

How To Configure SSL/TLS for Event-Based Data Collection in Nagios Fusion 2026R2

Purpose

This document describes how to configure SSL/TLS with Nagios Fusion 2026R2 for use with Event-Based Data Collection.

Terminology

For your information:

- SSL = Secure Sockets Layer
- TLS = Transport Layer Security

TLS replaces SSL, however, the tools used to implement both generally use SSL in their name/directives. For simplicity reasons, the rest of this document will use the term SSL.

To implement SSL, you need to generate a certificate. When you generate a certificate, you create a request that needs to be signed by a Certificate Authority (CA). This CA can be:

- A trusted company like VeriSign
- An internal CA that is part of your IT infrastructure, like Microsoft Windows CA
- The Nagios Fusion server itself (self-signed)

The CA will then provide you with a signed certificate. This documentation can be used to generate a request that can be submitted to any of these CA types.

Editing Files

In many steps of this documentation, you will be required to edit files. This documentation will use the vi text editor. When using the vi editor:

- To make changes press **i** on the keyboard first to enter insert mode
- Press **Esc** to exit insert mode
- When you have finished, save the changes in vi by typing **:wq** and press **Enter**

How To Configure SSL/TLS for Event-Based Data Collection in Nagios Fusion 2026R2

Installing Necessary Components

Establish a terminal session with your Nagios Fusion server and as **root** and execute the following command (this step only necessary if you haven't already loaded openssl for other purposes, such as TLS for web UI access) :

RHEL | CentOS | Oracle Linux

```
yum install -y mod_ssl openssl
```

Debian | Ubuntu

```
apt install -y openssl
```

Certificate Directory

The steps in this documentation will be performed from within the `/etc/fusion/certs` directory as **root**. Execute the following command to move to the directory:

```
cd /etc/fusion/certs
```

You will continue to use this terminal session throughout this documentation.

Generate Private Key File

The first step is to generate the private key file, execute the following command:

```
openssl genrsa -out collector.key 2048
```

How To Configure SSL/TLS for Event-Based Data Collection in Nagios Fusion 2026R2

Generate Certificate Request File

Next, generate the certificate request file by executing the following command.

Replace `{HOST}` with your Fusion server IP address, and either `{HOSTNAME}` or `{IP.Address}` with your Fusion server Hostname or IP address (choose only one option for your command). For example, if the hostname of your Fusion server were `fusion.domain.local`, the third line would be:

```
-addext "subjectAltName=DNS:fusion.domain.local" \
```

Note that this is a single long command with `\` line continuation characters after the first three lines :

```
openssl req -new -key collector.key -out collector.csr \
  -subj "/CN={HOST}" \
  -addext "subjectAltName=DNS:{HOSTNAME} OR IP:{IP.Address}" \
  -addext "basicConstraints=critical,CA:FALSE"
```

Sign Certificate Request

At this point you have created a certificate request that needs to be signed by a CA.

Using A Trusted CA Company

If you are going to use a trusted company like VeriSign to provide you with a certificate you will need to send them a copy of the certificate request. This can be viewed by executing the following command:

```
cat collector.csr
```

You'll get a lot of random text; this is what you will need to provide to your trusted CA. You must provide the CA with everything including the `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----` lines.

How To Configure SSL/TLS for Event-Based Data Collection in Nagios Fusion 2026R2

Once they send you the signed certificate you will need to copy the certificate into a new file called `fusion.pem`. The certificate you receive will also be a lot of random text, so you can just paste that text into the new file which you can open with the vi editor:

```
vi collector.pem
```

You must paste everything including the `-----BEGIN CERTIFICATE -----` and `-----END CERTIFICATE -----` lines when pasting them into the file.

Save the file and close vi.

You can now proceed to the [Set Permissions](#) section of this document.

Using Microsoft Windows CA

If you are going to use a Microsoft Windows CA to sign your certificate request, please follow the steps in this Doc Hub article:

[SSL/TLS - Signing Certificates With A Microsoft Certificate Authority](#)

After following the KB article, you will have the `fusion.crt` file and you can proceed to the [Set Permissions](#) section of this document.

Self-Signing The Certificate

You can also self-sign the certificate by executing the following command (Note that this is a single long command with a `\` line continuation characters after the first line) :

```
openssl x509 -req -in collector.csr -signkey collector.key -out collector.pem \
-days 365 -sha256 -copy_extensions copyall
```

This should produce output saying something like, "Certificate request self-signature ok"

Set Permissions

You need to set the correct ownership and permissions on the certificate files. Execute the following two commands:

```
chown fusion:fusion collector.*
```

```
chmod 644 collector.pem
```

How To Configure SSL/TLS for Event-Based Data Collection in Nagios Fusion 2026R2

Update Fusion Collector Config

Now that your certificates are ready to go, you'll need to update the collector.toml file.

First, open the file with this command:

```
vi /etc/fusion/collector.toml
```

Next, uncomment the TLS block, ensuring both the `cert_file` and `key_file` paths are correct, so that it looks like:

```
[tls]
cert_file = "/etc/fusion/certs/collector.pem"
key_file = "/etc/fusion/certs/collector.key"
```

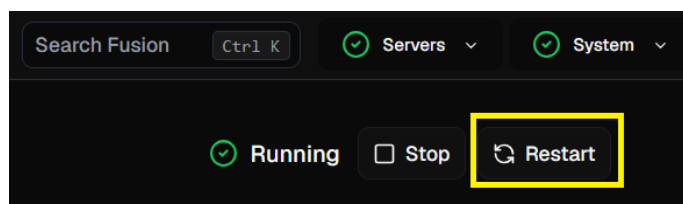
After uncommenting those lines, save the file and close vi.

Restart the Collector Service

Finally, restart the collector service by running this command:

```
systemctl restart fusion-collector.service
```

You can also restart it from the web interface, with the Restart button on the upper-right of the Fusion Collector menu.



Congratulations! You now have a **collector.pem** file containing the data you will use to add a certificate to your Nagios XI, Log Server, or Network Analyzer server to enable Event-Based collection via TLS in Nagios Fusion. You can find full details on adding certificates to the other tools here:

[Managing Fused Servers in Nagios Fusion 2026R2](#)

How To Configure SSL/TLS for Event-Based Data Collection in Nagios Fusion 2026R2

Finishing Up

This completes the documentation on Configuring SSL/TLS with Nagios Fusion 2026R2. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)