Can I add the SysLogAppender to EFT's logging.cfg file to send logging to a SIEM server?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

QUESTION

Can I add the SysLogAppender to EFT's logging.cfg file to send logging to a SIEM server?

ANSWER

Yes, you can add the SysLogAppender to EFT's logging.cfg file, found in **..\ProgramData\Globalscape\EFT Server**.

Add the following code to the bottom of the logging.cfg file. (Add comments to inform future users of its purpose.)

```
log4cplus.rootLogger=TRACE, syslog log4cplus.appender.syslog=log4cplus::SysLogAppender
log4cplus.appender.syslog.ident=syslog
log4cplus.appender.syslog.layout=log4cplus::PatternLayout
log4cplus.appender.syslog.layout.ConversionPattern=[%T] %-5p %b %x - %m%n
log4cplus.appender.syslog.host=localhost log4cplus.appender.syslog.udp=true
log4cplus.appender.syslog.port=514 log4cplus.appender.syslog.facility=user
```

SIEM = Security information and event management, pronounced "SIM."

For more information about logging.cfg, refer to the help for your version of EFT under "Log Format, Type, and Location."

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11616/Can-I-add-the-SysLogAppender...