globalscape™
securely connected

Use Case

Unreadable, Unhelpful Log Files

EFT™ Provides Detailed, Human-Readable Logs and Reports

When a computer system is running well, all is right with the world. When a computer system stops doing what it was designed to do, administrators need answers fast. Most of the time, those answers can be found in the log files. A log file can display details of a failure event in a text file, in the application's proprietary reader, or an external application. Ideally, the log file is in a human-readable format and easily accessible to the administrator. That is often not the case.

For example, suppose the log contained the following information:

```
Wed 18:09:09 slot.18.contained.0.10g invalid_route 2856
```

Although the information is "human readable" and can be opened in a text editor, it isn't clear what "invalid_route 2856" means.

Software providers can design the formatting and contents of a file so that only their proprietary software can read it. In that case, if the system is not working, you can't read the log file, and you must open a support ticket to get help on even the slightest errors. If the log file is designed so that it can be read in common software, such as a text editor, the administrator can open the log, scroll to the time stamp at which the error occurs, and troubleshoot from there—if the information is clear and not cryptic.

Logging in the Enhanced File Transfer™ (EFT™) Platform

The main log of Globalscape's Enhanced File Transfer™ (EFT™) Platform uses SourceForge's log4cplus, an Open Source logging API that is easy to configure to log only the information that you want and viewable in any text editor. For example, if you are tracking a suspected PGP error, you can enable PGP logging in the logging configuration file, which is accessible from the Windows file system. In the following log example, it's clear that the PGP signature verification failed, as well as on which file the task failed.

```
EFT.log: 02-08-10 WARN Events.Server <> - EVENT_ACTION_PGP: Signature
verification failed for file: D:\1.txt.pgp
```

Several log levels are available to limit the amount and details of logs returned (TRACE, DEBUG, INFO, WARN, ERROR, FATAL, or OFF), so you can log as much or as little detail as you need. After troubleshooting is complete, administrators can disable the specific logging function and log levels so as not to generate excessive logs.

EFT server service startup and failure events appear in the Windows Event Viewer Application logs. On EFT Enterprise, the client log, an ASCII text file sorted by date and time, is readable in any text editor, and tracks file download, copy, and move activity.

The built-in logs that EFT generates are far superior to what nearly every other server provides. Oftentimes, when troubleshooting connection issues with other servers, Globalscape Support will start with the EFT logs, because the other servers simply do not generate or save much, if any, information about what is actually happening outside of their server.

Unlike many managed file transfer systems, EFT provides detailed, human-readable logs and reports for security events, file transfer events, user events, and server/site alerts, so you always know what is going on in your network.