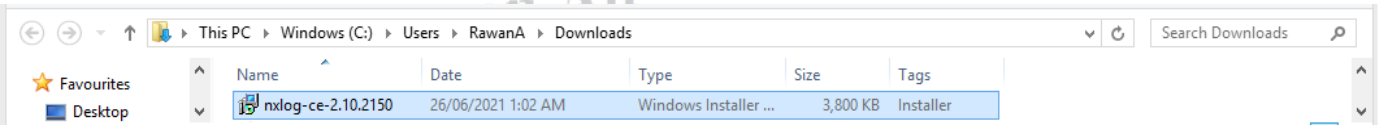
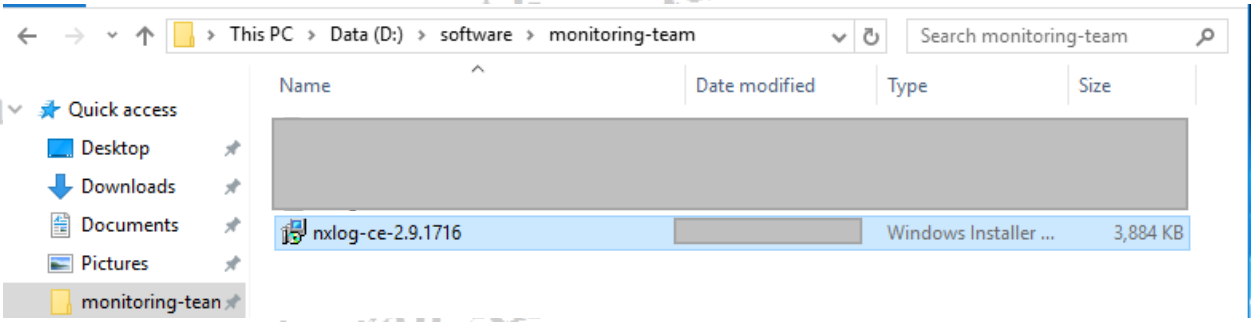
“NXLog is a multi-platform log collection and centralization tool that offers log processing features, including log enrichment (parsing, filtering, and conversion) and log forwarding. It supports all major operating systems, being compatible with many SIEM.” [1]

1- At first, download NXLog agent from the official website “https://nxlog.co/products/all/download”

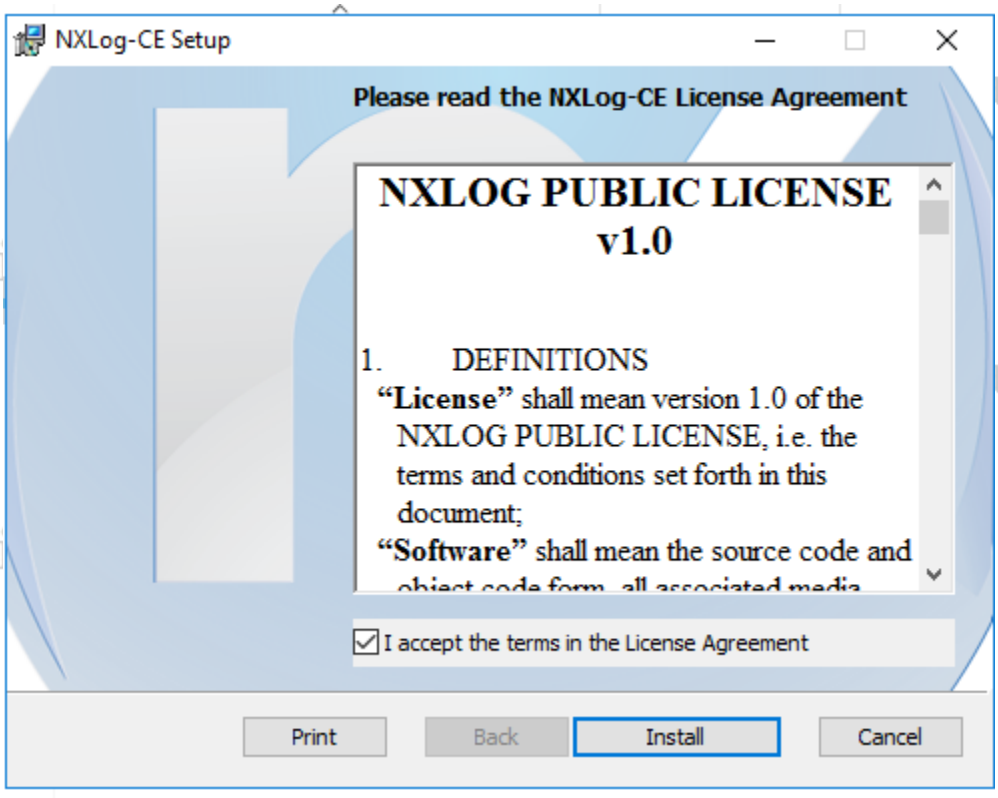


Kindly note in this tutorial I have used an older version of NXLog as shown below.

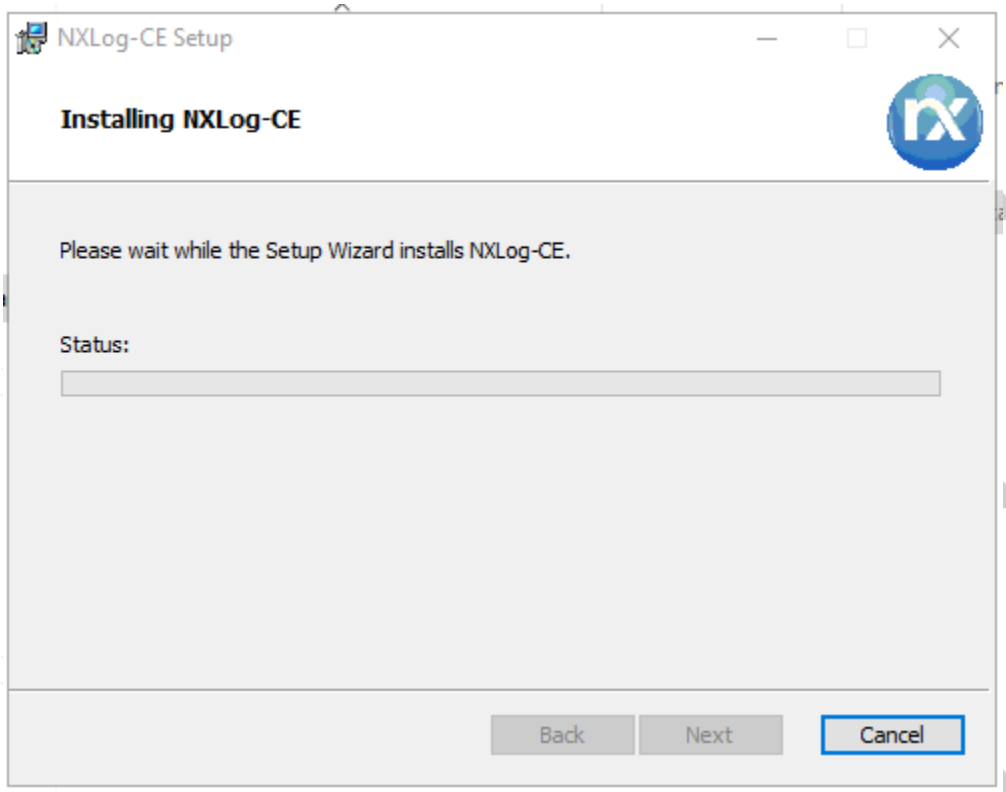
2- Double-click on it.



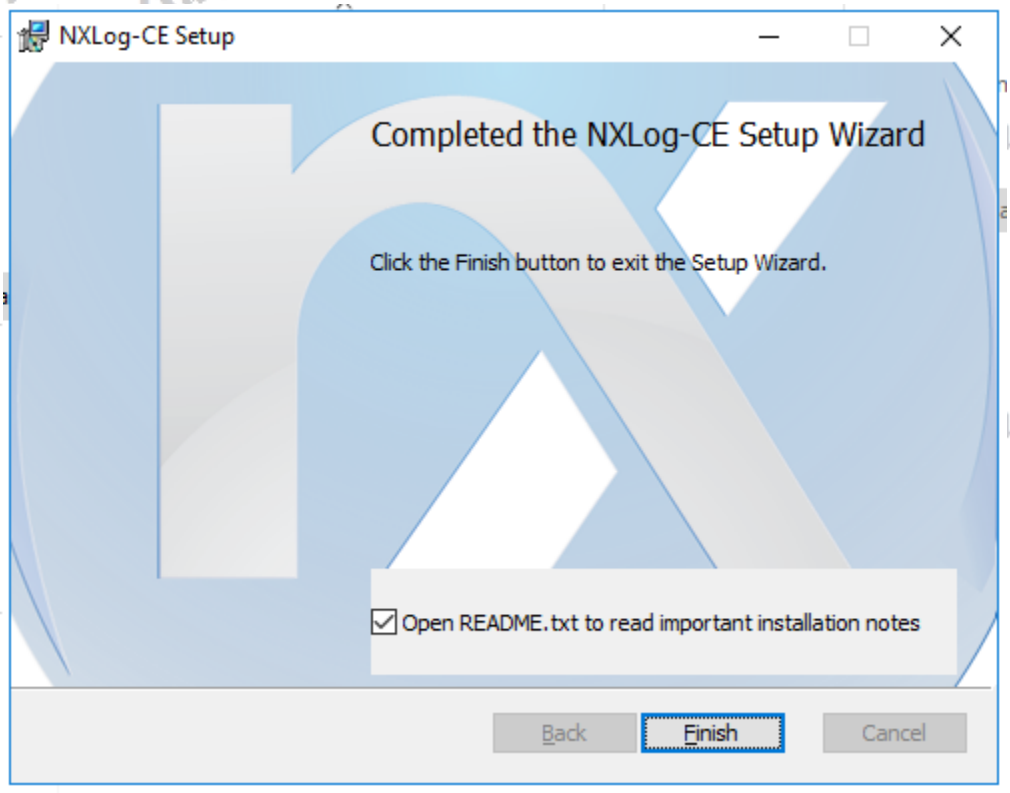
2- Click on “Install” to start the installation:



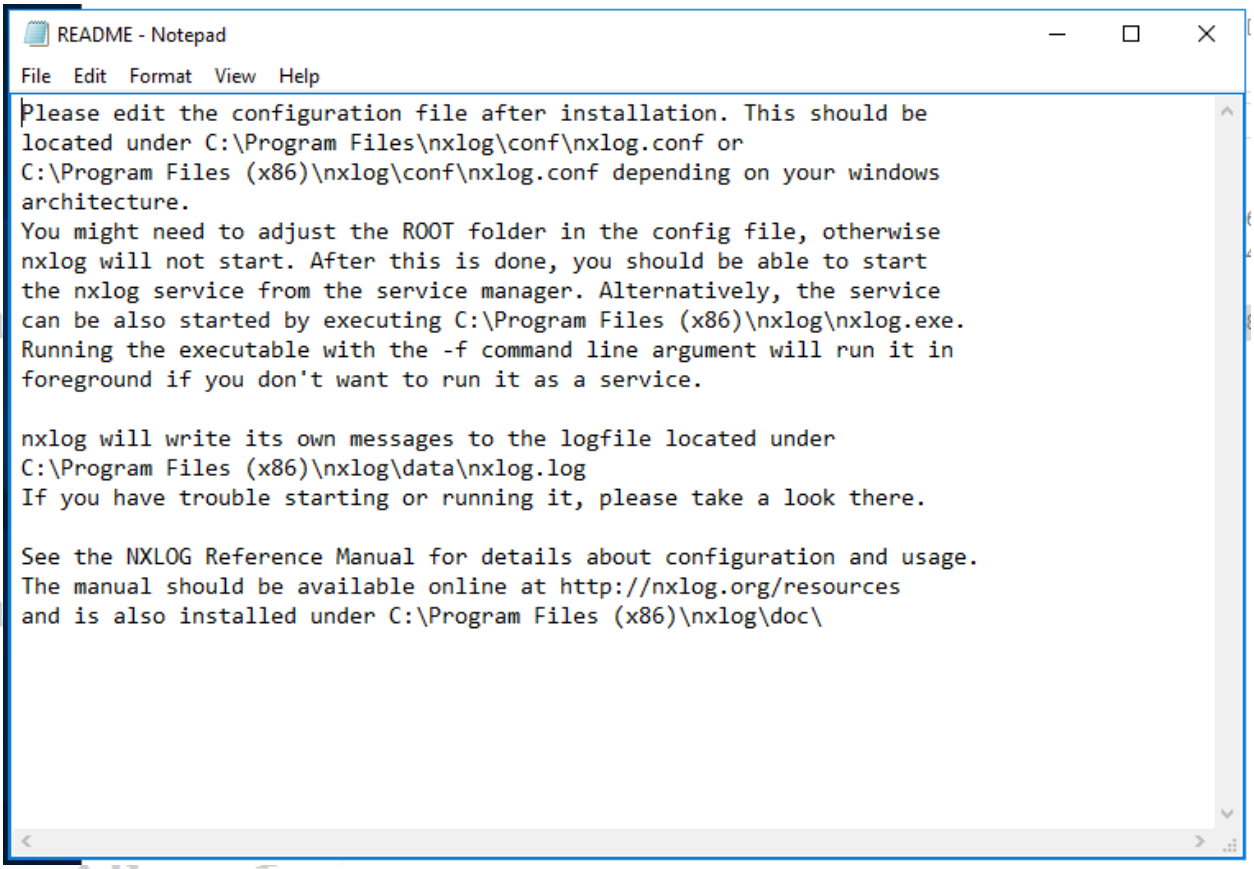
3- Waite for the installing:



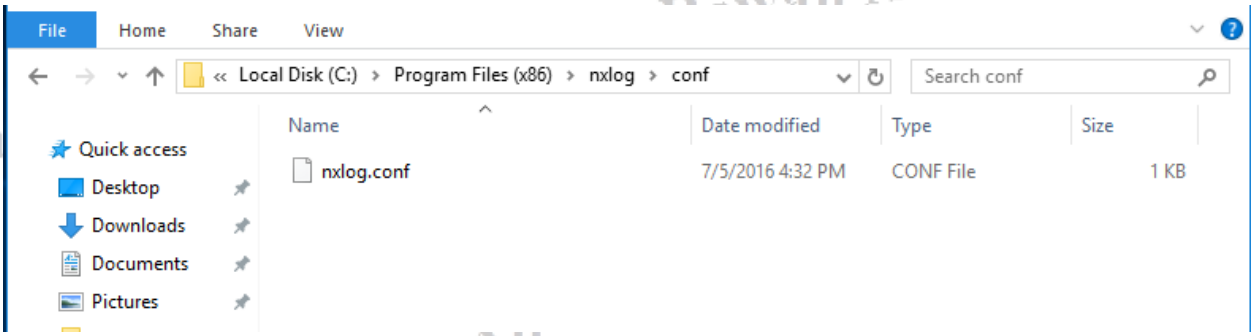
4- Click on “Finish”:



5- Since you marked the open README box, the below file will open, follow the instruction of it due to it understandable:



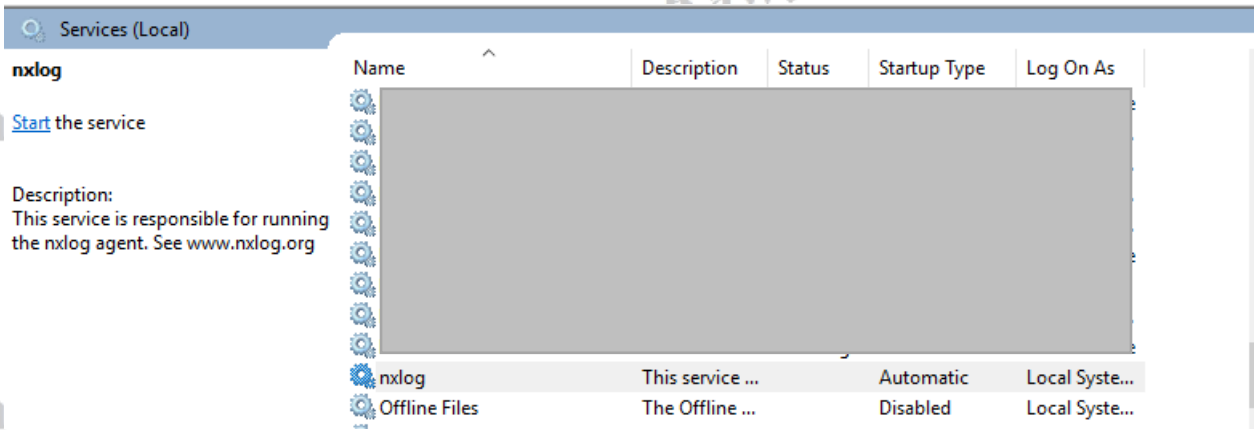
6- By following the previous instruction, you will find the configuration file in the below path:



7- Change the needed to your requirement then save the file:

```
## This is a sample configuration file. See the nxlog reference
manual about the
## configuration options. It should be installed locally and is
also available
## online at http://nxlog.org/docs/

## Please set the ROOT to the folder your nxlog was installed
into,
## otherwise it will not start.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
    Module      xm_syslog
</Extension>

<Input in>
    Module      im_msvistalog
# For windows 2003 and earlier use the following:
#   Module      im_mseventlog
</Input>

<Output out>
    Module      om_tcp
    Host        [redacted]
    Port        514
    Exec        to_syslog_snare();
</Output>

<Route 1>
    Path        in => out
</Route>
```

8- At the end start the NXLog service from services:



References:

1- https://en.wikipedia.org/wiki/NXLog#cite_note-1
2- https://nxlog.co/