

# FTICKS for NPS

**NOTE: This is untested.**

**This only applies to Federation Operators and not to individual sites**

## Installation

Download NXLog Community Edition from here:

<https://nxlog.co/products/nxlog-community-edition/download>

and install it. Make of note of where the nxlog.conf file is.

## Configuration

Edit the *nxlog.conf* file to read, making sure that the ROOT points to the directory it's installed in:

```
Panic Soft
#NoFreeOnExit TRUE

define ROOT      C:\Program Files (x86)\nxlog
define CERTDIR   %ROOT%\cert
define CONFDIR   %ROOT%\conf
define LOGDIR    %ROOT%\data
define LOGFILE   %LOGDIR%\nxlog.log
LogFile %LOGFILE%

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

<Extension _syslog>
    Module      xm_syslog
</Extension>

<Extension _exec>
    Module      xm_exec
</Extension>

<Output syslog_tls>
    Module      om_ssl
    Host       10.12.101.19
    Port       6514
#    CAFile     c:/Program Files (x86)/nxlog/data/cacert.pem
```

```
#      CertFile      c:/Program Files (x86)/nxlog/data/clientreq.pem
#      CertKeyFile   c:/Program Files (x86)/nxlog/data/clientkey.pem
      AllowUntrusted 1
      OutputType    Syslog_TLS
      Exec          to_syslog_ietf();
</Output>

<Output syslog_tcp>
  Module      om_tcp
  Host        10.12.101.19
  Port        601
  OutputType  Syslog_TLS
  Exec          to_syslog_ietf();
</Output>

<Input eventlog>
  Module      im_msvisatalog
  <QueryXML>
    <QueryList>
      <Query Id="0" Path="System">
        <Select Path="System">*[System[Provider[@Name='NPS']]］</Select>
        <Select Path="Security">*[System[Provider[@Name='Microsoft-
Windows-Security-Auditing']] and Task = 12552]</Select>
      </Query>
    </QueryList>
  </QueryXML>
  <Exec>
    if $ClientName =~ /NRPS/i drop();
    if $ProxyPolicyName =~ /NRPS/i drop();
    $FederationID = "000X0";
    if $ClientName == ''
    {
      $OperatorName = "1something.here";
    }
    else
    {
      $OperatorName = $ClientName;
    }
  </Exec>
</Input>

<Route 1>
  Path        eventlog => syslog_tcp
</Route>
```

```
Panic Soft
#NoFreeOnExit TRUE
define ROOT      C:\Program Files (x86)\nxlog
define CERTDIR   %ROOT%\cert
define CONFDIR   %ROOT%\conf
```

```
define LOGDIR    %ROOT%\data
define LOGFILE   %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data
<Extension _syslog>
    Module      xm_syslog
</Extension>
<Extension _charconv>
    Module      xm_charconv
    AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32
</Extension>
<Extension _exec>
    Module      xm_exec
</Extension>

<Output syslog_tls>
    Module      om_ssl
    Host       212.219.243.132
    Port       6514
#    CAFile     c:/Program Files (x86)/nxlog/data/cacert.pem
#    CertFile   c:/Program Files (x86)/nxlog/data/clientreq.pem
#    CertKeyFile c:/Program Files (x86)/nxlog/data/clientkey.pem
    AllowUntrusted 1
    OutputType  Syslog_TLS
    Exec       to_syslog_ietf();
</Output>

<Output syslog_tcp>
    Module      om_tcp
    Host       212.219.243.132
    Port       601
    OutputType Syslog_TLS
    Exec       to_syslog_ietf();
</Output>

<Input eventlog>
    Module  im_msvisatalog
    <QueryXML>
        <QueryList>
            <Query Id="0" Path="System">
                <Select Path="System">*[System[Provider[@Name='NPS']]］</Select>
                <Select Path="Security">*[System[Provider[@Name='Microsoft-
Windows-Security-Auditing']] and Task = 12552]</Select>
            </Query>
        </QueryList>
    </QueryXML>
</Input>
```

```
<Route 1>
  Path      eventlog => syslog_tcp
</Route>
```

Save the file and restart the service.

The stanza, syslog\_tls, is just there for information. It's not actually used in this configuration. At a later date we'll be looking at encryption but there's a PKI to build.

This is all fairly self-explanatory. **OutputType Syslog\_TLS** is needed to enforce the RFC5424 standards along with **Exec to\_syslog\_ietf()**. Not sure why both are needed but they really are.

In the Eventlog config the QueryXML is extracted from Windows Event Log (**Event Viewer → Custom View → Server Roles**. Right click on **Network Policy....** Choose **Properties, Edit Filter, XML** and copy the XML into the NXLog config).

Some customisation might be needed to filter only for traffic between sites, rather than traffic to/from Jisc NRPS.

From:  
<https://wiki.govroam.uk/> - Govroam



Permanent link:  
[https://wiki.govroam.uk/doku.php?id=siteadmin:fticks\\_for\\_ms\\_nps&rev=1714125742](https://wiki.govroam.uk/doku.php?id=siteadmin:fticks_for_ms_nps&rev=1714125742)

Last update: **2024/04/26 10:02**