FORTRA

Globalscape EFT Logging & Visibility

Copyright Terms and Conditions

202409270211

Table of Contents

EFT Logging and Visibility

EFT Transfer Activity Logging

As the EFT log file subsystem writes out the date for the log, it compares the current computer date/time to the value for the log rotation (hourly/daily/weekly/monthly/yearly) period specified on the logs tab of the Server. When a write-to-log operation occurs that is calculated to cross a period (that is, the prior write was within a former period, but the current date/time at write is a new period), EFT rotates the log file name and then writes to that new log.

EFT activities can be logged in various places.

- The EFT<servername>.log file is the root logger and controls all logging items as defined in logging.cfg. Individual loggers can be enabled and increased in verbosity as needed. Some loggers contain sub appenders to log specific aspects.
    - Domain-level EFT server logs
    - SFTP logging
    - SLS/TLS logging
    - Syslog/Appender
- For information about the Audit Database logs, refer to Auditing Database Errors and Logging. (Not to be confused with Audit Database Settings.)
- For event rule logging (such as *cl060312.log*) refer to Event Rules Client Log.
- For installation logs, refer to Installation Logging.
- For DMZ Gateway logging, refer to DMZ Gateway Logging.
- For Windows Event Logs, refer to Windows Event Log (WEL) Action.

EFT Client Activity Log

To monitor EFT client activity, you can reference EFT's log files, including registration state of modules, server/site functions, SFTP, SSL/TLS connections, and of course, errors and warnings.

- The EFT client activity log, also known as "TED6" logs, is used to log client connection information (event rules and outbound transfers), client commands/requests, remote server responses, and status messages.
- EFT client log files are saved in the **C:\ProgramData\Globalscape\EFT Server\Logs\** folder.
- Refer to Event Rules Client Log for more information.

Event Rules Client Log

When EFT's **Download** and **Copy/Move** Action offloads or downloads files, the outbound session is recorded to a log file that is named **cl[yymmdd].log** (for example, **cl060312.log**) and saved in the EFT installation folder (**C:\ProgramData\Globalscape\EFT Server\Logs\**). The log file is formatted as follows:

> Time; Protocol; Host Name:Port; User Name; Local Path; Remote Path; Operation; GetLastCode

For example:

```
2006-03-06 10:11:03; ftp; 192.168.20.171:21; ClientA;
 C:\test1.txt; /test1.txt; download; 226;
```

A tenth column can be added to the CL log by defining an advanced property. Refer to https://kb.globalscape.com/KnowledgebaseArticle10262.aspx for details.

The log can be used for troubleshooting connection and transfer errors. The "GetLastCode" value returns the protocol success or error code or socket error. For example, trying to connect to a non-existent website will result in the socket error code 10060, *connection timeout*. For example, if EFT was unable to make a connection to a remote host, a code that could appear in the cl log is 10061 (connection refused). If you are using FTP to make the connection and upload/download a file, you will also see FTP Status and Error Codes. Refer to "Windows Sockets Error Codes" in the Microsoft Developer Network for a complete list of common socket error codes.

In addition to the standard socket error codes, EFT defines the socket error codes described below.

#	Description
0	Success (connected OK)
1	General socks failure
2	Socket connection not allowed by ruleset
3	The network is unreachable
4	The host is unreachable
5	The remote server actively refused the connection
6	The Time To Live (TTL) expired. This could indicate a network problem.
7	The command was not supported by the remote host. Also a catchall error code.
8	The address type or format is not supported
10	Illegal socks name
11	Socks5 authentication failure (username/password incorrect)
12	Can't connect to socks server
2000	Internal timeout error code (multiple reasons, such as firewall blocking connection, etc.)

FTP and **FTP over SSL** only return protocol-level success and error codes. For example, a successful transfer would return 226 or a bad login password would return 530. Refer to RFC 959 for a complete list of FTP/S return codes.

SFTP (SSH2) returns the following success and error codes:

#	Description
-1	Undefined or unknown error (not enough information to determine exactly why it failed) When an OpenSSH client disconnects from EFT, it reports that the exit status is **-1**. The default return code is -1, unless an optional message is returned from the server. EFT does not return the optional message, so the exit status is always -1.
0	The operation completed successfully
1	The operation failed because of trying to read at end of file
2	The requested file does not exist
3	Insufficient privileges to perform the operation
4	The requested operation failed for some other reason
5	A badly formatted message was received. This indicates an error or incompatibility in the protocol implementation
6	Connection has not been established (yet) and a timeout occurred
7	Connection to the server was lost, and the operation could not be performed
8	A timeout occurred

EFT Server Activity Log

To monitor EFT activity, you can reference EFT's log files. EFT supports W3C, Microsoft IIS, and NCSA log file formats. Server events are logged to a file named *[log file format]yymmdd.log*, where YY, MM, and DD indicate the numeric year, month, and day respectively. Depending on the log file format selected, a 2-letter abbreviation is prepended to the filename, as described in the table below. For example, a log file in the Microsoft IIS format created on August 22, 2024 is named `in240822.log`.

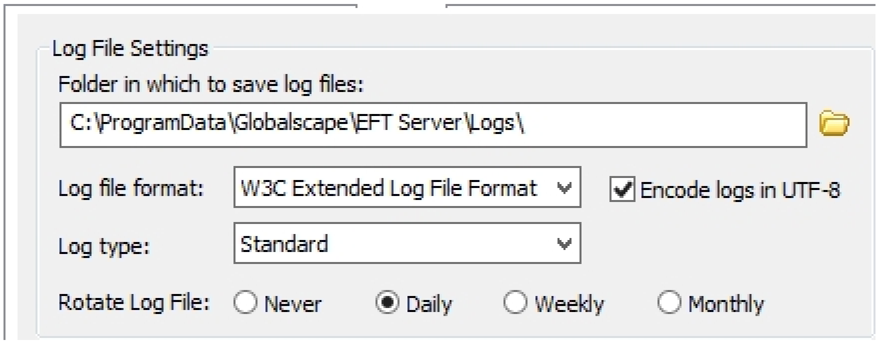
By default, log files are saved in the EFT data directory in the **Log** folder (for example, **C:\ProgramData\Globalscape\EFT Server\Logs**). Outbound connection information is audited in that same folder in a log named cl<date>.log.

When using HA, you need to specify a unique location (local) for the log files. This is for troubleshooting purposes (to know what node an issue occurred on). Also, having two nodes write to the same file causes issues with file locking, which will cause data in the logs to be lost.

Log Format, Type, and Location

To specify log settings

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Server node.
3. In the right pane, click the **Logs** tab.



Log File Settings

Folder in which to save log files: C:\ProgramData\Globalscape\EFT Server\Logs\

Log file format: W3C Extended Log File Format ☑ Encode logs in UTF-8

Log type: Standard

Rotate Log File: ○ Never ● Daily ○ Weekly ○ Monthly

4. In the **Log File Settings** area, in the **Folder in which to save log files** box, type the path to the directory in which to save this Server's log files. To browse for a path, click the folder icon 📂.
5. In the **Log file format** list, click **W3C Extended**, **Microsoft IIS**, **NCSA Common**, or **No Logging**. Changing the log file format disconnects all active users. It is recommended to stop all Sites or wait until all users are inactive before changing the log file format. The W3C format records all times in GMT (Greenwich Mean Time).
6. Clear the **Encode logs in UTF-8** check box if you do not want to encode logs in UTF-8 format. When the check box is cleared, the **u_ex*.log** file is named **ex*.log**.

From Microsoft TechNet:

When using the UTF-8 logging feature, note the following:

- A log file logged in UTF-8 does not contain a Byte Order Mark (BOM). File editors use this mark to identify text as UTF-8 text. Therefore, if you attempt to open a log file that is logged in UTF-8 in Notepad by double-clicking the file or by using the Open With option, the file might not display correctly. To open the file in a way that displays it correctly, use the Open command on the File menu and then select UTF-8 in the Encoding box.
- UTF-8 is a double-byte character-set standard. ASCII is a single-byte character-set standard. Because of this disparity, logging UTF-8 information to an ASCII file causes a ? to be logged for the characters that cannot be converted to the code page of the server.

7. In the **Log type** list, click **Standard** or **Verbose**. (Verbose provides more details, but makes larger files.)
8. In the **Rotate Log File** area, specify **Never**, **Daily**, **Weekly**, or **Monthly**.
9. Click **Apply** to save the changes on EFT.
10. Stop and restart EFT.

For information about the Audit Database Settings, refer to Auditing Database Errors and Logging.

Log File Format	Abbreviation
W3C	ex
NCSA	nc
Microsoft IIS	in

Log Example

Below is an example of an **ex**-formatted log:

```
#Version: 1.0
#Software: CuteLogger
#Date: 2010-04-08 20:07:50
#Fields: date time c-ip c-port cs-username cs-method
cs-uri-stem cs-uri-query sc-status sc-bytes cs-bytes s-name s-port
2010-04-08 20:07:07 192.168.241.1 - test [1]user test - 331 - - - 22
2010-04-08 20:07:07 192.168.241.1 - test [1]pass ******* - 230 - - - 22
2010-04-08 20:07:16 192.168.241.1 - test [1]created /Test+File+1.txt - 226 - 54 - 22
2010-04-08 20:08:23 192.168.241.1 - test [1]rnfr /Test+File+1.txt - 350 - - - 22
2010-04-08 20:08:23 192.168.241.1 - test [1]rnto /Test+File+2.txt - 250 - - - 22
2010-04-08 20:08:26 192.168.241.1 - test [1]sent /Test+File+2.txt - 226 - 54 - 22
2010-04-08 20:10:02 192.168.241.1 - test [1]dele /Test+File+2.txt - 250 - - - 22
2010-04-08 20:10:08 192.168.241.1 - test [1]ssh_disconnect timeout - 421 - - - 22
2010-04-08 20:10:09 192.168.241.1 - test [1]ssh_disconnect timeout - 421 - - - 22
2010-04-08 20:11:57 192.168.241.1 - test [2]user test - 331 - - - 990
2010-04-08 20:11:57 192.168.241.1 - test [2]pass ****** - 230 - - - 990
2010-04-08 20:12:04 192.168.241.1 - test [2]created /Test+File+1.txt - 226 - 54 - 990
2010-04-08 20:12:16 192.168.241.1 - test [2]rnfr /Test+File+1.txt - 350 - - - 990
2010-04-08 20:12:16 192.168.241.1 - test [2]rnto /Test+File+2.txt - 250 - - - 990
2010-04-08 20:12:28 192.168.241.1 - test [2]rnfr /Test+File+2.txt - 350 - - - 990
2010-04-08 20:12:28 192.168.241.1 - test [2]rnto /Test+File+3.txt - 250 - - - 990
2010-04-08 20:12:31 192.168.241.1 - test [2]sent /Test+File+3.txt - 226 122 - - 990
```

The log can be read as described below:

Field	Description	Example
(Each field in the log has either a value (for example, date) or a dash (-) if no value was sent for that field.)		
date	Date log was recorded	2010-04-08
time	Time log was recorded	20:07:16
c-ip	Client IP address	192.168.241.1
c-port	Client port	21
cs-username	Username	test
cs-uri-stem	Stem portion of URI	/Test+File+1.txt
cs-uri-query	Query portion of URI	-
sc-status	Status code	226 (Closing data connection. Requested file action successful.)
sc-bytes	The number of bytes that the server sent to the client.	541
cs-bytes	The number of bytes that the client sent to the server.	54
s-name		-
s-port	Server port	22

Field	Description	Example	
cs-method	Method (Command Sent)	ABOR	Abort an active file transfer
		ACCT	Account information
		ALLO	Allocate sufficient disk space to receive a file
		APPE	Append
		AUTH	Authentication/Security Mechanism
		CCC	Clear Command Channel
		CDUP	Change to Parent Directory
		CHANGEPASSWORD	Change the password
		CLIENTCERT	Client SSL certificate was rejected (reason is provided in the log entry).
		COMB	Combines file segments into a single file on EFT.
		CREATED	File was created (uploaded).
		CWD	Change working directory
		DELE	Delete file
		EPRT	Specifies an extended address and port to which the server should connect
		EPSV	Enter extended passive mode
		FEAT	Get the feature list implemented by the server
		HELP	Display a list of all available FTP commands

Field	Description	Example	
		KICK	Client connection was closed by administrator.
		LIST	Returns information of a file or directory if specified, else information of the current working directory is returned
		MDTM	Return the last-modified time of a specified file
		MKD	Make directory
		MLSD	Lists the contents of a directory if a directory is named
		MLST	Provides data about exactly the object named on its command line, and no others
		MODE	Sets the transfer mode (Stream, Block, or Compressed)
		NLIST	Returns a list of file names in a specified directory
		NOOP	No operation (dummy packet; used mostly on keepalives)
		OPTS	Select options for a feature
		PASS	Authentication password
		PASV	Enter passive mode
		PBSZ	Protection Buffer Size
		PORT	Specifies the port to which the server should connect

Field	Description	Example	
		PROT	Data Channel Protection Level
		PWD	Print working directory Returns the current directory of the host
		QUIT	Disconnect
		REIN	Re initializes the connection
		REST	Restart transfer from the specified point
		RETR	Transfer a copy of the file
		RMD	Remove a directory
		RNFR	Rename from
		RNTO	Rename to
		SENT	File was sent (downloaded).
		SITE	Sends site specific commands to remote server
		SIZE	Return the size of a file
		SMNT	Mount file structure
		SSCN	Set secured client negotiation
		SSH_DISCONNECT	SFTP (SSH) client connection was closed (reason is provided in the log entry).
		STAT	Returns the status
		STOR	Accept the data and to store the data as a file at the server site
		STOU	Store file uniquely
		STRU	Set file transfer structure

Field	Description	Example	
		SYST	Return system type
		TYPE	Sets the transfer mode
		USER	Authentication username
		WEBSERVICE	Web Service was invoked.
		XCRC	Compute CRC32 checksum on specified file

Installation Logging

The installation log file is intended for debugging purposes and contains messages that may help resolve issues that arise during installation.

- During installation and maintenance, the installer creates an **Installer.log** file in the **%TEMP%\<Product Name>** directory. For example:
  - **C:\Users\administrator\AppData\Local\Temp\EFT Server\Installer.log**
  - **C:\Users\administrator\AppData\Local\Temp\EFT Server\Installer.log**
- At the completion of the installation, either due to success or failure, the installer copies the final log to the **<InstallDir>\logs** directory, if it exists. If the installer fails during an initial clean installation, the **<InstallDir>\logs** directory may not exist. In this case, the final log file remains in the **%TEMP%\<Product Name>** directory.
- The installer attempts to append to the existing log file on subsequent runs of the installer (for example, if the user performs a Reinstall). It does this by copying any existing **Installer.log** file from the installation directory into the Temp directory, writing to it during installation, and then copying it back to the **<InstallDir>\logs** directory when the installation is finished.
- You can write out the same log messages to another log file of your choosing using the **/logfile=<Log file>** command line switch to the installer.

Debug Logging

The installer is capable of writing the same messages that go to the Main Installer Log using the Windows debug logging infrastructure. These messages may be viewed using a utility such as SysInternal's DebugView application. To enable this logging, the installer must be run from the command line with the **/debug** switch.

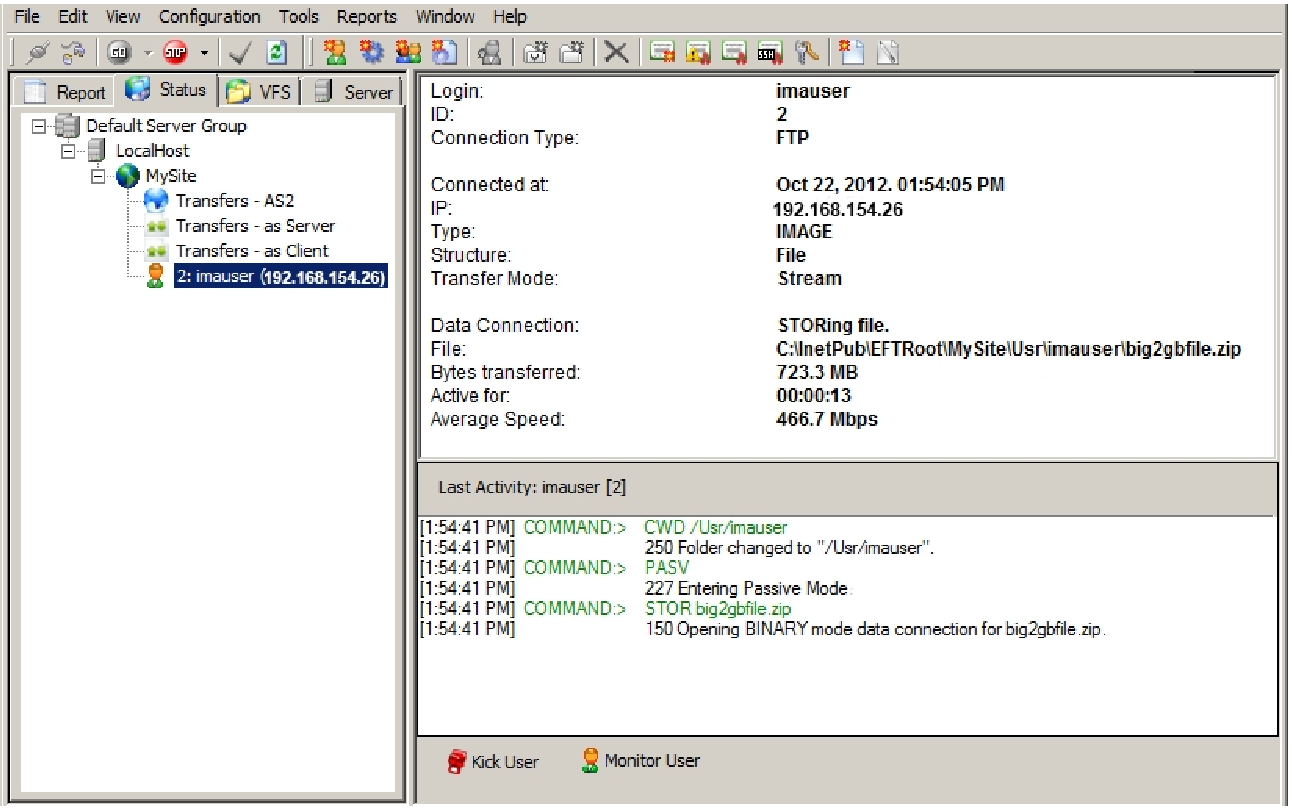
Viewing Connections to a Site

On the Status tab, expand the **Site** node to view connection status for the Site, AS2 transactions, and each connected user account.

For example, if a user is connected to EFT via SFTP, the Site tree displays an ID number, the username, the IP address of the Site, and "SFTP." For example, **4: jbite (192.168.174.235) - SFTP**. The right pane displays the Login (username), ID, Connection Type, date and time connected, IP address, Average Upload Speed, and Average Download Speed. The bottom of the right pane displays the connection log.

You can forcibly disconnect a user by selecting the user in the tree, and then clicking **Kick User** in the right pane.

You can see more details of the user's activity by selecting the user in the tree then clicking **Monitor User** in the right pane.



Login: imauser
ID: 2
Connection Type: FTP

Connected at: Oct 22, 2012. 01:54:05 PM
IP: 192.168.154.26
Type: IMAGE
Structure: File
Transfer Mode: Stream

Data Connection: STORing file.
File: C:\InetPub\EFTRoot\MySite\Usr\imauser\big2gbfile.zip
Bytes transferred: 723.3 MB
Active for: 00:00:13
Average Speed: 466.7 Mbps

Last Activity: imauser [2]

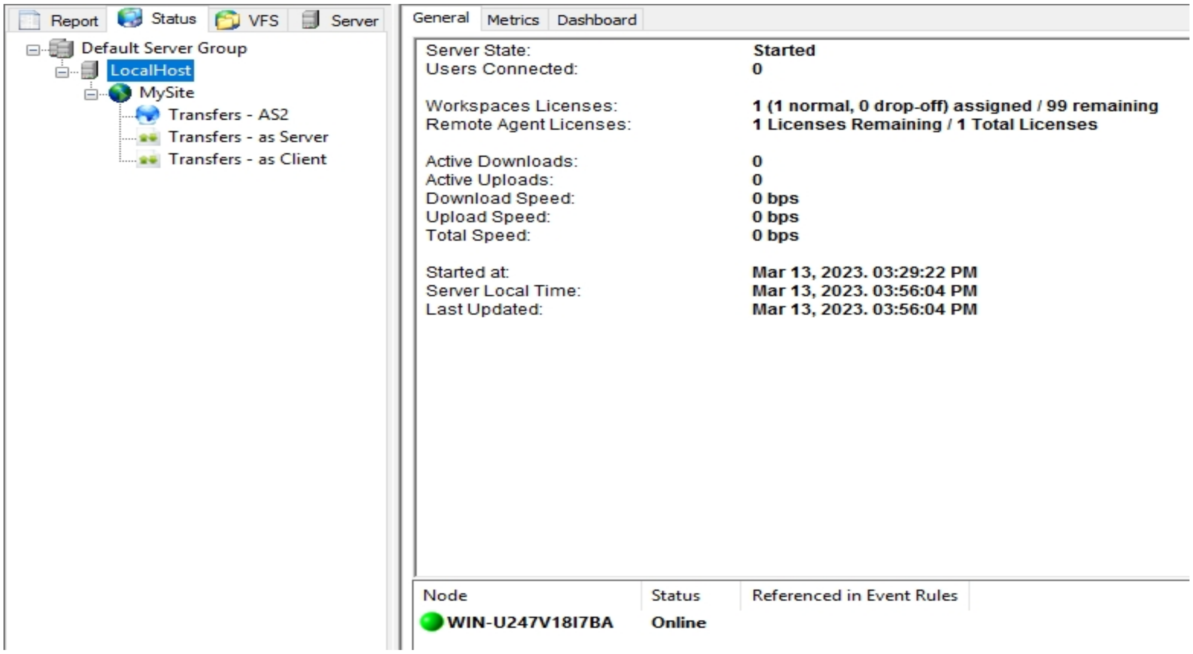
```
[1:54:41 PM] COMMAND:>  CWD /Usr/imauser
[1:54:41 PM]            250 Folder changed to "/Usr/imauser".
[1:54:41 PM] COMMAND:>  PASV
[1:54:41 PM]            227 Entering Passive Mode
[1:54:41 PM] COMMAND:>  STOR big2gbfile.zip
[1:54:41 PM]            150 Opening BINARY mode data connection for big2gbfile.zip.
```

Viewing Server or Node Status

In the administration interface, you can view the status of EFT in real time, such as number of users connected, average speed, and so on. You can view Server status on the **Status** tab or on the Server node's **General** tab.

To view status on the Status tab

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Status** tab, click the **Server** node. EFT's statistics appear in the right pane.



```
Server State:              Started
Users Connected:           0

Workspaces Licenses:       1 (1 normal, 0 drop-off) assigned / 99 remaining
Remote Agent Licenses:     1 Licenses Remaining / 1 Total Licenses

Active Downloads:          0
Active Uploads:            0
Download Speed:            0 bps
Upload Speed:              0 bps
Total Speed:               0 bps

Started at:                Mar 13, 2023. 03:29:22 PM
Server Local Time:         Mar 13, 2023. 03:56:04 PM
Last Updated:              Mar 13, 2023. 03:56:04 PM
```

Node	Status	Referenced in Event Rules
● WIN-U247V18I7BA	Online	

3. In an HA cluster, you can see the nodes and their status at the bottom of the **Status** viewer.
   - **Online**: EFT server service is up and communicating via Heartbeat to the rest of the node in the cluster
   - **Master**: Same status as **Online**, however this node is designated as the **Master** node for Event Rules Load balancing.

Only one node can be show as Master in the list of the nodes from the cluster. This status only is displayed if you have at least one Event Rule enabled and configured to run in more than one node from the cluster. If this status exists, the Master node will create an exclusive file lock onto **MasterNodeLock** file in the HA config shared folder.

- **Offline**: EFT server service is down; no communication via Heartbeat is performed
- **Unknown**: A node name is being reference in at least one Event Rule; however, this node name is not part of the cluster.

To view status on the Server tab

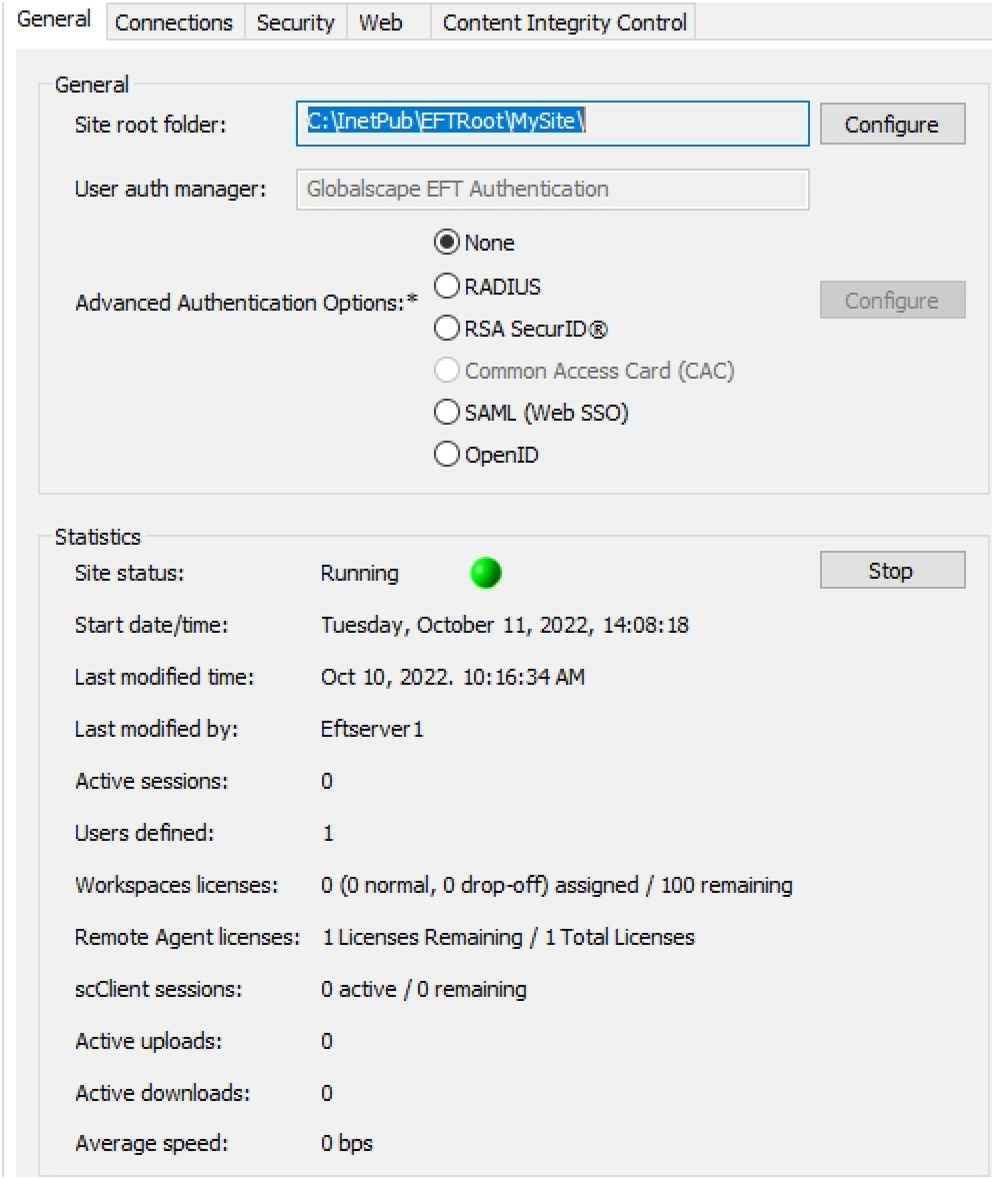
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the **Server** node.
3. In the right pane, click the **General** tab. EFT's statistics appear in the right pane.
    - **Server status**: Displays "Service is started" or "Service is stopped." You can also stop and start the EFT service on this tab.
    - **Start date/time**: Displays the date and time that the EFT service was last started.
    - **Uptime**: Displays the length of time that the EFT service has been running since it was last started.
    - **Last modified time**: Displays the date and time that EFT was last modified.
    - **Last modified by**: Displays the username of the user who last modified EFT.
    - **Active sessions**: Displays the number of users who are currently logged in to EFT.
    - **Active uploads**: Displays the number of uploads in progress.
    - **Active downloads**: Displays the number downloads in progress.
    - **Average speed**: Displays the average transfer speed.
    - **Workspaces licenses**: Displays the number of licenses used and number licensed (allowed)
    - **Web clients licenses**: Displays the number of licenses used and number licensed (allowed)

Viewing Site Statistics

In the administration interface, you can view the status of the Site in real time, such as number of users connected, average speed, the number of active Web Transfer Clients sessions, and so on.

To monitor current statistics on the Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the **Site** that you want to monitor.
3. In the right pane, click the **General** tab.



General

Site root folder: C:\InetPub\EFTRoot\MySite\

User auth manager: Globalscape EFT Authentication

Advanced Authentication Options:*
● None
○ RADIUS
○ RSA SecurID®
○ Common Access Card (CAC)
○ SAML (Web SSO)
○ OpenID

Statistics

Site status: Running ●

Start date/time: Tuesday, October 11, 2022, 14:08:18

Last modified time: Oct 10, 2022. 10:16:34 AM

Last modified by: Eftserver1

Active sessions: 0

Users defined: 1

Workspaces licenses: 0 (0 normal, 0 drop-off) assigned / 100 remaining

Remote Agent licenses: 1 Licenses Remaining / 1 Total Licenses

scClient sessions: 0 active / 0 remaining

Active uploads: 0

Active downloads: 0

Average speed: 0 bps

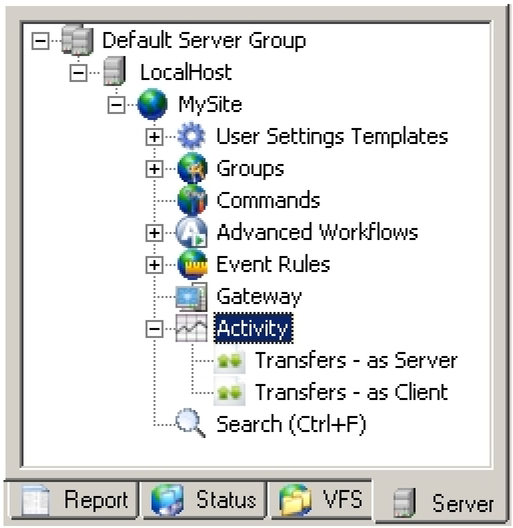
The Site's information appears in the **Statistics** area.

- **Site status**: Displays "Running" or "Stopped"; you can also stop and start the Site.
- **Start date/time**: Displays the date and time that the Site was last started.
- **Last modified time**: Displays the date and time that the Site was last modified.
- **Last modified by**: Displays the username of the user who last modified the Site.
- **Active sessions**: Displays the number of users who are currently logged in to the Site.
- **Users defined**: Displays the number of user accounts defined on the Site.
- **scClient sessions**: Displays the number of sessions in use and available. (scClient is part of the Accelerate module, which is no longer offered for EFT; however, some customers who upgrade still have Accelerate licenses.)
- **Active uploads**: Displays the number of uploads in progress.
- **Active downloads**: Displays the number downloads in progress.
- **Average speed**: Displays the average transfer speed.

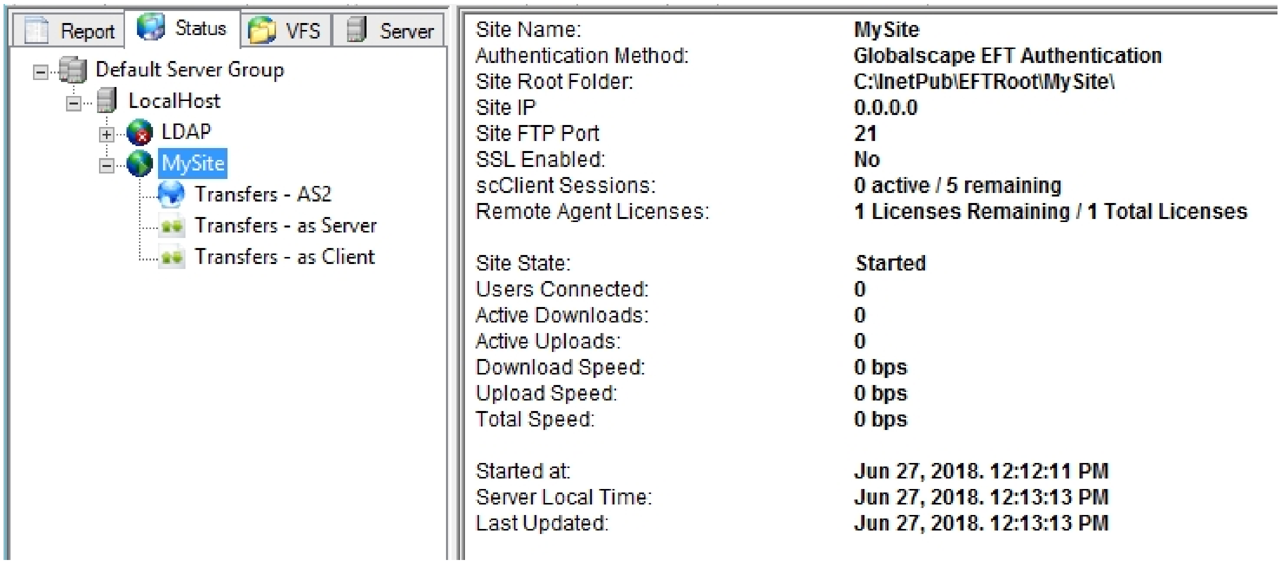
You can view details of transfers to and from EFT on the **Status** tab. Refer to Viewing Transfers To and From a Site for details.

Viewing Transfers To and From a Site

You can view details of transfers to and from EFT on the **Status** tab. On the **Server** tab, a node in the tree labeled **Activity** has two branches: **Transfers - as Server** and **Transfers - as Client**. Click one of the branches to open the **Status** tab to that view.



Or just click the Site's **Status** tab:

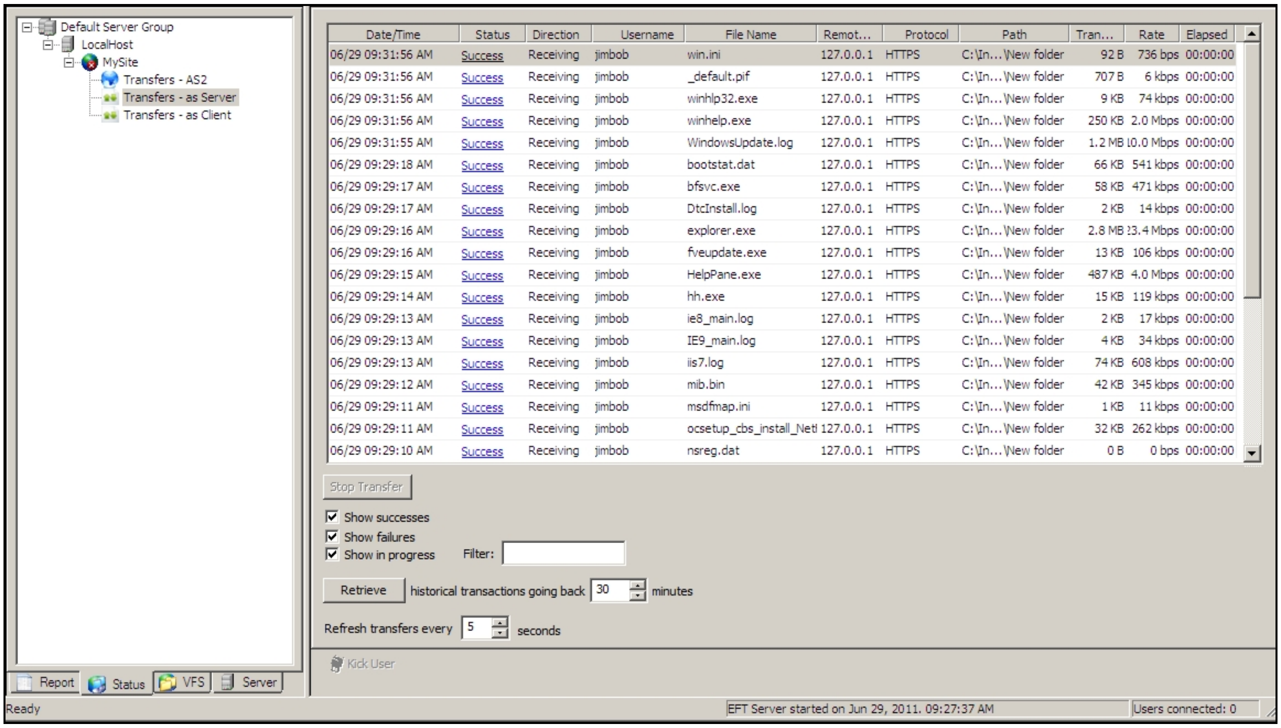


Site Name:	**MySite**
Authentication Method:	**Globalscape EFT Authentication**
Site Root Folder:	**C:\InetPub\EFTRoot\MySite\**
Site IP	**0.0.0.0**
Site FTP Port	**21**
SSL Enabled:	**No**
scClient Sessions:	**0 active / 5 remaining**
Remote Agent Licenses:	**1 Licenses Remaining / 1 Total Licenses**
Site State:	**Started**
Users Connected:	**0**
Active Downloads:	**0**
Active Uploads:	**0**
Download Speed:	**0 bps**
Upload Speed:	**0 bps**
Total Speed:	**0 bps**
Started at:	**Jun 27, 2018. 12:12:11 PM**
Server Local Time:	**Jun 27, 2018. 12:13:13 PM**
Last Updated:	**Jun 27, 2018. 12:13:13 PM**

Then click one of the nodes:

Transfers - as Server - Displays "Receiving" when uploading files to the Web Transfer Client or sharing files via Workspaces.

Transfers - as Client - Displays when you upload files using an FTP client or drag-and-drop into a user folder.



Date/Time	Status	Direction	Username	File Name	Remot...	Protocol	Path	Tran...	Rate	Elapsed
06/29 09:31:56 AM	Success	Receiving	jimbob	win.ini	127.0.0.1	HTTPS	C:\In...\New folder	92 B	736 bps	00:00:00
06/29 09:31:56 AM	Success	Receiving	jimbob	_default.pif	127.0.0.1	HTTPS	C:\In...\New folder	707 B	6 kbps	00:00:00
06/29 09:31:56 AM	Success	Receiving	jimbob	winhlp32.exe	127.0.0.1	HTTPS	C:\In...\New folder	9 KB	74 kbps	00:00:00
06/29 09:31:56 AM	Success	Receiving	jimbob	winhelp.exe	127.0.0.1	HTTPS	C:\In...\New folder	250 KB	2.0 Mbps	00:00:00
06/29 09:31:55 AM	Success	Receiving	jimbob	WindowsUpdate.log	127.0.0.1	HTTPS	C:\In...\New folder	1.2 MB	10.0 Mbps	00:00:00
06/29 09:29:18 AM	Success	Receiving	jimbob	bootstat.dat	127.0.0.1	HTTPS	C:\In...\New folder	66 KB	541 kbps	00:00:00
06/29 09:29:17 AM	Success	Receiving	jimbob	bfsvc.exe	127.0.0.1	HTTPS	C:\In...\New folder	58 KB	471 kbps	00:00:00
06/29 09:29:17 AM	Success	Receiving	jimbob	DtcInstall.log	127.0.0.1	HTTPS	C:\In...\New folder	2 KB	14 kbps	00:00:00
06/29 09:29:16 AM	Success	Receiving	jimbob	explorer.exe	127.0.0.1	HTTPS	C:\In...\New folder	2.8 MB	23.4 Mbps	00:00:00
06/29 09:29:16 AM	Success	Receiving	jimbob	fveupdate.exe	127.0.0.1	HTTPS	C:\In...\New folder	13 KB	106 kbps	00:00:00
06/29 09:29:15 AM	Success	Receiving	jimbob	HelpPane.exe	127.0.0.1	HTTPS	C:\In...\New folder	487 KB	4.0 Mbps	00:00:00
06/29 09:29:14 AM	Success	Receiving	jimbob	hh.exe	127.0.0.1	HTTPS	C:\In...\New folder	15 KB	119 kbps	00:00:00
06/29 09:29:13 AM	Success	Receiving	jimbob	ie8_main.log	127.0.0.1	HTTPS	C:\In...\New folder	2 KB	17 kbps	00:00:00
06/29 09:29:13 AM	Success	Receiving	jimbob	IE9_main.log	127.0.0.1	HTTPS	C:\In...\New folder	4 KB	34 kbps	00:00:00
06/29 09:29:13 AM	Success	Receiving	jimbob	iis7.log	127.0.0.1	HTTPS	C:\In...\New folder	74 KB	608 kbps	00:00:00
06/29 09:29:12 AM	Success	Receiving	jimbob	mib.bin	127.0.0.1	HTTPS	C:\In...\New folder	42 KB	345 kbps	00:00:00
06/29 09:29:11 AM	Success	Receiving	jimbob	msdfmap.ini	127.0.0.1	HTTPS	C:\In...\New folder	1 KB	11 kbps	00:00:00
06/29 09:29:11 AM	Success	Receiving	jimbob	ocsetup_cbs_install_Netl	127.0.0.1	HTTPS	C:\In...\New folder	32 KB	262 kbps	00:00:00
06/29 09:29:10 AM	Success	Receiving	jimbob	nsreg.dat	127.0.0.1	HTTPS	C:\In...\New folder	0 B	0 bps	00:00:00

☑ Show successes
☑ Show failures
☑ Show in progress   Filter:

historical transactions going back 30 minutes

Refresh transfers every 5 seconds

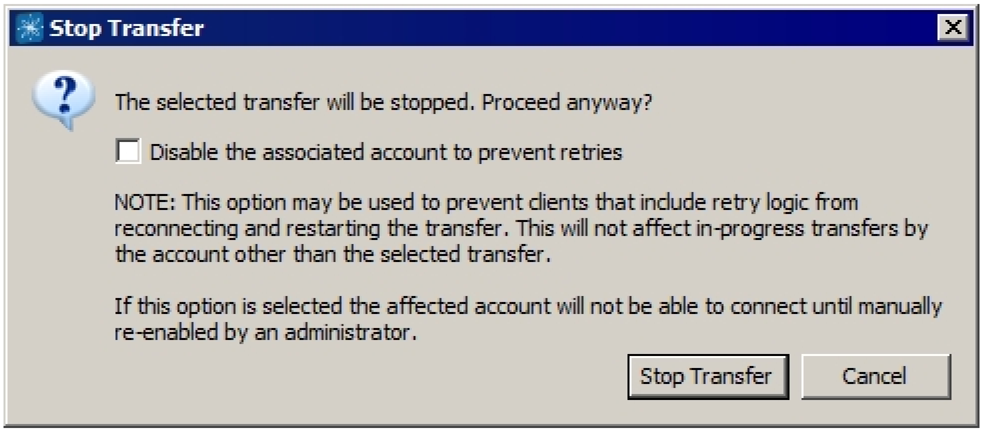
Ready | EFT Server started on Jun 29, 2011. 09:27:37 AM | Users connected: 0

Transfers appear at the top of the window. The Transfer list may not be up to date, depending on the size of transfer, network performance, and so on. Transfers that are small and quickly processed may not appear in the list or are quickly overwritten as others files are processed. If you click **Retrieve**, transfers stored in the database and in-progress transfers will appear in the list.

You can:

- Sort data by a column by clicking the column header.
- Filter results by typing characters in the **Filter** box. For example, display only transfers by a particular user or from a specific Remote IP address.
- Display or hide successful, failed, or in progress transfers by selecting or clearing the **Show successes**, **Show failures**, and **Show in progress** check boxes.

- Retrieve historical transactions by specifying the number of minutes (from 1 to 9999) in history that you want to retrieve, then clicking **Retrieve**. The maximum number of records that can be displayed is 10,000.
- Specify which columns to display or hide by right-clicking on the column header, and then clicking the column name to display or hide.
- Click the linked text (Success or Failure) to view the details of the transfer.
- Stop an in-progress transfer by clicking **Stop Transfer**. Stopping the transfer can free up bandwidth when large transfers are occurring and a higher priority transfer needs to get through. You can also select multiple transfers to stop them all at the same time.
  - The administrator Actions report includes transfers stopped by the administrator, as does other relevant file transfer activity reports.
  - Stopped client transfers will ***not*** retry automatically. Other connections from the user are unaffected.
  - Stopped outbound transfers are audited to the CL.log; stopped inbound transfers are audited to the EX.log.
  - When you click **Stop Transfer**, a prompt appears in which you can choose to disable the user account that initiated the transfer to prevent retries. If disabled, the account must be enabled by an administrator. (You will have to refresh the interface to see that the user is disabled.)



Stop Transfer

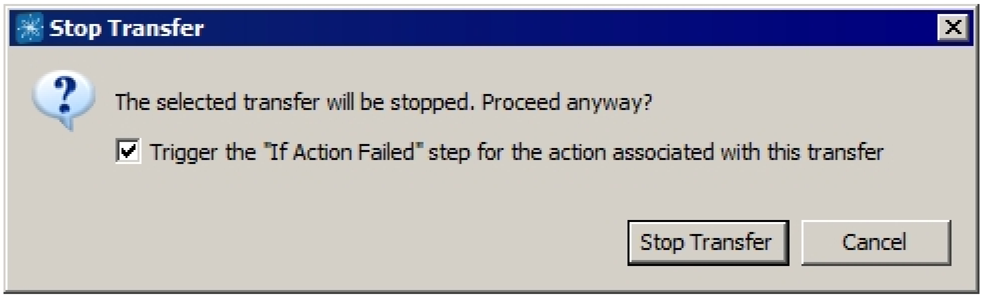
The selected transfer will be stopped. Proceed anyway?

□ Disable the associated account to prevent retries

NOTE: This option may be used to prevent clients that include retry logic from reconnecting and restarting the transfer. This will not affect in-progress transfers by the account other than the selected transfer.

If this option is selected the affected account will not be able to connect until manually re-enabled by an administrator.

- For client offload Event Rule actions (that is, Copy/Move file Actions), a prompt appears in which you can choose whether to consider the stopped transfer a failed transfer. If you do not want any "If Action Failed" Actions to occur when the transfer is stopped, clear the check box, and then click **Stop Transfer**.



Stop Transfer

The selected transfer will be stopped. Proceed anyway?

☑ Trigger the "If Action Failed" step for the action associated with this transfer

The available columns are listed in the table below.

Column	Description	Transfers as Server	Transfers as Client
Date/Time	Date and time of transfer in the format MM/DD HH:MM:SS AM/PM	x	x
Status	Success or Failed	x	x
Direction	Whether sending or receiving the file	x	x
Username	Username of account initiating the transfer	x	x
File Name	Filename of file being transferred	x	x
Remote IP	IP address of remote computer	x	x
Local IP	Server's IP address	x	n/a
Local Port	Server's port on which the file is transferred	x	n/a
Remote Port	Port of remote computer used for transfer	n/a	x
Protocol	Protocol over which the file is transferred	x	x
Path	Path on EFT to which file is transferred	x	n/a
Remote Path	Remote path of file being transferred	n/a	x
Local Path	Local path of file being transferred	n/a	x
Transferred	Size of file being transferred	x	x

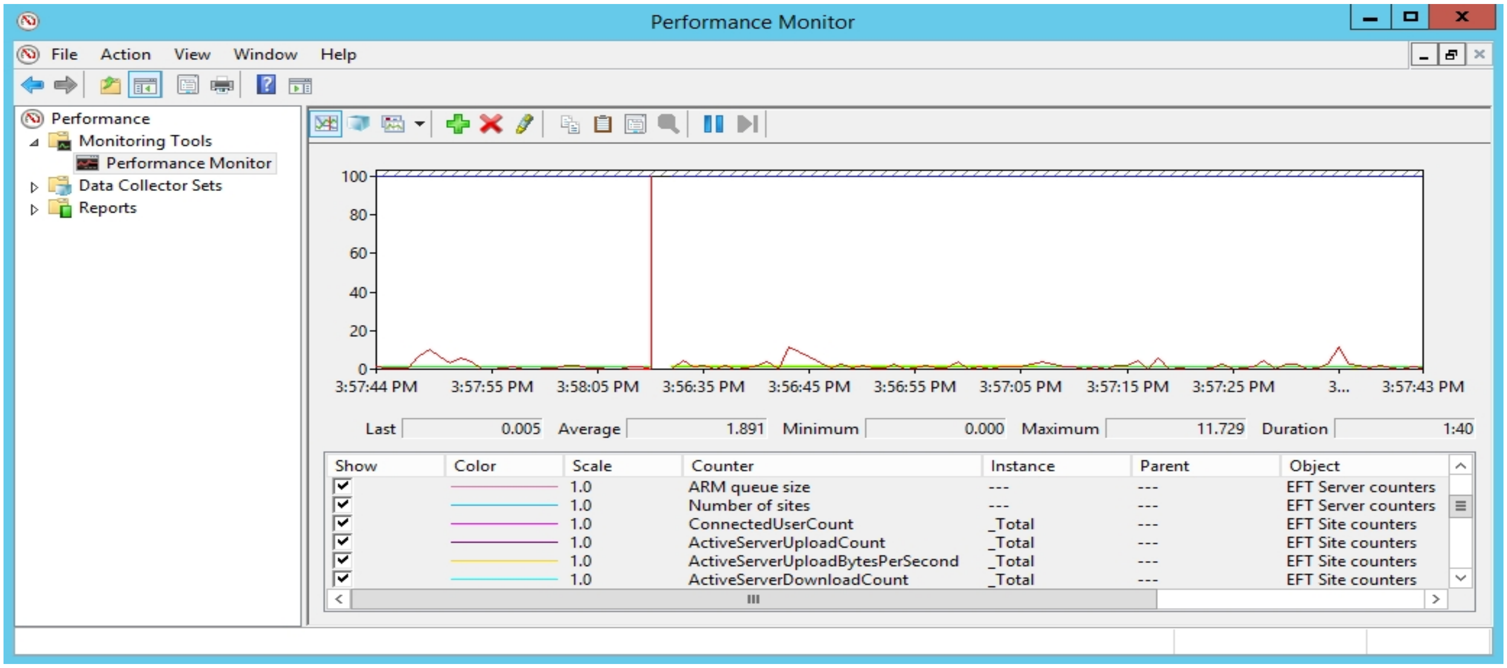
<table>
<tr><th>Column</th><th>Description</th><th>Transfers as Server</th><th>Transfers as Client</th></tr>
<tr><td>% Complete</td><td>Percentage of transfer completed; HTTP/S (both directions), and SFTP, FTP, and FTPS server downloads, and all client (outbound) transfers display % complete; SFTP, FTP, and FTPS inbound cannot display % complete.
<table>
<tr><td rowspan="2">Protocol</td><td colspan="2">EFT as server</td><td colspan="2">EFT as client
(that is, Event Rules)</td></tr>
<tr><td>Inbound (client push to server)</td><td>Outbound (client pull from server)</td><td>Outbound (EFT pushing to client)</td><td>Inbound (EFT pulling from client)</td></tr>
<tr><td>HTTP</td><td>%</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>HTTPS</td><td>%</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>FTP</td><td>n/a</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>FTPS</td><td>n/a</td><td>%</td><td>%</td><td>%</td></tr>
<tr><td>SFTP</td><td>n/a</td><td>n/a</td><td>%</td><td>%</td></tr>
</table>
</td><td>x</td><td>x</td></tr>
<tr><td>Rate</td><td>Rate, in kilobits per second (kbps), at which the file is transferred</td><td>x</td><td>x</td></tr>
<tr><td>Elapsed</td><td>Time in HH:MM:SS that it took to transfer the file</td><td>x</td><td>x</td></tr>
</table>

Performance Counters

EFT can publish a series of counters to Window's Performance Monitor (search Windows for *perfmon*). Counters are used to provide information as to how well a system is performing. This data can help administrators better understand crucial performance metrics and size the requirements of their EFT infrastructure as new requirements are placed on the system.

To view EFT counters

1. In the Windows **Search** box, type `perfmon`, and then click **Performance Monitor**.
2. In the navigation pane, expand **Monitoring Tools**, click **Performance Monitor**.
3. Click anywhere In the right pane, then click **Add Counters**.
4. In the **Add counters** dialog box, scroll through the alphabetized list to find EFT counters.
5. Click the counters, click **Add >>**, then click **OK**.
6. Clear or select the check boxes that you want to hide or show.



Last 0.005 Average 1.891 Minimum 0.000 Maximum 11.729 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object
☑	—	1.0	ARM queue size	---	---	EFT Server counters
☑	—	1.0	Number of sites	---	---	EFT Server counters
☑	—	1.0	ConnectedUserCount	_Total	---	EFT Site counters
☑	—	1.0	ActiveServerUploadCount	_Total	---	EFT Site counters
☑	—	1.0	ActiveServerUploadBytesPerSecond	_Total	---	EFT Site counters
☑	—	1.0	ActiveServerDownloadCount	_Total	---	EFT Site counters

Below is a description of each Counter:

Server-Level Counters	Counter	Description
	Admin Accounts	Number of administrator accounts defined for this server
	Admin Accounts Locked Out	Number of administrator accounts currently and temporarily locked out of the server
	Admin Sessions	Number of authenticated administrators with an active session
	ARM Queue Size	Size of audit queue. Values exceeding ten thousand may indicate problems with your database
	ARM Stalled Audit Events	Number of audit events delayed for longer than ARMLogStalledThreadministratorDuration (The duration is set to 1 second by default.)
Number of sites	Sites	Number of Sites currently defined for this server. Updated infrequently
	Sites Enabled	Number of Sites enabled
	Sites Started	Subset of defined Sites that are actively listening for connections. Updated infrequently

Server-Level Counters	Counter	Description
WorkspacesNormalLicensesUsed	Workspaces Licenses Assigned	Total number of Workspaces in use and not expired. Includes folder shares, file sends, and drop-offs
WorkspacesLicensesAvailable	Workspaces Licenses Available	Total number of Workspaces licenses available for use or assignment

Site-Level Counters	Counter	Description
Number of running event rules	Event Rules	Number of rules defined on the Site
	Event Rules Size of Async Events Queue	Size of asynchronous event queue. Values exceeding a few score should be looked at.
ActiveClientDownloadCount	Event Rules Client Downloads	Active downloads from a remote server originating from EFT as a client
ActiveClientDownloadBytesPerSecond	Event Rules Client Download Bytes /sec	Rate at which EFT-initiated downloads are occurring measured in bytes transferred
ActiveClientUploadCount	Event Rules Client Uploads	Active uploads to a remote server originating from EFT as a client
ActiveClientUploadBytesPerSecond	Event Rules Client Upload Bytes /sec	Rate at which EFT-initiated uploads are occurring measured in bytes transferred
	Event Rules Disabled	Event rules currently disabled. You can configure a script to alert you if this number exceeds a defined threshold
	Event Rules Running Async Events	Number of running asynchronous events. A high number could indicate a need for more nodes or improved rule logic
Number of running Advanced Workflow Actions	Event Rules Running Advanced Workflow Tasks	Number of running Advanced Workflow workflows. A high number could indicate a need for more nodes or improved workflow logic
Number of running Cloud Upload Actions	Event Rules Running Cloud Upload Actions	Number of event rule actions uploading to a cloud storage provider such as Azure or AWS

Site-Level Counters	Counter	Description
Number of running Cloud Download Actions	Event Rules Running Cloud Download Actions	Number of event rule actions download from a cloud storage provider such as Azure or AWS
Number of running Download Actions	Event Rules Running Download Actions	Number of event rule actions where the action is downloading a file from a remote host
Number of running Upload Actions	Event Rules Running Upload Actions	Number of event rule actions where the action is uploading a file to a remote host
	Event Rules Size of Async Events Queue	
Size of Advanced Workflow Actions queue	Event Rules Size of Advanced Workflow Actions Queue	Size of Advanced Workflow queue. Values exceeding a few score should be looked at
	Event Rules Triggered	Number of event rules currently active. A high number could indicate a need for more nodes or improved rule logic
	Folder Monitor Worker Threads	
	Socket Connection /sec	
	Templates	Number of Templates defined for this Site. Updated infrequently. (Note that the is a "hidden" template for Remote Agents.)
	Timer Rule Worker Threads	
Number of clients	User Accounts	Number of User accounts defined for this Site. Updated infrequently.
	User Accounts Disabled	Subset of this Site's User accounts that are currently in a disabled state. Updated infrequently.

Site-Level Counters	Counter	Description
	User Accounts Locked Out	Subset of this Site's User accounts that are currently locked out. Updated infrequently.
ActiveServerDownloadCount	User Downloads	Active downloads from EFT originating from remote clients. Juxtapose with CPU, disk, network, and similar metrics to assess performance impact
ActiveServerDownloadBytesPerSecond	User Downloads Bytes /sec	Rate at which downloads are occurring by connected clients measured in bytes transferred
	User Login Failed Bad Password /sec	Rate at which user are failing to authenticate due to a valid username but invalid password being provided. There are mitigation techniques you can use if frequent attacks on root or administrator
	User Login Failed Non-existent Username /sec	Rate at which user are failing to authenticate due to an invalid or non-existent username being provided.
	User Login Success /sec	Rate at which users are authenticating successfully and turn into an active session. See User Sessions for count of actively connected users.
ConnectedUserCount	User Sessions	Number of authenticated users with an active session. Does not count stateless HTTP/S connections
ActiveServerUploadCount	User Uploads	Active uploads to EFT originating from remote clients. Juxtapose with CPU, disk, network, and similar metrics to assess performance impact
ActiveServerUploadBytesPerSecond	User Upload Bytes /sec	Rate at which uploads are occurring by connected clients measured in bytes transferred
WorkspacesDropoffLicensesUsed	Workspaces Drop-offs	Number of drop-off requests active and not expired
	Workspaces File Sends	Number of file send operations that are active and have not yet expired
	Workspaces Folders Shared	Number of folder shares that are active and have not yet expired

See also Measuring EFT Performance with Perfmon.

For information about using Performance Monitor, refer to Windows Performance Monitor Overview on the Microsoft Tech Community website.