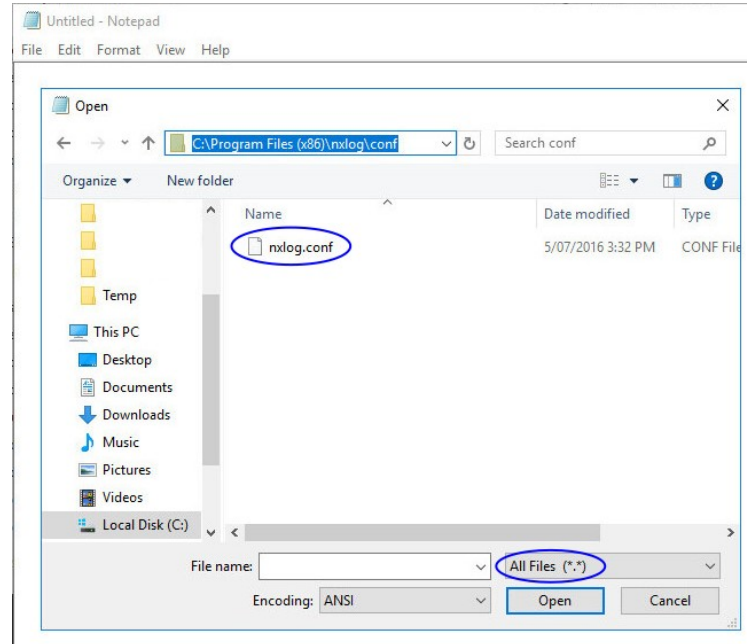
Configure NXLog CE

Now that NXLog CE is installed on your windows machine you will need to configure it. On the Nagios Log Server Windows source page at 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.

Open **Notepad** on your windows machine.

Open the `C:\Program Files (x86)\nxlog\conf\nxlog.conf` file.

You will need to use the drop down list in the bottom right and select **All Files (*.*)**.



The `nxlog.conf` file will open with a default configuration that is not required. Press **CTRL + A** on your keyboard to select it all and then press **DEL** on your keyboard to delete the existing contents.

Right-click your mouse on the empty `nxlog.conf` file in Notepad and select **Paste**, the config file will now have the configuration required for Nagios Log Server.

Click **File > Save** in Notepad to save these changes.

You can now close Notepad.

Nagios Log Server Sending Windows Logs To Nagios Log Server

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

To confirm that Nagios Log Server is receiving data from the Windows server navigate to the **Dashboards** page. Perform a **Query** on the host field using the **IP Address** of your **Windows** host:

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

Here is an example that show the received logs appearing in the ALL EVENTS panel.

The screenshot shows the Nagios Log Server interface. At the top, there is a 'QUERY' button and a search bar containing 'host:10.25.14.91'. Below the search bar is a 'FILTERING' section with a 'GRAPH' button. The main area is titled 'ALL EVENTS' and shows a list of log entries. The first entry is highlighted and expanded to show details.

| @timestamp | host | type | message | Actions |
|-------------------------------|-------------|----------|--|--|
| 2017-11-02T11:55:47.831+11:00 | 10.25.14.91 | eventlog | <p>The Windows Filtering Platform has blocked a connection.</p> <p>Application Information: Process ID: 3032 Application Name: \device\harddiskvolume2\windows\system32\svchost.exe</p> <p>Network Information: Direction: Inbound</p> <p>...</p> | Export as CSV ⓘ ⚙️ + ✕ |

Finishing Up

This completes the documentation on sending Windows logs to Nagios Log Server.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

<https://support.nagios.com/forum>

The Nagios Support Knowledgebase is also a great support resource:

<https://support.nagios.com/kb>