# AUTOMATING FILE TRANSFERS WITH EVENT RULES

EFT SERVER V6.5

**GlobalSCAPE, Inc. (GSB)**

| | |
|---|---|
| **Address:** | 4500 Lockhill-Selma Road, Suite 150<br>San Antonio, TX (USA) 78249 |
| **Sales:** | (210) 308-8267 |
| **Sales (Toll Free):** | (800) 290-5054 |
| **Technical Support:** | (210) 366-3993 |

Web Support: http://www.globalscape.com/support/



*Last updated: February 1, 2013*

# Table of Contents

# Introduction to Event Rules

Event Rules are based on a simple premise: an event occurs that triggers an action. In the EFT Server administration interface or with the COM API, you can specify *Actions* to occur when an *Event* takes place. You can also specify one or more *Conditions* that must exist before an Action is taken or that change the Action that is taken.

For example, suppose you have a folder into which remote partners can drop files. In EFT Server Enterprise, you can set up an Event Rule that monitors that folder, and when someone puts a file into that folder, EFT Server can encrypt that file, move it into another folder, and then send e-mails to anyone you specify informing them that a file has been moved. You can also set up a Rule that only moves certain files. For example, you can configure the Rule to move only the files with "Important" in the name, or you can route certain files to different folders.

*Two administrators can work on Event Rules at the same time, but if they are working on the same Rule at the same time, when one administrator saves a Rule, the other administrator will get a notice when he clicks **Apply**, saying that the changes could not be saved because changes have been made by someone else. The second administrator will have to refresh to see the other changes, and then make any changes to the Rule again.*

## Sample Logic

You can easily create complex programmatic Event Rules in EFT Server's administration interface. The Event Rule system contains objects that you click to add to the *Rule Builder*, and then you click within the Rule to modify parameters and add variables. Below are some examples of logic you can create (in pseudo code).

("ON FILE UPLOAD" is the Event triggers, the "if" statements are Conditions, and "PGP," "UNZIP," "MOVE," and "SEND NOTIFICATION" are the resulting Event Rule Actions.)

Always run an Action if an Event occurs:

```
ON FILE UPLOAD
{
      PGP Encrypt %FS.PATH%
}
```

Conditionally run an Action if an Event occurs (IF-THEN statement):

```
ON FILE UPLOAD
{
    if ( %FS.FILE_NAME% = "*.pgp" )
   {
      PGP Decrypt %FS.PATH%
   }
}
```

Multiple IF-THEN statements (if something, do this; if something else, do that):

```
ON FILE UPLOAD
{
   if ( %FS.FILE_NAME% = "*.pgp" )
   {
      PGP Decrypt %FS.PATH%
   }
   if ( %FS.FILE_NAME% = "*.zip" )
   {
      UNZIP %FS.PATH% to "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
   }
}
```

Else statements (if preceding Condition is not met, do something):

```
ON FILE UPLOAD
{
   if ( %FS.FILE_NAME% = "*.pgp" )
   {
      PGP Decrypt %FS.PATH%
   }
   if ( %FS.FILE_NAME% = "*.zip" )
   {
      UNZIP %FS.PATH% to "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
   }
   else
   {
      MOVE %FS.PATH% to "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
   }
}
```

Run always Action (Action that will always run when the Event occurs even if preceding IF-THEN-ELSE statements are true):

```
ON FILE UPLOAD
{
   if ( %FS.FILE_NAME% = "*.pgp" )
   {
      PGP Decrypt %FS.PATH%
   }
   else
   {
      MOVE %FS.PATH% to "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
   }
  MOVE "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\*.*" to
https://somehost/%USER.LOGON%/
  SEND NOTIFICATION e-mail TO %user.email%
}
```

Run the same Action more than once:

```
ON FILE UPLOAD
{
   SEND NOTIFICATION e-mail TO serveradmin@globalscape.com
   SEND NOTIFICATION e-mail TO %user.email%
}
```

Create *compound* conditional statements supporting AND and OR logical operators:

```
ON FILE UPLOAD
{
    if ( %FS.FILE_NAME% = "*.pgp" ) || ( %FS.FILE_NAME% = "*.encrypted" )
   {
      PGP Decrypt %FS.PATH%
   }
   else
   {
      MOVE %FS.PATH% to "%FS.PATH%\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%\"
   }
  SEND NOTIFICATION e-mail TO %user.email%
}
```

*It is possible to configure Event Rules that create infinitely recursive cycles. Because all Event Rules operate synchronously, a file upload Event cannot be completed until all corresponding Event Actions are finished. This could lead to unpredictable server behavior due to conflicts with shared access to the same files or deleting open files. Be careful not to create circumstances where such recursive cycles might occur. For file upload Events, recursive cycles are not typical. It is recommended that you move files on the same server using the file*

*system - not FTP.*

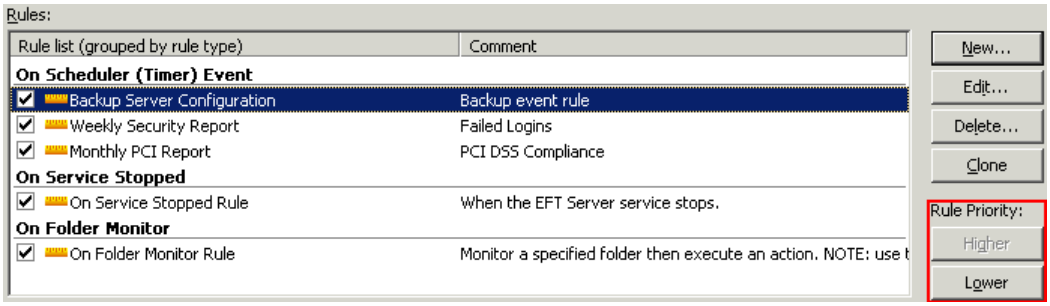
# Event Rule Order of Execution

Almost all of EFT Server's Event Rule Actions are executed *synchronously (execute 1, wait until it finishes, execute 2, wait until 2 finishes, execute 3 … etc.)*, because there may be more Actions that follow that depend on the prior Action completing successfully. Each Action is completed before continuing to the next, with a few exceptions, which are described below (Timer Rules, Folder Monitor Rules, and Rules that use the Execute Command Action or AWE Action).

If you create more than one Event Rule for a single type of event (e.g., Monitor Folder), EFT Server prioritizes the Rules in the order they appear on the **Rule list**. You change the priority by moving a selected Rule up or down in the **Rule list**. The **Rule list** is grouped by Rule type. You can only prioritize the Rules within a Rule type. For example, you cannot move an **On Folder Monitor** Rule above an **On Scheduler (Timer) Event** Rule, but you can prioritize the Rules within the Rule type (e.g., place one Timer Event to occur before another Timer Event).

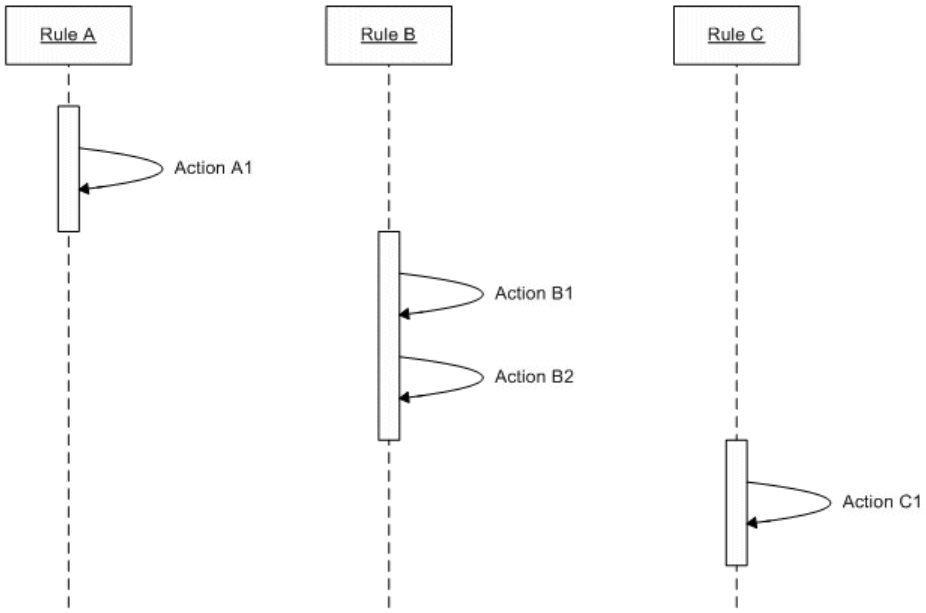
**To change the priority of a Rule**

1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, click the Site you want to configure, and then click **Event Rules**. The **Rule list** appears in the right pane.
3. In the right pane, select the Event Rule you want to move.
4. To reorder the Event Rules, under **Rule Priority**, click **Higher** and **Lower**.



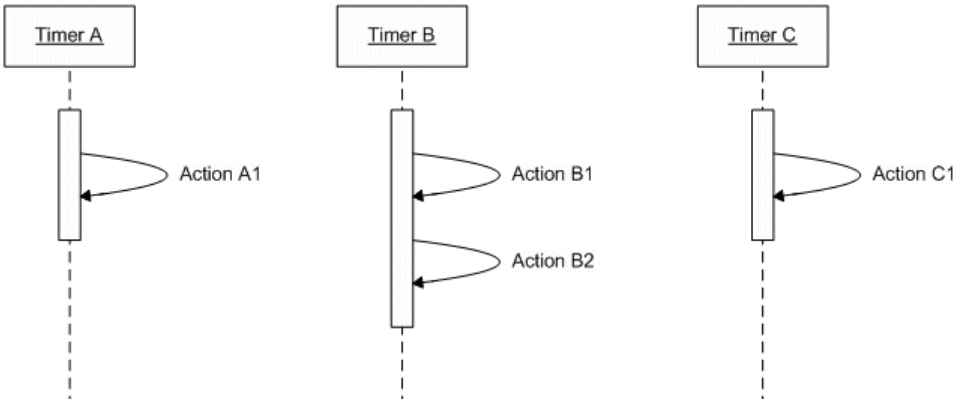
## Event Rule Sequence for Matching Event Rules

One or more Event Rules may be triggered when Conditions are met. For Event Rules with duplicate Event trigger definitions and Conditions, but with different Actions, the order of execution is sequential according to the sort order defined in the interface.



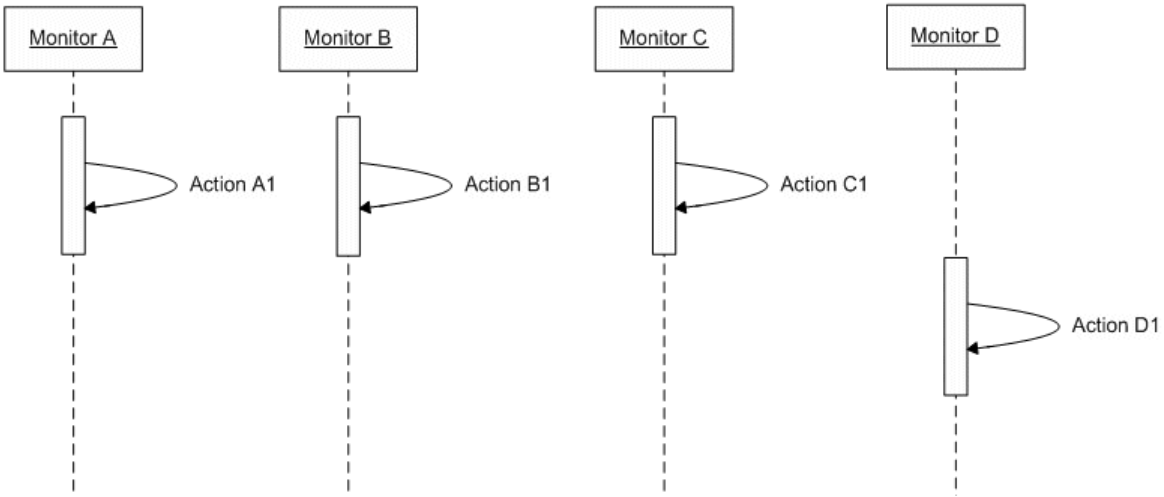

## Event Rule Sequence for Matching Timer or Folder Monitor Rules

This sequential firing of duplicate Event Rules applies to almost all of EFT Server's supported Events. However, the **Monitor Folder** and **Timer** Event Rules are executed asynchronously (i.e., not at the same time). When you stop the Site or the Server service, EFT Server breaks all existing connections and waits until all socket threads die. The service can terminate when **Timer** Event processing is still in progress. The triggering of **Monitor Folder** and **Timer** Event Rules occurs almost simultaneously and is controlled by the operating system, not by EFT Server.



## Event Rule Sequence for Matching Folder Monitor Rules

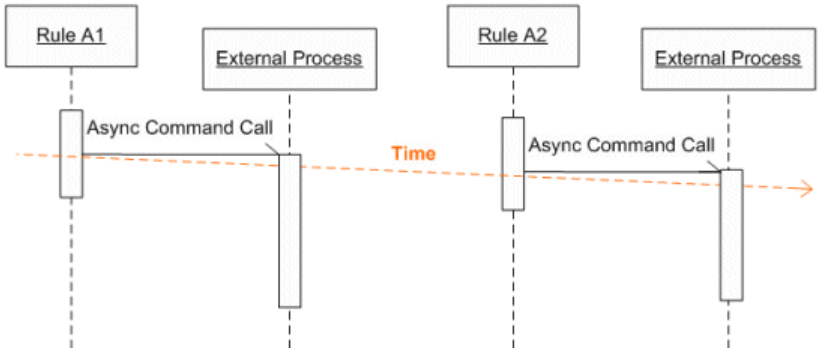
As mentioned above, matching **Timer** and **Monitor Folder** Events are not executed at the same time. However, **Monitor Folder** "threads" are limited to 3 concurrent threads by default. This means that if you have 5 **Monitor Folder** Event Rules monitoring the same folder and a file is added to the monitored folder, only 3 of the 5 Rules will fire, as determined by the operating system. The 4th and then 5th Rule execute only when one or more of those 3 threads are done firing and executing any Actions.




## Order in which Actions are Executed

EFT Server executes Event Rules according to whatever synchronicity applies to that Event Rule. For example:

- Triggering an **Execute Command** Action is asynchronous, unless the "If Failed" sequence has an Action defined for that command.
- Move, copy, and download operations are synchronous.
- PGP operations are synchronous and cause the Event dispatcher to wait until the operation is finished before moving on to the next Action/Condition.
- E-mail notifications are synchronous up to the point of generating the contents of the e-mail and putting the data into a queue. However, EFT Server has a separate thread that manages the e-mail notification queue to pick up ready messages and send them to the destination server. Therefore, e-mail notifications are roughly asynchronous.



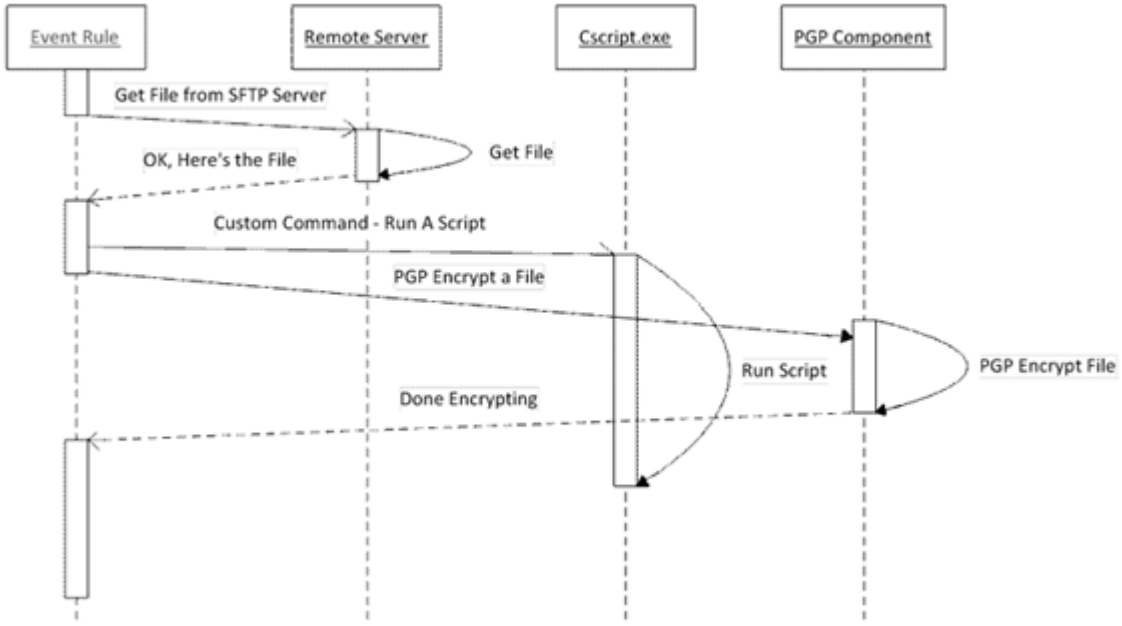
**Execute Command** Actions and **Execute Advanced Workflow** Actions execute asynchronously, which means that EFT Server does not wait for a reply before returning control to the Event Rule thread, *unless* an "if failed" Condition is specified, such as **Stop Processing this Rule**. If an "if failed" Condition is specified, regardless of whether the Command succeeded or failed, the Event Rule processor waits for a return message from the invoked process before moving on to the next Rule.

## Example: Command Action Followed by OpenPGP Action

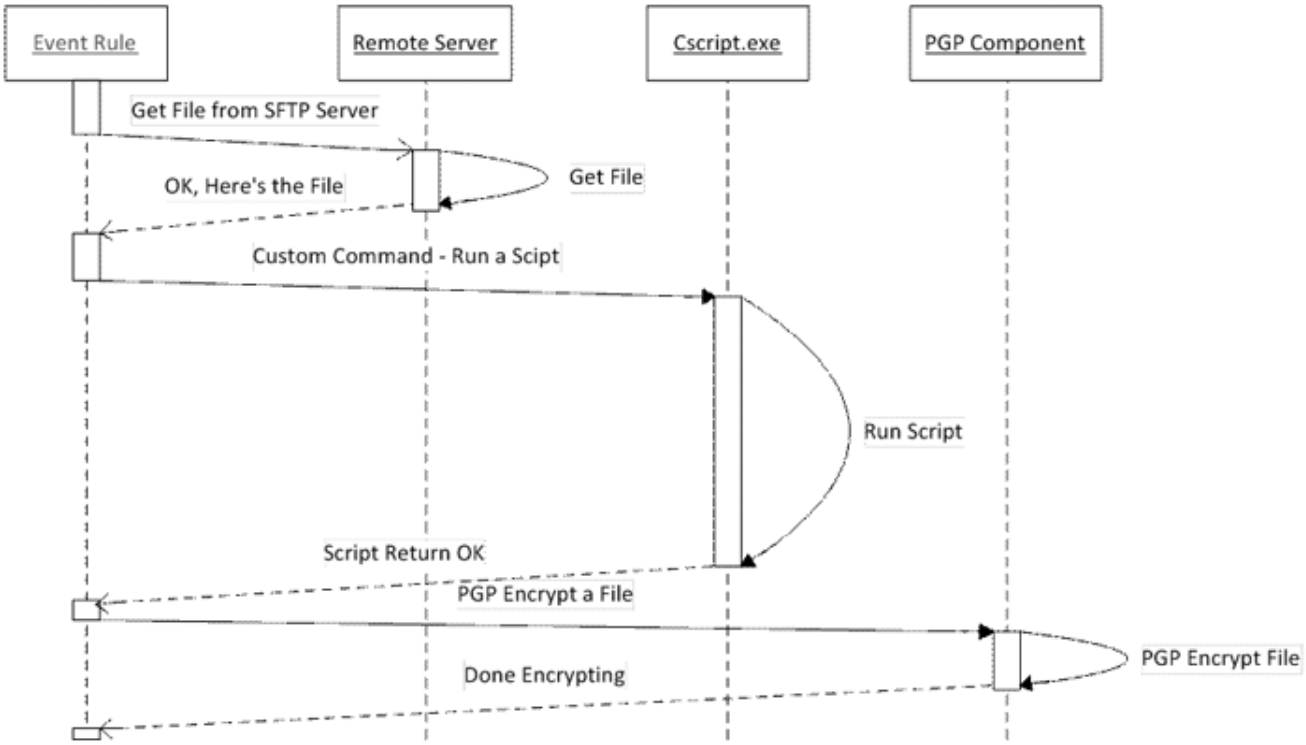
A common Event Rule scenario is downloading a file, running a script against that file (either with an **Execute Command** or an **Execute Advanced Workflow** Action), then encrypting or decrypting the file.

In the illustrations below, an Event Rule has three Actions: first an SFTP get (download a file from the Remote Server), followed by an **Execute Command** Action that runs a script (cscript.exe), followed by a PGP Action.

In Example 1, an "If failed" Condition was not defined for the Command, so when the Command executes, the next Action (OpenPGP) is called almost immediately after the script is called. If you are doing a transform on the file you just retrieved that must be completed PRIOR to the PGP operation, the potential risk is that there will be a race condition and likely PGP will lose; that is, the pre-transformed file will be PGPed or the Action will fail because the script has locked the file for some reason.




In Example 2 we've added the "If failed" Condition so that the **OpenPGP** Action does not start until after the Command has finished running the script.



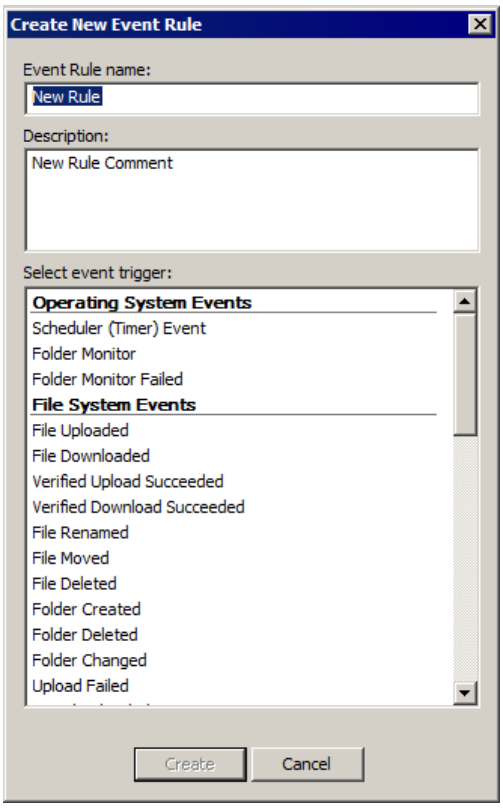

# Defining Event Rules

To define Event Rules in the administration interface, you begin with an Event you want to use as a trigger for the Event Rule. The Event could be when someone uploads a file, when a user quota is exceeded, when a change is detected in a folder, or many other Event triggers. Then you specify an Action to be taken when the Event occurs. The Action could be sending an e-mail to someone, encrypting a file, moving a file, or all three together. Optionally, you can then define Conditions that must be met for the Action to be taken. You can even branch the Actions and define one Action to be taken if specified criteria are met. You do this using standard *If>Else* logic.

**To define an Event Rule**

1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. Do one of the following:
    - Right-click in the left pane, and then click **New Event Rule**.
    - In the left pane, expand the Site you want to configure, and then click **Event Rules**. In the right pane, click **New**.
    - On the main menu, click **Configuration > New Event Rule**.

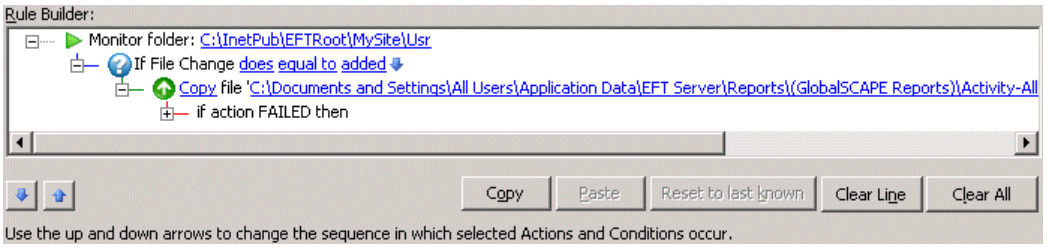
    The **Create New Event Rule** dialog box appears.



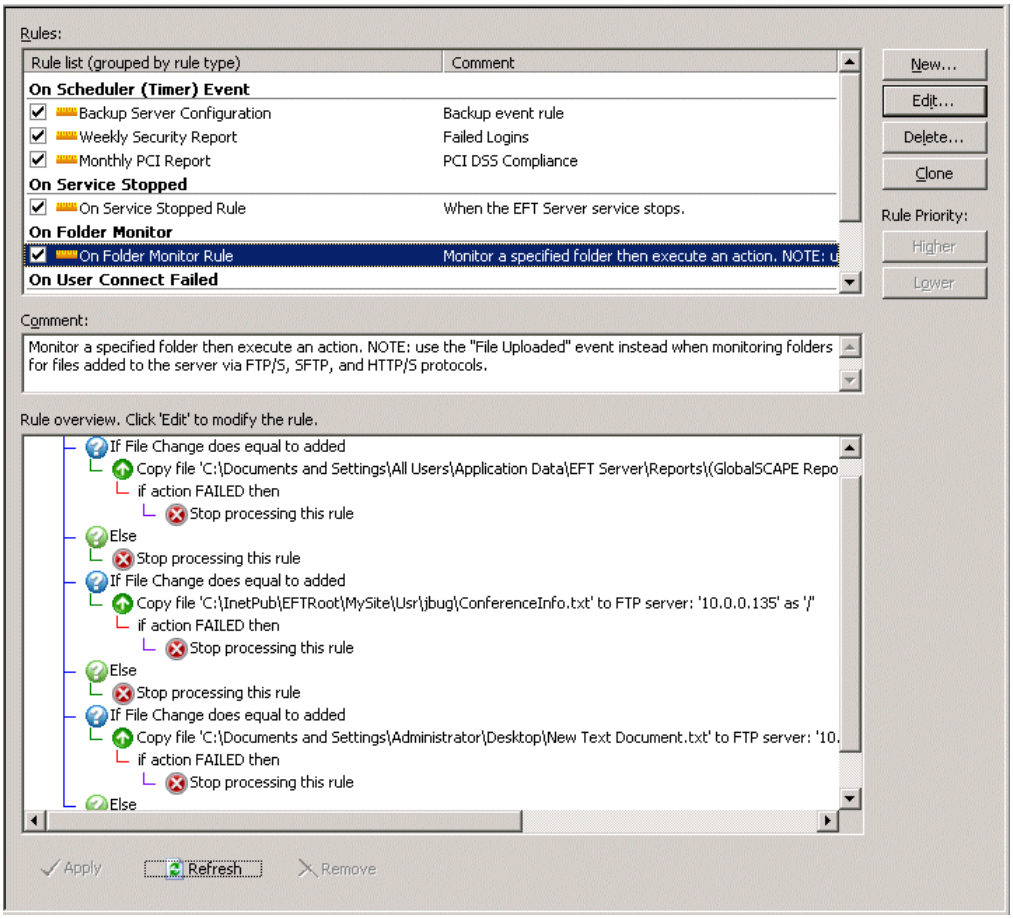

3. In the **Event Rule name** box, type a descriptive name for the Rule. This name will appear in the Event Rules node and in reports and logs. Therefore, name it something you will recognize, rather than something generic such as "Rule #24."
4. In the **Description** box, provide any notes about the Rule, such as "Periodically move and delete accounting files." You can edit these notes later in the **Comment** area for the Rule, if necessary.
5. In the **Select event trigger** box, click the Event you want to use as the basis of the Event Rule, such as **Folder Monitor**. For a description of the available Event triggers, refer to Events and Available Variables.
6. Click **Create**. The **Create Event New Rule** dialog box closes and the Conditions and Actions available for the Event Rule are displayed.
7. Conditions are optional. Available Conditions for the specified Event trigger appear in the **Conditions** list. When applicable to the Event Rule, the **Else** option also appears. To add a Condition to the Rule, double-click the Condition, or click to select it, and then click **Add Condition**.

   Not all Conditions that EFT Server supports are available for every Event. To learn more about available Conditions, refer to Event Rule Conditions.
8. Available Actions for the specified Event trigger display in the **Actions** list. To add an Action to the Rule, double-click it or click the Action, and then click **Add Action**. To learn more about Actions, refer to Event Rule Actions.

   As you add Conditions and Actions, they appear in the **Rule Builder**.




9. In the **Rule Builder**, click the underlined text to specify the parameters used in the definition of the Event Rule. You can also reorder the sequence of the Rule logic using the blue up and down arrows, or by clicking the Action or Condition and dragging it to the new location.
10. Click **Apply** to save the changes on EFT Server. EFT Server will not save the Rule unless it is adequately defined. Links displayed in the Rule box are parameters that must be defined before you can save and apply the Rule.
11. After the Rule is defined, click the Event Rules node in the Server tree in the left pane. In the right pane, each of the Rules defined on the Site appear.




12. In the right pane, in the **Rule List**, click a Rule. **Comments** for the Rule appear beneath the **Rule List** in the **Comment** box and the definition of the Rule (the Conditions and Actions defined) appears in the **Rule overview** box.
    - To edit the notes in the Comment box, click in the box and type or paste the changes.
    - To manage the Rules (edit, delete, clone, reorder), click the controls on the right. Refer to Managing Event Rules for details.

13. To delete a Rule, click to select it in the Event Rules node, and then click **Remove** at the bottom of the right pane or on the toolbar. A confirmation message appears. Click **Yes** to confirm or click **No** or **Cancel** to not delete the Rule.

# Managing Event Rules

When you click the Event Rules node for a Site, the right pane provides controls for managing the Event Rules defined for that Site. Using this interface, you can do the following:

Edit - You can fine tune your Rules by adding, editing, deleting, and rearranging Conditions and Actions.

Delete - If an Event Rule is no longer needed and you are sure you will not need it again in the future, you can delete it. However, you can also disable the Rule so that, if you need the Rule again, you can simply enable it.

Clone - You can create a copy of Rule and modify it to your needs. You can then rename the Rule.

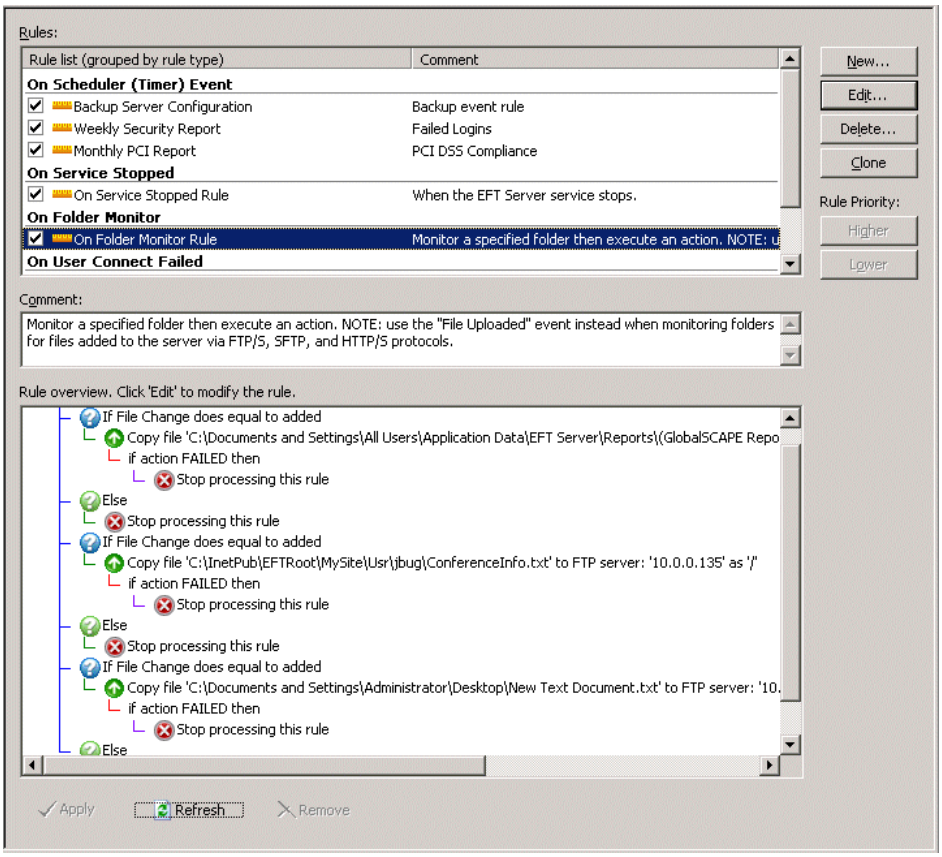
Prioritize - If you create more than one Rule for a single type of Event, EFT Server prioritizes the Rules in the order they appear on the Event Rules list. You can rearrange them using the **Rule Priority** buttons.

Disable - If you want to disable a Rule temporarily without deleting it, you can disable it by clearing the **Enable this rule** check box.

Rename - You can rename an Event Rule.

**To manage the Event Rules**

1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, click the Site you want to configure, and then click **Event Rules**. The list of configured Event Rules appears in the **Event Rules** node and in the right pane in the **Rule list**.



3. Click the Event Rule you want to change, and then click **Edit**, **Delete**, or **Clone**. The right pane updates to display the details specific to that Event Rule.

*Event triggers are indicated by a green triangle icon .*
*Conditions are indicated by a blue question mark icon .*
*Else Conditions are indicated by a green question mark icon .*
*Actions are indicated by their associated icons.*

**To edit an Event Rule**

1. To add a Condition to a Rule, click a Condition from the **Conditions** list then click **Add condition**. The Condition appears in the **Rule** pane below the current highlighted insertion point. You can add multiple Conditions to a single line and create AND/OR criteria.
2. To add an Action to a selected Condition, click it in the **Actions** list, and then click **Add action**. The Action appears in the **Rule** pane below the highlighted Condition.
3. Configure the Condition or Action by clicking the underlined variables (red or blue underlined text)
4. You can reorder Conditions and Actions by dragging them where you want them and using the up and down arrows.
5. Click **Apply** to save the changes on EFT Server.

**To delete an Event Rule**

1. In the right pane, click **Delete**. A confirmation message appears.
2. Click **Yes**. The Rule is deleted from the Site.

**To clone an Event Rule**

1. In the right pane, click **Clone**. A clone of the Rule opens in the Event Rule editing pane and is added to the **Rules** list.
2. Edit the copy of the Rule as needed, and then click **Apply** to save the changes on EFT Server. Your new Rule appears in the Event Rules node with "Copy" appended to the name.
3. To rename the Rule, in the left pane, right-click the Rule, and then click **Rename**.

**To change the priority of a Rule**

1. In the right pane, click the Rule you want to move.
2. Under **Rule Priority**, click **Higher** and **Lower**.

Refer to Event Rule Order of Execution for details of changing the priority of a Rule.

**To disable an Event Rule**

1. In the right pane, clear the **Enable this rule** check box.
2. Click **Apply** to save the changes on EFT Server.

**To re-enable an Event Rule**

1. In the right pane, click the **Enable this rule** check box.
2. Click **Apply** to save the changes on EFT Server.

**To rename an Event Rule**

1. In the Event Rules node, do one of the following to make the name editable:
   - Right-click the Event Rule, and then click **Rename**.
   - Click the Event Rule, and then click it again. (Do not double-click it.)
2. Type the new name, and then press ENTER or click away from the name. The name is changed.

# Variables

EFT Server uses *context variables* to pull data from the database. The variable contains specific information about an Event. You can use the variables below in Event Rules, e-mail notifications, Commands, and Advanced Workflows.

- Scheduler (Timer) Rule Variables - Used for Scheduler (Timer) Rules (For file operation triggers, use File System Variables.)
- Connection Variables - IP address, port, etc. for connecting to EFT Server
- Event Variables - Name, date, time, reason, etc. for Event trigger
- File System Variables - File name, date, size, path, etc. that was transferred; also report name and content
- Server Variables - Server status, logs, and computer name
- Site Variables - Site URL and status
- User Variables - User name, login information, etc.
- AS2-Related Variables - Status of AS2 transfers (available only in AS2-related Event triggers)

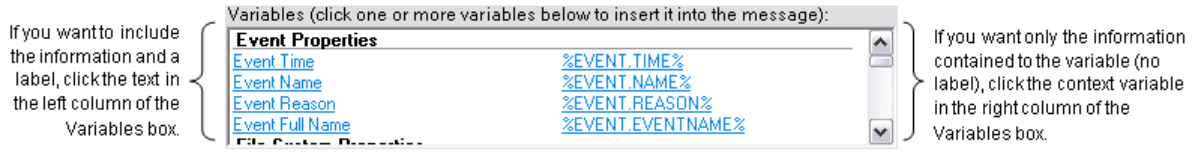
> *In the AWE module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, % CONNECTION.LOCAL_IP% is % CONNECTION_LOCAL_IP% in the AWE module.*

## How to Use the Variables

In the **Variables** box, click a property that you want to insert.

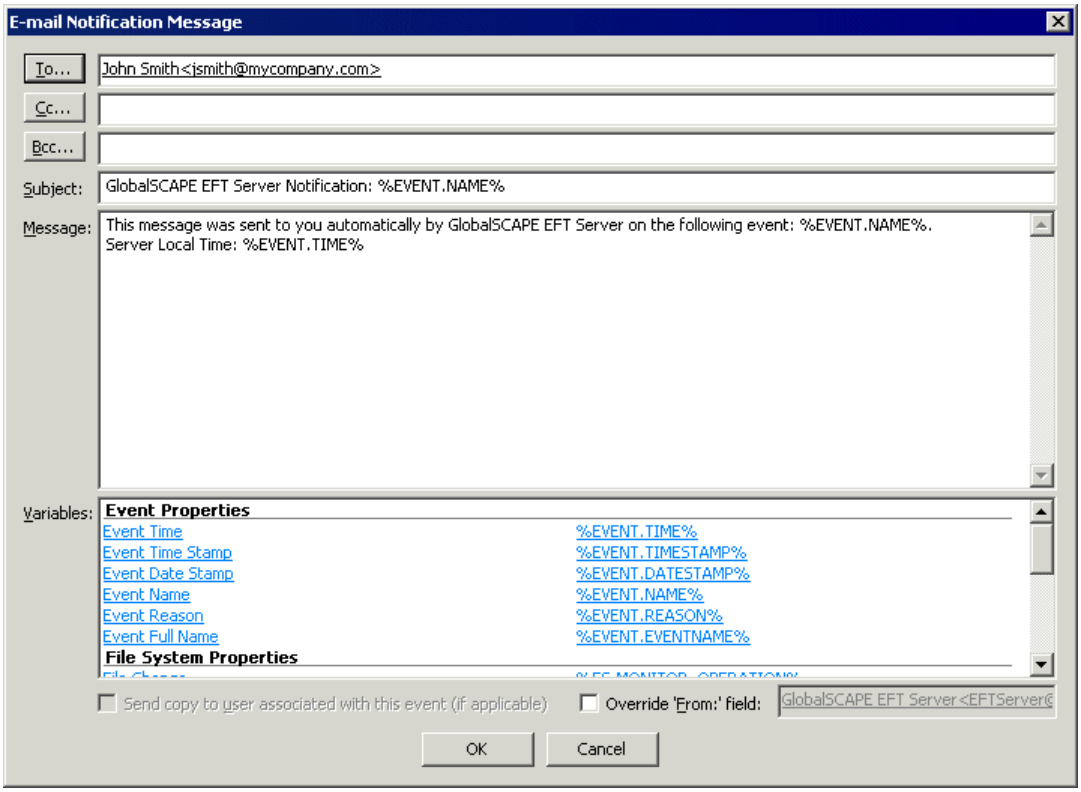
- If you just want the information contained to the variable, click the variable in the right column of the **Variables** box.
- If you want the information ***and*** a label, click the text in the left column of the **Variables** box.

For example, if you click Event Time in the left column the label "Event Time" and the time are displayed. If you select %EVENT.TIME% in the right column, the time will be displayed without a text label.




For example, when you create an Event Rule, you can configure an e-mail to be sent when the Event occurs. In the **Edit Mail Template** dialog box, you can send the default e-mail or you can add one or more variables listed in the **Variables** box at the bottom of the e-mail. Each of the variables defined in EFT Server is described in the Appendix; however, not all of the variables are available in the e-mail notification. In the e-mail notification, you can specify to display the text along with the value of the variable (e.g., File Creation Date: 8/28/2007), or just the value of the variable (e.g., 8/28/2007).

Suppose you configured this e-mail notification:




You then uploaded a file on August 28, 2007 at 10:01:56. The e-mail would appear similar to the following:

```
This message was sent to you automatically by EFT Server on the
following Event: File Uploaded.

Event Time: 28 Aug 07 10:01:56

File Creation Date: 8/28/2007

File Creation Time: 10:01:56

Event Date Stamp: 20070828

Event Time Stamp: 100156
```

*In Event Rules and Commands with a defined path or filename, do not use variables that add invalid filename characters, such as a slash, colon, parenthesis, etc.*
*For example, you cannot use %FS.FILE_CREATE_DATE% and %FS.FILE_CREATE_TIME% for file naming, because the output of these variables is DD/MM/YYYY and HH:MM:SS and the forward slash (/) and colon (:) are not valid characters for filenames. In most cases, the file created date and time is the same as the Event triggered time, therefore you can use %EVENT.DATESTAMP% (YYYYMMDD) and %EVENT.TIMESTAMP% (HHMMSS) when renaming files (because they do not use invalid characters), and %FS.FILE_CREATE_DATE% and %FS.FILE_CREATE_TIME% for e-mail notifications. For example, suppose an OnUpload Event Rule causes an Offload Action that moves myfile.txt to the following path:*
*C:/Inetpub/EFTRoot/Site1/Usr/jsmith/%EVENT.DATESTAMP%_%FS.FILE_NAME%*
*The resulting path is:*
*C:/Inetpub/EFTRoot/Site1/Usr/jsmith/20070728_myfile.txt*

# Events and Available Variables

EFT Server includes over 25 different Event triggers, based on the following Event types:

- AS2-related Events, such as the transfer was successfully completed (available only in EFT Server Enterprise)
- Connection-related Events, such as a user connections failed
- File system-related Events, such as file uploaded or file deleted.
- Operating System-related Events, such as a folder's contents changed or a recurring Timer has executed (available only in EFT Server Enterprise)
- Server-related Events, such as Server stopped or started
- Site-related Events, such as Site stopped or started
- User-related Events, such as User Account Locked

*Operating System Events and AS2-related Events are available only in EFT Server Enterprise. These Events are visible, but unavailable (grayed out) in EFT Server SMB edition.*

Not all variables are available with every Event trigger. For example, it does not make sense to use the %EVENT.REASON% variable with the **File Downloaded** Event, but it does make sense with the **Upload Failed** Event, because EFT Server can determine the reason for the failure.

Each of the Events and the variables that you can use with them are listed in the Appendix. Refer to Variables for a description of each variable and caveats (e.g., %EVENT.TIME% is not suitable for file naming and %FS.REPORT_FILE% should not be used in e-mail notifications).

# Event Rule Triggers and Examples

The topics in this section provide examples of some common uses of Event Rules.

## Scheduler (Timer) Event

**(Available in EFT Server Enterprise)** The **Scheduler (Timer) Event** allows you to execute a specified Action (e.g. send an e-mail or a report) only one time or to recur at specified intervals. For example, you could schedule the Cleanup in folder Action to occur on July 8 at midnight, or every Monday morning, or on the last Friday of every month at 2 a.m.

The PCI DSS requires that you develop a data retention and disposal policy. With the Cleanup in folder Action, you can configure EFT Server to clean up a specified folder at regularly scheduled intervals. If **Strict security settings for compliance with PCI DSS** was selected during Site setup, the **Data Retention and Disposal** dialog box appears in which you can create a **Scheduler Timer Event** with the **Cleanup in folder Action** to delete files matching the expressions you specify. You can also choose to define it in the administration interface on existing Sites.

A recurring Timer does not stop recurring if the Rule Actions fail; it will recur as scheduled until you disable or delete the Rule. For example, suppose you want to download a file from a remote server, delete the file from the remote location after transfer, and then send yourself an e-mail. If the file that you want to download is not yet in the remote directory, the Rule will fail for that particular instance of the Timer running, but it will run again at the next scheduled time (e.g., every four hours). In the case of Timer Rules, "Stop processing this rule" means "do not execute any further Actions with this Rule" (such as sending an e-mail), but it does NOT mean that the Timer will stop. For example, if you have defined the Rule to run every hour, the Timer Rule will fail when the file is not in the remote location, but the Timer Rule will run again the next hour, and the next hour, and so on, until you tell it to stop (by manually disabling it).

**To define a Timer Rule to download a remote file**

1. Follow the procedure in Creating Event Rules.
2. In the **Create New Rule** dialog box, click **Scheduler (Timer) Event**, and then click **OK**. The new Rule appears in the **Rule Builder**.
3. To specify the start date, start time, recurrence pattern, and/or interval, in the **Rule Builder**, click the link.
4. In the **Scheduler** dialog box, specify the parameters of the Timer Event: the **Run** frequency, whether to exclude holidays, when the Event should start, date the Event should end (optional), time the Event should end (optional), and recurrence frequency (optional). (When the End date is reached, the Rule will remain active in the Event Rule list, but will no longer execute any Actions.)
    - **Once**—The Event runs one time at a specified date and time, and never repeats. (e.g., Monday, September 27, 2010 at 8 AM)
    - **Continually**—The Event starts at a specified date and time and repeats every <n> **Hours**, **Minutes**, or **Seconds**. (e.g., Monday, September 27, 2010 at 8 AM and every hour thereafter)
    - **Daily**—The Event runs every <n> days or every weekday, starting at a specified date and time, and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the Event at a specified date and time. (e.g., Every weekday, excluding US holidays, starting Thursday, Monday, September 27, 2010 at 8 AM and every hour thereafter)
    - **Weekly**—The Event runs every <n> weeks on a specified day(s) of the week, starting at a specified date and time and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the Event at a specified date and time. (e.g., Every 2 weeks on Monday at 8 AM starting on Monday, September 27, 2010, with no defined end date)
    - **Monthly**—The Event runs on the <n> day of every <n> month(s) or the <nth> day of the week of <n> month(s) starting at a specified date and time and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the Event at a specified date and time. (e.g., The first day of every month, starting on Friday, October 1, 2010 at 8:00:00 AM, excluding US holidays with no defined end date)
    - **Yearly**—The Event runs every <month> <day> or on the <n> <day of the week> of <month> starting at a specified date and time and ending on a specified date and time or repeating every <n> hours, minutes, or seconds. You can also exclude certain holidays and/or end the recurrence of the Event at a specified date and time. (e.g., The first Monday of December, starting on Monday, December 6, 2012 at 8:00:00 AM, excluding US holidays with no defined end date)
    - **Custom**—The **Run Day Calendar** appears in which you can specify a date. (Past dates are dimmed and not selectable.)
        - Click to select the date(s) to run the Event. Selected dates are highlighted in green. Click the date again to clear it.
        - Click the right arrow to advance the calendar to the next year (up to 2037); click the left arrow to go back. Or click the name of a month to display the same month in subsequent years. With the month name selected, move the cursor up or down to scroll through the years, and then release the cursor to select the year. (For example, click October 2010 to jump to October 2012. The entire calendar jumps, not just the selected month.)

- The **Propagate selected date(s) to all subsequent years** check box is selected by default. Clear the check box if you do not want the Event to run on the same date every year.
- After you select one or more dates to run the Event, you can save the schedule by clicking **Save**. In the **Save Calendar** box that appears, provide a name for the calendar, and then click **OK**. The calendar is saved and its name appears in the **Run** box. You can edit your custom calendar by click the ellipsis button next to the **Run** dialog box. (Up to 100 custom calendars can be saved and/or displayed in the **Run** box.)
- You can **Export** your custom calendar (as <name>.csv) and **Import** custom calendars. After importing a custom calendar, you can use **Save As** to save it with a new name, **Rename** it, or **Delete** it from your custom calendars. (A confirmation prompt appears when you click **Delete**.)
- You can create up to 100 custom calendars.

5. Click **OK** to save your changes. The Timer Event is updated in the **Rule Builder**.
6. Specify the Action to occur when this Event is triggered.
7. Click **Run Now** to test your Rule.

> *When you create a Timer Rule, the **Run Now** button appears at the bottom of the **Rule Builder**. When you click **Run Now**, EFT Server executes any actions associated with the Event, and any Rule construction errors are identified. You cannot perform any other operations in the EFT Server administration interface while EFT Server tests the Rule. Multiple synchronous Actions defined in the Rule, such as move, copy, or download, take longer to test than asynchronous operations such as e-mail notifications.*

8. If there are no errors, a confirmation message appears asking you to verify the expected outcome. Click **Continue** to execute the Rule or **Cancel** to refine the Rule.
9. Click **Apply** to save the changes on EFT Server.

## Monitoring Folders

**(Available in EFT Server Enterprise)** EFT Server's **Folder Monitor** Event Rule trigger is used to detect the creation, deletion, and renaming of files in a monitored folder and to perform Actions based on these triggers. You can use a **Folder Monitor Rule** to trigger when files are added to a folder using the network file system. When monitoring folders for files added to EFT Server via the FTP/S and HTTP/S protocols, use File Uploaded, File Downloaded, and other File System Events. **Folder Monitor** Rules are not fired for Events happening to folders, such as the addition, renaming, or removal of a folder; it only applies to file changes within the folder or subfolders.

The **Folder Monitor** Rule can pass Unicode filenames to the Event Rule system, including the Advanced Workflow Engine, Custom Commands, text-based log files, and ARM. The Unicode filename will be saved in the auditing database, but the reporting tool cannot display Unicode filenames.

### Folder Sweep

Occasionally, file system notification will fail (e.g., due to network errors), so files added to the monitored folder are missed and not processed (e.g., not moved to another location) if the Rule is using only notifications to detect files. After the Folder Monitor Rule is created, the Event Rule system can periodically poll the monitored folder (and subfolders, if specified) to ensure that all files have been processed. This "Folder Sweep" feature is allowed only for "file added" Actions. The Folder Sweep polling occurs at a user-specified frequency. Immediately upon Site or Event Rule start, the initial polling occurs and will trigger any Actions added to the Rule. Folder Sweep is enabled by selecting the **Scan for files every** check box in the **Monitor Folder** dialog box. If the check box is not selected, the associated frequency controls are disabled. Refer to the procedure below for instructions for enabling Folder Sweep.

A new Event type named "Folder Monitor – sweep" is defined and used to populate the `eventType` field in the auditing database when reporting Folder Monitor Rules that were triggered because of Folder Sweep. Also, the Folder Sweep archiving of files will be recorded using the EVENT_ACTIONS value of EVENT_ACTION_FS_ARCHIVED.

The following table describes the Folder Sweep information entered in the log:

| Log Level | Event |
|---|---|
| Debug | • When a Folder Monitor Rule starts execution, log which triggering mechanism(s) are being employed and whether subfolders are being monitored. Also log:<br>o If folder sweep is on, show frequency, time units, and archive subfolder name.<br>o If RDCW* is on, show whether health check is on and its frequency.<br>• When a monitored folder is polled for its contents with special indication for the first poll.<br>• Log which mechanism, RDCW notification or folder polling, triggers the processing of a file.<br>• Log when file has been archived.<br>• Log when file is still in folder after Event Rule Actions have completed and user chose not to archive.<br>• Record trigger collisions by logging if Event is being ignored because file is already in process.<br>• For folder sweep, log when folder contents have been received and are about to be processed.<br>*RDCW = ReadDirectoryChangesW function (Windows); Retrieves information that describes changes within the specified directory. |
| Error | • Log reason for archive folder creation failure.<br>• Log reason for file archive Action failure. |

Risks associated with Folder Sweep include:

- If you do not use the archive feature and the file is not removed from the Monitored Folder due to an Action failure, the file will unintentionally be reprocessed in the next Folder Sweep cycle.
- If the Event Rule has been placing files in the Archive subfolder specified in the Folder Monitor and then you change the name of the Archive subfolder, files that were previously archived by Folder Sweep will be reprocessed.
- If multiple Folder Monitor Rules point to same folder, a "race condition" can occur when the two Rules attempt to concurrently process the same file.

## Archiving

After all Folder Monitor Rule Actions have been executed and if the archive option is enabled, the Folder Monitor Rule will determine whether a file is still in the monitored folder. For this reason, Rule Actions are forced to be synchronous (i.e., "Stop processing" is selected) so that execution returns to the Rule only after all Actions have finished. If the file is still in the folder, the Folder Monitor Rule creates the **Archive** subfolder (if not there already) in the folder containing the file to be archived. If an error occurs while creating the **Archive** subfolder, a message containing the failure reason will be logged; otherwise, the file is moved from the monitored folder into the **Archive** subfolder. If an error occurs during archival, a message containing the failure reason is logged. Whatever the reason, if a file's archival fails, the file is left alone. If the archive feature is not enabled, files are left in the monitored folder, if Event Rule Actions have not otherwise disposed of them. Archive folders will have the same permissions as their parent folders and will not be given special attributes for connecting clients.

## Creating a Folder Monitor Rule

EFT Server keeps track of the number of active threads over time and periodically calculates the average number of concurrent active threads over that time period. The sample rate is once every 5 seconds, and the sample period is 10 samples. After sampling 10 times and finding the average concurrent active threads over that period, the system can grow the pool of the concurrent active threads, up to a set maximum number of threads. This means that if EFT Server is currently running close to or above the prior average of concurrent threads, it will grow the thread pool to allow for room for more Events. By default, EFT Server starts with 3 threads in the pool per Site, and can grow to a maximum of 32 threads.

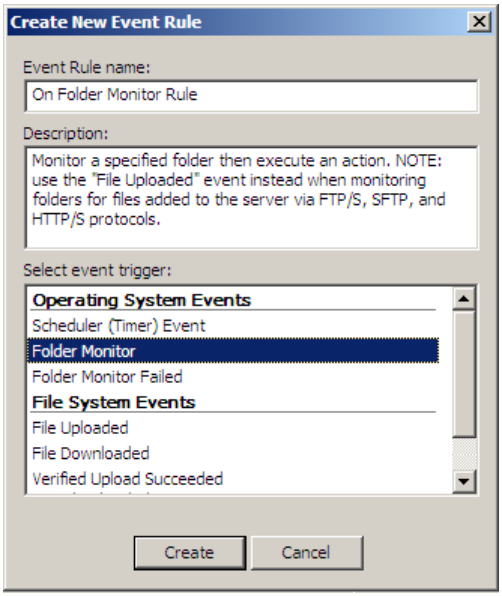
EFT Server will only reset affected (modified) folders when applying configuration changes to an Event Rule, rather than resetting all folders.

*When monitoring a folder, EFT Server watches for any file being added to, removed from, or renamed in the monitored folder. Moving a file, performing PGP operations, and other Actions can trigger the Rule again, resulting in failures. This can be avoided by selecting the* ***Stop processing this rule*** *check box after* ***if action failed then****.*

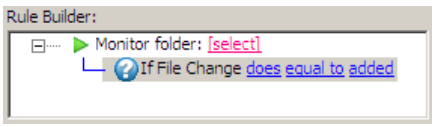
*The* ***Require Active Directory domain trust relationship*** *check box is cleared by default for new installs and selected by default when upgrading from a version prior to EFT Server v6.4, if the FolderMonitorUseNonInteractiveLogon registry entry is present during the upgrade. The* ***Scan for files every*** *check box is not selected and associated controls are disabled. All other control settings are carried over from existing Rules during upgrade (health check yes/no and rate, subfolders yes/no, login credentials).*

**To configure a Folder Monitor Rule**

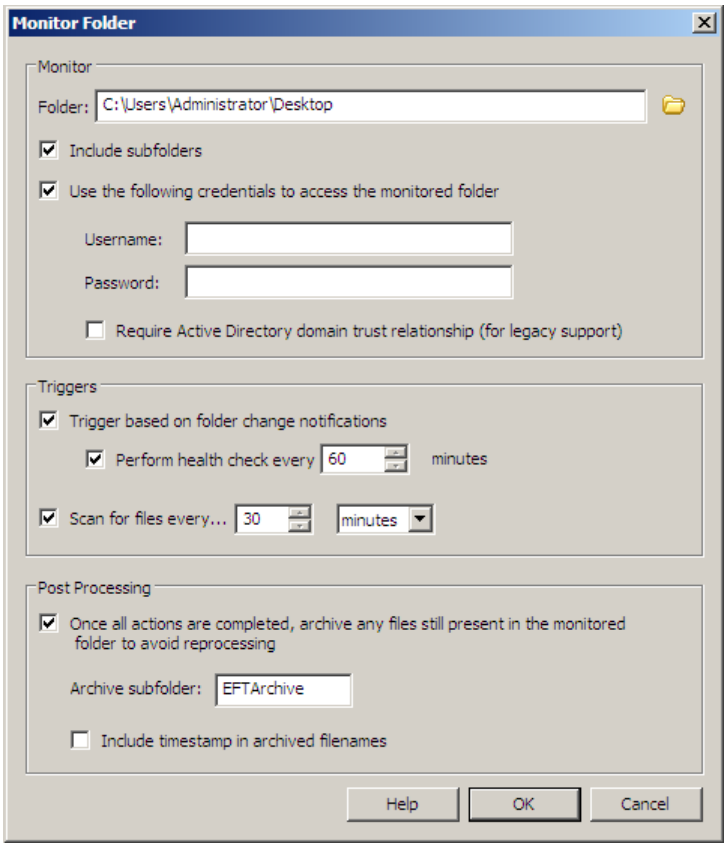
1. Open the Create a New Event Rule dialog box.
2. In the **Create New Event Rule** dialog box, click **Folder Monitor**, and then click **OK**.




The new, blank Rule appears in the **Rule Builder**.




3. In the **Monitor folder** Event, click **[select].** The **Monitor Folder** dialog box appears.




4. Next to the **Folder** box, click the folder icon to specify a folder to monitor.

> *To monitor a folder on a remote, non-EFT Server FTP server, supply the full **UNC** path to the network share. (The format for a UNC path is **\\server\volume\directory** and is not case-sensitive. For example: **\\Shared1_svr\Shared1\WGroups\Network**). Make sure that the EFT Server service has sufficient privileges to perform READ operations on the remote share. If you are using the "health check" feature, it must also have WRITE permissions. This is generally easiest if you set the EFT Server service to run as a domain account, or specify a dedicated "run as" account in the **Monitor Folder** dialog box. Wildcards are not supported.*

5. If you also want to monitor subfolders, select the **Include subfolders** check box. For example, if you are monitoring a user folder and the user has created subfolders, unless you select the **Include subfolders** check box, files added to or changed in subfolders do not trigger the Rule.
6. If login credentials are required to access the folder and subfolders, select the **Use the following credentials to access the monitored folder** check box, and then specify the username and password.

> *The Microsoft definition of noninteractive login states: "Noninteractive authentication can only be used after an interactive authentication has taken place. During noninteractive authentication, the user does not input logon data; instead, previously established credentials are used. Noninteractive authentication is the mechanism at work when a user connects to multiple machines on a network without having to re-enter logon information for each machine." In this case, EFT Server has joined the domain and/or the Server service runs as a domain user. You could supply different credentials to run as a different user for this Action.*

7. The **Require Active Directory domain trust relationship** check box specifies how the Event Rule will log in to monitor remote folders. Selecting this check box indicates that Folder Monitor must establish a "trustful" connection to the system containing the folder(s) being monitored. This control is not enabled unless the **Use the following credentials to access the monitored folder** check box is selected. (Please also refer to the note above regarding this check box.)

8. In the **Triggers** area, select the **Trigger based on folder change notifications** check box to cause Events to be set off by the receipt of directory change notifications (add, delete, and rename) generated by the system.
9. To monitor the status of the network connection and report failures, select the **Perform health check every** check box, and specify an interval. An hour (60 minutes) is specified by default.

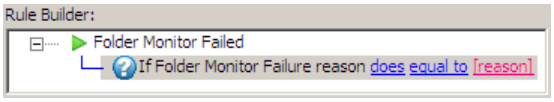
   When the check box is selected, EFT Server periodically writes a special file to the folder specified and then waits for the "file added" notification to verify that it can receive notifications of changes within the folder. When there is a loss of connectivity, EFT Server attempts to re-establish a link to the folder and triggers the **Folder Monitor Failed** Event internally. If you want to receive e-mail failure notifications (or other Actions) when the Folder Monitor health check returns a connection failure, create an additional Event Rule using the **Folder Monitor Failed** Event, and add the **Send notification e-mail** Action to it.

   
   *The time EFT Server waits for the notification from Windows when a Folder Monitor health check file is created can be controlled by a registry value. Refer to the knowledgebase article at http://kb.globalscape.com/KnowledgebaseArticle10682.aspx.*
10. To enable Folder Sweep, select the **Scan for files every** check box and specify the frequency. The default is 30 minutes. A value between 1 and 9999 can be specified with units of seconds, minutes, or hours. The timer for the next sweep cycle is not started until all the files for the current sweep cycle have processed through all Event Rule Actions. Folder Sweep limits its processing to 1000 files at a time. If the monitored folder contains more than 1000 files, up to 1000 of the remaining files will be processed during the next sweep cycle. Selecting the **Scan for files every** check box will cause a Folder Monitor scan upon Event Rule start up (such as when you create the Rule and then click **Apply**). If you have Actions in the Rule, such as an e-mail notification, those Actions will be triggered. (This check box is not selected by default.)
11. All files in a monitored folder will be processed every sweep cycle so if a user neglects to remove processed files or if a Rule Action that was supposed to remove the file fails, the file will be reprocessed. In the **Post Processing** area, select the **Once all actions are completed, archive any files still present in the monitored folder to avoid reprocessing** check box, and then specify the name of the folder in which to archive any remaining files. The default is `EFTArchive`. The **Archive** subfolder will reside directly under the folder in which the file was added. The **Archive** subfolder name cannot contain any of the following characters: `| / \ ? * < " : > + [ ]` and is limited to 248 characters. (The total cannot exceed Windows path limit.)
    - Select the **Include timestamp in archived filenames** check box to avoid overwriting any files of the same name in the **Archive** subfolder. The file name will be appended using the Event Rule variables %EVENT.DATESTAMP% and %EVENT.TIMESTAMP_PRECISE% (time to the millisecond).
    - If Folder Sweep is enabled and you have specified an **Archive** subfolder, the **Archive** subfolder is ignored when **Include subfolders** is enabled.
    - If you change the name of the **Archive** subfolder, the existing **Archive** subfolders will be unaltered. If processing of subfolders is enabled, notifications and polling for contents of the former **Archive** subfolders will begin immediately upon applying the Rule changes.
12. Click **OK**. If the **Once all actions** check box is selected and an invalid name or no name is given for the **Archive** subfolder, it will revert to the default name (`EFTArchive`) and a warning message appears.
13. The **If File Change** Condition is added automatically to restrict the triggering of the Rule. Click the links in the **If File Change** Condition to specify whether the Rule should trigger when a file in the folder is or is not renamed, added, or removed. If Folder Sweep is enabled (as described above), the **If File Change** Condition is forced to "does equal to added," because Folder Sweep only applies to files added to a folder or subfolders.

14. Specify any Action/Conditions to occur when this Event is triggered:
    - Add an e-mail notification. (Refer to E-mail Notification Action.)
    - Copy or move a file added to the monitored folder to another location. (Refer to Copy/Move File to Host Action.)
    - Add Conditions, such as the **If File Change** Condition so that the Rule doesn't trigger again after the file is moved or renamed. (Refer to Using Conditions.)
15. Click **Apply** to save the changes on EFT Server.

### Folder Monitor Failure

To audit failures of Folder Monitor Rules, use the **Folder Monitor Failed** Event, and then add the **If Folder Monitored Failure reason** Condition.




Click the **reason** link to specify a failure reason that will trigger the Rule: **any failure**, **archive failure**, **health check failed**.

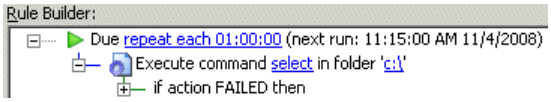
Folder Monitor archive folder errors will also trigger this Event and write to the Windows Event log.

## Using an Event Rule to Execute a Command (Run a Process)

You can configure EFT Server to run executables, batch files, and scripts automatically when specific events occur. EFT Server calls these *Commands*. When the Event Rule is triggered, EFT Server executes the specified custom command and attributes.

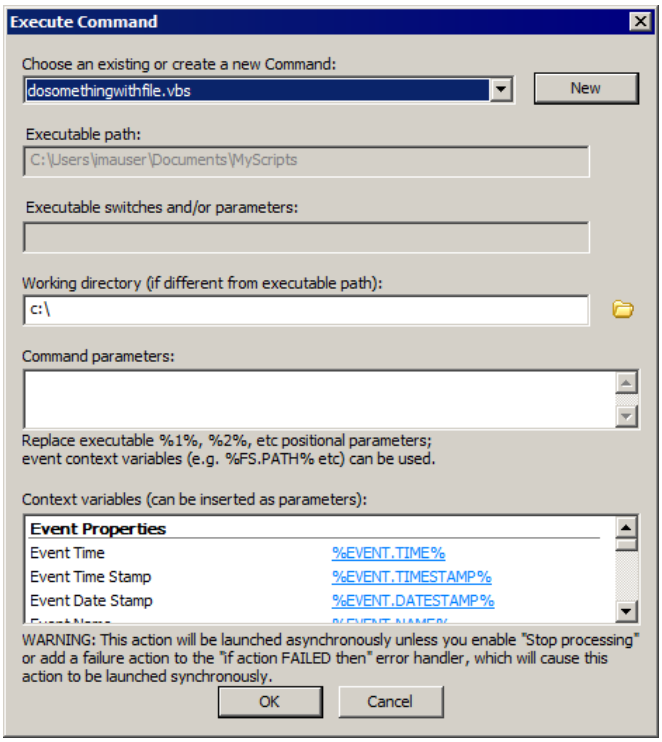
**To execute a Command from EFT Server's Event Rule system**

1. Identify the Command you want to execute with the Event Rule or create a new custom Command using the procedure in Creating a Command. Or you can create a new Command later from within the Event Rule (in step 6 below).
2. Open the Event Rule with which you want to execute the Command or create a new Event Rule using the procedure in Defining Event Rules.
3. (Optional) If you need to apply any conditional behavior, click it in the **Conditions** list.
4. In the **Actions** list, double-click **Execute command in folder**. The Action is added to the Event in the **Rule Builder**.




*Links in the **Rule Builder** indicate parameters that must be defined to save the Rule.*

5. In the **Rule Builder**, click one of the underlined text links. The **Execute Command** dialog box appears.




6. In the **Choose an existing or create a new Command** list, click the list to select the Command. (If you did not create the Command in step 1, click **New** to create the Command now.)
7. The **Executable path** and **Executable switches and/or parameters** boxes display the path and switches for the selected Command. (If you want to change anything, you will have to close this dialog box, apply any changes to the Event Rule, go edit the Command, and then reopen the Event Rule to continue defining it.)
8. In the **Working directory** box, type the path or click the folder icon to specify the folder in which the script or executable resides e.g., **C:\EFTscripts**. For mapped drives, use their UNC path. (File browse operations are disabled when you are connected remotely. You can't click the folder icon and browse, but you can type a path that is relevant to the EFT Server computer, not the remote interface).
9. (Optional) In the **Command parameters** box, include any parameters for the command. For example, type the script name if the command will be running a script.

   You can also select the items in the **Context variables** list to add them as parameters. For example, suppose you want to run a script on a file that was uploaded and triggered the Event Rule. You would type the script name and the tag `%FS.FILE_NAME%`, as shown below:

   ```
   dosomethingwithfile.vbs -file %FS.FILE_NAME%
   ```

   *Refer to Variables for details of available variables and how to use them.*
   *EFT Server passes the complete variable along to the command; however, due to limitations of some command line applications, they may not be able to interpret the command properly. In certain instances, such as when there is a semicolon in a file name, you may need to enclose the variable in quotation marks in the Command Parameters box after you insert it from the Context variables box.*

10. Click **OK** to save the Command.
11. Add other Actions as needed, and then click **Apply** to save the Event Rule.

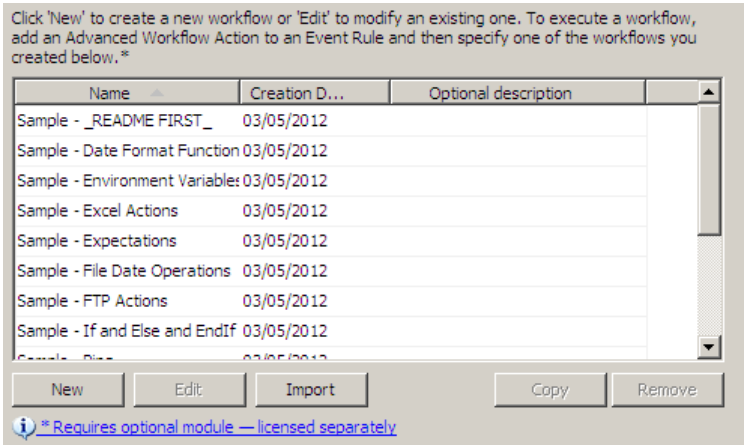
# Creating Workflows for Use in Event Rules

(The Advanced Workflow Engine is available as an add-on module in EFT Server Enterprise. Refer to the *Advanced Workflow Engine User Guide* for more information.) Similar to Commands, Workflows are used in Event Rules as Actions or triggers. When you create a Workflow, the Advanced Workflow Engine creates a file with an extension of **.aml** and saves it in EFT Server's **AWE** folder (by default, **C:\Program Files\Globalscape\EFT Server Enterprise\AWE**). The filename is the name of the workflow, prepended with an underscore and the name of the Site. For example, if you create a Workflow called **FTP** on a Site called **Boston**, the Workflow's filename is **Boston_FTP.aml**.

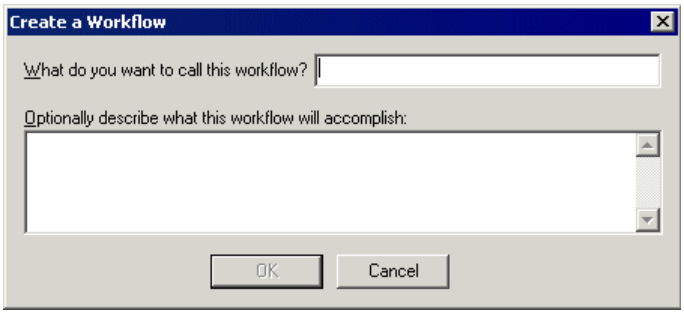
*During the AWE trial, when a new Workflow is created, a message appears (prior to the **Create a Workflow** dialog box) informing you that the Advanced Workflow module is an optional module and that the 30-day trial begins when the first Workflow is created.*

**To create a Workflow**

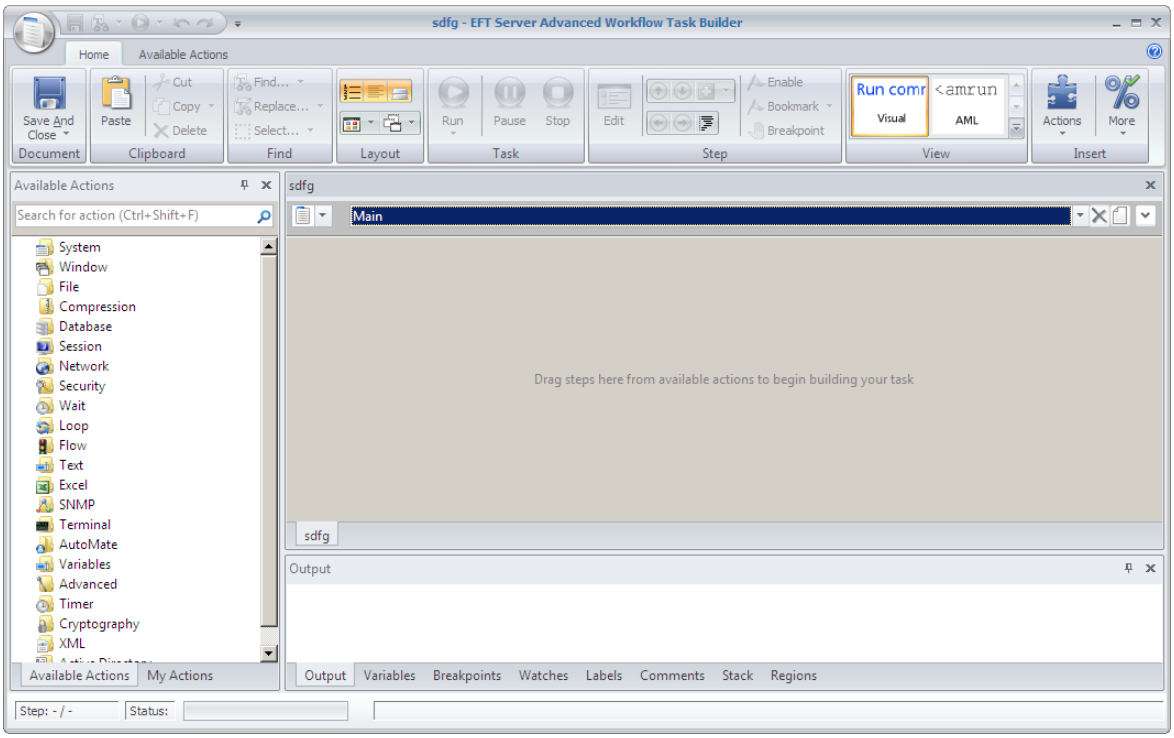
1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, click the **Advanced Workflows** node.
3. In the right pane, the **Advanced Workflows** tab appears.




4. In the right pane, click **New**. The **Create a Workflow** dialog box appears.




5. In the **What do you want to call this workflow** box, specify a name for the Workflow. When you add the workflow to Event Rules, the name you specify here appears in the Rule.
6. (Optional) Provide a description of the Workflow, and then click **OK**. The **Workflow Task Builder** appears.

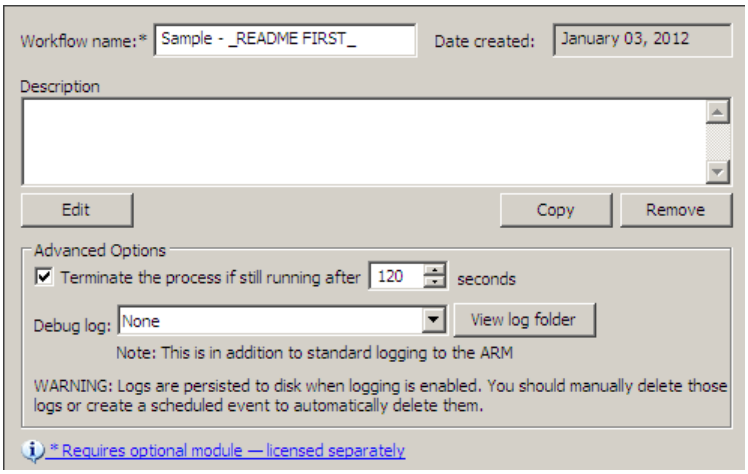



7. The tree in the left pane lists the steps that you can add to the Workflow. The right pane displays the steps in the Workflow.
8. Drag items from the **Available Actions** list to the **Steps** pane to create your Workflow.
9. Use the **Run** icon on the Debug toolbar to test the steps. You can run it all at once, run only a selected step, or the whole Workflow starting with a step other than the first step.


The Output pane displays the result of each step. For example:

```
Executing line 5
Starting Input Box with message "What is your name?"...
Creating message box "What is your name?"... >
Populating variable "theUserName"...
Finished Input Box "What is your name?".
The step was okay.
```

10. After you have created your Workflow, click **Save and Close**. The Workflow appears in the **Advanced Workflows** node of the Site tree and is ready to be used in Event Rules.




11. (Optional) In the **Advanced Options** area, select the **Terminate the process** check box and specify the number of seconds after which to terminate the Workflow if it fails to execute.
12. (Optional) Specify the level of debug logging in the **Debug log level** box, **None**, **Minimal**, **Normal**, or **Verbose** (None is the default).
    - When you are logged in to the EFT Server computer, you can click **View log folder** to view the logs created by this Workflow.

Your Workflow is now ready to insert into an Event Rule. The Auditing and Reporting module Event Rule reports will show the AWE Workflow task name.

## Backing Up AWE Workflows

If you plan to edit the sample Workflows and/or create custom Workflows, you should create an Event Rule to periodically back up (save a copy of) the Workflows.

**To backup the Workflows**

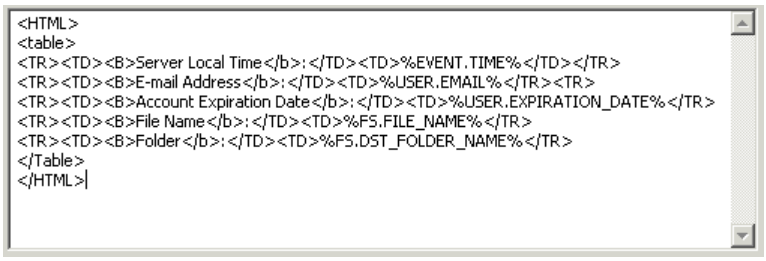
1. Define a Timer Rule. Specify the frequency depending on how often you create new Workflows.
2. Add the Copy/Move (push) file to host Action to the Rule.
3. For the **Source** path, specify the location of the Workflow (**.aml**) files. For example, to copy all of the Workflows for the Site named "MyGSSite, " in the **Source** box type:
   `C:\ProgramData\Globalscape\EFT Server Enterprise\AWE\MyGSSite_?.*`
   If you use * you will back up everything in that folder.
   (Do ***NOT*** select the **Delete source file** check box!)
4. For the **Destination** path, specify a location on a remote drive (in case the local drive fails).
5. Click **Apply**.

## File Uploaded Event with User Details

Suppose you want to be sent an e-mail each time any user uploads a file to EFT Server, and you want to include information about the user account that uploaded the file.

**To define the Event Rule**

1. Create a **File Uploaded** Event Rule.
2. Add an E-mail Notification Action.
3. In the Message of the e-mail, add the desired user variables, such as %USER.LOGIN%, %USER.EMAIL%, and %USER.PHONE%. For example:




4. Click **Apply**.

With this very simple Rule, an e-mail is sent whenever ***any*** user uploads a file to EFT Server. You can further customize the Rule to suit your needs:

- If you only want to know when a specific user uploads a file, add the Condition "If Login name is" and select the username.
- If you only want to know when someone in a specific Group uploads a file, add the Condition "If User is a member of" and select the Group.

### Defining the E-Mail with User Details

The default e-mail body contains a table. If you can edit HTML and if the account that the e-mail is sent to accepts HTML e-mails, you can format the e-mail to suit your needs. Review your tags carefully, however, since no HTML code verification is performed by EFT Server.

Using the example code above, when a user with the username `jbite` uploads a file, the following e-mail might be sent:

This message was sent to you automatically by EFT Server on the following Event: File Uploaded.

**Server Local Time**: 12/5/2007 14:00:00
**E-mail Address**: jbite@mycompany.com
**Account Expiration Date**: 12/1/2008 11:59:59
**File Name**: file.txt
**Folder**: C:\InetPub\EFTRoot\Standard\Usr\jbite

## Using a Command in an Event Rule to Copy Files

If you want to copy EFT Server's files to another location based on the date (e.g., all log files created on a specified date), you can create a custom Command that points to the Windows XCopy command. The executable is (by default) in **c:\windows\system32\xcopy.exe**. Numerous switches are available for this command. (You can see all of the options by typing `xcopy /?` at a command prompt.) You must type the *source path* and the *destination path*.

You can add a switch, `/d:mm-dd-yy`, to copy files that were changed on or after a specified date. If no date is provided (just the `/d` with no date), it copies all source files that are newer than existing destination files. That is, it will not copy a file with the same name/same date or same name/older date.

To define an Event Rule to copy files, assuming that EFT Server has permissions to access the files, you can create a Folder Monitor Rule and specify that if the Condition "If File Change does equal to added" exists, and then execute the Command to `xcopy` the newer files to the destination location.

**To define an Event Rule to copy files**

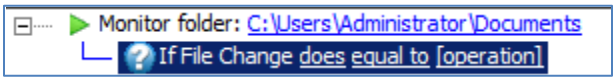
1. Create a custom command to execute the Windows xcopy command. The executable is (by default) in **c:\windows\system32\xcopy.exe**.
2. In the **Working directory** box, type the path or click the folder icon to specify the folder in which the script or custom command executable resides (**C:\windows\system32**).

3. In the **Parameters** box, type the source folder (the location of the files), the destination folder (the location to which to copy the files), and any other xcopy parameters you need. For example, type:

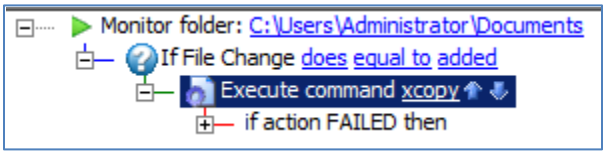
   ```
   "C:\ProgramData\Globalscape\EFT\Logs\*.log" "C:\Temp\" /d
   ```

   The parameters tell the xcopy command to copy all **.log** files in the **EFT\Logs** directory to **C:\Temp**. The parameter `/d` (with no date) copies all source files that are newer than destination files.

4. Create a Folder Monitor Event Rule.
5. Add the Condition **If File Change equal to operation**, and then click **operation** to change it to **added**.

6. Add the **Execute command in folder** Action to the Rule, and then click **select**. The **Execute Command** dialog box appears.
7. In the **Choose an existing or create a new Command** box, click the XCopy Command that you defined in step 1.

8. Click **OK** to close the **Command Configuration** dialog box, and then click **Apply** to save the Rule on EFT Server.

The Rule is now defined to copy log files from the monitored folder (**C:\ProgramData\Globalscape\EFT\Logs**) to the new location. (Note that they are copied, not moved.)

You could also add an E-mail Notification Action to let you know when the Command is executed.

*Always use caution when giving program access to your system32 directory (especially an FTP server).*

## Copying or Moving a File Triggered on Monitor Folder Event and Renamed

**(Available in EFT Server Enterprise)** You can configure an Event Rule triggered by a Folder Monitor Event to copy or move files in the folder and save them with a different name. Refer to Copy/Move File to Host Action for details of defining an Event Rule using the **Copy/Move file to host** Action.

***IMPORTANT:*** If you want to move a modified (renamed) file, use the DST-based variables (e.g., `%FS.DST_FILE_NAME%`) because they contain the modified values.

For example, when you configure an Event Rule to copy/move a file that is triggered on a **Monitor Folder** Event with a Condition of **If file change does equal to rename**, use the following variables:

- `%FS.DST_PATH%` instead of `%FS.PATH%`
- `%FS.DST_FILE_NAME%` instead of `%FS.FILE_NAME%`.

If the file is renamed, the new name context is lost to `FS.PATH` and `FS.FILE_NAME`, which retain the old path/name, but the new path/name is passed to `%FS.DST_PATH%` and `%FS.DST_FILE_NAME%`.

For example, suppose the monitored folder contained a file called `Robert.txt` and you rename the file `Bob.txt`.

%FS.DST_FILE_NAME% contains the new value Bob.txt, but %FS.FILE_NAME% contains the old value Robert.txt.

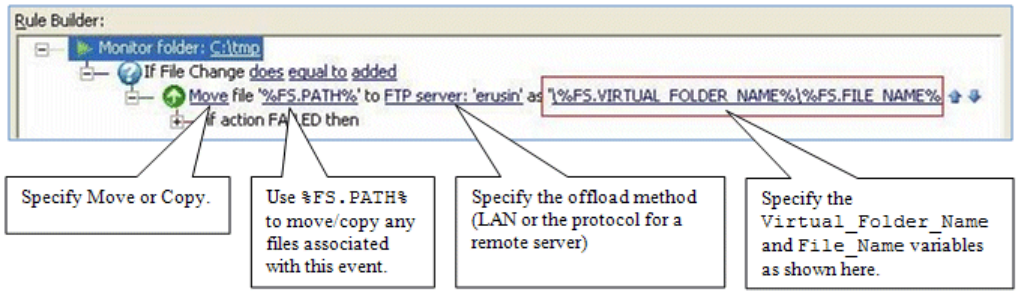
For details of the Copy/Move Action, refer to Copy or Move File to Host Action.

*The client offload/download RENAME and the Folder Monitor RENAME are two different events/stimulus. The Folder Monitor RENAME uses the DST variables, whereas the client download/offload RENAME uses the SOURCE FILE NAME-related variables.*

## Copying Folder Structure When Offloading Files

In a Monitor Folder Event Rule, you can move a file that is added to the monitored folder. If you use the variables %FS.VIRTUAL_FOLDER_NAME%\%FS.FILE_NAME% as the Destination Folder path, the Event Rule will copy all of the files and folders and keep the folder structure. VIRTUAL_FOLDER contains the structure of the folders under the monitored folder.

The Event Rule in the illustration below will copy all of the files and keep their folder structure.




Refer to Monitoring Folders for details of creating a Folder Monitor Rule. Refer to Copy/Move (push) File to Host Action for details of using the **Copy/Move** Action.

## Routing Outbound Traffic through a Proxy

You can connect to EFT Server through a proxy. DMZ Gateway can also be configured as an outbound proxy. There are several places in the administration interface in which you can configure proxy settings. Each of the configurations use the **Proxy Settings** dialog box.

Outbound connections that originate from EFT Server will route through normal network mechanisms to reach the destination. However, it is possible to configure EFT Server's Event Rules using the **Copy/Move file to host** Action to use a remote proxy.

**To configure an Event Rule to route outbound traffic through a proxy**

1. Create an Event Rule, such as a Scheduler (Timer) Event.
2. Add the **Copy/Move File to Host** Action, and follow the procedures in Copy/Move File to Host Action to complete the Rule.

For the procedure for using a SOCKS proxy server, refer to Using a SOCKS Proxy Server.

## Using a SOCKS Proxy Server

When you create an Event Rule that uses a Copy/Move File to Host Action, you can specify a SOCKS proxy server for the connection to the remote server. You can also specify a SOCKS server in AWE's HTTP Download and HTTP Post Actions.

*If you enable the use of DMZ Gateway as the proxy in the **Proxy Settings** dialog box, SOCKS options are disabled. EFT Server does not support the use of DMZ Gateway as a proxy and SOCKS settings in combination; however, the combination of FTP or HTTP proxy and SOCKS is allowed.*

**To use a SOCKS proxy server**

1. Create an Event Rule with a Copy/Move File to Host Action.
2. In the Event Rule Action, click **%FS.PATH%**. The **Offload Action** wizard appears.
3. Click **Socks**. The **SOCKS Settings** dialog box appears.
4. Select the **Use SOCKS settings** check box to enable the **Socks Type** options.
5. In the **Socks Type** area, specify a SOCKS server type of either SOCKS4 or SOCKS5.
    - When SOCKS4 is specified, **Use authentication** is disabled.
    - When SOCKS 5 is specified, **Use authentication** can be enabled, allowing you to provide a username and password for the SOCKS connection. If you selected SOCKS5 and the **Use authentication** check box, specify the **Username** and **Password** required to connect to the SOCKS server.
6. Click **OK** to save the SOCKS options.
7. Continue with the wizard to complete the File Offload Configuration.

## Too Many Connections per Site

You can define an Event Rule to send you an e-mail when a user login fails because there are too many connections to a Site. If the Rule is triggered frequently, you might want to change the maximum concurrent socket connections setting for the Site and/or purchase more licenses for the Web Transfer Client.

**To define the Event Rule**

1. Define an Event Rule using the **User Login Failed** Event trigger. The Event trigger appears in the **Rule Builder**.
2. In the **Conditions** list, double-click **if Event Reason** (or click it, and then click **Add condition**) to add it to the Rule.
3. In the **Rule Builder**, click the linked text **[specific reason]**. The **Event Reason** dialog box appears.
4. Click the **Specify the event reason** drop-down menu to specify a reason that will trigger the Event Rule:
    - Account Disabled
    - Account Locked Out
    - Invalid password
    - Protocol not supported
    - Restricted IP
    - Too many connections per IP
    - Too many connections per Site
    - Too many connections per user

    For this example, click **Too many connections per Site**.
5. Click **OK**.
6. In the **Actions** list, double-click **Send notification email** (or click it, and then click **Add action**) to add it to the Rule.

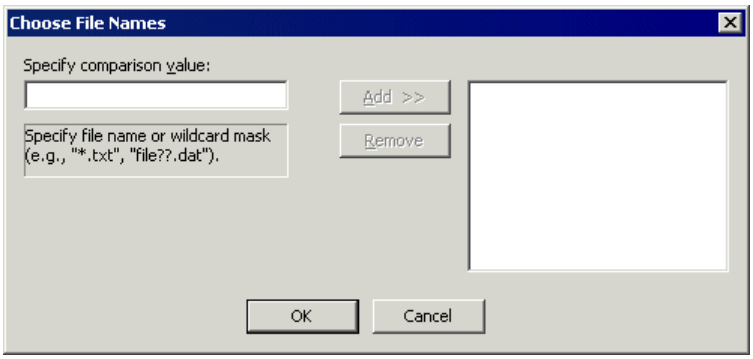
7. In the **Rule Builder**, click the linked text **[select]** and configure an e-mail to send yourself a notification (or link to your defined e-mail template) then click **OK**.
8. Click **Apply** to save the changes on EFT Server.

## Moving an Uploaded File Based on Filename

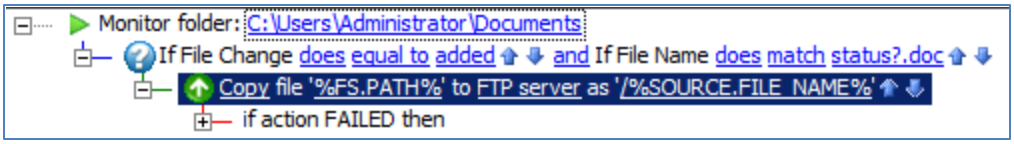
Suppose every Friday the manager of Engineering uploads a status report named `status<date>.doc` to EFT Server. You want the manager of Marketing to have access to that file, but not to any other files in the Engineering manager's folder. The example below describes how to create an Event Rule so that when a file with "status" in the name is uploaded to EFT Server, EFT Server makes a copy of it in another user's folder.

**To move an uploaded file based on the filename**

1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, expand the Site you want to configure, and then click **Event Rules**. In the right pane, click **New**. The **Create New Event Rule** dialog box appears.
3. In the **Create New Rule** dialog box, click **Folder Monitor**, and then click **Create**. The new Rule appears in the **Rule Builder** and includes the **If File Change** Condition.
4. In the **Rule Builder**, in the Monitor folder Event, click **[select]**. The **Monitor Folder** dialog box appears.
5. Define the Monitor Folder trigger. If necessary, refer to Monitoring Folders for details of creating a Folder Monitor Rule. Note that if you create a Folder Monitor Rule to monitor a folder that is already being monitored by another Folder Monitor Rule, a warning message appears because the two Folder Monitor Rules can cause a race condition that may result in errors or undesirable results. If that is the case, you can add the new Conditions and Actions to the existing Rule
6. Click the **If File Change** Condition in the **Rule Builder** to select it, and then in the **Conditions** list, double-click the **If File Name** Condition. The **If File Name** Condition appears in the **Rule Builder** on the same line as the **If File Change** Condition. (See the screen shot in step 9 below.)
7. In the **If File Name** Condition, click the **[path mask]** link. The **Choose File Names** dialog box appears.




8. In the **Specify comparison value** box, specify the file name and/or a wildcard mask, click **Add**, and then click **OK**. For example, to filter for a Word document whose filename starts with "status," type: `status?.doc`
9. Next, you must specify the Action to occur when this Event is triggered. In the right pane, in the **Actions** list, click **Copy/Move (push) file to host**. The Action is added to the **Rule Builder**.




10. Click one of the undefined parameters (e.g., '%FS.PATH%'). The **Offload Action Wizard** appears.
11. In the **Offload method** box, specify a protocol type for the connection. For this example, we will choose **Local (Local Files or LAN)**. (Refer to Copy/Move (push) File to Host Action for other protocol types.)
12. Click **Next**. The **Source File Path** page appears.
13. In the **Source path** box, type %FS.PATH% (or you can leave it blank).
14. If you want to **Delete source file after it has been offloaded**, select the check box. (If the file is marked read-only, it will not be deleted.)
15. Click **Next**. The **Destination File Path** page appears.
16. In the **Destination path** box, click the folder icon and specify the location in which to save the offloaded file. (No validation is performed.)
17. Click **Finish** then click **Apply** to save the changes on EFT Server. (You could also add other Actions, such as e-mail notifications.)

    Now when a user uploads a file called status?.doc, EFT Server will move it to the destination folder specified.

If you are copying or moving the file to another location, and the file upload is a regularly occurring Event with a file of the same name, in the **Offload Action** wizard, you can add the variables `%EVENT.DATESTAMP%` and/or `%EVENT.TIMESTAMP%` to the path so that the date (YYYYMMDD) and/or time (HHMMSS) are added to the filename when it is moved/copied.

> Do ***not*** use `%EVENT.TIME%`, because the colon (e.g., `28 Aug 07 10:01:56`) makes it invalid for file naming.

For example, type:

```
C:\Documents and Settings\Administrator\My
Documents\upload\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%_%FS.FILE_NAME%
```

With this path and variables, when a file is uploaded to the monitored folder, the file is moved to \My Documents\upload and the date and time are prepended to the filename (for example, 20080422_101212_mydailyprogress.doc).

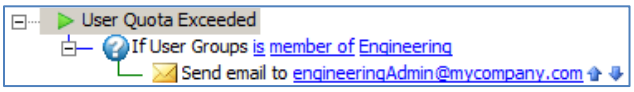
## Applying a Rule to a Specific User or Group

You can use the **If User is a member of** Condition to apply the Event Rule to one or more Groups (By default, all Rules apply to all users.) For example, suppose the Engineering department has its own user administrator for EFT Server and you want the administrator to get an e-mail when one of the user accounts exceeds its quota. You would set up a **User Quota Exceeded** Event with an **If user is a member of** Condition and a **Send notification email** Action, as described below.

**To create the Rule**

1. Define an Event Rule using the **User Quota Exceeded** Event trigger.
2. Add the **If User Groups** Condition.
3. In the **Rule Builder**, click the **specific group(s)** link. The **Event Target Users and Groups** dialog box appears.

4. Clear the **All Users** check box and select the check box of one or more Groups to which you want this Rule to apply, and then click **OK**.
5. Add the Send notification e-mail Action to the Rule and provide the e-mail address of the user administrator and anyone else you want to receive the e-mail.
6. Click **Apply**. The Rule appears similar to the following example:

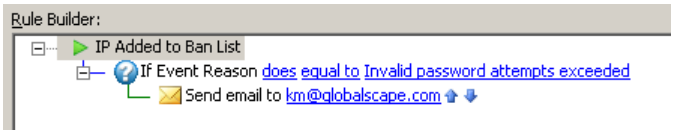



## IP Added to Ban List

This Event is triggered when an IP address is added to the ban list by the system (not manually by an administrator). Administrators can configure Event Rules to capture this Event and send notifications or write to logs. (Wildcards are not supported for IPv6 addresses.)

**To define an IP Added to Ban List Event**

1. Follow the procedures in Defining Event Rules.
2. In the **Create New Rule** dialog box, under **Site Events**, click **IP Added to Ban List**, and then click **OK**. The new Rule appears in the **Rule Builder**.
3. Add any (optional) Conditions (e.g., If Event Reason, If Remote IP, If Server Running, etc.) and one or more Actions (e.g., Send notification email).
    - The possible Event Reasons include DoS/Flood prevention trigger, Invalid password attempts exceeded, and Invalid username attempts exceeded.
4. Click **Apply** to save the Rule. The Rule appears similar to the Rule below.



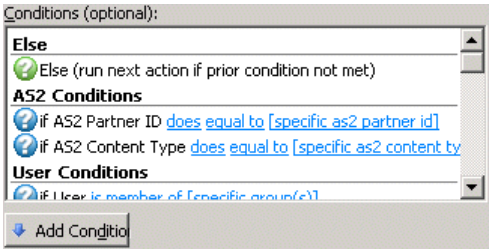

# Event Rule Conditions

*Conditions* allow you to define more narrowly the trigger for an Event Rule. Conditions are optional; you do not have to define a Condition on an Event Rule to make it trigger an Action, but Conditions allow fine control over when an Action can take place.

You can further fine-tune each Event trigger to execute only if certain Conditions are met. These optional Conditions act like filters or compound IF statements so that IF a specific Event occurs and IF a Condition is met, and then an Action is executed. For example, an Event trigger that is called whenever a file is uploaded can be fine-tuned to trigger only if that file's extension is **.txt** and nothing else.

**To add a Condition to a Rule**

1. Create the Rule. In the **Conditions** list, the Conditions available for the selected Event appear. When applicable to the Rule, the **Else** option also appears.



2. Double-click a Condition in the list or click the Condition, and then click **Add Condition**.
3. Complete the Rule by adding one or more Actions, and then click **Apply** to save the Rule.

Refer to the List of Conditions for the Conditions supported by EFT Server. Conditions that require you to specify a value or parameter have further instructions with their description in the List of Conditions.

*Conditions are NOT REQUIRED for an Event Rule to work. In its base form, the Event trigger itself is a sort of Condition, therefore you can execute Actions when/if an Event triggers, without adding any additional Conditions.*

## Condition Placement

Where Conditions are placed within the **Rule** pane when they are added depends on which item is selected in the **Rule** pane.

- When the Event Rule *trigger* (the very first item in the **Rule** pane) is selected and a Condition is added, the Condition is placed directly beneath the Event Rule Trigger. This is considered a "root" level condition.

```
ON FILE UPLOAD
{
    if ( %FS.FILE_NAME% = "*.pgp" )  //a root level condition. No action added
yet
    {
    }
}
```

- When an Action inside another Condition is the selected item and a new Condition is added, that new Condition is placed directly beneath the Action and to the left, or outside of the container Condition. Otherwise, it would become a nested Condition, which EFT Server does not support.

```
ON FILE UPLOAD
{
    if ( %FS.FILE_NAME% = "*.pgp" )
    {
       PGP Decrypt %FS.FILE_PATH%
    }
if ( %FS.FILE_NAME% = "" ) //new condition added placed at root level
{
}
}
```

- When an Action (that is not contained within a Condition) is the selected item, and a new Condition is added, the new Condition is placed immediately beneath that Action, at the same root level (see above example).
- When a Condition is the currently selected item and another Condition is added, the new Condition is ANDed to the selected Condition. If the Condition being added is the same Condition as the one selected, the new Condition is ORed to the selected condition. Using this method, you can create compound Conditions.

```
ON FILE UPLOAD
{
    if (%FS.FILE_NAME% = "*.pgp" ) AND (%FS.FILE_SIZE% <300,000b)  //a
compound condition
    {
       PGP Decrypt %FS.FILE_PATH%
    }
}
```

## Changing Condition Placement

Conditions can be moved using the up/down arrows next to the Condition or at the bottom of the dialog box, or by using copy/paste. When a Condition is moved, the Condition and any actions inside of that Condition also move. If a Condition has an else statement under it, the else statement is also moved. This is because the Condition, any actions inside that Condition, and any attached Else clauses are considered a conditional block, and the entire block is moved.

**Example:**

```
Condition A
Action 1
Action 2
Condition B
Action 3
```

Click the Condition A down arrow ONCE, and Condition A and its child Actions are moved as a block:

```
Condition B
Action 3
Condition A
Action 1
Action 2
```

This same behavior does not apply when the Condition being moved is part of a compound Condition. To move one of the Conditions inside of a compound Condition down (or up), and, therefore, outside of that conditional block, you need to click on one of the Condition's up/down arrows:

```
Condition C1 and C2
Action 1
Action 2
Condition C3
Action 3
```

Now click on the down arrow to the right of C1:

```
Condition C2
Action 1
Action 2
Condition C1
Condition C3
Action 3
```

To move a compound Condition, you need to select the ENTIRE Condition by clicking the icon at the far left of the Condition:

```
Condition C1 and C2
Action 1
Action 2
Condition C3
Action 3
```

Click the icon then either drag the cursor down or click the blue down arrow at the bottom of the dialog box (not the down arrow to the right of the Condition). A page icon appears if you drag it to an applicable location.

```
Condition C3
Action 3
Condition C1 and C2
Action 1
Action 2
```

## Condition Evaluation

Regardless of placement, ALL Conditions are evaluated, because all Conditions exist at the root level.

For example:

```
ON FILE UPLOAD
{
    if (%FS.FILE_NAME% = "*.pgp")  //if filename extension is PGP then decrypt
it
    {
       PGP Decrypt %FS.FILE_PATH%
    }
    if (%FS.FILE_NAME% = "*.zip") //even if the prior condition was true, still
evaluate this condition.
    {
        UNZIP %FS.FILE_PATH% to "%FS.FILE_PATH%\%EVENT.DATE%_%EVENT.TIME%\"
    }
}
```

## Else Clauses

**(Available in EFT Server Enterprise)** The Else clause or statement is a type of Condition and appears in the **Conditions** list box when at least one Condition has been added to the **Rule** pane. The Else clause executes if the Condition preceding the Else statement is not met.

This is your typical Else statement as part of an IF/THEN/ELSE block:

```
If A Then
{ Run B }
Else >
{ Run C }
```

An Else statement must always follow a Condition. Else statements cannot be moved around independently. If you want to move the else statement, you need to move the entire conditional block or delete the else statement and re-create it elsewhere.

Below is an Event Rule example of using an Else clause.


Only the last Condition is considered before the ELSE statement is evaluated. That is, the ELSE statement will be TRUE only if the last Condition is FALSE, even if the preceding Conditions are TRUE.

## Logical Operators

When a Condition is added to another compound conditional statement, the newly added Condition will be ANDed to the Condition already present:

**Example 1:**

```
If Filename = bob.txt
```

Now add another Condition:

```
If Filename = bob.txt and If Filesize < 100 MB
```

When the second Condition being added is the SAME Condition type as the previous one, the newly added Condition will be ORed to the previous Condition.

```
If Filesize < 200 MB
```

Now add another same Condition:

```
If Filesize < 200 MB or If Filesize > 500 MB
```

If there are more than two Conditions already existing in a compound Conditional line, and another Condition is added (regardless of Condition type), the new Condition will use the same logical operators that are already present for that compound statement.

```
If Filesize < 200 MB or If Filesize > 500 MB
```

Now add another same Condition:

```
If Filesize < 200 MB or If Filesize < 400 MB or If FileName = rob.txt
```

You can change the AND and OR operator values by clicking the **and** or the **or** hyperlink. Please note that logical operators separating conditional statements must be the SAME across the entire compound statement. You cannot mix and match AND and OR statements. When changing the logical operator for a compound conditional statement, ALL subsequent logical operators for that statement also change to match that operator. This is necessary to prevent problems with evaluation precedence, especially in conditional blocks with more than 2 conditional expressions to evaluate. There are ways around this limitation, discussed in Evaluating Expressions.

**Example 2:**

```
If Filename = bob.txt
```

Now add another Condition:

```
If Filename = Bob.txt and If Filesize < 100 MB
```

Now add another Condition:

```
If Filename = Bob.txt and If Filesize <100 MB and If group is one of Admins
```

Now click one of the AND hyperlinks to change it to OR. Resulting line:

```
If Filename = Bob.txt OR If Filesize <100 MB OR If group is one of  Admins
```

**Example 3:**

```
If Filesize is < 200 MB
```

Now add another Condition:

```
If Filesize < 200 MB or If Filesize > 500 MB
```

Now click the OR hyperlinks to change it to AND. Resulting line:

```
If Filesize < 200 MB and If Filesize > 500 MB
```

Note that in the second example, the statement will never evaluate to true. You must change the comparison types or the comparison values, or switch back to the OR logical operator to avoid creating expressions that can never evaluate to true.

## Evaluating Expressions in Event Rules

EFT Server will always evaluate expressions from left to right, regardless of how many conditional checks there are within that same expression. One exception to this is described below.

Certain Conditions are able to test multiple values, such as the **If User is Member of** condition or the **If Filename is one of** Condition. These Conditions are evaluated first and independently, with the resulting atomic unit evaluated as part of the complete expression.

For example, the **If User is Member of** Condition allows you to select from a list of Server Groups, therefore, the **If User is member of** expression is evaluated first, after which the rest of the expression is evaluated from left to right.

## Compound Conditional Statement

```
If Filename (F)= Bob.txt AND If User is Member of Admins (MA), Users (U), Power Users (PU)
```

If this expression were evaluated from left to right, the results would not match our expectations:

```
If (((F and MA) or U) or PU)
```

Instead, EFT Server evaluates the conditional statement first as its own atomic unit and then evaluates the resulting expression from left to right:

```
If (F and (MA or U or PU))
```

This allows you to create expressions that contain order-of-precedence grouping without having to use parentheses. The evaluative OR statement is hidden inside the conditional statement, as long as that conditional statement can evaluate against multiple criteria.

Only the following Conditions can evaluate against multiple criteria (strings):

- If User is Member of
- If Login name
- If Virtual Path
- If Physical Path
- If Physical Folder Name
- If Physical Destination Path
- If Physical Destination Folder Name
- If Destination File Name
- If Virtual Destination Path
- If Filename

**To define multiple criteria for a Condition**

1. Double-click a Condition in the list to add it to the **Rule Builder**. (To learn more about available conditions, refer to Conditions.)
2. If you are adding an additional Condition, highlight the existing Condition in the **Rule Builder**, and then in the **Conditions** list, double-click the Condition you want to add. The Condition appends to the existing one and adds a logical operand (AND/OR).


3. Click the logical operand (and/or) to change it.

   You can insert multiple Conditions. That is, you can have Condition 1 **AND** Condition 2 **OR** Condition 3.

*If you need to use more complex criteria using AND and OR, you can use wildcard logic to create any logic that wildcards support. For example, if you add the **File Name** Condition to the **Rule** pane, you can then define the path mask using complex logic with wildcards.*

# Event Rule Actions

The topics in this section provide information regarding defining and using Event Rule Actions.

Once an Event Rule is triggered, assuming all Conditions are met, EFT Server can launch one or more of the following user-definable Actions:

- Execute command in folder - The custom command in a specific location is triggered.
- Execute Advanced Workflow - (available only in EFT Server Enterprise) An Advanced Workflow is triggered.

- Send notification e-mail - An e-mail message is sent to the address specified.
- Copy/Move (push) File to Host - (available only in EFT Server Enterprise) The designated file is automatically moved to another location.
- Download (pull) File from Host - (available only in EFT Server Enterprise) Downloads a specified file
- OpenPGP operations - The designated cryptographic action is performed on the file.
- Cleanup in folder - Cleans up a specified folder
- Generate Report - A report is generated and e-mailed or saved to a file at a specific date and time.
- AS2 Send file to host - (available only in EFT Server Enterprise) You can send files via AS2 to a partner that does not have inbound access defined in EFT Server's account management system. For details of the **AS2 Send file to host** Action, refer to Sending Files to an AS2 Partner.
- Backup Server Configuration - Automatically backs up Server configuration for use in disaster recovery or Server migration.
- Write to Windows Event Log - (available only in EFT Server Enterprise) Defines the parameters to display in the Windows Event Log when the Event is triggered.
- Stop processing: If the previous trigger or Condition occurs, stop processing this Rule (default), more Rules, or this Rule and more Rules:
    - **this rule** - this Rule is not processed.
    - **more rules** - this is Rule is processed but no further Rules are processed.
    - **this and more rules** - no more Rules are processed.

For details of adding Actions to Rules, see the examples at the links above.

## Adding an Action to an Event Rule

After you have created an Event Rule and added one or more Conditions (optional) to the Rule, follow the procedure below to add one or more Actions to the Rule.

**To add an Action to a Rule**

1. In the right pane, in the **Actions** list, double-click an Action or click it, and then click **Add Action**. The Action appears in the Event in the **Rule** pane.
2. Select the linked text (blue or red) to specify parameters for the Action. For example, when you click the linked text in the **Copy** Action, the File Offload Configuration wizard appears.

**Refer to the Event Rule examples below for instructions for using the various Actions.**

- Using an Event Rule to Execute a Command (Run a Process)
- Copy/Move (push) File to Host Action
- File Uploaded Event with User Details
- OpenPGP Action
- Cleanup in folder Action
- Download (pull) File from Host Action
- E-mail Notification Action
- Stop Processing Action

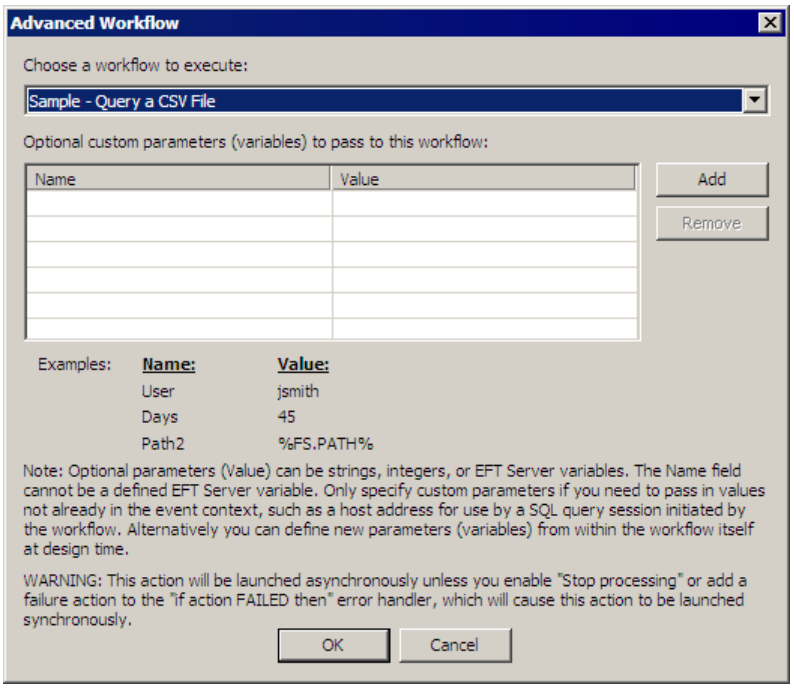
- Generate Report Action

## Execute Advanced Workflow Action

(Requires the Advanced Workflow Engine module, available in EFT Server Enterprise.) Advanced Workflow Actions execute asynchronously, which means that EFT Server does not wait for a reply before returning control to the Event Rule thread, *unless* an "if failed" Action was specified, such as **Stop Processing this Rule**, in which case the Action waits for a return message indicating success or failure from the invoked process.

**To add a Workflow to an Event Rule**

1. Create the Workflow.
2. Create an Event Rule.
3. In the **Actions** list, click **Execute Advanced Workflow**. The Action is added to the Rule.
4. In the **Rule Builder**, click the **Advanced Workflow** link. The **Advanced Workflow** dialog box appears.




1. The defined Workflows appear in alphabetical order in the **Choose a workflow to execute** list (at the top of the **Advanced Workflow** dialog box). Click the down arrow to select a Workflow.
2. (Optional) Specify custom parameters to pass to the Workflow in the **Name** and **Value** columns, and then click **Add**.
5. Click **OK**. The **Advanced Workflow** link in the **Rule Builder** updates with the name of the Workflow.
6. Add other Actions as needed, and then click **Apply** to save the changes on EFT Server.

## Send Notification E-Mail Action

You can create an e-mail notification Action for Event Rule and AS2 Transaction success/failure notifications. To save time, you can create an e-mail notification template.

*On Sites using AD Authentication, the EFT Server must have "Log On as a domain user" permission for e-mail notifications to work.*

**To customize an Event Rule e-mail message**

1. Follow the procedure in Creating Event Rules to create a new Rule or select an existing Rule to which you want to add the Action.

   *If you want to copy the involved user when the Event is triggered, the Rule must be based on a **User Event.***

2. In the **Actions** list, double-click **Send notification email** or click it, and then click **Add Action**.
3. Click the **[select]** link. The **E-Mail Notification Message** dialog box appears. The **To** box displays the first e-mail address defined in EFT Server's address book on the **SMTP** tab, but you can change that, if needed. If you want to specify a different address than the prepopulated one from the **SMTP** tab, select the **Override 'From' field** check box, and then specify the address.
4. Type the e-mail address of other recipients in the **To**, **Cc**, and **Bcc** boxes or click **To**, **Cc**, or **Bcc** to open the **Select Names** dialog box, which is populated with names and e-mail addresses defined on EFT Server in the **User Account Details** of each user account and on the SMTP tab. In the **Select Names** dialog box, you can type a name in the **Type Name or Select from List** box (not case sensitive) to find it in a heavily populated list. Select one or more recipients, and then click **To, CC**, or **BCC**. If you double-click a recipient, it is added to the **To** box. For multiple selections, press SHIFT (contiguous) or CTRL (non-contiguous). Click **OK** to save the changes.

*You can use the variable %USER.EMAIL% in the **To**, **Cc**, and **Bcc** boxes (%USER.EMAIL% is the e-mail address of the logged-in user who is uploading a file, for example, if defined in the **User Account Details** dialog box).*

5. In the **Subject** box, type a descriptive "title" for the e-mail to indicate to the recipient the purpose of the e-mail. You can also add variables. For example, if you want to see the reason an Event was triggered without opening the e-mail, add the variable `%EVENT.REASON%` to the **Subject** line.

   For example, if you add the following text and variables to the Subject Line:

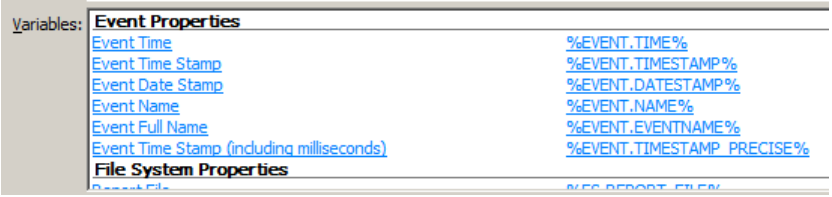
   ```
   EFT Server Notification: %EVENT.NAME%: %USER.LOGIN%, %EVENT.REASON%
   ```

   when username `jbite` uses the wrong password, an e-mail is sent with the following **Subject** line:

   ```
   Globalscape EFT Server Notification: User Login Failed: jbite, Invalid
   password
   ```

   *%EVENT.NAME% is the Server-defined name for the Event (e.g., File Renamed); %EVENT.EVENTNAME% is the user-defined name for the Event (e.g., My File Renamed Event Rule). Also, be aware that your recipient might get hundreds of e-mails every day; therefore, "Here's the info you wanted" might not be descriptive enough.*

6. In the **Message** box, type the text of the e-mail. You can use HTML tags within the body of the e-mail. (Be sure to include the opening and closing <html> and <body> tags.) You can also define an e-mail template for common e-mails and provide a link to the template in the **Message** area. If the account to which the e-mail is sent accepts HTML-formatted e-mail, you can format the e-mail to suit your needs; you are only limited by your knowledge of HTML. (If the recipient's e-mail server does not accept HTML e-mail, the recipient will see the e-mail in plain text.)
7. In the Variables box, click a property that you want to insert in the e-mail message. The text surrounded by percent signs, the *context variable*, is inserted into the body of the e-mail, and will be replaced by EFT Server with specific information about the Event when the e-mail is sent. Review the available Variables when deciding which variables to add, because some variables cannot be used in e-mail notifications.




- If you want only the information contained to the variable in your e-mail message, click the context variable in the right column of the **Variables** box. (For example, if you select %EVENT.TIME% in the right column, the time will be displayed without a text label.)
- If you want the information and a label, click the text in the left column of the **Variables** box. (For example, if you click Event Time, the label and the time appear in the e-mail).

8. If this is a User Event and you want to send a copy of the message to the involved user, select the **Send copy to user** check box.
9. Click **OK**.
10. Click **Apply**. When the Event is triggered, the e-mail notification is sent.

## Creating an E-mail Notification Template

The Conditions and Actions for every Event Rule you create, including e-mail notifications, is saved in EFT Server's configuration file. Each time the administration interface connects, it reads in the configuration file. Multiple Event Rules and e-mail notifications can grow the configuration file quite large. If you expect to have numerous e-mail notifications that are basically the same (e.g., you have default text that you always want to appear in the body of the e-mail), you can define the body of the e-mail in an HTML file, and then reference it in the **Message** box of the **E-mail Notification Message**.

**To create an e-mail notification template**

1. Create an HTML document that contains the text that will be the body of the e-mail notification. You can include any HTML tags and EFT Server variables. For example:

```
<HTML>
<BODY>
<P>This message was sent to you automatically by Globalscape EFT Server on
the following event: %EVENT.NAME%.</p>
<HR>
<P><B>Server Local Time:</B> %EVENT.TIME%</P>
<P><B>Logon Name:</B> %USER.LOGIN%</P>
<P><B>E-mail Address:</B> %USER.EMAIL%</P>
<P><B>Home Folder:</B> %USER.HOME_FOLDER%</P>
</BODY>
</HTML>
```

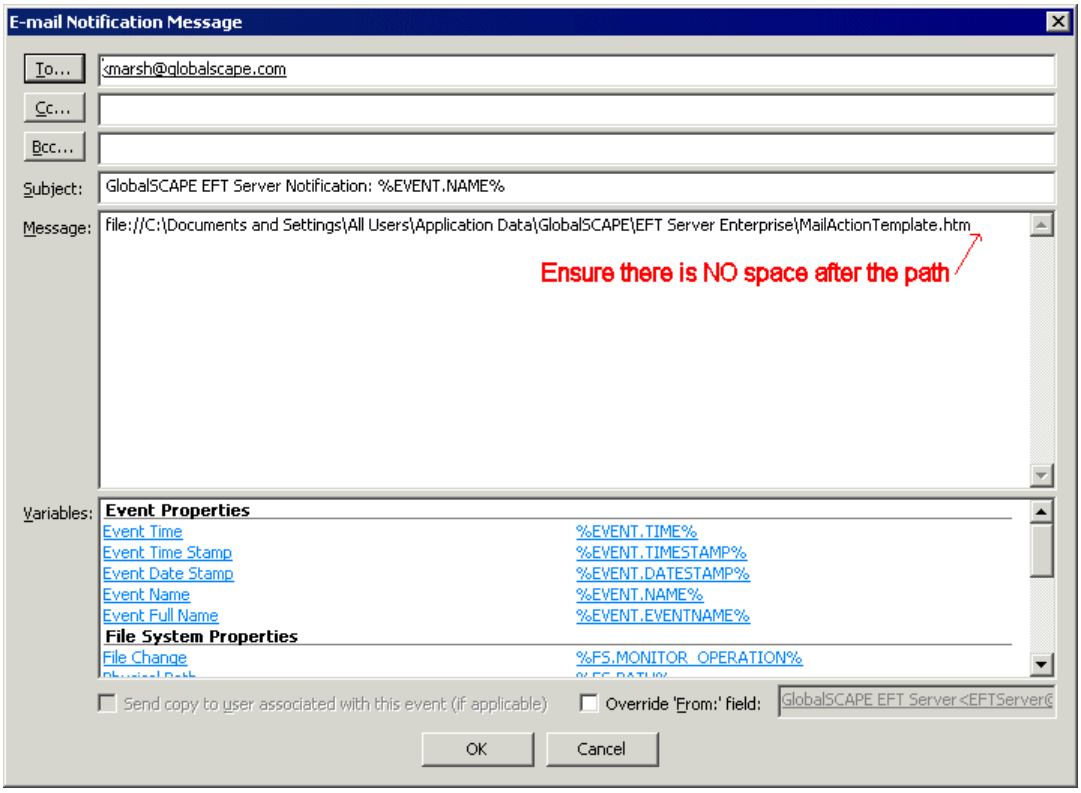
2. Define the e-mail adding each of the variables that you want. You can add your custom EFT Server administrator signature, your company's logo, any information that you need to pass on to the user, and so on. Be sure to include the opening and closing <html> and <body> tags. Use the interface to add variables and labels to the message.
3. Copy and paste the message into a text file, and save it with an **.htm** extension.

   ***Review your tags carefully, however, since no HTML-code verification is performed. As a test, you can copy and paste the text into Notepad, save it with an .htm extension, and then open it in your browser.***
4. Save the file in a location that can be accessed by EFT Server. (If you are logging into EFT Server on an Active Directory-authenticated Site, the Event Rule engine is running as that logged-in user, so the user account must have access to the template.)
5. Define the Event Rule and add the e-mail notification.

6. In the **Message** box of the **E-Mail Notification Message** dialog box, type `file://` and the path to the e-mail template, and then click **OK**. For example, type:

   ```
   file://C:\Documents and Settings\All Users\Application
   Data\Globalscape\EFT Server Enterprise\MailActionTemplate.htm
   ```

   ***IMPORTANT**: There can be no spaces or line breaks before or after the link!*




7. Click **OK** to add the notification to the Event Rule.

The referenced HTML file will appear in the body of the e-mail that is triggered by EFT Server. It is highly recommended that you do a test to be sure you get the results you want.

## Transferring Files with Event Rules

You can configure EFT Server's Event Rules to copy, move, download, upload, or offload one file or a group of files automatically based on filename, username, location, folder changes, date or time of day, or many other variables. You can copy an entire folder structure when you offload (copy/move) files.

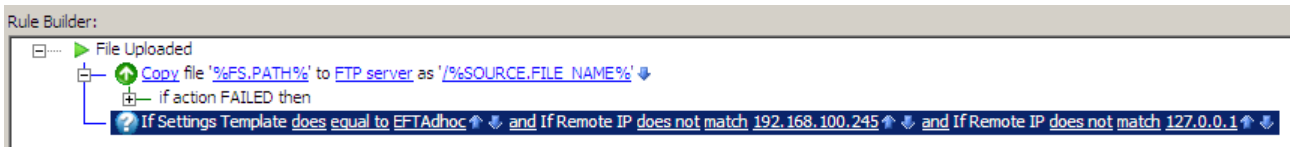
For details of copying or moving (offloading/pushing) a file to a specific server (host), refer to Copy/Move (push) File to Host Action.

For details of downloading (pulling) a file from a specific server (host), refer to Download (pull) File from Host Action.

## Copy/Move (Push) File to Host Action

**(Available in EFT Server Enterprise)** You can configure EFT Server to copy or move (also known as "offload") files to a specific location using a particular protocol whenever certain Events occur, such as when a report is created. You must provide EFT Server with connection information (protocol and login details) and file information (source path and destination path). The copy/move Action can be applied to all File System Events; the User Events "User Quota Exceeded," "User Logged in," and "User Logged Out"; and the Server Events "Timer" and "Log Rotated."

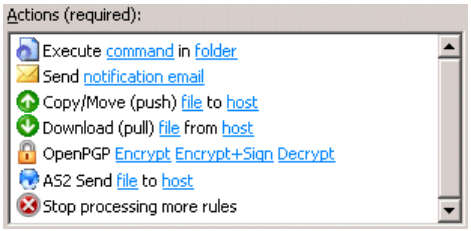
- If you create an Upload Rule that sends a file transfer activity report, the file transfer that triggered the Rule is not included in the report.
- When you add a **Copy/Move file to host** Action to a Rule, the Client FTP offload engine performs retries upon failures (network failures is the typical example) based upon the settings in the Advanced Options dialog box. Be aware that the **Copy/Move file to host** Action takes place synchronously; that is, EFT Server follows the logic of doing the transfer, including all retries, before moving on to the next Action, such as an e-mail notification. A long-running transfer that also retries numerous times with large delays will cause the Event Rule to take a long time to complete.
- If you are using Secure Ad Hoc Transfer, and if EFT Server and IIS are installed on the same computer, when creating the Event Rule for Upload notifications, create an additional Condition for "REMOTE IP does not match 127.0.0.1." The Event Rule Conditions should be something like the following example:




- A **Move** Action over the local file system updates the variables `FS.PATH`, `FS.FILE_NAME`, and `FS.FOLDER_NAME` to match the NEW file location.

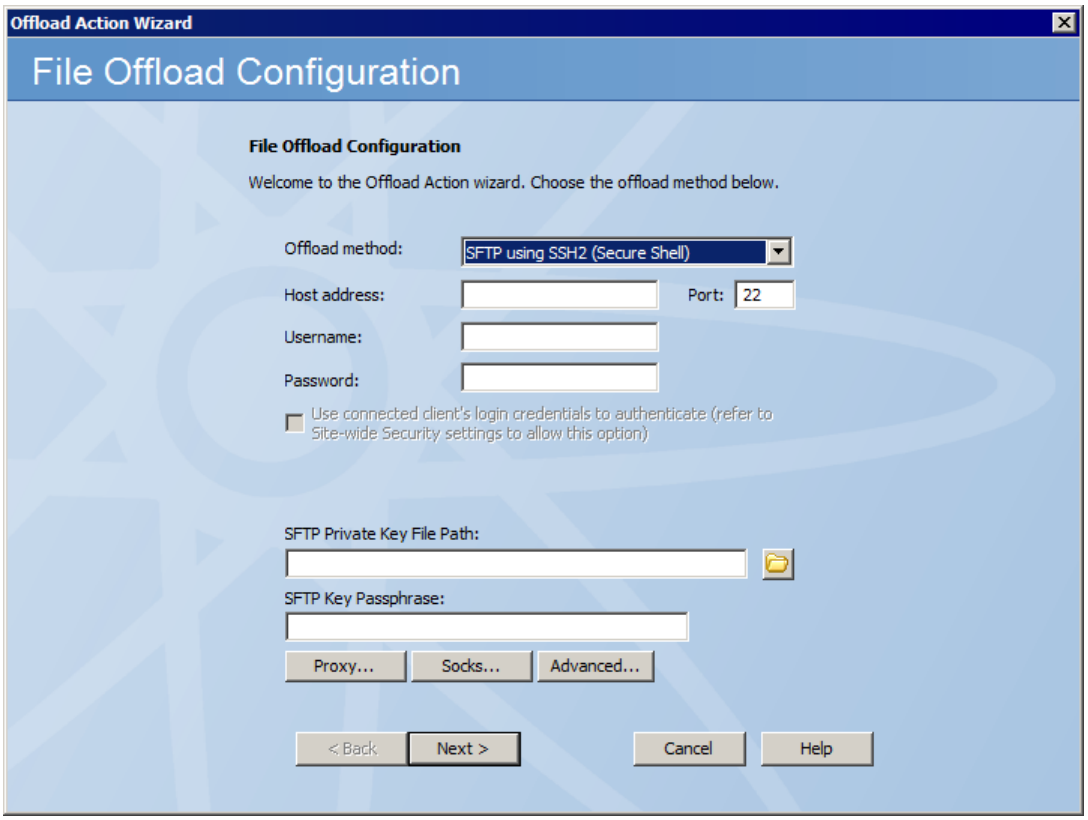
**To configure EFT Server to copy/move files**

1. Follow the procedure in Creating Event Rules, or select the Rule to which you want to add the Action. For example, create a Scheduler (Timer) Event.
2. In the right pane, in the **Actions** list, double-click **Copy/Move (push) file to host**.

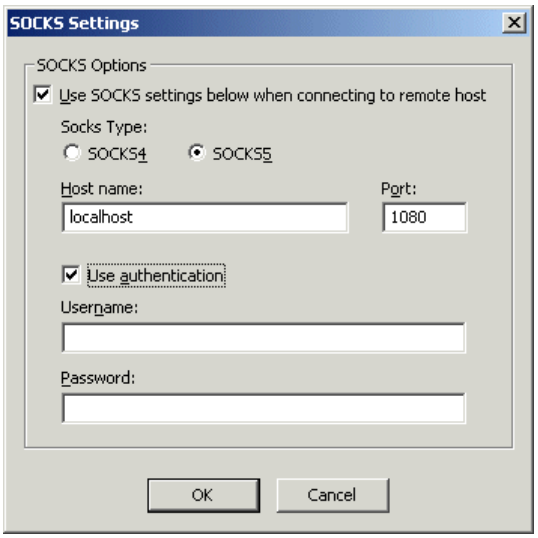



3. In the **Rule Builder**, click **Copy** to toggle between **Copy** and **Move** to choose the Action you want for this Rule.
4. In the **Rule Builder**, click one of the undefined parameters (e.g., '%FS.PATH%').


The **Offload Action Wizard** appears.




5. On the **Offload method** box, specify a protocol type for the connection.
6. (Optional) If you selected **Local (Local Files or LAN)**, provide the **Windows account** username and **Password**. These credentials are used only if/when a resource cannot be accessed using the credentials under which the EFT Server service is running.
7. If you chose anything but **Local** do the following; if you chose **Local**, skip to the Source File Path page step.
   a. In the **Host address** box, type the IP address.
   b. The **Port** number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
   c. Provide the **Username** and **Password** needed to establish the connection.
8. Select the **Use connected client's login credentials to authenticate** check box if you want to use the local system account to authenticate. The availability of this check box is controlled by the Persist username and password credentials for use in Event Rule context variables check box on the Site's **Security** tab.
9. If you chose **SFTP**, provide the client SFTP certificate information.
10. If you chose a protocol that uses SSL (FTPS or HTTPS), provide the client SSL certificate information.
11. If are connecting to a remote host through a SOCKS server, click **SOCKS**.



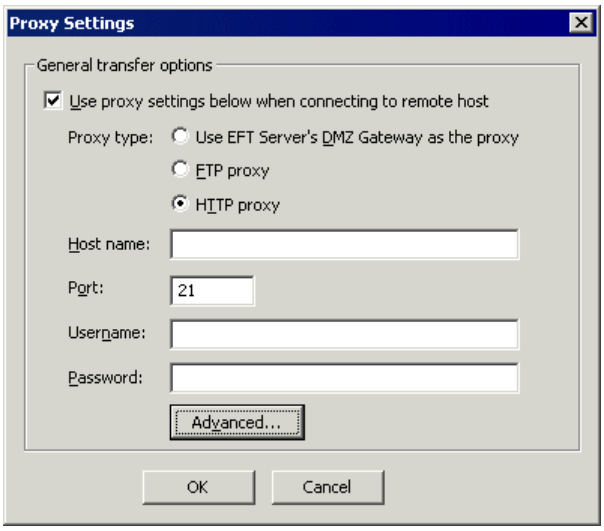

a. Specify the **Socks Type** (SOCKS4 or SOCKS5).

b. Specify the **Host name** and **Port**.

c. If you specified SOCKS5 and the server requires authentication, select the **Use Authentication** check box, and then provide a **Username** and **Password**.

d. Click **OK**.

12. If you are connecting to a remote host through a proxy, click **Proxy**. The **Proxy Settings** dialog box appears.




a. Specify the **Proxy type**, **Host name**, **Port**, **Username**, and **Password**.

> *Using the DMZ Gateway as proxy is available only in the Enterprise edition of EFT Server. Contact your system administrator for the proper host name, port, username, password, and proxy type, as well as any required advanced authentication methods.*

b. To specify an **Authentication Type** and login sequence, click **Advanced**. You must select **FTP Proxy** or **HTTP Proxy** to specify advanced settings. (Advanced proxy settings are not available when using the DMZ Gateway as the outbound proxy.)


c. Specify one of the following Authentication Types:

- **USER user@site** if your proxy server requires the USER command followed by your user name and the Site name to allow connection with a remote Site. You can change the @ symbol if a different separator is required by your proxy server.
- **SITE site** if your proxy server requires the SITE command followed by the address of the remote FTP site to allow a connection.
- **USER with logon** if your proxy server requires the USER command followed by a user name and password to allow connection with a remote Site.
- **USER/PASS/ACCT** if your proxy server requires all three commands before allowing a connection to a remote Site.
- **OPEN site** if your proxy server requires the OPEN command followed by the Site name before allowing connection to the Site.
- **Custom** if your proxy server requires a login sequence different from those above. Refer to To create a custom authentication method for a proxy server below for details of creating a login sequence.
- **To create a custom authentication method for a proxy server**

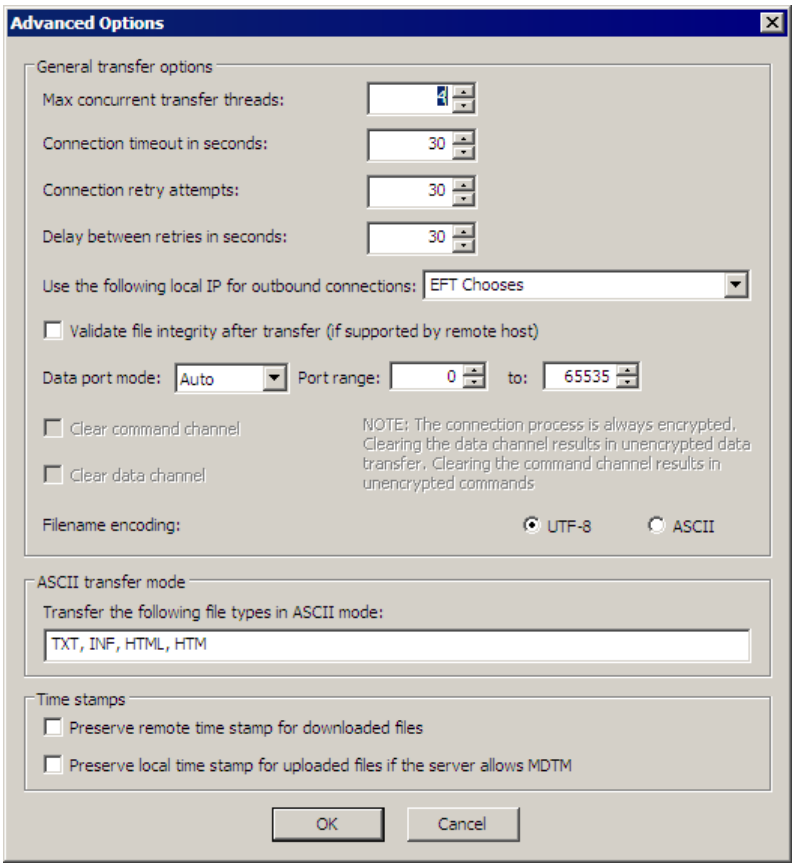
  i. In the **Advanced Proxy Settings** dialog box, click **Custom**, and then specify the login sequence in the text box using the following variables: %host%, % user%, %pass%, %port%, %fire_pass%, %fire_user%. Be sure to type each variable with percent signs before and after, and press ENTER to separate commands.

  ii. Type any other commands and variables, separating commands with a line break (press ENTER).

  iii. Click **OK** to accept the changes and close the **Advanced Proxy Settings** dialog box.

d. Click **OK** to accept the changes and close the **Proxy Settings** dialog box.

13. To specify transfer options and time stamps, in the Offload wizard, click **Advanced**. The **Advanced Options** dialog box appears.




a. In the **General transfer options** area, you can provide more control over **Max concurrent transfer threads**, **Connection timeout**, **Connection retry attempts**, and **Delay between retries**. When files are being transferred with Event Rules (copy/move), if there are connection problems (e.g., the network is unavailable), the server will attempt to establish a connection the number of times specified in **Connection retry attempts**. When EFT Server is able to re-establish the connection, it continues to transfer the file even if there are multiple interruptions.

b. In the **Use the following local IP for outbound connections** box, click the list box to specify which local IP address to use for the proxy or keep the default of **EFT Chooses** to let the EFT Server decide which local IP address to use.

c. Select the **Validate file integrity after transfer** check box to specify that EFT Server should double check binary files to ensure the files downloaded completely and correctly. (Not applicable to SFTP.)

d. In the **Data port mode** box, click the drop-down list and select one of the following (not applicable to SFTP):

- **Auto**—When Auto is selected, EFT Server initially makes connections in PASV mode. If the PASV connection fails, EFT Server attempts to connect in PORT mode automatically.
- **Active**—When Active mode is selected, EFT Server opens an additional port and tells the remote server to connect to <IP:PORT_RANGE> to establish a data connection. This is useful when the server is behind a firewall that closes all unnecessary ports. If you select this mode, specify the port range from which the client will choose. (For security best practices, Active mode is not allowed when brokering outbound connections through DMZ Gateway.)

- **Passive**—When Passive mode is selected, EFT Server tells the remote server to provide <IP:PORT> to which EFT Server can connect to establish a data connection. This is useful when a client is behind a firewall that closes all unnecessary ports. Helps avoid conflicts with security systems.

e. Select the **Clear command channel** check box to send FTP commands in clear text. (Only available when FTPS is specified.)

f. Select the **Clear data channel** check box to transfer files without encryption. (Only available when FTPS is specified.)

g. In the **Filename encoding** area, specify whether the filename is encoded as **UTF-8** or **ASCII**.

- To conserve Unicode file **names**, the remote server must support UTF-8 and advertise UTF-8 in its FEAT command.
- To conserve Unicode file **content** you must transfer the file using binary transfer mode or save the file using UTF-8 encoding before offloading it in ASCII mode. (Refer to Knowledgebase article #11113 for more information.)
- To enforce binary transfer mode for text files with UTF-8 encoded content, you should remove all the extensions from the **ASCII transfer mode** area in the next step or transfer files with extensions that don't match those on the ASCII types list.
- Text (ASCII) files transferred in binary mode will retain their carriage return (CR) and line feed (LN) hidden characters which are not supported by *nix systems by default.

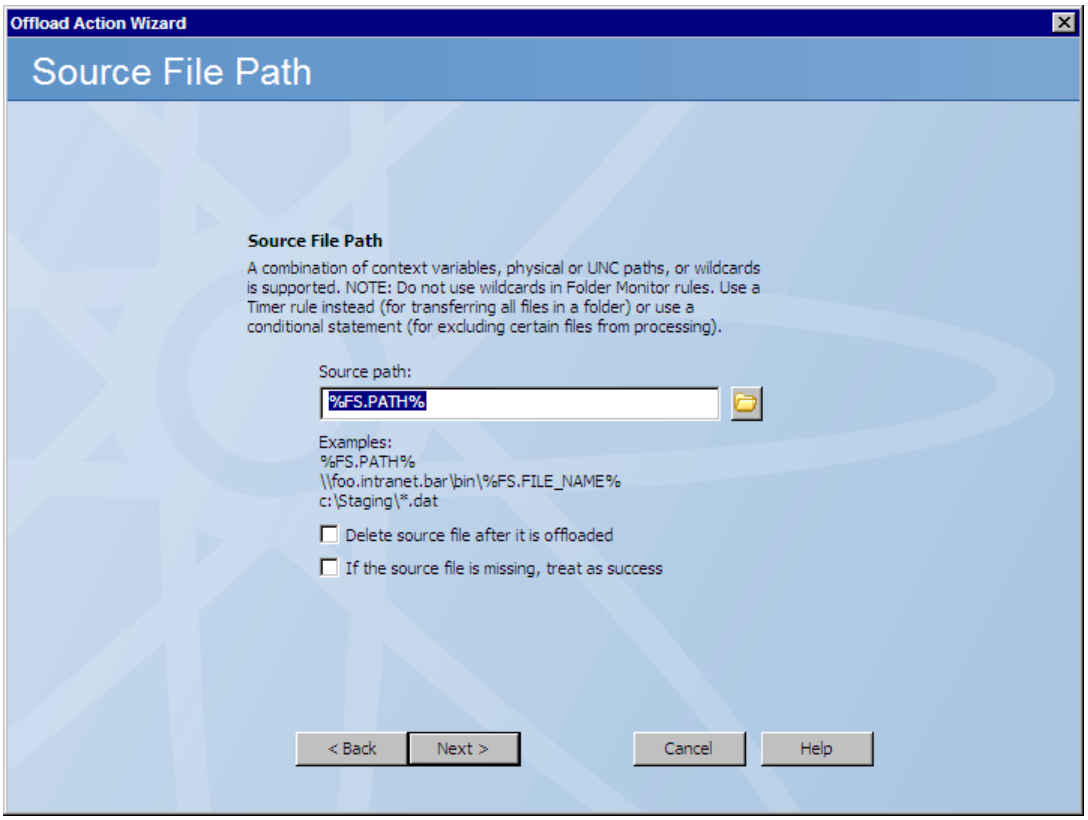
h. In the **ASCII transfer mode** area, specify the file types that can be transferred. Use a comma ***and a space*** between extensions. If you use only a comma with no space, and then the Rule will not recognize the extension/file type. TXT, INF, HTML, and HTM are specified by default. If an asterisk (*) is specified, all files are downloaded in ASCII mode, even if that file doesn't have an extension. (To conserve Unicode file **content**, you must transfer the file using binary transfer mode. To force download in binary, clear the file types box.)

i. In the **Time stamps** area, select one of the following:

- Select the **Preserve remote time stamp for downloaded files** check box to keep the time stamp the same on the destination file as it is on remote file.
- Select the **Preserve the local time stamp for uploaded files if the server allows MDTM** check box to keep an uploaded file's time stamp the same on remote server as it is on the source file system. (Not applicable to SFTP.)

j. Click **OK**.

14. Click **Next**. The **Source File Path** page appears.

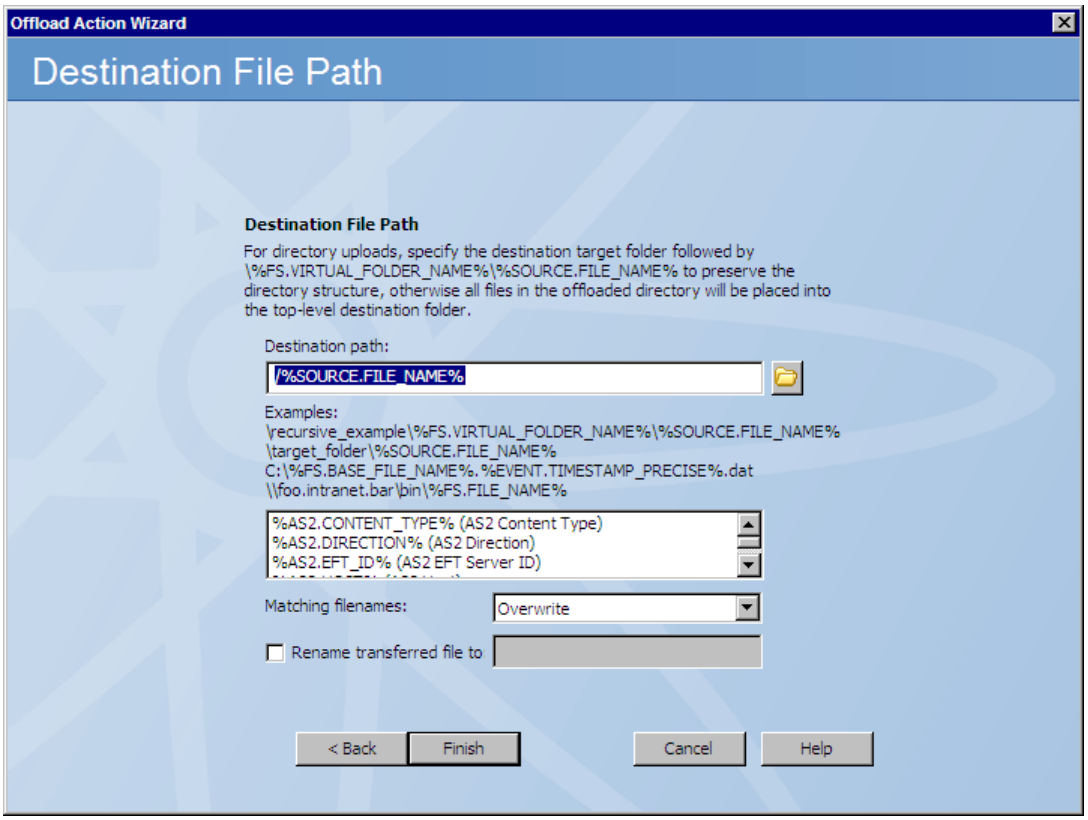



15. In the **Source path** box, provide the path to the file(s) that you want to offload. (No validation is performed.) For example, type:

    C:\Staging*.dat or \\mydomain\common\jsmith\file.txt

> *You can leave **Source path** blank or use %FS.PATH% to offload the files associated with the Event that triggered the Action. In a Timer Event, there is no context variable available for the path, so you must specify a filename.*

16. Select the **Delete source file after it has been offloaded** check box if you want to delete the file after it is copied/moved. (If the file is marked read-only, it will not be deleted.)
17. Select the **If the source file is missing treat as success** check box if you want the Action to be considered successful even if the source file is missing.
18. Click **Next**. The **Destination File Path** page appears.




19. In the **Destination path** box, specify the location in which to save the offloaded file. (No validation is performed when you type a path; the Folder icon is only available for local transfers.)

> *If you type a path to a folder that does not exist, the Event Rule will fail. Be sure you have the path defined correctly, e.g., make sure to use the proper slash. In general, forward slashes / are used in remote paths, and backward slashes \ are used in local Windows paths. Do not use both.*

- You can specify variables, such as `\pub\usr\%USER.LOGIN%\%FS.FILE.NAME%`.
- In the **Variables** box, double-click the variable(s) that you want to add to the path.
- In *Move* Actions over the LOCAL FILE SYSTEM, the %FS.PATH%, %FS.FILE_NAME%, and %FS.FOLDER_NAME% context variables are updated to match the new file location.
- In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, **Smart Overwrite**, or **Numerate** files that exist with the same name. (Refer to Smart Overwrite for more information about Smart Overwrite.)
    - **Overwrite**—Overwrite any existing file with the same name.
    - **Skip**—Skip the offload if a file with the same name exists in the destination directory.
    - **Smart Overwrite**—EFT Server performs a CRC match for the files. If the files are identical, the destination file is not overwritten. Refer to Smart Overwrite for more information about this feature.
    - **Numerate**—If a file in the destination folder has the same name as the file you are transferring, EFT Server renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT Server renames the transferred file to "Copy (2) of file.txt" and so on.

- If you want to rename the file, select the **Rename transferred file to** box and specify a new name.
    - You can rename the file when it is transferred. For example, when "myfile.doc" is uploaded, you might want to save it as "status_%EVENT.DATESTAMP%.doc" or something else more identifiable.
    - You can also use variables in the **Rename transferred file to** box. For example, /%FS.FILE_NAME%.%EVENT.TIMESTAMP%
    - For LAN renames, you must include the full path to the file.
    - EFT Server executes a RNFR + RNTO sequence for FTP transfers on the remote server. If the remote server supports cross-folder rename (as EFT Server does), it is possible for Rename-Pathname-Filename variable to point to a different folder than the Offload Destination folder.
    - The Offload transaction status will be FAILED if the rename fails, even though the file was transferred.
    - The **Status Viewer** will display the Rename-To value in the **Remote Path** field for Offload.

20. Click **Finish** then click **Apply** to save the changes on EFT Server and/or add other Actions and Conditions to the Rule.

    If you are copying or moving the file to another location, and the file upload is a regularly occurring Event with a file of the same name, in the **Offload Action** wizard, add the variables `%EVENT.DATESTAMP%` and/or `%EVENT.TIMESTAMP%` to the path so that the date (YYYYMMDD) and/or time (HHMMSS) are added to the filename when it is moved/copied. Do ***not*** use `%EVENT.TIME%`, because the colon (e.g., `28 Aug 07 10:01:56`) makes it unsuitable for file naming.

    For example, in the **Offload Action wizard**, in the **Destination path** box, provide the path and variables. For example, type:

    ```
    C:\Documents and Settings\Administrator\My
    Documents\upload\%EVENT.DATESTAMP%_%EVENT.TIMESTAMP%_%FS.FILE_NAME%
    ```

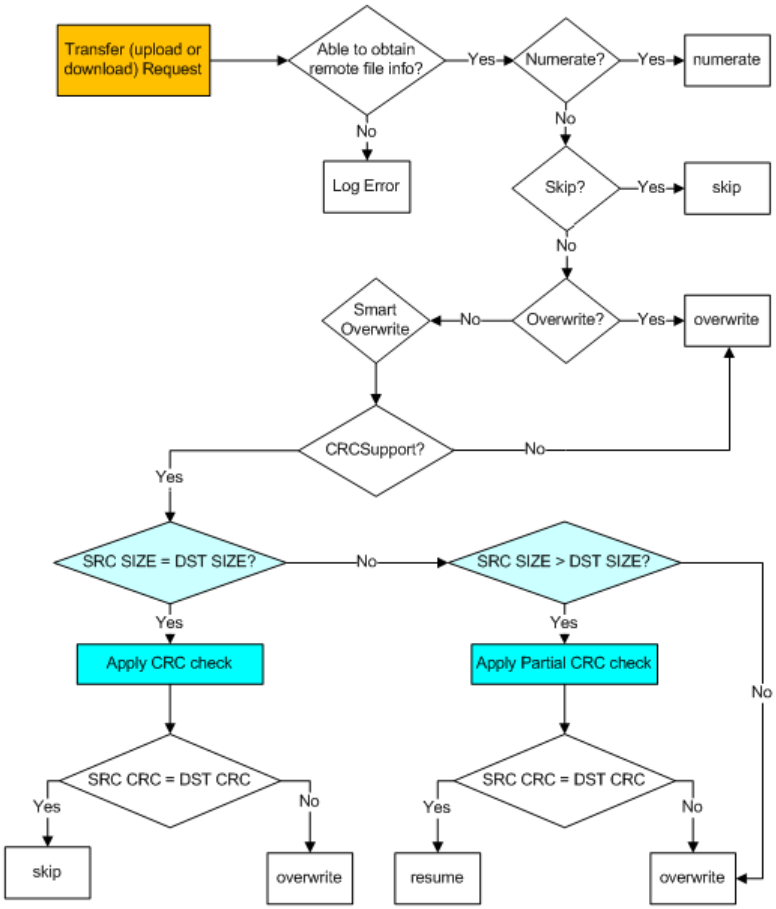
    With this path and variables, when a file is uploaded to the monitored folder, the file is moved to \My Documents\upload and the date and time are prepended to the filename. For example, 20080422_101212_mydailyprogress.doc.

## Smart Overwrite

On the **Destination File Path** page of the Copy/Move Action wizard, you can specify what EFT Server is to do if the file you are copying or moving has the same file name as a file in the destination path. Depending on what it detects, Smart Overwrite can overwrite the file in the destination path, skip the copy/move, numerate the copied/moved file, or overwrite the destination file after performing a CRC match of the files.

- **Overwrite =** Overwrite any existing file with the same name.
- **Skip =** Skip the offload if a file with the same name exists in the destination directory.
- **Numerate =** If a file in the destination folder has the same name as the file you are transferring, EFT Server renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT Server renames the transferred file to "Copy (2) of file.txt" and so on.
- **Smart Overwrite =** EFT Server performs a CRC match of the files.
    - If the destination and source file sizes are the same, then the CRC determines whether it should skip the file or overwrite the file. If the file contents are identical, the destination file is not overwritten.

- If the destination size is ***smaller*** than the source size (meaning a partial file likely exists in the destination file path), then EFT Server will perform CRC on the portion of the source file that matches the length of the destination file. If the contents match, then EFT Server resumes the download. If they do not match, then the file is overwritten.
- If the destination file size is ***larger*** than the source file, then EFT Server overwrites the file without performing CRC first.



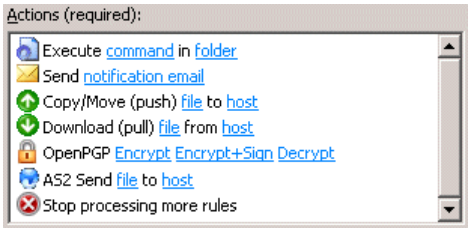

## Download (Pull) File from Host Action

**(Available in EFT Server Enterprise)** You can configure a Server Event Rule to copy or download from a specific location to a specified local folder using a particular protocol when an Event occurs. You must provide EFT Server with connection information (protocol and login details) and file information (source path and destination path). The Download Action is available with all Events except Site Stopped and Service Stopped.

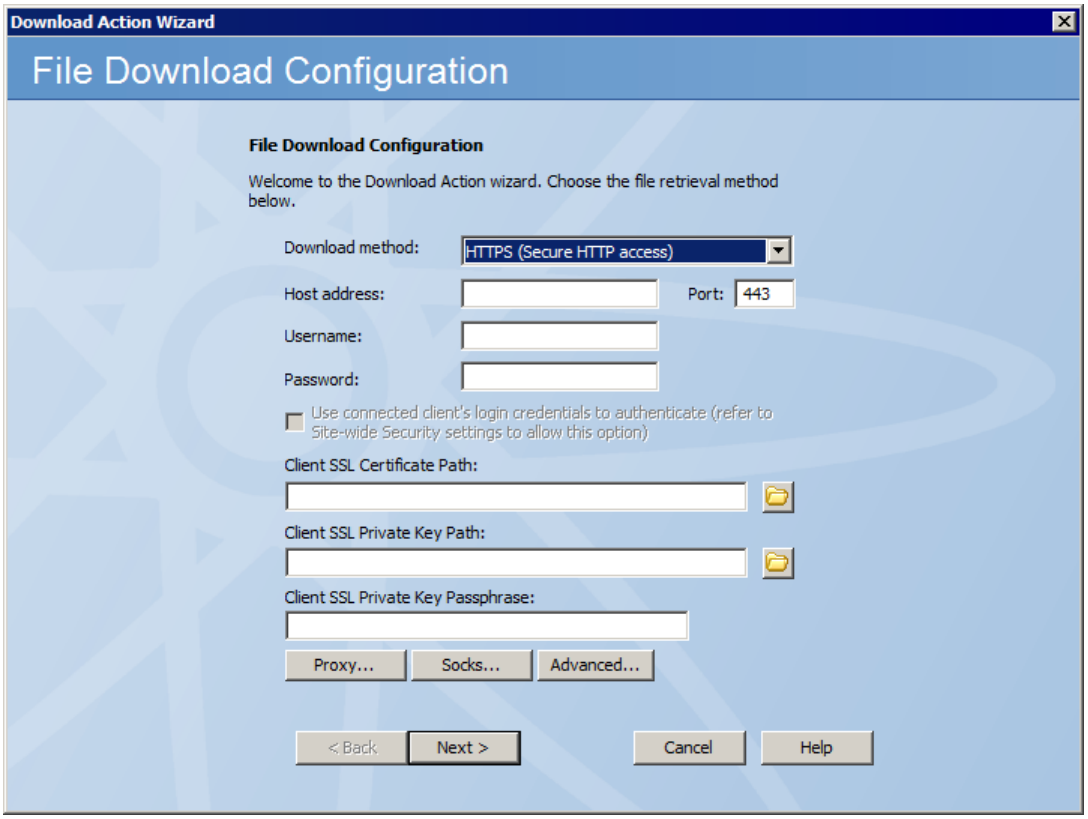
When you add a **Download file from host** Action to a Rule, the Client FTP offload engine performs retries upon failures (network failures is the typical example) based upon the settings in the Advanced Options dialog box. Be aware that the **Download file from host** Action takes place synchronously; that is, EFT Server follows the logic of doing the transfer, including all retries, before moving on to the next Action, such as an e-mail notification. A long-running transfer that also retries numerous times with large delays will cause the Event Rule to take a long time to complete.

**To set up EFT Server to download files**

1. Follow the procedure in Creating Event Rules or select the Rule to which you want to add the Action.
2. In the **Actions** list, click **Download (pull) file from host**. The Rule parameters are added to the Rule in the **Rule** pane.




3. Click one of the undefined parameters where the parameters are listed in the **Rule** pane. The **Download Action** wizard appears.

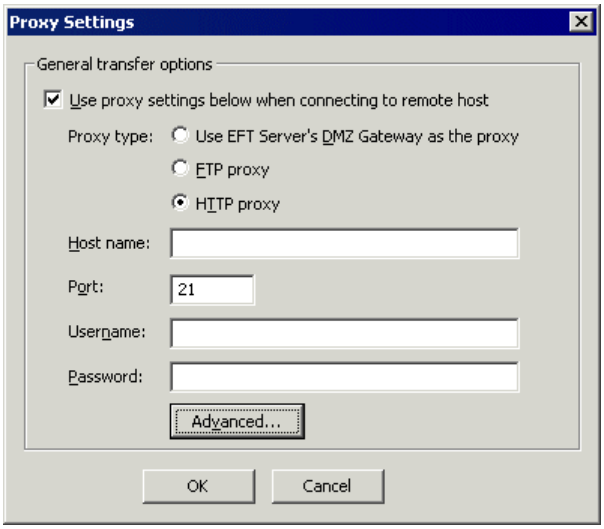



4. Click the list to specify a **Download method** for the connection: **Local (Local File or LAN)**, **FTP (standard File Transfer Protocol)**, **FTP SSL/TLS (AUTH TLS)**, **FTP with SSL (Explicit encryption)**, **FTP with SSL (Implicit encryption)**, **SFTP using SSH2 (Secure Shell)**, **HTTP (HyperText Transfer Protocol)**, **HTTPS (Secure HTTP access)**.
5. (Optional) If you selected **Local (Local Files or LAN)**, provide the **Windows account** username and **Password**. These credentials are used only if/when a resource cannot be accessed using the credentials under which the EFT Server service is running.
6. If you chose anything but **Local** do the following; otherwise, skip to the Source File page step.
   a. In the **Host address** box, type the IP or host address of the EFT Server to which you want to connect.

b. The **Port** number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.

c. In the **Username** and **Password** boxes, type the username and password used to authenticate.

7. Select the **Use connected client's login credentials to authenticate** check box if you want to use the local system account to authenticate. The availability of this check box is controlled by the Persist username and password credentials for use in Event Rule context variables check box on the Site's **Security** tab.
8. If you chose **SFTP**, provide the client SFTP certificate information.
9. If you chose a protocol that uses SSL (**FTPS** or **HTTPS**), provide the client SSL certificate information.
10. If you connect to EFT Server through a proxy server, click **Proxy**. The **Proxy Settings** dialog box appears.




a. Specify the **Proxy type**, **Host name**, **Port**, **Username**, and **Password**.

*Using the DMZ Gateway as proxy is available only in the Enterprise edition of EFT Server. For security best practices, selecting PORT mode in the **Advanced Options** dialog box below is not allowed when brokering outbound connections through DMZ Gateway.*

b. To specify an **Authentication Type** and login sequence, click **Advanced**. You must select **FTP Proxy** or **HTTP Proxy** to specify advanced settings.


c. Specify one of the following Authentication Types:

- **USER user@site** if your proxy server requires the USER command followed by your user name and the Site name to allow connection with a remote Site. You can change the @ symbol if a different separator is required by your proxy server.
- **SITE site** if your proxy server requires the SITE command followed by the address of the remote FTP site to allow a connection.
- **USER with logon** if your proxy server requires the USER command followed by a user name and password to allow connection with a remote Site.
- **USER/PASS/ACCT** if your proxy server requires all three commands before allowing a connection to a remote Site.
- **OPEN site** if your proxy server requires the OPEN command followed by the Site name before allowing connection to the Site.
- **Custom** if your proxy server requires a login sequence different from those above. Refer to the procedure below for details of creating a custom authentication method (login sequence).
- **To create a custom authentication method for a proxy server**

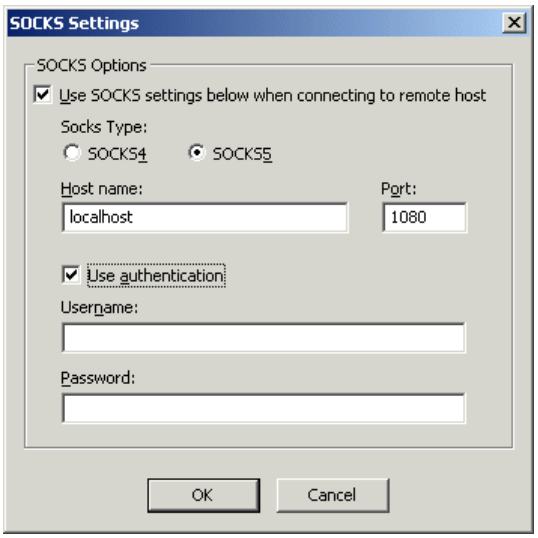
  i. In the **Advanced Proxy Settings** dialog box, click **Custom**, and then specify the login sequence in the text box using the following variables: %host%, % user%, %pass%, %port%, %fire_pass%, %fire_user%. Be sure to type each variable with percent signs before and after, and press ENTER to separate commands.

  ii. Type any other commands and variables, separating commands with a line break (press ENTER).

  iii. Click **OK** to accept the changes and close the **Advanced Proxy Settings** dialog box.

*Contact your system administrator for the proper Host name, Port, User name, Password, and proxy type, as well as any required advanced authentication methods.*

11. Click **OK** to accept the changes and close the **Advanced Proxy Settings** dialog box.
12. If you connect to EFT Server through a Socks server, click **SOCKS**.



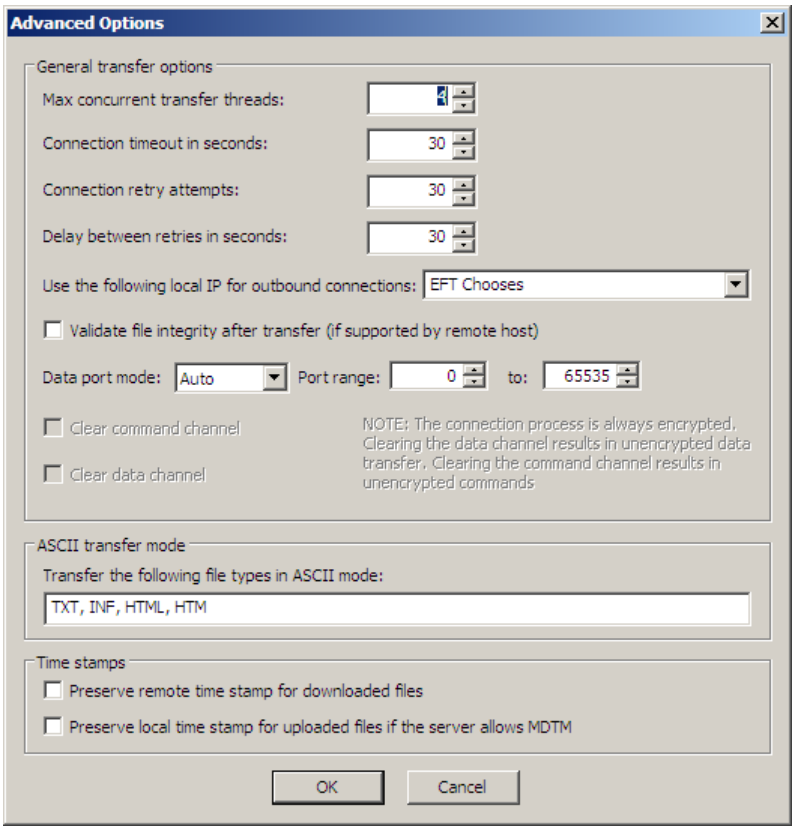

a. Specify the **Socks Type** (SOCKS4 or SOCKS5).

b. Specify the **Host name** and **Port**.

c. If you specified SOCKS5 and the server requires authentication, select the **Use Authentication** check box, and then provide a **Username** and **Password**.

d. Click **OK** to save the changes and close the SOCKS Settings dialog box.

13. To configure advanced transfer options, in the **Download Action** wizard, click **Advanced**. The **Advanced Options** dialog box appears.



a. In the **General transfer options** area, you can provide more control over **Max concurrent transfer threads**, **Connection timeout**, **Connection retry attempts**, and **Delay between retries**. When files are being transferred with Event Rules (copy/move), if there are connection problems (e.g., the network is unavailable), the Server will attempt to establish a connection the number of times specified in **Connection retry attempts**. When EFT Server is able to re-establish the connection, it continues to transfer the file even if there are multiple interruptions.

b. If the computer has multiple IP addresses available and/or both IPv4 and IPv6 addresses, you can let EFT Server choose which IP address to use or you can specify which one it is to use. If you do not want EFT Server to choose, in the **Use the following local IP for outbound connections** box, click the menu to specify an address.

c. Select the **Validate file integrity after transfer** check box to specify that EFT Server should double check binary files to ensure the files downloaded completely and correctly. (Not applicable to SFTP.)

d. In the **Data port mode** box, click the drop-down list and select one of the following (not applicable to SFTP):

- **Auto**—When Auto is selected, EFT Server initially makes connections in PASV mode. If the PASV connection fails, EFT Server attempts to connect in PORT mode automatically.
- **Port**—When Port mode is selected, EFT Server opens an additional port and tells the remote server to connect to <IP:PORT_RANGE> to establish a data connection. This is useful when the server is behind a firewall that closes all unnecessary ports. If you select this mode, specify the port range from which the client will choose.
- **Pasv**—When Pasv mode is selected, EFT Server tells the remote server to provide <IP:PORT> to which EFT Server can connect to establish a data connection. This is useful when a client is behind a firewall that closes all unnecessary ports. Helps avoid conflicts with security systems

e. Select the **Clear command channel** check box to send FTP commands in clear text. (Only available when FTPS is specified.)

f. Select the **Clear data channel** check box to transfer files without encryption. (Only available when FTPS is specified.)

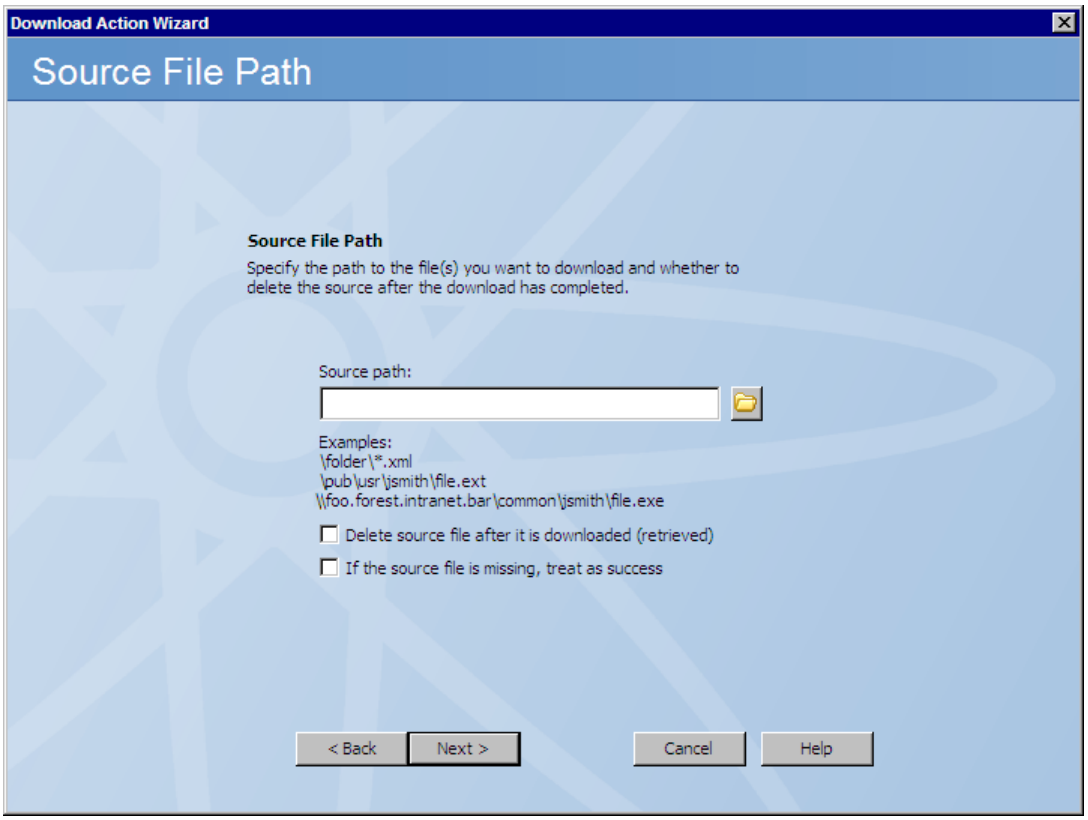
g. In the **ASCII transfer mode** area, specify the file types that can be transferred. TXT, INF, HTML, and HTM are specified by default. If an asterisk (*) is specified, all files are downloaded in ASCII mode, even if that file doesn't have an extension. (To conserve Unicode file **content**, you must transfer the file using binary transfer mode. To force download in binary, clear the file types box.)

h. In the **Time stamps** area, select one of the following:

- Select the **Preserve remote time stamp for downloaded files** check box to keep the time stamp the same on the destination file as it is on remote file.
- Select the **Preserve the local time stamp for uploaded files** if the server allows MDTM check box to keep the time stamp the same on the remote file as it is on the source file. (Not applicable to SFTP.)

i. Click **OK** to accept the changes and close the **Advanced Options** dialog box.

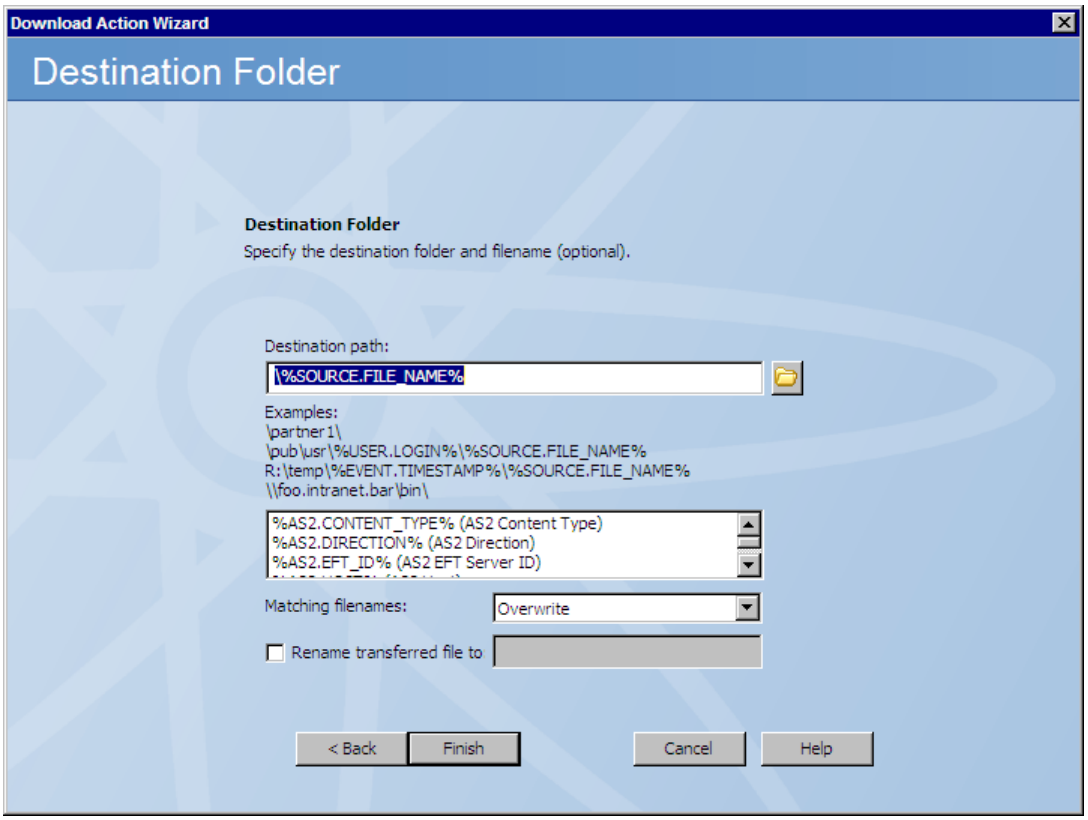
14. Click **Next**. The **Source File Path** page appears.




15. In the **Source path** box, provide the path to the file(s) that you want to download. For example, type:
`/pub/usr/jsmith/file.txt or \\mydomain\common\jsmith\file.txt`

> *If you type a path to a remote folder that does not exist, the Event Rule will fail.*

16. Select the **Delete source file after it is downloaded** check box if you want to delete the file after it is retrieved. (If the file is marked read-only, it will not be deleted.)
17. ***For LAN/local transfers only***, select the **If the source file is missing treat as success** check box if you want the Action to be considered successful even if the source file is missing.
18. Click **Next**. The **Destination File Folder** page appears.




19. In the **Destination folder** box, click the folder icon and specify the location in which to save the downloaded file. You can insert variables by double-clicking them in the box below the **Destination folder** box.

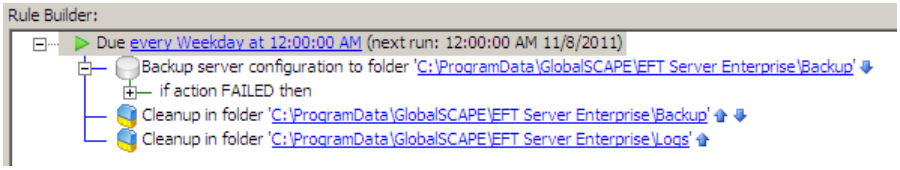
*If you type a path to a remote folder that does not exist, the Event Rule will fail.*

- In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, or **Numerate** files that exist with the same name. If **Overwrite** is selected, EFT Server performs a CRC match for the files.

20. Click **Finish**, and then click **Apply** to save the changes on EFT Server and/or add other Actions and Conditions to the Rule.

## Cleanup in Folder Action

**(Available in EFT Server Enterprise)** When you create your first Site, a Timer Rule is created that runs the **Backup Server Configuration** Action once each day at midnight, using all defaults for naming and backup location (\backup\Server Configuration Backup [Month] [Day] [Year].bak). The Rule includes a **Cleanup in folder** Action to delete backup files (*.bak) older than 30 days in that same folder and another **Cleanup in folder** Action to remove old log files. This **Backup and Cleanup** Rule is enabled by default, but you can disable it and edit it as necessary.



The **Cleanup in Folder** Action is available only with the **On Timer** Server Event. At the interval that you specify, EFT Server compares the filter parameters of the Cleanup in folder Action to the files in the designated folder, then determines the creation or modification time of the file and deletes ("cleans up") files that match the cleanup parameters. For example, if you specify to cleanup files that are older than 7 days named **dailyreport*.doc** in the folder **D:\WorkFolder\Sales\Daily Reports**, any Microsoft Word files in that folder with **dailyreport** in the file name are deleted after 7 days. However, if you create a **Cleanup in folder** Action and set a file to be cleaned after 7 days, but then modify the file on the 6th day, the file will not be deleted until 7 days after the modification date.

**To set up EFT Server to cleanup files**

1. Follow the procedure in Creating Event Rules to create a **Scheduler (Timer) Event**. The Event Rule appears in the **Rule Builder**.
2. In the Actions list, double-click **Cleanup in folder**. The Action is added to the Rule in the **Rule Builder**.
3. In the **Rule Builder**, click the **'[select]'** link. The **File Cleanup in folder Action Parameters** dialog box appears.
4. In the **Delete file(s) older than <n>** box, specify the minimum age of a file to delete from the folder. The default is 7 days.
5. In the **Folder** box, click the folder icon to specify the folder that you want to clean up.
6. To clean up subfolders in the specified folder, select the **Include sub-folders** check box.
7. If you don't want to delete all of the files older than a certain age, create a **File delete filter mask**. In the **Filenames** box, an asterisk appears by default, which means delete all files. You can **Include** or **Exclude** specific files from the **Cleanup in folder** Action, and/or use wildcards for file types, partial names, and so on.

   For example, the **Backup and Cleanup** Event Rule that is defined automatically in EFT Server Enterprise is configured to delete all *.bak files in **C:\ProgramData\GlobalScape\EFT Server Enterprise\Backup** that are older than 30 days.

   Or, maybe you want delete everything in the folder except for the files with "new" in the file name. To do that, you would click **Exclude** and then in the **Filenames** box, type ***new***.
8. Click **OK** to close the dialog box.
9. Click **Apply** to save the changes on EFT Server.

## Sending Files to an AS2 Partner via Event Rules

**(Available in EFT Server Enterprise)** You can send files via AS2 to a partner for whom you have not previously provisioned an outbound profile by manually specifying that partner's profile in the **AS2 Send File** Event Rule Action. Alternatively, if the AS2 partner has an outbound profile defined, you can select that profile when you define the **AS2 Send File** options.

For example, you could define a Rule with a Timer Event so that every Monday at 8 a.m., all files in a certain folder are sent either to a partner that already has a profile defined on the Server or to a partner that you will define "on the fly" in the **AS2 Send File** dialog box.

*The **AS2 Send File to host** Action is a synchronous Event even if asynchronous MDN receipts are requested. Synchronous means that the Event Rule executes Actions sequentially from top to bottom; when EFT Server encounters an AS2 outbound Action, it performs the transfer, and then if MDN is synchronous, EFT Server waits for the result before moving to the next Action (with success/failure set appropriately). If MDN is asynchronous, EFT Server proceeds to the next Action based only on the HTTP result of the SEND operation, NOT the result of the asynchronous MDN receipt.*

The **AS2 Send File to host** Action can be used for Folder Monitor, Timer, and all file-based Events.

*UTF-8 filenames/non-ASCII characters are not supported over the AS2 protocol. It is the responsibility of the trading partners to determine the file-naming limits imposed by their trading environments. Refer to RFC 2183, section 2.3 for details of filename parameters.*

When triggered, the **AS2 Send File to host** Action offloads one or more user-defined files or one or more context files. Depending on the **AS2 Send File to host** Action's retry configuration, the Action fails if any error occurs when attempting to send the AS2 payload. Those errors may include any connection, authentication, transport, or navigation errors; receipting errors or failures; payload errors, including transfer errors or integrity mismatch errors or failures; server communicated errors; and unknown or undefined errors, such as:

- No receipt was provided
- The receipt was not signed
- The MIC value returned did not match the original file/message MIC
- EFT Server was unable to:
    - verify the receipt signature
    - establish a connection to the remote host
    - upload the file to the remote host
    - send an the receipt asynchronously
    - send the receipt synchronously

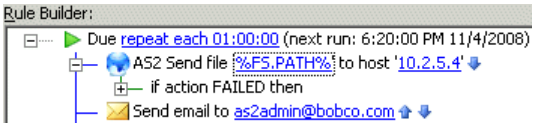
**To send files using the AS2 Send File to host Action**

1. Create a new Event Rule, such as a Scheduler (Timer) Event. (Refer to Creating Event Rules for details of creating Event Rules, if necessary.)
2. Add the **AS2 Send file to host** Action to the Rule, and then click one of the underlined text links. The **AS2 Send File** dialog box appears.
3. In the **File(s) to upload** box, type the path or click the folder icon to specify the file to send to this partner. Include the entire path to the file. You can also use File System context variables such as %FS.PATH% or wildcard masks. For example, to send all files in a folder, type the folder path and ***.***. (The files will not be sent all at once; each file will have a unique message ID.)
4. In the **Partner Configuration** area, specify the AS2 Partner profile using one of the following methods:
    - In the **Partner profile** box, select a defined AS2 outbound partner profile. The fields in the **AS2 connection details** area is completed automatically.
    - Provide the connection details in the **AS2 connection details** area. (Refer to AS2 Send File Dialog Box Fields below for details of each field.)
    - Click **Setup Wizard** to use the wizard to set up the profile.

    *The **Partner profile** box is linked to the selected profile configuration. If you are using Globalscape authentication, if the profile is updated, the information in the **AS2 Send File** dialog box is updated also; if a referenced profile is deleted, disabled, or not allowed to use AS2, any Event Rule using the profile will fail.*

    *When you use AD, LDAP, or ODBC authenticated accounts as AS2 partners, if the account in the external database is changed, deleted, or disabled, any Event Rule or Command that references the account will fail. For example, if an AD user SSmith is renamed SJones, you will have to update any Event Rule or Command manually to reflect the new name of the account.*
5. To test the configuration, click **Test.**

6. To configure a proxy server for this partner, click **Proxy**.
7. To clear all of the partner connection details and start over, click **Clear All**.
8. Click **OK** to save the AS2 Partner profile in the Event Rule.
9. Add other Conditions and/or Actions, as needed (e.g., add an e-mail notification).




10. Click **Apply** to save the Event Rule on EFT Server.

## AS2 Send File Dialog Box Fields

The AS2 Send File dialog box can be used in Folder Monitor, Timer, and file-based Event Rules. The table below describes each field in the **AS2 Send File** dialog box.

| Field | Required/Optional | Description |
|---|---|---|
| File(s) to upload | Optional | Used to specify the file(s) to upload to the partner.<br>Can be variables or paths. e.g. **c:\temp\robert.txt** or (if relative path) **\rob.txt**<br>Defaults to %FS.FILE_NAME%; same as if blank. Accepts FS.FILE variables and path strings to drive or UNC paths or relative path where applicable (e.g., if using a Folder Monitor Rule). |
| Partner profile | Required | Used to select a defined partner profile or left blank (the default) if the partner profile is not defined. If blank, complete the fields in the **AS2 Partner profile** area. |
| Delete source | Required | Used to indicate whether to delete sources files after sending them to the destination, after the MDN is received and verified from the remote AS2 host. Select the check box to delete source files after the MDN is received and verified from the remote AS2 host. |
| Host address | Required | AS2 outbound host address. Requires protocol prefix in URL (http:// or https://). Specified in **AS2 Partner Access** wizard. |
| Port | Required | AS2 Outbound port. Range is 1-65K; defaults to 80 if host address is preceded by http; 443 if host address is preceded by https. |
| Path (a.k.a. inbox, outbox, or mailbox) | Optional | Relative path (similar to User Home Folder); forward slash ( / ) by default |
| Username | Optional | User login name |
| Password | Optional | Password |
| Message subject | Optional | AS2 message subject |
| Content type | Required | AS2 content type. Options include:<br>• **X12** - Format used by many healthcare, insurance, government, transportation, and finance organizations.<br>• **EDIFACT** - Format adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735.<br>• **XML** - File format used for structured documents.<br>• **EDI Consent** - Provides a standard mechanism for "wrapping" the EDI objects but does not specify any details about those objects.<br>• **Binary** (default) - e.g., executables, word processing files, database, spreadsheet, and multimedia files<br>• **Plaintext** - e.g., text and HTML files |

| Field | Required/Optional | Description |
|---|---|---|
| Compress message | Required | When selected, specifies that the AS2 message should be compressed when sent. (Cleared by default.) |
| Encrypt message | Required | When selected, specifies that outbound AS2 messages should be encrypted. (Selected by default.) |
| Sign message | Required | When selected, specifies that outbound AS2 messages should be signed. (Selected by default.) |
| Your certificate | Required | Displays the AS2 certificate public key path to use for signing, copied from the Site. (Can be on a drive or UNC path.) |
| Partner certificate | Required | Specifies the AS2 certificate to use for encrypting outbound transactions and for validating signed MDN receipts. (Can be on a drive or UNC path.) |
| Your AS2 identifier | Required | Used to apply a unique **AS2-From** ID to outbound messages. |
| Partner AS2 identifier | Required | Used to apply a unique **AS2-To** ID to outbound messages. |
| Receipt policy | Required | Used to request an MDN receipt. Options include:<br>• Request a signed receipt (default)<br>• Don't request a receipt<br>• Request an unsigned receipt |
| Receipt delivery | Required | Specifies receipt delivery method<br>• Synchronous (default)<br>• Asynchronous |

The following fields are used to determine whether a message send attempt has failed due to a timeout, error, synchronous MDN receipt failure, or other error, after which EFT Server will attempt to resend the same message at regular intervals, if specified.

| Field | Required/Optional | Description |
|---|---|---|
| Message send attempt timeout (seconds) | Optional | Specifies the timeout after which a message send attempt is considered a failure if no response or errors are received from the remote server. Range: 0-600, 60 by default, 0 means no timeout |
| Message send attempt retries | Optional | Number of times to reattempt to send the message. Range: 0 (no retry) to 999, 10 is the default.<br>*Retries do not include the initial attempt. That is, 3 retries means 3 in addition to the first attempt (4 total).* |
| Send attempt delay between retries | Optional | Specifies the time to wait between retries if the send attempt was unsuccessful, in seconds. 30 seconds is the default. |
| Asynchronous receipt timeout | Optional | Specifies the time to wait for receipt before timing out, in minutes. The default is 7200 minutes (2 hours). |

## Backup Server Configuration Action

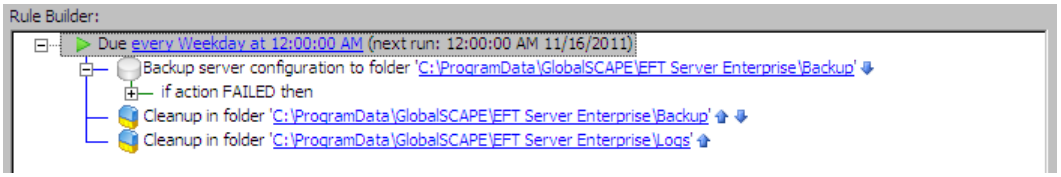
**(Available in EFT Server Enterprise)** A Backup Server Configuration Event Rule is defined and enabled by default to back up EFT Server configuration automatically on a recurring schedule. You can also run the wizard manually. For more information about the Migration wizard, refer to "Backup Server Configuration Wizard" in the *EFT Server User Guide*.

When you create your first Site, a new Timer Rule is created that runs the **Backup Server Configuration** Action once a day at midnight, using all defaults for naming and backup location (**\backup\Server Configuration Backup [Month] [Day] [Year].bak**). The default Rule includes a **Cleanup in folder Action** to delete backup files (***.bak**) older than 30 days in that same folder. The Rule is created and enabled when EFT Server Enterprise is installed, but you can disable it and edit it as necessary.

*It is a good idea to save the backup on a drive other than on the one on which the EFT Server is installed. If EFT Server's hard drive fails, you will want to use the backup to restore configuration.*

**To create (or edit) the Backup Server Configuration Event Rule**

1. Create a Rule using the Timer, Service Stopped, or Service Started Events.
2. If you are using the Timer Event, click the hyperlink to define the backup schedule. The **Timer Event** dialog box appears. Refer to Scheduler (Timer) Event for details, if necessary.
3. Double-click the **Backup Server Configuration** Action or click it, and then click **Add**. The Action is added to the Rule.
4. Click the hyperlink in the **Backup Server Configuration** Action. The **Browse for Folder** dialog box appears in which you can specify where to save the backup file. (Use a UNC path.) By default, the backup file is saved to the EFT Server's Application Data folder (e.g., C:\ProgramData\Globalscape\EFT Server Enterprise\Backup). ***You should change this location to a hard drive other than the one on which EFT Server is installed.***
5. Click the folder icon to select the folder in which to save the backup file, and then click **OK**.
6. (Optional) Add the **Cleanup in folder Action** to removed old backups. Refer to Cleanup in folder Action for details, if necessary. The default Rule is configured to delete **.bak** files that are older than 30 days. You can delete backups manually, if desired. Be sure to point to the location where the backup file is saved.
7. Add other Actions as needed, such as e-mail notifications.
8. Click **Apply** to save the changes on EFT Server.
9. If you used the Timer Event, you can click **Run Now** to test the Rule.

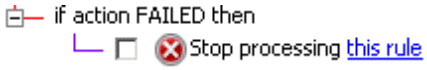



The **Backup server configuration** Event Rule also includes a **Cleanup in folder** Action to clean up the **Logs** folder. If you do not want to save logs created by LAN transfers, you can disable the logs using a registry entry. For more information about the registry entry and these logs, refer to The Client Log (Event Rule Logging).

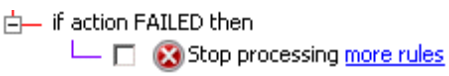
**Be sure to change the paths if yours are different from the defaults.**

## Stop Processing

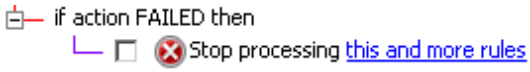
The *Stop Processing* Action is added automatically with each of the Actions except for the Send notification email Action, or you can add it after an Event or Condition. The Stop Processing Action ends processing of Event Rules, depending on your selection:




- **this rule**—The current Rule is aborted, and the next Rule in order is started. That is, it only affects subsequent Actions for THIS Rule. Other matching Rules will continue to process.




- **more rules**—The current Rule continues executing, the next Rules in order are not started. That is, it allows the current Rule to complete its processing, but no further matching Rules will continue to process.

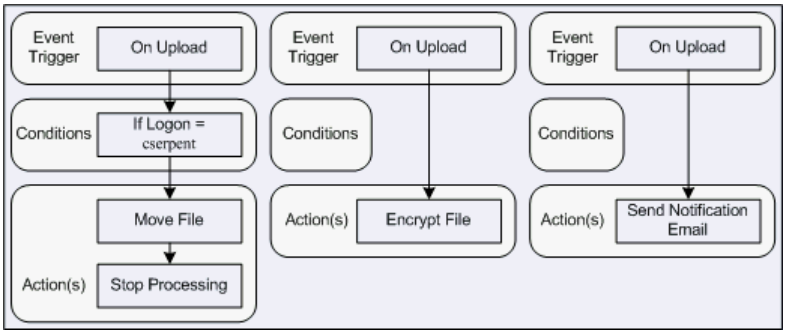



- **this and more rules**—The current Rule is aborted, and the next Rules in order are not started. That is, stop any subsequent Actions for this Rule and don't process any subsequent matching Rules.

Some exceptions/clarifications to consider:

- Folder Monitor and Timer Rules are not ordered, because there is only one Rule corresponding to a specific Folder Monitor/Timer ("one Event - one Rule" correspondence); only "Stop processing this Rule" is available for them. Certain "server-wide" Events ("Monitor Folder Failed," "Service started," "Service stopped," "Log rotated") allow "Stop processing this Rule" behavior only.
- The Stop Action affects only the current Event; when a client uploads the next file (i.e., when the next "File Uploaded" Event happens), EFT Server will execute all Rules (from first to last) again.

The example below shows three Rules that are triggered with an On Upload Event. "Stop processing this and more Rules" causes the other two processes in this example to stop:




Based on these Rules, cserpent's file will be moved, but uploaded files will not be encrypted, nor will cserpent receive an e-mail notification when a file is uploaded.

*A recurring Timer does not stop recurring if the Rule Actions fail; it will recur as scheduled until you disable or delete the Rule. In the case of Timer Rules, "Stop processing this rule" means "do not execute any further Actions with this Rule" (such as sending an e-mail), but it does NOT mean that the Timer will stop. For example, if you have defined the Rule to run every hour, an Action in the Rule could fail (such as downloading a file from a remote computer), but the Timer will run again the next hour, and the next hour, and so on, until you tell it to stop (by manually disabling it).*

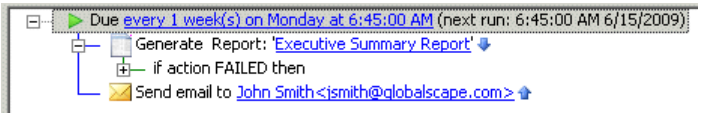
## Generate Report Action

When the Auditing and Reporting module is activated, you can configure a Server Event Rule to generate a report, and then e-mail it or save it to a file. If you add the Generate Report Action to a Rule, you must also tell EFT Server what to do with the report (save it or e-mail it or both). When a report is generated by the Generate Report Action, a temporary, enumerated copy of the report is created and stored locally in the EFT Server installation folder. The temporary copy is deleted once the Event Rule context is out of scope.

*To facilitate compliance with PCI DSS requirement 10.6, EFT Server automatically generates a report of PCI/High Security-related configuration and functions. The report is converted to HTML and then e-mailed or saved to a file specified by the EFT Server administrator.*

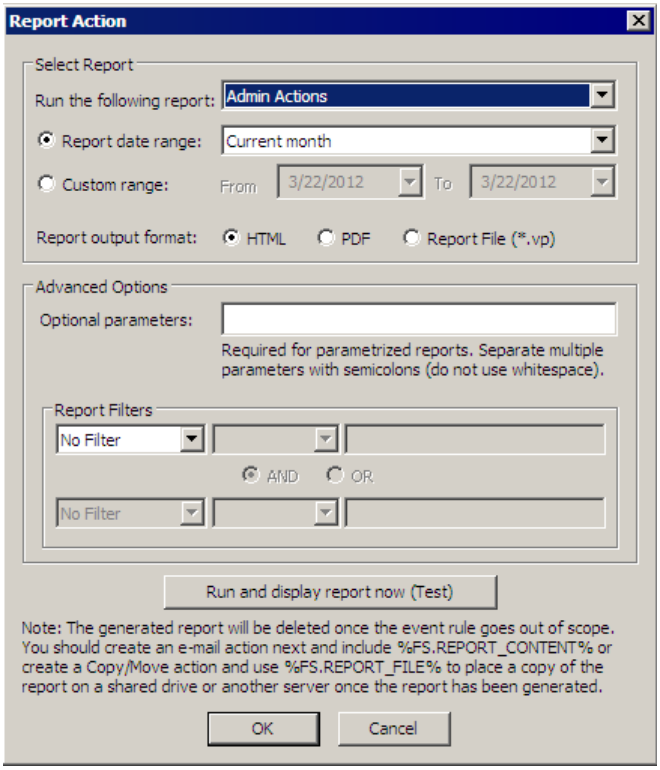
*The automatic **Generate Report** Action never prompts for parameters because it will be run from the service on a timer, and thus does not allow interaction by a user. Reports that require parameters but do not have sufficient administrator-defined parameters will not run.*

**Example of a Report Event:**




**To create an Event Rule with the Generate Report Action**

1. Follow the procedure in Creating Event Rules to create a new Rule, or select the Rule to which you want to add the Action.
2. In the **Actions** list, double-click **Generate Report**, or click it, and then click **Add Action**. The **Report Action** dialog box appears.




3. In the **Run the following report** box, click the down arrow to select a report from the Reports directory. (Custom reports also appear in the list.) Refer to "Descriptions of Preconfigured Reports" in the *EFT Server User Guide* for a description of the Globalscape-defined reports.
4. Click **Custom range** to specify a custom date range in the **From** and **To** boxes or click **Report date range** and click the drop-down list to specify one of the following options:
    - **Include all dates**. If the selected dates include future transactions (e.g., if the ending date for the report is today's date), the future transactions will not appear in the report.
    - **Today.** From 00:00:00 to the current time.
    - **Yesterday.** The previous day from 00:00:00 to 00:00:00.
    - **Last 24 hours.** The previous 24 hours from the current time.
    - **Month to date**; **Quarter to date**; **Year to date**. Starting from the first day of this month, quarter, or year, and ending today. (Quarters begin January 1, April 1, July 1, and October 1.)

- **Current week**; **Current month (default)**; **Current quarter**; **Current year**. Starting from the first day of this week, month, quarter, or year, and ending with the last day of this week, month, quarter, or year. (Quarters begin January 1, April 1, July 1, and October 1.)
- **Last week**; **Last month**; **Last quarter**; **Last year**. Starting from the first day of last week, month, quarter, or year, and ending with the last day of last week, month, quarter, or year. (Quarters begin January 1, April 1, July 1, and October 1.)
- **Last 30 days**. Starting from 30 days ago, and ending with today's date.
- **Last 12 months**. Starting 12 months ago from today's date, and ending with today's date. For example, if today is July 2, 2007 and this date range is selected, the report would run from July 2, 2006 through July 2, 2007.

5. In the **Report output format** area, specify the format of the report output: HTML, PDF, or VP (report file).
6. In the **Advanced Options** area, specify **Optional parameters** (separated by semicolons) for the report, which are evaluated from left to right. You can specify Event Rule variables. For example, if the report definition chosen in the **Run the following report** box requires two parameters for filename and username (in that order in the report definition), and then the **Optional parameters** box can be populated with `*.txt;myname` to specify a filename parameter of `*.txt` and a username parameter of `myname`.
7. In the **Report Filters** area, specify filters with AND or OR. Available filters depend on report selected. (If you test the report and do not see the desired results, adjust your filters.)
8. To run the report in real time to verify that the Action was configured correctly, click **Run and display report now (Test)**.
9. Next, you should create an e-mail Action and include the %FS.REPORT_CONTENT% variable or create a Copy/Move Action and use the %FS.REPORT_FILE% variable to place a copy of the report on a shared drive after the report has been generated.

   The variable %FS.REPORT_CONTENT% can be added to e-mail notifications. When %FS.REPORT_CONTENT% is added to the body of e-mail notifications, the content is displayed inline in the e-mail in HTML format, regardless of the format chosen in the **Report Action** dialog box.

*The variable %FS.REPORT_FILE% can be used in copy/move, PGP, and Custom Command Actions that are executed synchronously (i.e., Custom Commands that have a failure Event defined), but should not be used for Actions that are executed asynchronously (e.g., Custom Commands that do not have a failure Event defined). Instead, use %FS.REPORT_CONTENT% for e-mail notifications, because this variable represents a copy of the contents of the file rather than a link to the file, which is only good as long as the file exists. For a complete list of EFT Server variables, see Variables. Do not use %FS.REPORT_FILE% in e-mail notifications.*

## OpenPGP Event Rule Action

You can configure EFT Server's OpenPGP Event Rule Action to do things like encrypt, sign, and decrypt, even on files larger than 2GB. The OpenPGP Action is available with Server Events (the **On Timer** and **On Rotate Log** events), certain File System Events (**File Upload**, **File Move**, and **File Rename**), and a User Event (**User Logout**). To use this Action, the Site must be configured for OpenPGP and the appropriate PGP keys must be generated.

## Using the OpenPGP Encryption/Decryption Action in Event Rules

*When OpenPGP is used with a Folder Monitor Rule, OpenPGP operations will result in the creation of new files that will trigger the Folder Monitor Rule a second time. Although EFT Server provides an implicit filter that will ignore **.pgp**, **.sig**, **.asc** or **.gpg** file extensions for encrypt operations, you should still add an Event Rule Condition that provides an explicit exclusion next to the "If File Change does equal to added" Condition that is created by default when the Folder Monitor Rule is first created.*

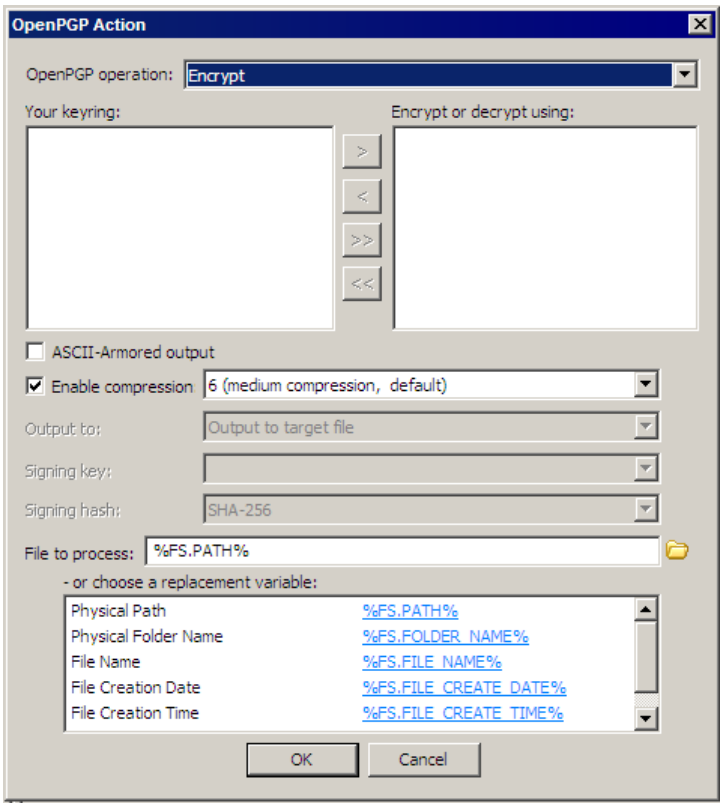
- *When encrypting a file: "If File Name does not match *.pgp"*
- *When decrypting a file: "If File Name does match *.pgp"*
- *When verifying the signature: "If File Name does match *.sig"*
- *When signing a file "If File Name does not match *.sig'"*
- *When verifying signature only: "If File Name does match *.pgp"*
- *When signing: "If File Name does not match *.pgp"*


One limitation is that you cannot "Encrypt and Sign" and then "Verify Only"; that will fail. The scenarios below are valid:

| PGP Source | PGP Receiver |
|---|---|
| Encrypt+Sign | Decrypt+Verify |
| Encrypt+Sign | Decrypt |
| Sign Only | Verify Only |

**To set up EFT Server to use OpenPGP for particular Event Rules**

1. Follow the procedure in Creating Event Rules or select the Rule to which you want to add the Action.
2. In the right pane, in the **Actions** list, double-click **OpenPGP Encrypt**, **Encrypt + Sign**, **Decrypt**. The Action appears in the Event in the **Rule Builder**.
3. In the **Rule Builder**, select either of the underlined elements (links). The **OpenPGP Action** dialog box appears.




4. Specify the **OpenPGP operation** (Encrypt, Encrypt and Sign, Sign Only, Self-Decrypting Archive (SDA), Decrypt, Decrypt and Verify Signature, Verify Signature Only).
5. The options that appear in the dialog box depend on what you select in the **OpenPGP operation** box:
    a. If you designated a default key for the Site, that key is displayed in the **Encrypt or decrypt using** (right) pane. If there is no default key, the right pane will be blank. Use the arrow icons to add or remove keys between the **Your keyring** pane and the **Encrypt or decrypt using** pane, or double-click the key in the list.

If you would like to encrypt a single file such that multiple recipients will be capable of decrypting it, add the individual keys of the intended recipients to the list of keys to use for the encryption Action to the **Encrypt or decrypt using** (right) pane. This prevents you from having to create multiple copies of a file and then encrypt and manage each file separately for each intended recipient.

**Example Use Cases:**

- You have a report containing sensitive data in PDF format. You want to encrypt and send that report to three people. In this case you would configure the "Encrypt" or "Encrypt and Sign" Action with all three public keys that correspond to those individuals. You can then send a copy of that one file to each of the recipients, and they can each decrypt the file with their private key in order to view the report in their PDF reader.
- You are required to keep an archived copy of all outbound files, including any encrypted files. If you encrypt with only the intended recipient's key, then the resulting encrypted file will not be acceptable for archival since you will not be able to decrypt it later. Therefore, you encrypt the file with not only the public key of the intended recipient but also the public key to which you have the corresponding private key. Not only will the recipient be able to decrypt the file as usual, but you will also be able to decrypt the archived copy of that file, if needed.

    b. To specify **ASCII-Armored output**, select the check box.

c. Select the **Enable compression** check box, and then click the down arrow to specify a level of compression, from 1 (least compression, fastest) to 9 (max compression, slowest). The default is 6 (medium compression, default).

d. In the **Output To** box, click the down arrow to specify an option: Output signature to target file (.pgp), Output signature to target file ASCII armored (*asc), Output signature to separate file (*.sig), Output signature to separate file ASCII armored (*.asc).

e. In the **Signing key** box, click the down arrow to specify the signing key.

f. In the **Signing hash** box, click the down arrow to specify a hash: Use default (MD5 or SHA-256), MD5, SHA-1, RIPEMD160, SHA-256, SHA-384, or SHA-1512. The default value depends on the version of the key used to sign the message. For version 3 keys (RSA Legacy keys), MD5 is used as default value. For all other keys, SHA-256 is used.

g. In the **File to process** box, specify the file or folder to process. The default target file is selected. Alternatively, click a variable to add it to the **File to process** box or use actual file/folder names. Use the folder icon to browse to a file or folder.

6. Click **OK** to close the dialog box and apply the parameters.
7. Click **Apply** to save the changes on EFT Server.

## Using Wildcards with Event Rule Actions

The **OpenPGP** Action, the **Copy/Move** Action, and the **File Name** Conditions support the use of wildcards. This is useful for Event Rules that batch process groups of files. Standard Windows/DOS format wildcards are used, such as *.*file extension, search term* .???, *search term* ?.*, *.*, and so on. This functionality is particularly useful with the Timer Event.

### Wildcards with OpenPGP

In the OpenPGP Action configuration dialog, the **File to Process** field supports wildcards. Each matching file is acted upon according to the Action definition.

### Wildcards with Copy/Move

In the **Offload Action** wizard, the **Source** path field on the **Target File** tab supports wildcards.

When a wildcard is specified here, the **Destination** path field specifies the target folder to which each matching file is moved or copied. The files moved or copied into the destination file are given the same name as the files from the source.

**Example**

Source:

```
c:\test\*.txt
```

Destination:

```
/%FS.FILENAME%
```

Here, each "*.txt" file that is uploaded goes to "/", with a matching file name. Note that the destination file name is not overwritten.

### Configuration Notes

- If the **source** of an Action is specified as a wildcard without any path information, the path defaults to the folder with the Event Rule that triggered this Action (for example, there is a "%FS.PATH%" variable for an **On Upload** Event.) If there is no folder like that available - for example, if the Event is an **On Timer** Event - the current working directory of the application is set as the source of the wildcard patterns. Typically, that is the installation directory of the application.

- When you define a wildcard in the source path for a copy/move Action and the protocol type is set to Local (Local Files or LAN), EFT Server respects Windows path syntax:

Source:

```
c:\Work\Today\*.*
```

Destination:

```
g:\Backup\Work\Today\
```

You can also use \\Work, if appropriate.

- The Destination Path (Upload Event target file as:) ignores any path information you enter after the trailing backslash. So if you type:

```
g:\Backup\Work\Today
```

EFT Server disregards "Today" and executes the move/copy into:

```
g:\Backup\Work\
```

*Test an Event Rule using a wildcard before you deploy it to ensure it works as expected and does not cause any unwanted behavior. For example, if you do not define the source path appropriately when a wildcard is used, it is possible to set up an Action that moves all the files out of a user's c:\windows directory, which is most likely an undesired result.*

## Using Login Credentials in Event Rules

User name and password variables are used by Event Rules to use a single Event Rule to support multiple users with a single Copy/Move Action. This allows EFT Server to store user name and password variables in memory for the duration of a client session. You can enable or disable this feature on the Site. The default is disabled. For more information on using this in an Event Rule, refer to Copy/Move File to Host Action.

**To persist login credentials in memory for use in Event Rules**

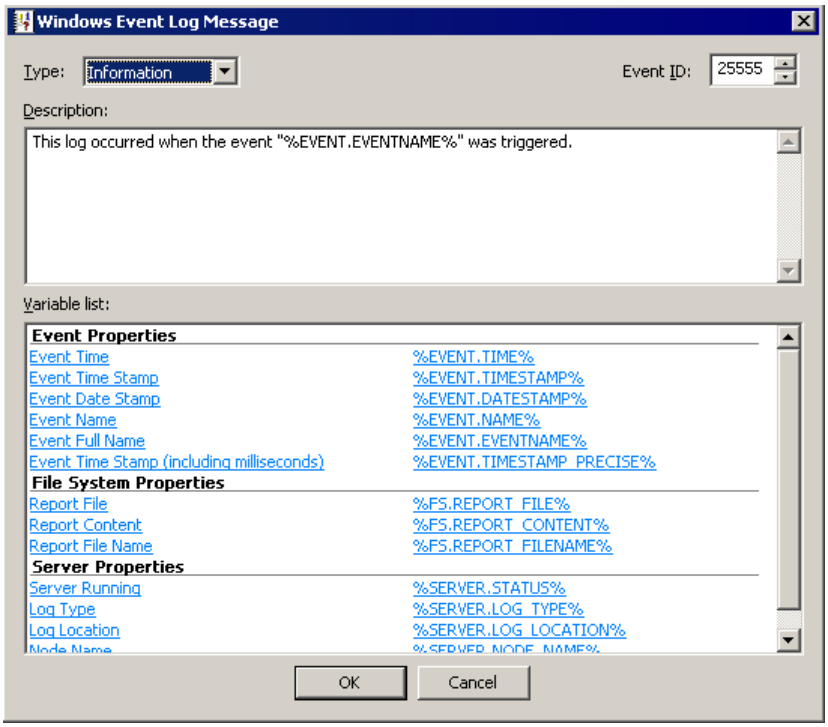
1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. Select the **Persist username and password credentials for use in Event Rule context variables** check box.
5. Click **Apply** to save the changes on EFT Server.

*Allowing user name and password replacement variables introduces a potential security vulnerability because it allows passwords to reside in memory on EFT Server. The risk is low, but should be avoided unless you require the variables for an Event Rule.*

## Write to Windows Event Log (WEL)

**(Available in EFT Server Enterprise)** The **Write to Windows Event Log** Action is available for all Event Triggers.

When you add the **Write to Windows Event Log** Action to the **Rule Builder** and then click the hyperlink in the Action, the **Write to Windows Event Log** dialog box appears. Use this dialog box to specify the WEL message parameters.

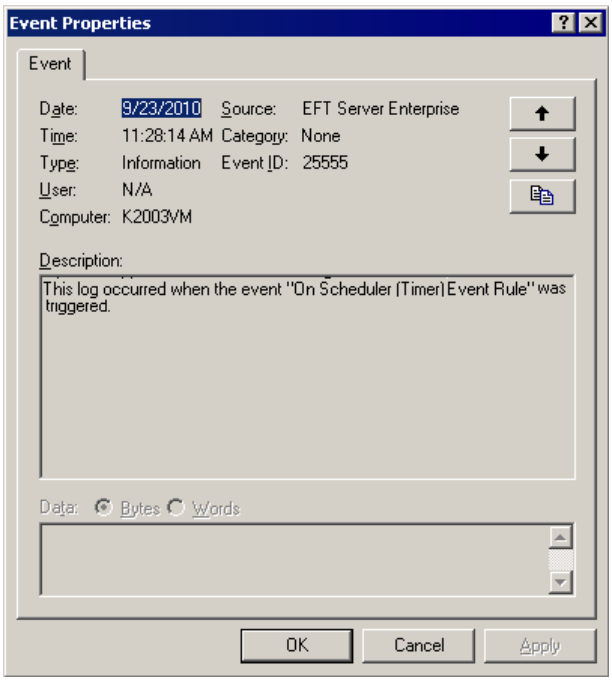



**To configure the WEL message**

1. In the **Type** box, click the down arrow and specify whether the message is an **Information**, **Warning**, or **Error** message.
2. In the **Event ID*** box, click the up or down arrows to specify a number to assign to the Event, from 1 to 99,999 (defaults to 2).
3. In the **Description** box, provide a text description that will appear in the WEL when the Event is triggered, up to up to 2048 characters.
4. (Optional) In the **Variable list** box, click an EFT Server context variable to appear in the message. You can add multiple variables. The value of the variable will appear in the message when the Event is triggered.
5. Click **OK** to save the parameters in the Action.

**To view the Windows Event Log**

1. Click **Start > Run**.
2. Type `eventvwr.msc`, and then press ENTER. The **Event Viewer** appears.
3. Double-click an EFT Server Enterprise (Source) Event. The **Event Properties** dialog box appears.




4. Notice that the **Type**, **Event ID**, and **Description** areas display the parameters that you provide in the **Windows Event Log Message** dialog box.

For details of the log that is created during Download and Copy/Move Actions, refer to The Client Log (Event Rule Logging).

## Client Log

When EFT Server'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** (e.g., **cl060312.log**) and saved in the EFT Server installation folder (**C:\Documents and Settings\All Users\Application Data\Globalscape\EFT Server Enterprise\logging.cfg**). On Windows 2008, Application Data files for all users are in a hidden folder named **%systemroot%\ProgramData**). 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 a registry entry. The tenth column indicates status of the Event, Success (0) or Failure (1). To enable the tenth column, create the DWORD `Enable10ColumnInClientLog` at the following path:*

*32-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Globalscape Inc.\EFT Server 4.0`*

*64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Globalscape Inc.\EFT Server 4.0`*

*Value:*

*0 or not present = disabled*

*1 = enabled*

*With the tenth column enabled, the CL log columns are:*

*`TIME; PROT: HOST:PORT; USER; LOCAL_PATH; REMOTE_PATH; OPERATION; LAST_RESULT_CODE; ACTION_RESULT`*

*When `ACTION_RESULT` = 1, the transfer failed and the "IF FAILED" Action in the Event Rule will be executed.*

*When `ACTION_RESULT` = 0, the transfer succeeded and the "IF FAILED" Action in the Event Rule is not executed.*

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 Server 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 Server 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) |

| # | Description |
|---|---|
| 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)<br>*When an OpenSSH client disconnects from EFT Server, it reports that the exit status is **-1**. The default return code is -1, unless an optional message is returned from the server. EFT Server 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 Web Service

In EFT Server Enterprise edition, the Web Service allows you to initiate EFT Server workflow from an external application such as an enterprise scheduler. The WebService interface follows the model of ASP.NET Web services, providing a page for the services definition document (WSDL) and an HTML form that can be used to test available service methods. Access to Web Service requires authentication with a COM-enabled Server Administrator account; without proper authentication and COM privileges, EFT Server returns a `401 Unauthorized HTTP error` to the requestor.

The Web Service requires an SSL certificate, because EFT Server sends the HTTP Web Service requests via HTTPS. EFT Server allows you to turn on Web Service without selecting the **HTTPS** check box, but it checks for an SSL certificate, because it will automatically redirect HTTP to HTTPS. Even when the **HTTPS** check box is not selected, Web Service requests are handled by the HTTPS engine (port 443 listener, by default), but other HTTPS requests will still get the 503 Service unavailable response.

The Web Service is enabled in the Site's **Listener Settings** area. Refer to "Enabling Web Services" in the *EFT Server User Guide* for the procedure for enabling the Web Service on the Site.

Requests to any **/WebService** URL are logged to the text log and ARM database just as any other HTTP request. A request that does not match the **/WebService/InvokeEventRule** URL or that does not include the required parameters, results in a `400 Bad Request HTTP error`.

The **/WebService** page displays a list of Web services available with EFT Server. This page is generated from an HTML page in EFT Server installation folder, in a subfolder called **WebService**.

By default, the following files are installed in:

**C:\Program Files\GlobalScape\EFT\web\public\EFTClient\WebService**

- **\EFTWebServices_MAIN.html** - Used to define the Web Services landing page; provides a link to **InvokeEventRule.html**.
- **\InvokeEventRule\EFTWebServices_InvokeEventRule.html** - Used to define the Web interface from which you can remotely invoke Event Rules on EFT Server.
- **\InvokeEventRule\EFTWebServices.wsdl** - Web Services Description Language (WSDL) configuration file. (For details of how WSDL files are used, refer to the World Wide Web Consortium documentation at http://www.w3.org/TR/wsdl.)

*EFT Server uses a template for the WSDL to construct the final WSDL. External tools can use the WSDL by pointing to the URL that deploys the WSDL file at* ***http://localhost/WebService/InvokeEventRule?wsdl****, where "localhost" is the IP address, computer name, or DNS name that points to the EFT Server service that is hosting the web service.*

## How EFT Server Supports Web Service

EFT Server supports both POST and GET HTTP requests to "/WebService/InvokeEventRule" with two parameters "EventRuleName" and "EventParams" and triggers an Event Rule that is specified in the "EventName" as a synchronous operation. The Web Service supports the REST invocation model, supporting both POST and GET methods for invocation.

1. If an input is missing any of "EventRuleName" or "EventParams" it returns an HTTP 400 error.
2. If both "EventRuleName" and "EventParams" are presented but:
    a. "EventRuleName" is wrong (no Event Rule exists with such name), it returns .xml with result code of -1.
    b. "EventParams" are incorrect (wrong variable names, too many, too few), EFT Server looks for Rule variables in the input and replaces those values with found ones. All additional variables are ignored. If a Rule variable is not found in URL then it will be set to "N/A." The result code in .xml will be the Event execution result code.

*Requests to any /WebService URL is logged to the text log and ARM system just as any other HTTP request.*

### HTTP GET

The following is a sample HTTP GET request and response. Replace the **placeholders** with actual values.

```
GET /WebService/InvokeEventRule?EventRuleName=string&EventParams=string
HTTP/1.1 Host: localhost

HTTP/1.1 200 OK Content-Type: text/xml; charset=utf-8 Content-Length: length
<?xml version="1.0" encoding="utf-8"?> <int xmlns="http://mydomain/ ">int</int>
```

### HTTP POST

The following is a sample HTTP POST request and response. Replace the **placeholders** with actual values.

```
POST /WebService/InvokeEventRule HTTP/1.1 Host: localhost Content-Type:
application/x-www-form-urlencoded Content-Length: length
EventRuleName=string&EventParams=string

HTTP/1.1 200 OK Content-Type: text/xml; charset=utf-8 Content-Length: length
<?xml version="1.0" encoding="utf-8"?> <int xmlns="http://mudomain/ ">int</int>
```

## Web Service Timeout

The Web Service timeout is set to 60 seconds. You can change the timeout value with the following registry setting:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Globalscape Inc.\EFT Server 4.0]
"WebServiceTimeout"=dword:<value, in seconds>
```

If this value is absent, the default is 60 seconds. This value is checked for each Web Service connection, so the EFT Server service does not need to be restarted for this setting to take effect.

## Executing Event Rules Using Web Service

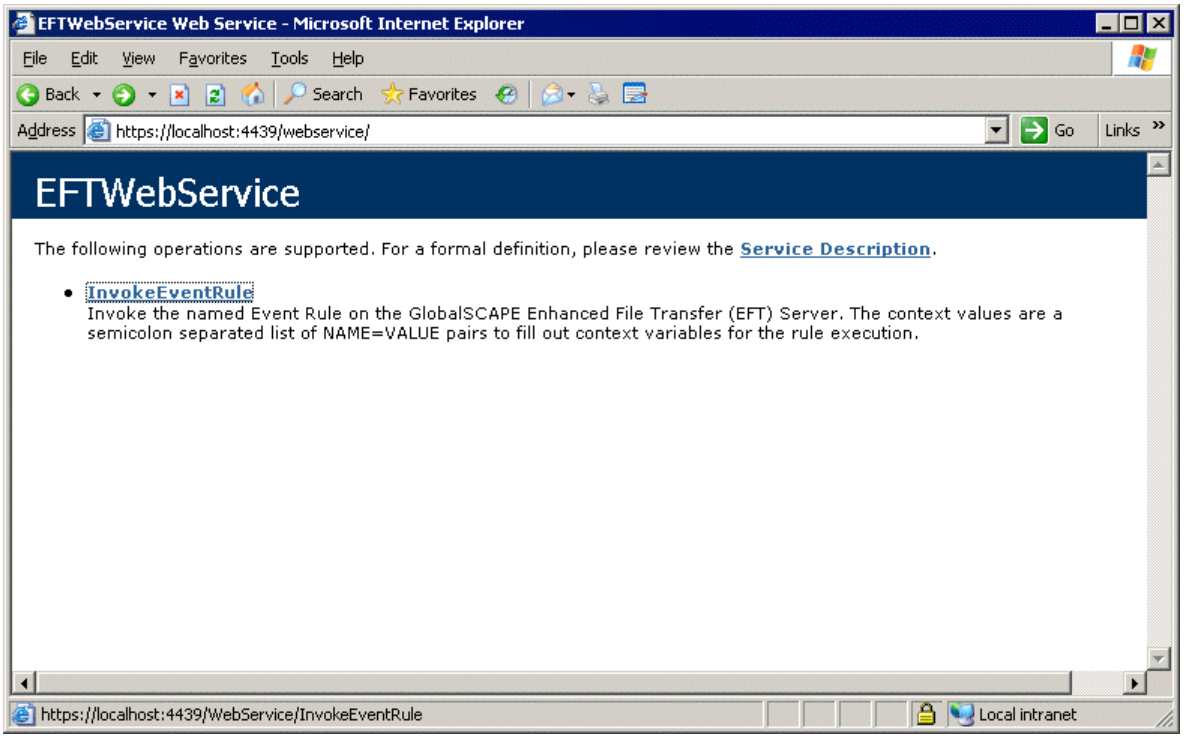
In EFT Server Enterprise edition, the Web Service allows you to initiate EFT Server Event Rules via a browser.

For more information about how EFT Server supports Web Service, refer to EFT Server Web Service.

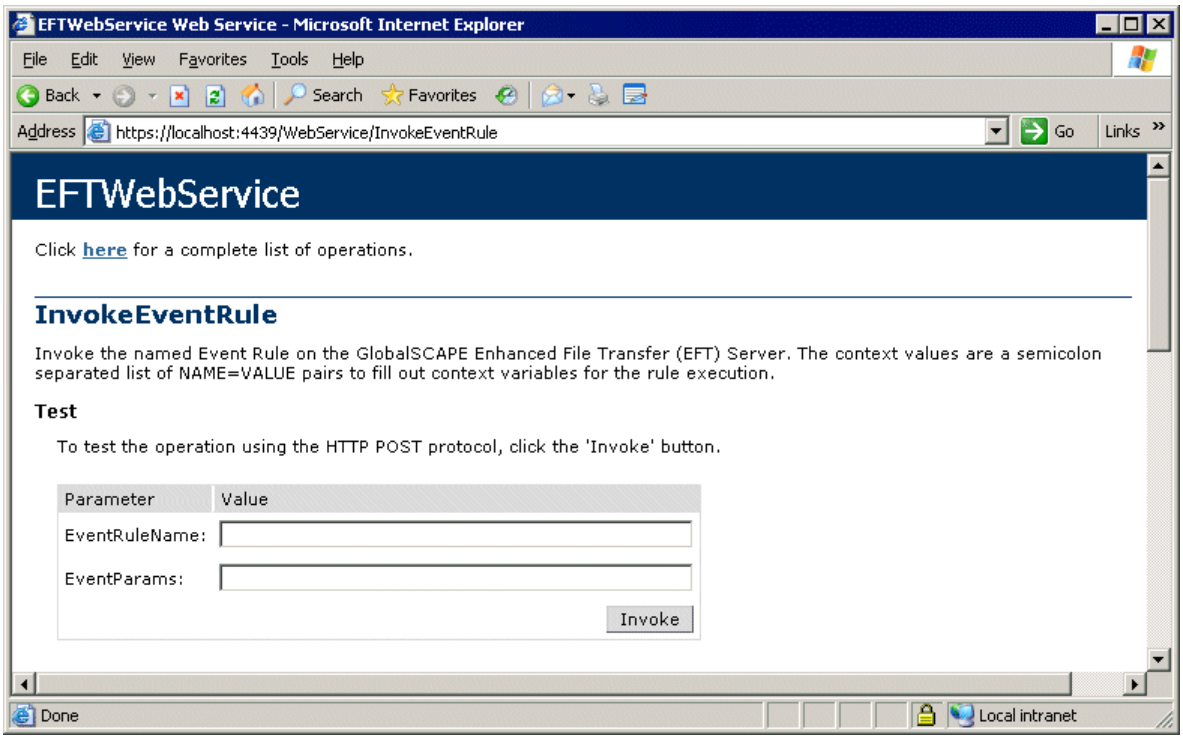
*The administrator account must have the COM administration privilege for access to any /WebService URL (or sub-URLs).*

**To execute an Event Rule using WebService**

1. Open a browser and navigate to EFT Server URL appended with `/WebService`. The **WebService** page appears.




2. Click **InvokeEventRule.** Another Web page, **/WebService/InvokeEventRule**, displays a form for invoking an Event Rule.




3. In the **EventRuleName** box, type the name of the Event Rule.
4. In the **EventParams** box, type one or more variables, separated by semicolons.
5. Click **Invoke**. The Event Rule is executed.

*All WebService responses use the Site's domain name as the namespace for the WebService.*

6. After the Event Rule finishes dispatching, the Web service responds with an XML document that consists of a single "Result" element. The Result Code can be any one of the following:
    - 0 indicates failure
    - 1 indicates success
    - -1 indicates EFT Server could not find the Event Rule (e.g., the requested EventName does not exist or was not typed correctly)

# Changing the Number of Concurrent Threads Used by Event Rules

Q: Is there a thread limit as to how many files can be transferred via the same Event Rule?

A: The Event Rule Monitor Folder process is limited to 3 concurrent threads by default. This means that if you have 5 Folder Monitor Event Rules monitoring the same folder, and a file is added to the monitored folder, only 3 of the 5 Rules will fire, as determined by the operating system. The 4th and then 5th Rule execute only when one or more of the first three threads are done firing and executing any Actions. If you have, for example, 100 concurrent Monitor Folder Event Rules, they are not all triggered simultaneously.

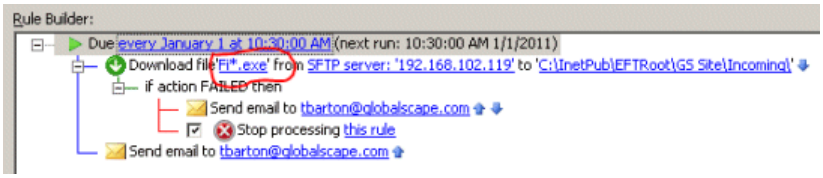
For details of overriding the default "concurrent threads" settings in the registry, refer to Knowlegebase article #11036.

# Using Wildcards with WinSSHD

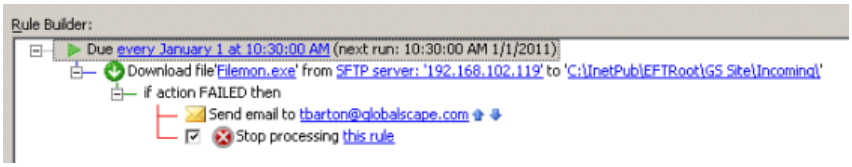
WinSSHD is Bitvise's SSH server for all Windows NT-series operating systems. When accessing WinSSHD through EFT Server's Event Rules, you must supply the home folder path on the WinSSHD server if you want to pull files using a wildcard.

The following Event Rule configuration will work, because it includes the path with the wildcard:


The following Event Rule configuration will ***not*** work, because it has a wildcard and does not include the full path:




The following Event Rule configuration will work, because it specifies the filename completely, without a wildcard:

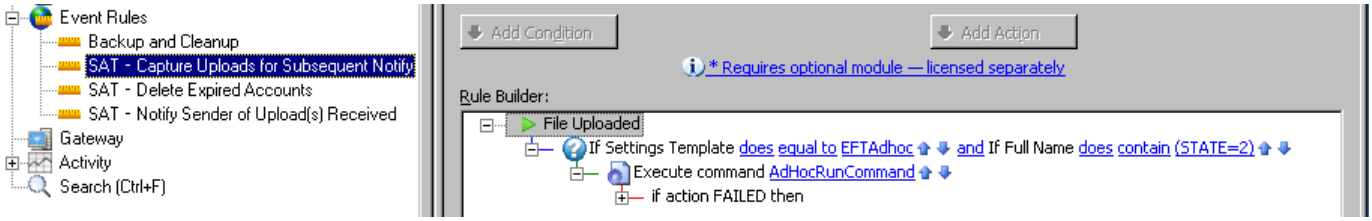



# SAT Event Rules

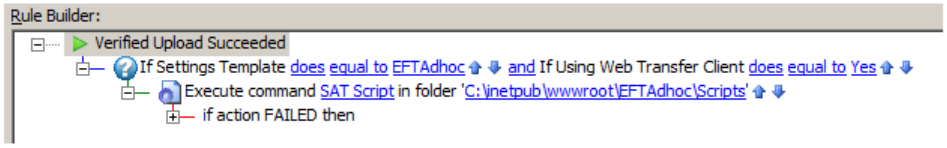
When you install the Secure Ad Hoc Transfer (SAT) module, the following Event Rules are created by the installer. (If you are using a 64-bit system, the Event Rules and Command need to be updated to reflect the 64-bit paths.)

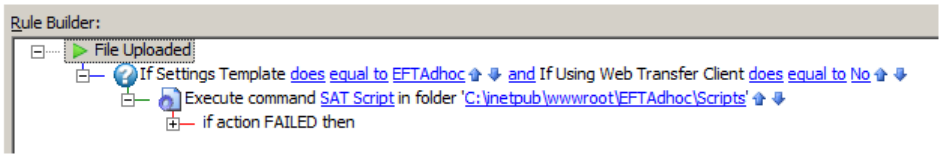
See below for a description of the **AdHocRunCommand** Custom Command.

- **SAT - Capture Uploads for Subsequent Notify**—If the Settings Template is "EFTAdhoc" and if the remote IP address does not match *.*.*.* (All Incoming), execute the **AdHocRunCommand** custom Command in **C:\Program Files\Globalscape\EFT Server Enterprise\SATScripts** to runs the **SendUploadNotification.wsf** script.

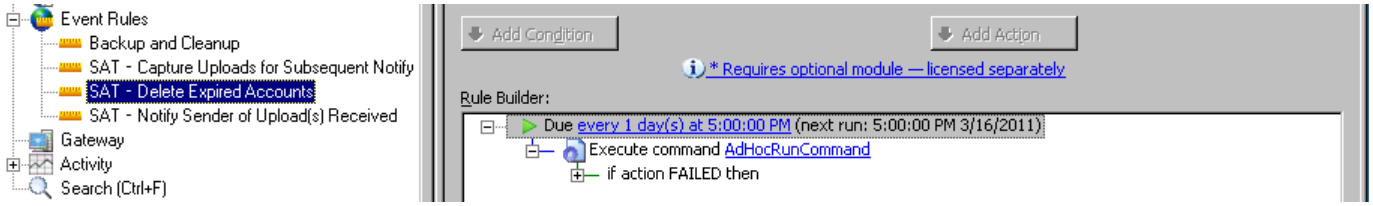


*The Rule above works best with the Plain-Text Client. If end users are uploading with the Web Transfer Client, add a second Rule using the "Verified Upload Succeeded" Event and add the Condition "If Using Web Transfer client does equal to Yes." Also add the "If Using Web Transfer client does equal to No" Condition to the Rule above.*

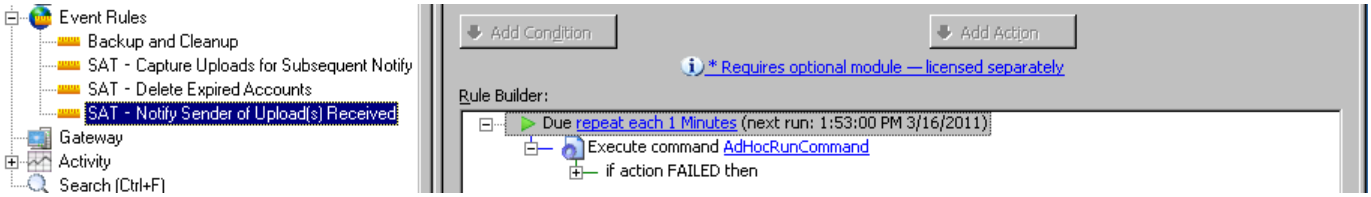



- **SAT - Delete Expired Users**—Every day, execute the **AdHocRunCommand** custom Command in **C:\Program Files\Globalscape\EFT Server Enterprise\SATScripts** to run the **EFTDeleteExpiredUsers.wsf** script.



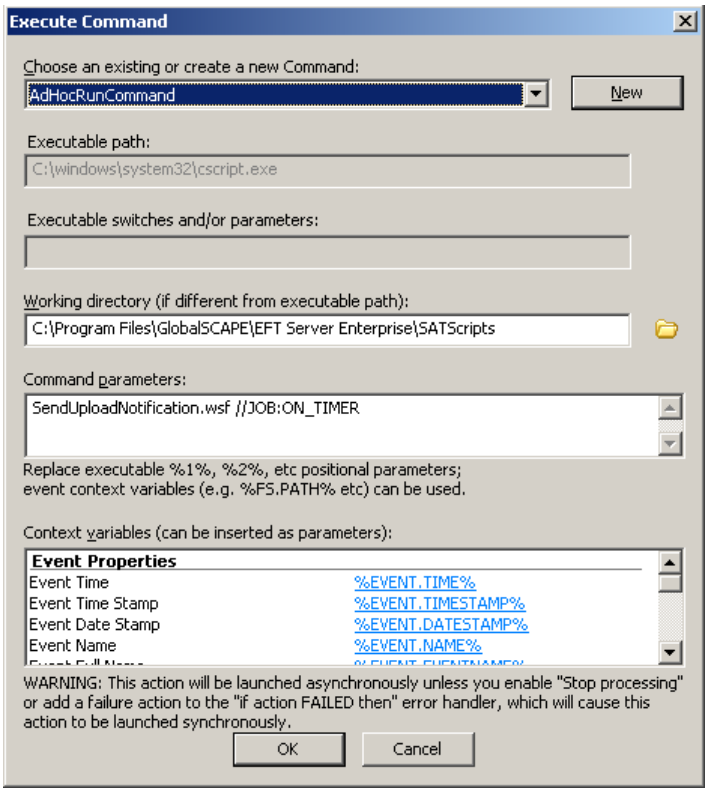

- **SAT - Notify Sender of Upload(s) Received**—Each minute, execute the **AdHocRunCommand** custom Command in **C:\Program Files\Globalscape\EFT Server Enterprise\SATScripts** to run the **SendUploadNotification.wsf** script.




These Event Rules automatically perform tasks that you had to configure manually in previous versions of SAT. The SAT Event Rules are enabled by default. You can edit the Rules and disable them as needed. Refer to Event Rules for details of managing Event Rules.

## AdHocRunCommand Custom Command

The **AdHocRunCommand** Custom Command is created in EFT Server the when the SAT module is installed. **AdHocRunCommand** executes **C:\windows\system32\cscript.exe** (or **C:\windows\syswow64\cscript.exe** on 64-bit systems) and includes some custom **Command parameters** for executing the SAT scripts in the default SAT Event Rules.




- In the **SAT - Notify Sender of Upload(s) Received** Event Rule, **AdHocRunCommand** includes `SendUploadNotification.wsf //JOB:ON_TIMER` in the **Command parameters** box.
- In the **SAT - Delete Expired Users** Event Rule, **AdHocRunCommand** includes `EFTDeleteExpiredUsers.wsf //JOB:DELETE_USERS` in the **Command parameters** box.

If you edit the custom Command, you might introduce errors, causing the script to not execute as designed. Instead, you should create a separate command, if necessary, and then you can add it as a subsequent Action to the Rule.

# Secure Mobile Access Integration

EFT Server integrates the Secure Mobile Access™ (SMA) module using Event Rules. SMA will automate the provisioning and sharing of user's home folders using TappIn™ by Globalscape® allowing authorized remote users to author, read, edit, and share their files that are stored on EFT Server.

Event Rules and COM API functions have been added or modified to accommodate SMA. EFT Server's Event Rule system performs updates to TappIn's access permissions based on various events in the system. The Event Rules are used to run a Custom Command that executes an SMA script. This executable contacts the TappIn servers to perform the appropriate configuration changes.

**Some details to consider regarding SMA:**

- A Tappin Agent should be installed on the same computer as EFT Server. (You can install Tappin Agents on multiple computers. Refer to the Tappin documentation for details.)
- The TappIn Agent must be configured to "Run As" a user account instead of SYSTEM. This user account must be configured with the appropriate proxy configuration AND the appropriate permissions to access the directories in EFT Server that the TappIn Agent is using for its home directories.

    - To configure the Tappin Agent to "Run As" a user account instead of SYSTEM, in the Services control panel, right-click the TappIn Agent service, and then click **Properties**. Click the **Logon** tab, and then click **This account**, and specify the user account to run the TappIn Agent service. Then restart the TappIn Agent service.
- When a user account is disabled in EFT Server, SMA will disable the user's shared folders in Tappin.
- The installation of the SMA module will automatically create the necessary Event Rules within EFT Server and enable them. The Event Rules are editable and can be disabled/enabled, just like any other Event Rule.

Refer to the *Secure Mobile Access Module User Guide* for details of installing and configuring the Secure Mobile Access module.

# Using Ciphers for Outbound (Event Rule) SSL Connections

EFT Server uses the following ciphers for outbound SSL (HTTPS and FTPS) connections from the Server. The table below lists available EFT Server client (Event Rule) *outbound* algorithms, for TLS only.

| Default Cipher List (FIPS not enabled) | Cipher list when FIPS is enabled |
|---|---|
| DHE-RSA-AES256-SHA | DHE-RSA-AES256-SHA |
| DHE-DSS-AES256-SHA | DHE-DSS-AES256-SHA |
| AES256-SHA | AES256-SHA |
| DHE-RSA-CAMELLIA256-SHA | EDH-RSA-DES-CBC3-SHA |
| DHE-DSS-CAMELLIA256-SHA | EDH-DSS-DES-CBC3-SHA |
| CAMELLIA256-SHA | DES-CBC3-SHA |
| EDH-RSA-DES-CBC3-SHA | DHE-RSA-AES128-SHA |
| EDH-DSS-DES-CBC3-SHA | DHE-DSS-AES128-SHA |
| DES-CBC3-SHA | AES128-SHA |
| DHE-RSA-AES128-SHA | EDH-RSA-DES-CBC-SHA |
| DHE-DSS-AES128-SHA | EDH-DSS-DES-CBC-SHA |
| AES128-SHA | DES-CBC-SHA |
| DHE-RSA-CAMELLIA128-SHA | EXP-EDH-RSA-DES-CBC-SHA |
| DHE-DSS-CAMELLIA128-SHA | EXP-EDH-DSS-DES-CBC-SHA |
| CAMELLIA128-SHA | EXP-DES-CBC-SHA |
| IDEA-CBC-SHA | |
| DHE-DSS-RC4-SHA | |
| RC4-SHA | |
| RC4-MD5 | |
| EXP1024-DHE-DSS-DES-CBC-SHA | |
| EXP1024-DES-CBC-SHA | |
| EDH-RSA-DES-CBC-SHA | |
| EDH-DSS-DES-CBC-SHA | |
| DES-CBC-SHA | |
| EXP1024-DHE-DSS-RC4-SHA | |
| EXP1024-RC4-SHA | |
| EXP-EDH-RSA-DES-CBC-SHA | |
| EXP-EDH-DSS-DES-CBC-SHA | |
| EXP-DES-CBC-SHA | |
| EXP-RC2-CBC-MD5 | |
| EXP-RC4-MD5 | |

For the procedure for **inbound** SSL connections on EFT Server, refer to "Using Ciphers for Inbound SSL Connections" in the *EFT Server User Guide*.

# Commands

EFT Server's *Commands* can execute programs, scripts, or batch files with or without command line arguments, providing administrators almost limitless extensibility. These Commands can be invoked directly by a user from their client (if permitted by the Server administrator) or as an automated Action from EFT Server's Event Rules.

When the Event Rule is triggered, EFT Server executes the specified custom Command and attributes. To configure EFT Server to execute Commands, you first create the command, and then add the command to an Event Rule. In the administration interface, the Commands appear in the tree in the left pane within the Site for which they are defined.

With the **Server** tab selected, when you click the **Commands** node in the left pane, the **Commands List** appears in the right pane.

- Click **New** to open the **Custom Command Wizard** and create a new Command.
- Click a Command then click **Edit** to edit an existing Command.
- Select a Command in the list, and then click **Remove** to delete it. (A confirmation message appears.)

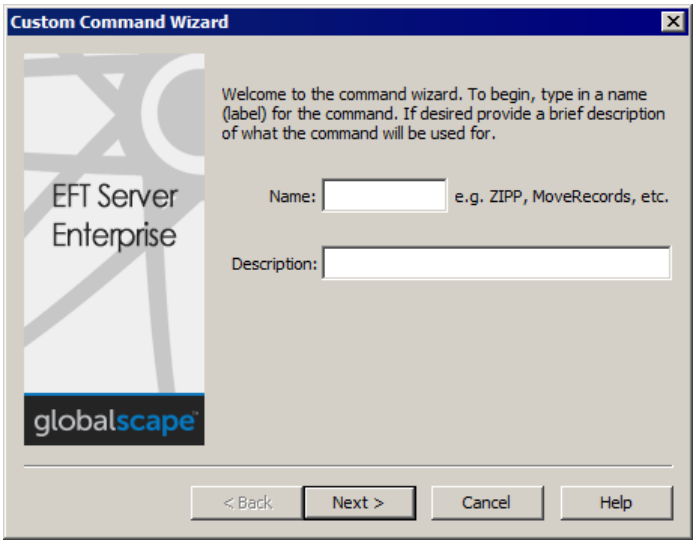
## Creating a Command with the Custom Command Wizard

The **Custom Command** wizard steps you through the process of creating a Command to tell EFT Server to execute programs, scripts, or batch files.

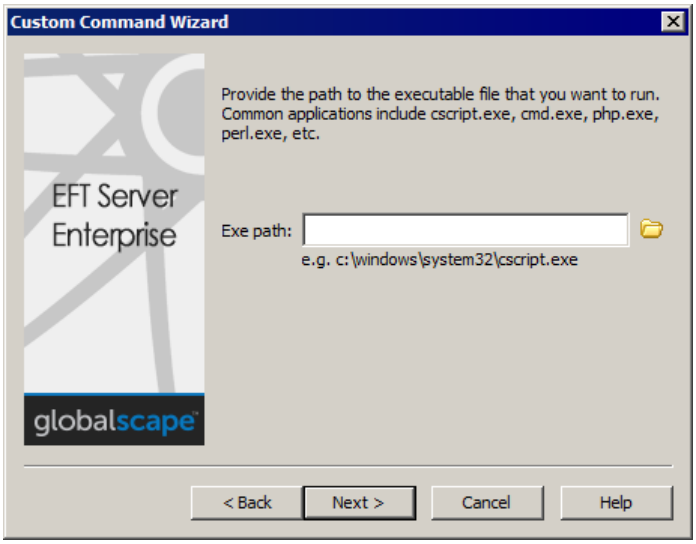
**To create a command with the Custom Command wizard**

1. Do one of the following:
   - On the toolbar, click the **New Command** icon  .
   - On the main menu, click **Configuration > New Command**.
   - In the left pane, right-click the **Commands** node, and then click **New Command**.
   - Click the **Commands** node in the left pane, then, in the right pane, click **New**.
   - Press CTRL+M.

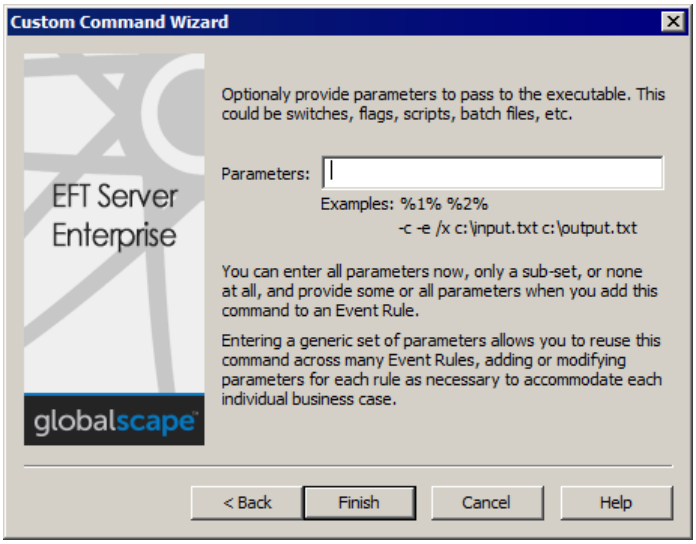
   The **Custom Command Wizard** appears.



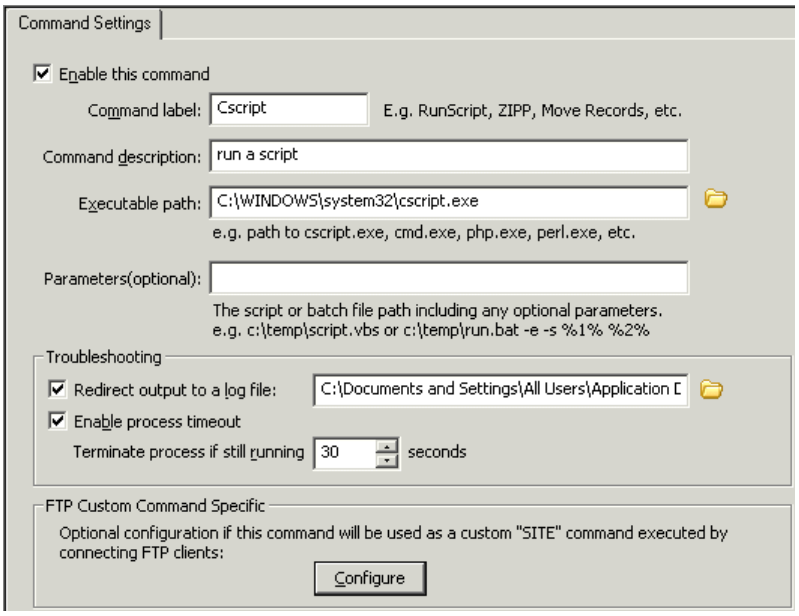
2. In the **Name** box, type a descriptive name for the command. You will reference the Command name in Event Rules, so you should give the Command an intuitive name. For example, instead of `Command 1`, you might call it `Run CScript`.
3. Provide a **Description** that will help you identify the command.
4. Click **Next**. The path page appears.



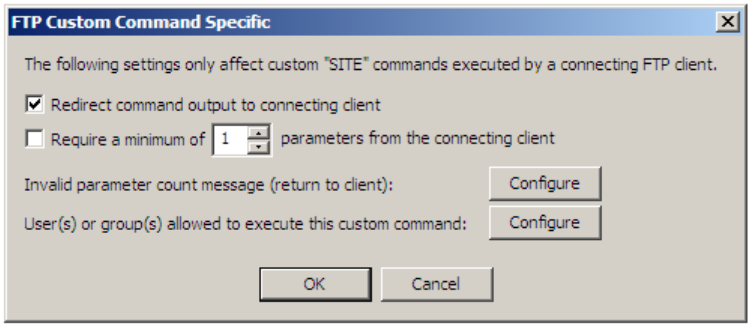

5. In the **Path to executable** box, browse to or type the path to the executable. For example, you can specify a program, a batch file, or a Windows scripting executable, such as cscript.exe or wscript.exe. If you are connected to EFT Server remotely, you can type the path to the file, but be sure the path is relevant to the EFT Server computer, not the remote interface.



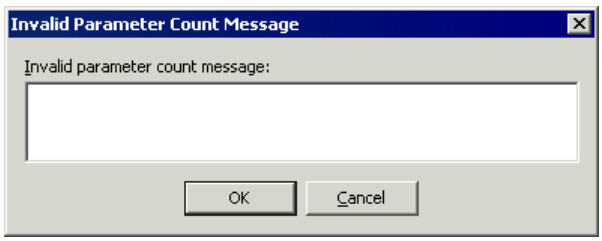

6. (Optional) Specify any required parameters. Alternately, you can specify the parameters when you add the Command to an Event Rule. If there are "standard" parameters that you will always use with the script, you can specify them here, and then modify them or add additional parameters when you add the Command to an Event Rule.
7. Click **Finish**. The Command is added to the **Commands** node for the Site and appears in the Command Settings tab in the right pane.



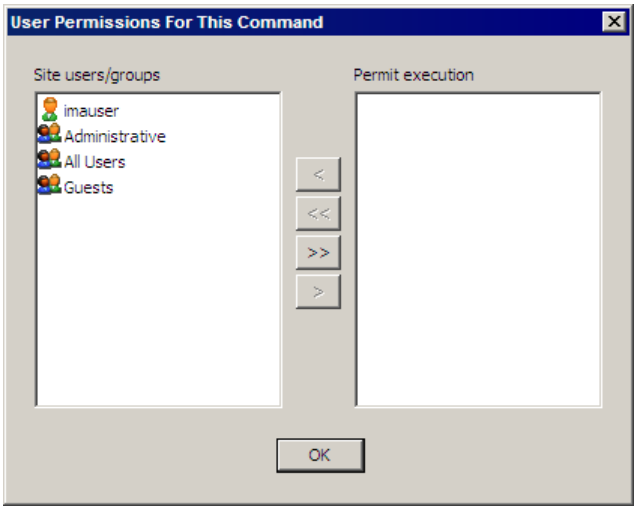

8. If the Command is a custom SITE command executed by a connecting FTP client, you can also configure the **FTP Custom Command Specific** settings, the invalid parameter count message, and which Groups are allowed to execute the Command by clicking **Configure**. The **FTP Custom Command Specific** dialog box appears.




9. Select the **Redirect command output to connecting client** check box to redirect the output from the executed command to the client in a 220 response message. If the check box is not selected, then the output of the command is not returned to the client, even though the command is still executed on the server. Redirecting command output can help the end user ascertain whether the command worked properly (depending on result codes returned by the script or application executed by the custom command on the server).
10. If you want to force the FTP client to send a minimum number of parameters, select the **Require a minimum of** check box and specify the minimum number of parameters required.
    - To provide a message that users will receive when the parameter number is not met, next to **Invalid parameter count message**, click **Configure**. Provide the message, and then click **OK**.



- To specify the users and Groups that can execute the Command, next to **User(s) or group(s) allowed to execute this custom command**, click **Configure**. Double-click the users and/or groups, or use the arrows to move them between the **Site users/groups** list and the **Permit execution** list, and then click **OK**.




11. Click **Apply** to save the changes on EFT Server.

## Editing a Command

The procedure below describes how to edit a command that you can execute with an Event Rule. For a general introduction to Commands, refer to Introduction to Commands. To create a command, refer to Creating a Command with the Custom Command Wizard.

**To edit a command**

1. In the administration interface, connect to EFT Server, and then click the **Server** tab.
2. In the left pane, expand the Site node for the Site that you want to configure, and then click the **Commands** node.
3. In the right pane, double-click the Command that you want to edit. The **Command Settings** tab appears.
4. The **Command label** box displays the name you gave the Command. You will reference the Command label in the Event Rule and **Custom Command** dialog box (in the **Select Command** drop-down menu), so you should give the Command an intuitive name. For example, instead of `Command 1`, you might call it `Run CScript`.
5. The **Command description** box displays the description that you gave the Command.
6. The **Executable path** box displays the path to the file that you want the Command to execute.
7. The **Parameters** box displays any parameters that the client must send. (Parameters are optional.)
8. To create a log that you can use to troubleshoot the command in case of failure, select the **Redirect output to a log file** check box, and then type the path to the log file or click the folder icon to browse to and select the file.
9. If you want EFT Server to return an error if the launched process fails to respond, select the **Enable process timeout** check box and specify the number of seconds the Server should wait before terminating the command.
10. To specify FTP client settings, in the **FTP Custom Command Specific** area, click **Configure**. The **FTP Custom Command Specific** dialog box appears.

11. Select the **Redirect command output to connecting client** check box if the command will be launched by a connecting FTP client. If you select **Redirect command output to connecting client**, the result is sent to the connecting FTP client in a 220 message response.
12. If you want to force the FTP client to send a minimum number of parameters, select the **Require a minimum of** check box and specify the minimum number of parameters required.
    - To provide a message that users will receive when the parameter number is not met, next to **Invalid parameter count message**, click **Configure**. Provide the message, and then click **OK**.
    - To specify the users and Groups that can execute the Command, next to **User(s) or group(s) allowed to execute this custom command**, click **Configure**. Double-click the users and/or groups, or use the arrows to move them between the **Site users/groups** list and the **Permit execution** list, and then click **OK**.
13. Click **Apply** to save the changes on EFT Server.

# Custom Command Example

The following example Command shows the configuration of a custom command from the perspective of both EFT Server and a client. To follow the example exactly, you will need to download and install CuteFTP, which is available as a free 30-day trial and can be downloaded from http://www.globalscape.com/downloads. However, any client that supports custom commands or raw FTP commands will work.

## Creating the Example Command

This command copies EFT Server log files from the **Logs** folder to **C:\Temp** using the Windows xcopy command and CuteFTP's command-line functions.

**To create a custom command**

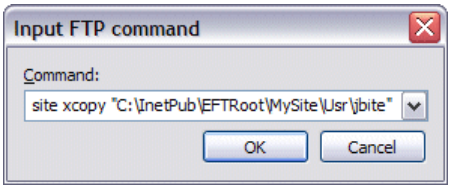
1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, expand the Site node for the Site that you want to configure, and then click **Commands**.
3. In the right pane, click **New**. The **Custom Command Wizard** appears.
4. Follow the instructions in The Custom Command Wizard to define the Command.

## Executing the Example Command

You can run the Command "on the fly," configure the Command in the FTP client (in this example, CuteFTP Professional), or insert the Command in an Event Rule.

**Using the Command "on the fly" in CuteFTP**

1. Start CuteFTP, and create a connection to EFT Server. (Refer to the CuteFTP help for details of how to connect to a server.)
2. If not already displayed, open the **Session Log** pane. (On the main menu, click **View > Show Panes > Individual Session Logs** or press ALT+2.)
3. Right-click a blank area of the **Session Log**, and then click **Input Raw FTP Command**, or press CTRL+SHIFT+I. The **Input FTP Command** dialog box appears.



4. In the **Command** box, type `site`, the name of the Command as defined in EFT Server and any required parameters. For this example, type:
   `site xcopy "C:\InetPub\EFTRoot\MySite\Usr\jbite" "C:\Temp"`
5. Click **OK**. The Command executes. In this example, each of the files in the **\Usr\jbite** folder was copied to the **\Temp** folder. If you selected the **Return output to client** check box when you defined the Command in EFT Server (step 8 above), the **Session Log** displays the results of the Command. For example:

```
COMMAND:> site xcopy "C:\InetPub\EFTRoot\MySite\Usr\jbite" "C:\Temp"
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\cftpsaiProperties.gif
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\EFTtaxonomy_filelist.xml
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\EFTtaxonomy_image001.png
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\inheritance.doc
220-220-C:\InetPub\EFTRoot\MySite\Usr\jbite\Message3.gif
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\RE Certificate Chaining.htm
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\Root Migration Scripts.htm
220-C:\InetPub\EFTRoot\MySite\Usr\jbite\Thumbs.db
220-8 File(s) copied
220-220-
220 Command completed with code 0.
```

**Configuring the Command in CuteFTP**

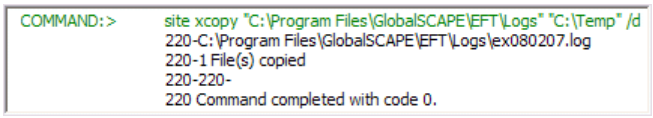
1. Start CuteFTP and connect to EFT Server. (Refer to the CuteFTP help for details of how to connect to a server.)
2. On the main menu, click **Tools > Custom Commands > Edit Custom Commands**. The **Custom Commands** dialog box appears.

   *You must be connected to an FTP server in order for the Commands option to be available.*
3. Click **New** then type a name for the command. For this example, type `xcopy`.
4. Click the command in the tree, and then click **Edit** or right-click the new command and click **Properties**. The **Custom Command Properties** dialog box appears.
5. In the **Label** box, the name of the command appears.
6. In the **Command** box, type:

```
site xcopy "C:\InetPub\EFTRoot\MySite\Usr\jbite" "C:\Temp" /d
```

   *Commands must start with `site` and then the command name you used in EFT Server, not the name you gave the command in CuteFTP. The `/d` parameter copies all new files in the specified folder.*
7. Optionally, specify any key or key combination for the Shortcut Key and any icon for the **Toolbar Icon**.
8. Select the **Place on the Custom Commands toolbar** check box, and then click **OK** to close the **Custom Commands Properties** dialog box.
9. Click **OK** to close the **Commands** dialog box. Your custom command is now enabled and the icon, if specified, appears on the toolbar. (If the command is not displayed, click **View > Toolbars > Custom Commands Bar**.)
10. Start CuteFTP and connect to EFT Server.
11. If it not already displayed, open the **Session Log** pane. (On the main menu, click **View > Show Panes > Individual Session Logs** or press ALT+2.)
12. On the toolbar, click the Command icon that you just created.

13. Monitor the output in the **Session Log**. You should receive various response messages indicating the progress of the archive.




## Executing the Example Command Automatically Using an Event Rule

If you want to copy the log file automatically every day, you can create a Scheduler (Timer) Event and insert the **Execute command in folder** Action. Using this method, you would have to define the parameters in the **Execute Command** dialog box from within the Event Rule.

**Possible Error Situations**

- If you repeat the hard coded parameters in both the client and EFT Server, then the first parameter that the client sends will be used. For example, if *SITE ZIP -c %at[archive name] %ff* is configured in the client, and *-c %1% %2%* is configured in EFT Server, then the first parameter (*-c*) that the client sends will be used as *%1%* and the resulting string would be `-c -c filename.ext`. Therefore, it is important to educate the FTP user on the proper syntax and supply most of the hard-coded parameters on the EFT Server side.
- You must give the FTP client user permission to run the Command on the **Permissions** tab on EFT Server; otherwise, they will receive a "Permission Denied" error.
- Certain command line utilities that may show a Windows prompt or other dialog may not execute properly when called from the FTP engine while it is running as a service. This is especially true when the service is being logged in to from a Local System account.
- EFT Server can return an error if the client provides the wrong number of parameters or invalid parameters.
- To limit security vulnerabilities to EFT Server, the EFT Server administrator should only allow limited access to commands that launch processes.

> ⚠ *Always use caution when giving program access to your system32 directory (especially an FTP server).*

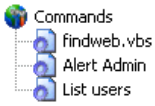
# Viewing and Deleting Commands

Custom Commands defined on a Site appear in the left pane under the Commands node for the Site and in the right pane when the Commands node is selected. To create a command, refer to The Custom Command Wizard. On the **Commands List** tab, you can view and delete Commands, and add new Commands.

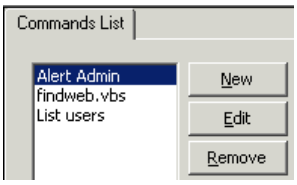
**To view the Commands defined on a Site**

1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, expand the Site node for the Site that you want to configure, and then click **Commands**.

   The Commands appear under the **Commands** node.




   The **Commands List** tab appears in the right pane.




Double-click a Command to view its properties.

**To delete a command, do one of the following:**

- In the right pane, click the Command in the **Commands List**, and then click **Remove**.
- In the left pane, click the Command, and then press DELETE.
- In the left pane, right-click the Command, and then click **Delete**.

## Enabling and Disabling Commands

You can enable and disable Commands as needed, without deleting them.

**To enable or disable a Command**

1. In the administration interface, connect to EFT Server and click the **Server** tab.
2. In the left pane, expand the Site node for the Site that you want to configure, click **Commands**, and then click a Command in the tree. The Command's definition appears in the right pane on the **Command Settings** tab.

   When you create a new Command, the **Enable this command** check box is selected on the **Command Settings** tab.
3. To disable the Command, clear the **Enable this command** check box, and then click **Apply**. When the Command is disabled, an x within a red circle appears over the Command's icon.

# Appendix A: Variables

Below are descriptions of variables that can be used in Event Rules.

## Connection Variables

| Text Displayed | Variable | Description |
|---|---|---|
| Local IP | %CONNECTION.LOCAL_IP% | Local IP address used to connect |
| Local Port | %CONNECTION.LOCAL_PORT% | Local port used to connect |
| Protocol | %CONNECTION.PROTOCOL% | Protocol used to connect |
| Remote IP | %CONNECTION.REMOTE_IP% | Remote IP address used to connect |
| Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% | Indicates whether the user connected via the Web Transfer client |

## Event Variables

| Text Displayed | Variable | Description |
|---|---|---|
| Event Date | %EVENT.DATESTAMP% | Date that the Event was triggered, e.g., `20070828` (suitable for file naming) |
| Event Full Name | %EVENT.EVENTNAME% | User-defined name for the Event Rule (e.g., My File Renamed Event Rule) |
| Event Monitor Health | %EVENT.MONITORHEALTH% | Health of network share |
| Event Name | %EVENT.NAME% | Server-defined name for the Event trigger (e.g., File Renamed) |
| Event Reason | %EVENT.REASON% | Action completed successfully or Action Failed |
| Event Time | %EVENT.TIME% | Date and time that the Event was triggered, e.g., `28 Aug 07 10:01:56` (This variable is **not** suitable for file naming because of the colons; use %EVENT.DATESTAMP% and %EVENT.TIMESTAMP% when using variables for a filename.) |
| Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% | Time to the millisecond when Event was triggered (e.g., Event Time Stamp (including milliseconds): 154207233) |
| Event Timestamp | %EVENT.TIMESTAMP% | Time that the Event was triggered, e.g., `100156` (suitable for file naming) |
| Folder Monitor Failure Reason | %EVENT.MONITORFAILUREREASON% | Reason why the Folder Monitor Rule failed. |

## File System Variables

| Text Displayed | Variable | Description |
|---|---|---|
| Destination File Name | %FS.DST_FILE_NAME% | Destination file name |
| Physical Destination Folder Name | %FS.DST_FOLDER_NAME% | Physical destination folder |
| Physical Destination Path | %FS.DST_PATH% | Physical destination path of the file |
| Virtual Destination Path | %FS.DST_VIRTUAL_PATH% | Virtual destination path of the file involved in the Event |
| CRC | %FILE_CRC% | Indicates whether CRC is in use. |
| File Creation Date | %FS.FILE_CREATE_DATE% | Date the file was created, in the format YYYY/MM/DD, e.g., `8/28/2007` (**not** suitable for file naming because of the slashes) |
| File Creation Time | %FS.FILE_CREATE_TIME% | Time the file was created, in the format HH:MM:SS, e.g., `10:01:56` (**not** suitable for file naming because of the colons) |
| File Name | %FS.FILE_NAME% | Name of the file |
| File Size | %FS.FILE_SIZE% | Size of the file involved in the Event |
| Physical Folder Name | %FS.FOLDER_NAME% | Name of the physical folder |
| File Change | %FS.MONITOR_OPERATION% | File change that triggered the Event (added, removed, etc.) |
| Physical Path | %FS.PATH% | Original physical location of the file |
| Report Content | %FS.REPORT_CONTENT% | Content of the report generated by the Generate Report Action |

| Text Displayed | Variable | Description |
|---|---|---|
| Report Name | %FS.REPORT_FILE% | Name of the report generated by the Generate Report Action. This variable can be used in copy/move, PGP, and custom command actions that are executed synchronously (i.e., custom commands that have a failure Event defined), but should not be used for custom command actions that are executed asynchronously (i.e., custom commands that do not have a failure Event defined.)<br>In some cases, it may be more appropriate to use %FS.REPORT_CONTENT% because this variable represents a copy of the contents of the file rather than a link to the file, which is only good so long as the file exists. For example, since the file will be deleted when EFT Server stops processing the Event Rule, **do not use this variable in e-mail notifications**; use %FS.REPORT_CONTENT% instead. |
| Report File Name | %FS.REPORT_FILENAME% | Location of generated report. This variable can be used in e-mail notifications to include a link to the new location for the file after a copy/move Action. |
| Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% | The structure of the virtual folders |
| Virtual Path | %FS.VIRTUAL_PATH% | Original virtual location of the file |

## Scheduler (Timer) Rule Variables

The %SOURCE.FILE_NAME% variable is available in the list box of the **Destination Folder** page of the **Copy/Move** Action and **Download** Action wizards if the Rule is a Timer/Scheduler Rule.

- If the Rule has a file operation as a trigger (Folder Monitor, On File Upload, File Renamed by Connected Client, etc.) then the variable selection list will include the %FS.*% family of variables and they will have a valid value.
- If the Rule does not have a file operation as a trigger (Timer, User Connected, etc.) then the variable selection list will include the %SOURCE.*% family of variables.

If one of these non-file-trigger Rules contains an %FS.FILE_NAME% variable, it will be converted to %SOURCE.FILE_NAME% and a WARNING will record the change in the EFT.log.

The %SOURCE.FILE_NAME% and %SOURCE.BASE_FILE_NAME% can be used in a Timer Rule to download a mask of files (e.g., *.xml), and then FTP offload each of those files to a remote server with a *.TMP extension (%SOURCE.BASE_FILE_NAME%.TMP). After each file transfer is complete, you can then rename each individual file back to its original name (%SOURCE.FILE_NAME%).

| Variable | Description |
|---|---|
| %SOURCE.BASE_FILE_NAME% | Source file name without extension |
| %SOURCE.FILE_NAME% | Source file name with extension |

## Server Variables

| Text Displayed | Variable | Description |
|---|---|---|
| Log Location | %SERVER.LOG_LOCATION% | Location of the log file |
| Log New Name | %SERVER.LOG_NEW_NAME% | New name of the log file |
| Log New Path | %SERVER.LOG_NEW_PATH% | New path of the log file |
| Log Old Name | %SERVER.LOG_OLD_NAME% | Old name of the log file |
| Log Old Path | %SERVER.LOG_OLD_PATH% | Old path of the log file |
| Log Type | %SERVER.LOG_TYPE% | Either Standard or Verbose, per the setting on the Logs Tab |
| Node Name | %SERVER.NODE_NAME% | Computer name on which EFT Server is running |
| Server Running | %SERVER.STATUS% | Indicates whether the EFT Server service was running when the Event was triggered. (Yes or No) |
| Private Key ring path | %SERVER_PRIVATE_KEYRING_PATH% | Pass the location of the private key ring to the AWE module |
| Public Key ring path | %SERVER_PUBLIC_KEYRING_PATH% | Pass the location of the private key ring to the AWE module |
| Install Directory | %SERVER.INSTALL_DIRECTORY% | Directory in which the server is installed |

## Site Variables

| Text Displayed | Variable | Description |
|---|---|---|
| Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% | Site account management URL, **https://../manageaccount:<port>** (if port is not equal to 443) |
| Site Name | %SITE.NAME% | Site name. |
| Site Status | %SITE.STATUS% | Indicates whether the Site was running when the Event was triggered. (Yes or No) |

## User Variables

| Text Displayed | Variable | Description |
|---|---|---|
| User can connect using FTP | %USER.ALLOW_FTP% | Indicates whether user is allowed to connect using FTP (Yes or No) |
| User can connect using SFTP | %USER.ALLOW_SFTP% | Indicates whether user is allowed to connect using SFTP (Yes or No) |
| User can connect using SSL | %USER.ALLOW_SSL% | Indicates whether user is allowed to connect using SSL (Yes or No) |
| User can change password | %USER.CAN_CHANGE_PASSWORD% | Indicates whether the user is allowed to change the login password (Yes or No) |

| Text Displayed | Variable | Description |
|---|---|---|
| Comment | %USER_COMMENT% | Text in the **Comment** box, if defined in the **User Account Details** dialog box |
| Custom 1 | %USER.CUSTOM1% | Text in the **Custom 1** box, if defined in the **User Account Details** dialog box |
| Custom 2 | %USER.CUSTOM2% | Text in the **Custom 2** box, if defined in the **User Account Details** dialog box |
| Custom 3 | %USER.CUSTOM3% | Text in the **Custom 3** box, if defined in the **User Account Details** dialog box |
| Description | %USER.DESCRIPTION% | Description of the user account, as defined on the **General** tab |
| E-mail Address | %USER.EMAIL% | E-mail address of the user, if defined in the **User Account Details** dialog box. In EFT Server v6.4 and later, you can pass multiple addresses to the using this variable. |
| Account Enabled (v6 and earlier only) | %USER.ENABLED% | Indicates whether the user account is enabled. (Yes or No) |
| Account Expiration Date | %USER.EXPIRATION_DATE% | Indicates the date (in the default system locale) when the user account expired. Date , or `Never` (See HSM note, below.) |
| Fax Number | %USER.FAX% | Fax number of the user, if defined in the **User Account Details** dialog box |
| Full Name | %USER.FULL_NAME% | Full name of the user, if defined on the **User Account Details** dialog box |
| Groups | %USER.GROUPS% | Groups in which the user is a member |
| Home Folder | %USER.HOME_FOLDER% | User's home folder |
| Home IP | %USER.HOME_IP% | IP address of the user |
| Home Folder is Root | %USER.HOME_IS_ROOT% | Indicates whether the **Treat Home Folder as Root** check box is selected. (Yes or No) |
| Invalid login attempts | %USER.INVALID_LOGINS% | Number of invalid login attempts by the user |

| Text Displayed | Variable | Description |
|---|---|---|
| Account Locked Out (v6 and earlier only) | %USER.IS_LOCKED_OUT% | Indicates whether user account is locked out. Yes or No (See HSM note, below.) |
| Last Login Date | %USER.LAST_LOGIN% | Provides the date and time (in the default system locale) the user last logged in to EFT Server |
| Logon Name | %USER.LOGIN% | Login username of the user |
| Pager Number | %USER.PAGER% | Pager number of the user, if defined in the **User Account Details** dialog box |
| Logon Password | %USER.PASSWORD% | Login password of the user |
| Password Expiration Date | %USER.PASSWORD_EXPIRATION% | Provides the date and time (in the default system locale when the user account is set to expire, or `Never` (See HSM note, below.) |
| Phone Number | %USER.PHONE% | Phone number of the user, if defined in the **User Account Details** dialog box |
| Quota Max | %USER.QUOTA_MAX% | Max disk space specified for the user |
| Quota Used | %USER.QUOTE_USED% | Amount of disk space in use by the user |
| User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% | Indicates whether user is required to reset the account password at first log in (Yes or No). (See HSM note, below.) |
| Settings Template | %USER.SETTINGS_LEVEL% | Settings Template of the user |

*For %USER.EXPIRATION_DATE%, %USER.RESET_PASSWORD_AT_FIRST_LOGIN% and %USER.PASSWORD_EXPIRATION%, if the HSM is disabled (not in Activated or Trial state), `No` or `Never` is displayed.*

## AS2 Variables

| Text Displayed | Variable | Value Contained in Variable |
|---|---|---|
| AS2 Content Type | %AS2.CONTENT_TYPE% | Transfer's content type: Application, EDIFACT, XML, Mutually defined EDI, Binary, Plaintext |
| AS2 Direction | %AS2.DIRECTION% | Direction of the transfer |
| AS2 EFT ID | %AS2.EFT_ID% | EFT Server ID used in this transfer |
| AS2 Host | %AS2.HOST% | Address of the host being sent to (outbound) or received from (inbound) |
| AS2 Local MIC | %AS2.LOCAL_MIC% | Local AS2 message identification code (MIC) |
| AS2 MDN | %AS2.MDN% | Message Disposition Notification. The Internet messaging format used to convey a receipt. |
| AS2 Message ID | %AS2.MESSAGE_ID% | AS2 message identifier |
| AS2 Partner ID | %AS2.PARTNER_ID% | Transaction partner's AS2 ID |
| AS2 Payload | %AS2.PAYLOAD% | Name of the file (or an array of file names if MA is used) being transferred over the AS2 session |
| AS2 Remote MIC | %AS2.REMOTE_MIC% | Remote AS2 message identification code (MIC) |
| AS2 Transaction Error | %AS2.TRANSACTION_ERROR% | Error (if any) in the AS2 transaction |
| AS2 Transaction Result | %AS2.TRANSACTION_RESULT% | Overall transaction result (**In Progress**, **Failure**, or **Success**) of the in-context AS2 transaction |
| AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% | Verbose message for the AS2 transaction |

# Appendix B: Events and Available Variables

Each of the Events and the variables that you can use with them are listed below. Refer to Variables for a description of each variable and caveats (e.g., %EVENT.TIME% is not suitable for file naming and %FS.REPORT_FILE% should not be used in e-mail notifications).

## Operating System Events (available only in EFT Server Enterprise)

Scheduler (Timer)—Execute a specified Action one time or repeat at a specified interval. (Enterprise only)

| **... can take these Variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

Folder Monitor—Monitor a specified folder, and then execute an Action whenever a change is detected. (Enterprise only)

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | File Change | %FS.MONITOR_OPERATION% |
| | Physical Path | %FS.PATH% |
| | Physical Folder Name | %FS.FOLDER_NAME% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | File Name | %FS.FILE_NAME% |
| | Physical Destination Path | %FS.DST_PATH% |
| | Physical Destination Folder Name | %FS.DST_FOLDER_NAME% |
| | Destination File Name | %FS.DST_FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

Folder Monitor Failed—Monitor a specified folder, and then execute a specified Action whenever a failure is detected. (Enterprise only.)

*Use the **File Uploaded** file system Event to notify you when a file is uploaded to the Site.*

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Folder Monitor Health | %EVENT.MONITORHEALTH% |
| | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Folder Monitor Failure Reason | %EVENT.MONITORFAILUREREASON% |
| File System Properties | Physical Path | %FS.PATH% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

## File System Events

- Before Download
- Download Failed
- File Deleted
- File Downloaded
- File Moved
- File Renamed
- File Uploaded
- Folder Changed
- Folder Created
- Folder Deleted
- Upload Failed
- Verified Download Failed
- Verified Download Succeeded
- Verified Upload Failed
- Verified Upload Succeeded

File Uploaded—File is uploaded to the Site.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| AS2 Properties | AS2 Payload | %AS2.PAYLOAD% |
| | AS2 MDN | %AS2.MDN% |
| | AS2 Local MIC | %AS2.LOCAL_MIC% |
| | AS2 Remote MIC | %AS2.REMOTE_MIC% |
| | AS2 Message ID | %AS2.MESSAGE_ID% |
| | AS2 Host | %AS2.HOST% |
| | AS2 Transaction Error | %AS2.TRANSACTION_ERROR% |
| | AS2 Transaction Result | %AS2.TRANSACTION_RESULT% |
| | AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% |
| | AS2 Direction | %AS2.DIRECTION% |
| | AS2 Partner ID | %AS2.PARTNER_ID% |
| | AS2 EFT Server ID | %AS2.EFT_ID% |
| | AS2 Content Type | %AS2.CONTENT_TYPE% |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**File Downloaded**—File is downloaded from the Site.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**Verified Upload Succeeded**—Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | File CRC | %FS.FILE_CRC% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**Verified Download Succeeded**—Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | File CRC | %FS.FILE_CRC% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**File Renamed**—File on the Site is renamed by a connected client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Virtual Destination Path | %FS.DST_VIRTUAL_PATH% |
| | Physical Destination Path | %FS.DST_PATH% |
| | Physical Destination Folder Name | %FS.DST_FOLDER_NAME% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Destination File Name | %FS.DST_FILE_NAME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**File Moved—**File is moved from one folder in the VFS to another by a connected client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Virtual Destination Path | %FS.DST_VIRTUAL_PATH% |
| | Physical Destination Path | %FS.DST_PATH% |
| | Physical Destination Folder Name | %FS.DST_FOLDER_NAME% |
| | Destination File Name | %FS.DST_FILE_NAME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**File Deleted**—File is deleted from the Site by connected client

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Virtual Destination Path | %FS.DST_VIRTUAL_PATH% |
| | Physical Destination Path | %FS.DST_PATH% |
| | Physical Destination Folder Name | %FS.DST_FOLDER_NAME% |
| | Destination File Name | %FS.DST_FILE_NAME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**Folder Created**—Folder is created on the Site by a connected client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**Folder Deleted**—Folder is deleted from the Site by a connected client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**Folder Changed**—User navigates to a new folder on the Site.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**Upload Failed**—Upload fails to transfer successfully.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| AS2 Properties | AS2 Payload | %AS2.PAYLOAD% |
| | AS2 MDN | %AS2.MDN% |
| | AS2 Local MIC | %AS2.LOCAL_MIC% |
| | AS2 Remote MIC | %AS2.REMOTE_MIC% |
| | AS2 Message ID | %AS2.MESSAGE_ID% |
| | AS2 Host | %AS2.HOST% |
| | AS2 Transaction Error | %AS2.TRANSACTION_ERROR% |
| | AS2 Transaction Result | %AS2.TRANSACTION_RESULT% |
| | AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% |
| | AS2 Direction | %AS2.DIRECTION% |
| | AS2 Partner ID | %AS2.PARTNER_ID% |
| | AS2 EFT Server ID | %AS2.EFT_ID% |
| | AS2 Content Type | %AS2.CONTENT_TYPE% |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**Download Failed**—Download fails to transfer successfully.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**Verified Upload Failed**—Integrity check of uploaded file fails when transferred using the Web Transfer Client.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | File CRC | %FS.FILE_CRC% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**Verified Download Failed**—Integrity check of downloaded file fails when transferred using the Web Transfer Client.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | File CRC | %FS.FILE_CRC% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**Before Download**—If a download is requested, perform the Action(s) defined in this Event, and then continue with the download.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Virtual Path | %FS.VIRTUAL_PATH% |
| | Physical Path | %FS.PATH% |
| | Virtual Folder Name | %FS.VIRTUAL_FOLDER_NAME% |
| | Physical Folder Name | %FS.FOLDER_NAME% |
| | File Name | %FS.FILE_NAME% |
| | Base File Name | %FS.BASE_FILE_NAME% |
| | File Size | %FS.FILE_SIZE% |
| | File Creation Date | %FS.FILE_CREATE_DATE% |
| | File Creation Time | %FS.FILE_CREATE_TIME% |
| | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

## Server Events

- Service Stopped
- Service Started
- Log Rotated

**Service Stopped**—When the EFT Server service stops.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**Service Started**—When the EFT Server service starts.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**Log Rotated**—When the current activity log closes and EFT Server opens a new log file.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Site Properties | Site Running | %SITE.STATUS% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |
| | Old Log File Path | %SERVER.LOG_OLD_PATH% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | New Log File Path | %SERVER.LOG_NEW_PATH% |
| | Old Log File Name | %SERVER.LOG_OLD_NAME% |
| | New Log File Name | %SERVER.LOG_NEW_NAME% |

## Site Events

- Site Stop
- Site Started
- IP Added to Ban List

**Site Stop**—When the Site stops.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |

**Site Started**—When the Site starts.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |

IP Added to Ban List— This Event will trigger when an IP address is banned by EFT Server (non-interactively) due to invalid login attempts exceeded or other security criteria.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Protocol | %CONNECTION.PROTOCOL% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

# User Events

- User Account Created
- User Account Deleted
- User Account Disabled
- User Account Enabled
- User Account Locked
- User Logged In
- User Logged Out
- User Login Failed
- User Password Changed
- User Quota Exceeded

**User Account Created**—The administrator has created a new user.

*It is possible for a new account to be in a disabled state when the User Account Created event fires. Typically this occurs when using AD or LDAP authentication. When a synchronization occurs with the user data source, EFT Server creates the necessary users on the Site, but if the user is disabled in the user data source, then the new user account will be created in a disabled state. You can use the If Account Enabled Condition if the enable/disable state is part of the Action(s) you want to trigger.*

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Email Address | %USER.EMAIL% |
| | Account Enabled | %USER.ENABLED% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Home Folder | %USER.HOME_FOLDER% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| | Site Running | %SITE.STATUS% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Account Deleted**—An administrator deletes a user account from the Site.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and | Source file name without extension | %SOURCE.BASE_FILE_NAME% |

| | | |
|---|---|---|
| Download Action) | Source file name with extension | %SOURCE.FILE_NAME% |

**User Account Disabled**—The user account is disabled via the Account Security settings or the Invalid login options on the user account's **Security** tab. This Event is also checks at midnight for any expired accounts.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| | Site Running | %SITE.STATUS% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Account Enabled**—When an administrator enables a user account on the Site.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Account Locked**—The user account has been locked out by the server (e.g., invalid login attempts).

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Logged In**—The user logs in to EFT Server.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Logged Out**—The user closes a session gracefully.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Login Failed**—The user attempted an incorrect username or password.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Logon Name | %USER.LOGIN% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Password Changed**—The user or administrator changes a user's password.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| | Site Running | %SITE.STATUS% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Quota Exceeded**—The user has taken too much disk space on EFT Server.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

## Connection Events

- User Connected
- User Connect Failed
- User Disconnected

**User Connected**—When a user connects to the Site (this occurs before log in).

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Connect Failed**—When a user attempts to connect and fails (this can occur before log in).

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| | Event Reason | %EVENT.REASON% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

**User Disconnected**—When a user disconnects from the Site (this can occur before log in).

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| Connection Properties | Remote IP | %CONNECTION.REMOTE_IP% |
| | Local IP | %CONNECTION.LOCAL_IP% |
| | Local Port | %CONNECTION.LOCAL_PORT% |
| | Protocol | %CONNECTION.PROTOCOL% |
| | Using Web Transfer Client | %CONNECTION.USING_WEB_TRANSFER_CLIENT% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |

## AS2 Events (available only in EFT Server Enterprise)

- AS2 Inbound Transaction Succeeded
- AS2 Inbound Transaction Failed
- AS2 Outbound Transaction Succeeded
- AS2 Outbound Transaction Failed

*In AS2 Inbound Transaction Succeeded and AS2 Inbound Transaction Failed Events, the `FS.FILE_NAME` variable contains the name of the file uploaded (for a simple transaction) or an empty string (for a Multiple Attachment (MA) transaction).*

**AS2 Inbound Transaction Succeeded**—Triggers if the inbound transmission was successful, MDN was successfully sent, MICs all match, and no other errors occurred.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| AS2 Properties | AS2 Payload | %AS2.PAYLOAD% |
| | AS2 MDN | %AS2.MDN% |
| | AS2 Local MIC | %AS2.LOCAL_MIC% |
| | AS2 Remote MIC | %AS2.REMOTE_MIC% |
| | AS2 Message ID | %AS2.MESSAGE_ID% |
| | AS2 Host | %AS2.HOST% |
| | AS2 Transaction Error | %AS2.TRANSACTION_ERROR% |
| | AS2 Transaction Result | %AS2.TRANSACTION_RESULT% |
| | AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% |
| | AS2 Direction | %AS2.DIRECTION% |
| | AS2 Partner ID | %AS2.PARTNER_ID% |
| | AS2 EFT Server ID | %AS2.EFT_ID% |
| | AS2 Content Type | %AS2.CONTENT_TYPE% |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**AS2 Inbound Transaction Failed**—Triggers if the AS2 file upload failed for some reason, such as bad MIC, no permissions/access, duplicate message ID, or other AS2 transfer-related error.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| AS2 Properties | AS2 Payload | %AS2.PAYLOAD% |
| | AS2 MDN | %AS2.MDN% |
| | AS2 Local MIC | %AS2.LOCAL_MIC% |
| | AS2 Remote MIC | %AS2.REMOTE_MIC% |
| | AS2 Message ID | %AS2.MESSAGE_ID% |
| | AS2 Host | %AS2.HOST% |
| | AS2 Transaction Error | %AS2.TRANSACTION_ERROR% |
| | AS2 Transaction Result | %AS2.TRANSACTION_RESULT% |
| | AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% |
| | AS2 Direction | %AS2.DIRECTION% |
| | AS2 Partner ID | %AS2.PARTNER_ID% |
| | AS2 EFT Server ID | %AS2.EFT_ID% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | AS2 Content Type | %AS2.CONTENT_TYPE% |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**AS2 Outbound Transaction Succeeded**—Triggers if EFT Server has offloaded a file to a remote partner, and that partner replied with a receipt asynchronously over HTTP/S, indicating that the transfer was successfully completed.

| ... can take these variables | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| AS2 Properties | AS2 Payload | %AS2.PAYLOAD% |
| | AS2 MDN | %AS2.MDN% |
| | AS2 Local MIC | %AS2.LOCAL_MIC% |
| | AS2 Remote MIC | %AS2.REMOTE_MIC% |
| | AS2 Message ID | %AS2.MESSAGE_ID% |
| | AS2 Host | %AS2.HOST% |
| | AS2 Transaction Error | %AS2.TRANSACTION_ERROR% |
| | AS2 Transaction Result | %AS2.TRANSACTION_RESULT% |
| | AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% |
| | AS2 Direction | %AS2.DIRECTION% |
| | AS2 Partner ID | %AS2.PARTNER_ID% |
| | AS2 EFT Server ID | %AS2.EFT_ID% |
| | AS2 Content Type | %AS2.CONTENT_TYPE% |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

**AS2 Outbound Transaction Failed**—Triggers if the expected MDN receipt was not received in the expected time or the receipt signature or MIC failed.

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| AS2 Properties | AS2 Payload | %AS2.PAYLOAD% |
| | AS2 MDN | %AS2.MDN% |
| | AS2 Local MIC | %AS2.LOCAL_MIC% |
| | AS2 Remote MIC | %AS2.REMOTE_MIC% |
| | AS2 Message ID | %AS2.MESSAGE_ID% |
| | AS2 Host | %AS2.HOST% |
| | AS2 Transaction Error | %AS2.TRANSACTION_ERROR% |
| | AS2 Transaction Result | %AS2.TRANSACTION_RESULT% |
| | AS2 Transaction Verbose | %AS2.TRANSACTION_VERBOSE% |
| | AS2 Direction | %AS2.DIRECTION% |
| | AS2 Partner ID | %AS2.PARTNER_ID% |
| | AS2 EFT Server ID | %AS2.EFT_ID% |
| | AS2 Content Type | %AS2.CONTENT_TYPE% |
| Event Properties | Event Time | %EVENT.TIME% |
| | Event Time Stamp | %EVENT.TIMESTAMP% |
| | Event Date Stamp | %EVENT.DATESTAMP% |
| | Event Name | %EVENT.NAME% |
| | Event Full Name | %EVENT.EVENTNAME% |
| | Event Time Stamp (including milliseconds) | %EVENT.TIMESTAMP_PRECISE% |
| File System Properties | Report File | %FS.REPORT_FILE% |
| | Report Content | %FS.REPORT_CONTENT% |
| | Report File Name | %FS.REPORT_FILENAME% |
| User Properties | Groups | %USER.GROUPS% |
| | Logon Name | %USER.LOGIN% |
| | Logon Password | %USER.PASSWORD% |
| | Settings Template | %USER.SETTINGS_LEVEL% |
| | Full Name | %USER.FULL_NAME% |
| | Description | %USER.DESCRIPTION% |
| | Comment | %USER.COMMENT% |
| | Email Address | %USER.EMAIL% |
| | Phone Number | %USER.PHONE% |
| | Pager Number | %USER.PAGER% |
| | Fax Number | %USER.FAX% |
| | Home Folder | %USER.HOME_FOLDER% |
| | Home folder is root | %USER.HOME_IS_ROOT% |
| | Quota Max | %USER.QUOTA_MAX% |
| | Quota Used | %USER.QUOTA_USED% |

| **... can take these variables** | | |
|---|---|---|
| **Type** | **Label (can appear in e-mail notification)** | **Variable** |
| | Invalid login attempts | %USER.INVALID_LOGINS% |
| | User can change password | %USER.CAN_CHANGE_PASSWORD% |
| | Home IP | %USER.HOME_IP% |
| | User can connect using SSL | %USER.ALLOW_SSL% |
| | User can connect using FTP | %USER.ALLOW_FTP% |
| | User can connect using SFTP | %USER.ALLOW_SFTP% |
| | Last Login Date | %USER.LAST_LOGIN% |
| | Password Expiration Date | %USER.PASSWORD_EXPIRATION% |
| | User Must Change Password at Next Login | %USER.RESET_PASSWORD_AT_FIRST_LOGIN% |
| | Account Expiration Date | %USER.EXPIRATION_DATE% |
| Site Properties | Account Management URL | %SITE.ACCOUNT_MANAGEMENT_URL% |
| Source Properties (used in Copy/Move and Download Action) | Source file name without extension | %SOURCE.BASE_FILE_NAME% |
| | Source file name with extension | %SOURCE.FILE_NAME% |
| Server Properties | Server Running | %SERVER.STATUS% |
| | Log Type | %SERVER.LOG_TYPE% |
| | Log Location | %SERVER.LOG_LOCATION% |
| | Node Name | %SERVER.NODE_NAME% |
| | Install Directory | %SERVER.INSTALL_DIRECTORY% |

# Appendix C: List of Conditions

Conditions allow you narrow the trigger definition for an Event Rule. Conditions are optional; you do not have to define a Condition on an Event Rule to make it trigger an Action. Conditions allow more control over when an Action can take place. For example, you might create an Event Rule using the **User Logged In** Event, and then add the **If Logon Name** Condition to trigger the Rule only when a specific user logs in.

Conditions are organized by type:

- AS2-related Conditions—Event is triggered based on criteria such as protocol or AS2 ID.
- Connection Conditions—Event is triggered based on connection information such as remote IP or if user connected via the Web Transfer Client
- File System Conditions—Event is triggered based on criteria such as file size or virtual path.
- Server Conditions—Event is triggered based on criteria such as whether EFT Server is running or log name.
- Site Conditions—Event is triggered based on whether the Site is started or stopped.
- User Conditions—Event is triggered based on criteria such as whether the user account has a particular protocol enabled or login name.
- Event Properties—Event is triggered based on a specific Event reason.

Each of the available Conditions and which Events they can be used with is described below. There are no Conditions available for the **Site Stopped** or **Site Started** Events.

## AS2 Conditions

You can apply these Conditions to File Uploaded and AS2-related events. **(AS2 available with EFT Server Enterprise)**

- **If AS2 Content Type**. Tests whether the AS2 content matches the specified content type.
    1. Add the Condition to a Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the content type **does/does not** equal to **[specific AS2 content type]**. The **Select Content Type** dialog box appears.
    3. Click the **Select Content Type** drop-down list to select a content type (X12, EDIFACT, XML, EDI Consent, Binary, Plaintext).
    4. Click **OK**.
- **If AS2 Partner ID**. Tests whether the AS2 Partner ID matches the specified mask.
    1. Add the Condition to a Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the partner ID **does/does not** equal to **[specific AS2 Partner ID]**. The **Partner Identifier** dialog box appears.
    3. Click the **Select AS2 partner ID** drop-down list to select a partner.
    4. Click **OK**.

You can also specify the AS2 protocol with the **If Protocol Condition** described below.

## Connection Conditions

You can apply these Conditions to Connection Events, File system Events, and certain User Events.

- **If Remote IP**—a connection is made from a remote IP address that matches/does not match an IP address or IP mask.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text.
    3. In the **Edit Value** dialog box, type a string and/or wildcards, and then click **OK** to add the Condition to the Event trigger.
- **If Local IP**—a connection is made to a local IP address that matches/does not match an IP address or IP mask.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text.
    3. In the **Edit Value** dialog box, type a string and/or wildcards, and then click **OK** to add the Condition to the Event trigger.
- **If Local Port**—a connection is made/not made on a port/range of ports.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text.
    3. In the **Edit Value** dialog box, type a string and/or wildcards, and then click **OK** to add the Condition to the Event trigger.
- **If Protocol**—Trigger the Rule when a specific protocol is used or not used.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click **[ftp/ssl/tls/sftp/http/https/as2/adhoc]**. The **Connection Protocol** dialog box appears.
    3. Click the **does** link to specify whether the protocol **does** or **does not** equal certain protocol.
    4. Click the **Select Connection Protocol** drop-down list to select the protocol (or specify **Any Protocol**).
    5. Click **OK**.
- **If Using Web Transfer Client**—the user connected/did not connect via the Web Transfer Client.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the WTC **does/does no**t equal to **Yes/No**.

## Site Conditions

You can apply this Condition only to the **User Account Disabled**, **User Password Changed**, **User Account Created** Events.

- **If Site running**—The Site is started or stopped.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the Site Running **does/does no**t equal to **Yes/No**.

## File System Conditions

You can apply these Conditions only to File system Events and the Folder Monitor Event.

- **If File Change**—a file is/is not added, removed, or renamed in a folder. This Condition is added automatically when you create a **Folder Monitor** Event.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the file change **does/does not** equal to **added**, **removed**, or **renamed**.
- **If Virtual Path**—the file or folder exists, does not exist at a virtual location and/or wildcard.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
    3. In the **Choose Virtual Paths** dialog box, specify a path or wildcard, and then click **Add** to move the path to the right text box. You can add multiple paths.
    4. To remove a path, in the right text box, click the path or wildcard, and then click **Remove**.
    5. Click **OK** to add the Condition to the Event trigger.
- **If Physical Path**—the file or folder exists, does not exist at a physical location (the full folder path including the file name or wildcard).
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
    3. In the **Choose Physical Paths** dialog box, specify a path or wildcard, and then click **Add** to move the path to the right text box. You can add multiple paths.
    4. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
    5. Click **OK** to add the Condition to the Event trigger.
- **If Physical Folder Name**—the file or folder exists, does not exist in a physical folder (the folder path or wildcard without a file name).
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
    3. In the **Choose Folder Names** dialog box, specify a folder name or wildcard, and then click **Add** to move the folder name or wildcard to the right text box. You can add multiple folders.
    4. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
    5. Click **OK** to add the Condition to the Event trigger.
- **If Virtual Folder Name**—the file or folder exists, does not exist in a virtual folder.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the virtual folder name **does/does not match/start with [path mask]**.

3. In the **Choose Folder Names** dialog box, specify a folder name or wildcard, and then click **Add** to move the folder name or wildcard to the right text box. You can add multiple folders.
4. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
5. Click **OK** to add the Condition to the Event trigger.

- **If File Name**—the file name matches/does not match a string of characters and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not** match **[path mask]**.
  3. In the **Choose File Names** dialog box, specify a file name or wildcard, and then click **Add** to move the file name or wildcard to the right text box. You can add multiple file names.
  4. To remove a path, in the right text box, click the file name or wildcard, and then click **Remove**.
  5. Click **OK** to add the Condition to the Event trigger.
- **If Base File Name**—The portion of the filename to the left of the right most period; provided as a way to support rename. For example, if a file is downloaded as SomeFile.ext.tmp, the Base File Name is: SomeFile.ext.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not** match **[mask]**.
  3. In the **Choose File Names** dialog box, specify a file name or wildcard, and then click **Add** to move the file name or wildcard to the right text box. You can add multiple file names.
  4. To remove a file name or wildcard, in the right text box, click the file name or wildcard, and then click **Remove**.
  5. Click **OK** to add the Condition to the Event trigger.
- **If File Size**—the file size is or is not less than, equal to, or greater than a specified number of bytes.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the file size **is/is not equal to, greater than or equal to, less than, less than or equal to [size (B)]**.
  3. In the **Edit Value** dialog box, specify a file size in bytes, and then click **OK**.
- **If Physical Destination Path**—(for **File Moved** Event) the file or folder exists, does not exist at a physical location and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. In the **Choose Physical Paths** dialog box, specify a path or wildcard, and then click **Add** to move the path or wildcard to the right text box. You can add multiple paths.
  4. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.

5. Click **OK** to add the Condition to the Event trigger.

- **If Virtual Destination Path**—(for **File Moved** Event) the file or folder exists, does not exist at a virtual location (the full folder path including the file name and/or wildcard).
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. In the **Choose Virtual Paths** dialog box, specify a path or wildcard, and then click **Add** to move the path to the right text box. You can add multiple paths.
  4. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
  5. Click **OK** to add the Condition to the Event trigger.
- **If Physical Destination Folder Name**—(for **File Moved** Event) the physical folder name matches/does not match a physical folder name and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. In the **Choose Folder Names** dialog box, specify a folder name or wildcard, and then click **Add** to move the folder name or wildcard to the right text box. You can add multiple names.
  4. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
  5. Click **OK** to add the Condition to the Event trigger.
- **If Destination File Name**—(for **File Moved** Event) the destination file name matches/does not match a string of characters and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the virtual path **does/does not** match **[path mask]**.
  3. In the **Choose File Names** dialog box, specify a file name or wildcard, and then click **Add** to move the file name or wildcard to the right text box. You can add multiple names.
  4. To remove a file name or wildcard, in the right text box, click the file name or wildcard, and then click **Remove**.
  5. Click **OK** to add the Condition to the Event trigger.

## Server Conditions

You can apply these conditions to certain Server Events, Operating System Events, File System Events, and the **IP Added to Ban List** Site Event.

- **If Server Running—**The EFT Server service is currently running.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the Server **does/does not** equal to **Yes/No**.
- **If Log Type**—The log type is/is not a specific type.
  1. Add the Condition to the Event Rule.

2. In the **Rule Builder**, click the linked text to specify whether the log type **does/does not** equal to **[specific type]**.
3. In the **Select Log Type** dialog box, specify a Log Type, and then click **OK**.

- **If Log Location**—The log location matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the log location **does/does not** match **[path]**.
  3. In the **Edit Value** dialog box, specify a path or wildcard, and then click **OK**.
- **If Node Name**—EFT Server name matches/does not match a specific character string.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the node name **does/does not** equal to **[name]**.
  3. In the **Edit Value** dialog box, specify a name or wildcard, and then click **OK**.
- **If Old Log File Path**—(Used with the **Log Rotated** Event only) The old log file path matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the old log location **does/does not** match **[path]**.
  3. In the **Edit Value** dialog box, specify a path or wildcard, and then click **OK**.
- **If New Log File Path**—(Used with the **Log Rotated** Event only) The new log file path matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the new log location **does/does not** match **[path]**.
  3. In the **Edit Value** dialog box, specify a path or wildcard, and then click **OK**.
- **If Old Log File Name**—(Used with the **Log Rotated** Event only) The old log file name matches a specific name.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the old log location **does/does not** match **[path]**.
  3. In the **Edit Value** dialog box, specify a path or wildcard, and then click **OK**.
- **If New Log File Name**—(Used with the **Log Rotated** Event only) The new log file name matches a specific name.
  1. Add the Condition to the Event Rule.
  2. In the **Rule Builder**, click the linked text to specify whether the new log location **does/does not** match **[path]**.
  3. In the **Edit Value** dialog box, specify a path or wildcard, and then click **OK**.

## User Conditions

You can apply user conditions to User Events and File system Events.

- **If User Groups**—the user account is or not a member of one or more Groups.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the user group **is/is not** a member of **[specific group(s)]**.
    3. In the **Specify target users and groups** area, select the check box of the users/groups that will trigger the Event and clear the **All Users** check box if you don't want the Condition to apply to all users.
    4. Click **OK** to add the Condition to the Event trigger.
- **If Logon Name**—the user's username matches/does not match a specific username.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the logon name **is/is not** one of **[specified name(s)]**.
    3. In the **Specify target users and groups** area, select the check box of the user that will trigger the Event and clear the **All Users** check box if you don't want it to apply to all users.
    4. Click **OK** to add the Condition to the Event trigger.
- **If Logon Password**—the user's password matches/does not match a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the logon password **is/is not** one of **[specified password(s)]**.
    3. In the **Choose Passwords** dialog box, specify a password, and then click **Add** to move the password to the right text box.
    4. To remove a password, in the right text box, click the password, and then click **Remove**.
    5. Click **OK** to add the Condition to the Event trigger.
- **If Account Enabled**—the user account is enable or not enabled
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the account **does/does not** equal to **Yes/No**.
- **If Settings Template**—the user belongs/does not belong to a Settings Template.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the Settings Template **does/does not** equal to **[Settings Template]**.
    3. In the **Select Settings Template** dialog box, specify a Settings Template, and then click **OK**. (Even if there is only one Settings Template, you still have to click **OK** in the **Select Settings Template** dialog box to complete the Condition.)

- **If Full Name**—a user's name matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the user account name **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Description**—the user's description matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the description **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a word, and then click **OK**.
- **If Comment**—the user's comment matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the comment **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If EMail Address**—the user's e-mail address matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the email address **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Phone Number**—the user's phone number matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the phone number **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Pager Number**—the user's pager number matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the pager number **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Fax Number**—the user's fax number matches/does not match, contains/equals a specific string.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the fax number **does/does not equal to/contain [specific word]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **If Home Folder**—the location of a user's home folder matches/does not match a physical location.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the home folder **does/does not** match **[path]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Home Folder is root**—the user's home folder is/is not their root directory.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether home folder root **does/does not** equal to **[yes/no]**.
- **If Quota Max**—the user's account has a size limit less than/equal to/not less than/not equal to a size in kilobytes.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the maximum quota **does/does not** equal to **[size (MB)]**.
    3. In the **Edit Value** dialog box, specify string, and then click **OK**.
- **If Quota Used**—the user's filled disk space is/is not less than/equal to/greater than an amount of allowed disk space.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the home folder **is/is not equal to, greater than or equal to, less than, less than or equal to [size (MB)]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Invalid login attempts**—the user's failed login attempts are/are not less than, equal to, greater than a number.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether invalid login attempts **is/is not equal to, greater than or equal to, less than, less than or equal to [number]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If User can change password**—the user has/does not have permission to change the login password.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether user can change password **does/does not** equal to **[yes/no]**.
- **If Home IP**—the user's allowed IP address matches/does not match an IP address or set of IP addresses.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the home IP **does/does not** match **[ip mask]**.
    3. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **If User can connect using SSL**—the user has/does not have SSL enabled.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether user can connect using SSL **does/does not** equal to **[yes/no]**.
- **If User can connect using FTP**—the user has/does not have FTP enabled.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether user can connect using FTP **does/does not** equal to **[yes/no]**.
- **If User can connect using SFTP**—the user has/does not have SFTP enabled.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether user can connect using SFTP **does/does not** equal to **[yes/no]**.

## Event Properties

- **If Folder Monitor Failure reason**—Available only with the Folder Monitor Failed Event.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the Failure reason **does/does not** equal to **[reason]**.
    3. Click the **[reason]** link to specify which sort of failure to trigger on: **any failure**, **archive failed**, or **health check failed**.
- **If Event Reason**—The Event was triggered by one of the reasons in the table below. Available reasons depend on the Event trigger (**User Connect Failed**, **User Login Failed**, **User Logged Out**, **Download Failed**, **Upload Failed**, **Verified Upload Failed**, **Verified Download Failed**). For example, **IP address was rejected** can apply to the **User Connect Failed** Event; but cannot apply to any other Event triggers.
    1. Add the Condition to the Event Rule.
    2. In the **Rule Builder**, click the linked text to specify whether the Event Reason **does/does not** equal to **[specific reason]**.
    3. Click the **[specific reason]** link to specify which sort of failure to trigger on (refer to table below for Event Reasons).

| Event Reason | Event Trigger | | | | | | |
|---|---|---|---|---|---|---|---|
| | **User Connect Failed** | **User Login Failed** | **User Logged Out** | **Download Failed** | **Upload Failed** | **Verified Upload Failed** | **Verified Download Failed** |
| Aborted by user | | | | X | X | X | X |
| Access denied | | | | X | X | X | X |
| Account Disabled | | X | | | | | |
| Account Locked Out (v6.1 and later) | | X | | | | | |
| Client SSL certificate was rejected | X | | | | | | |
| Connection closed | | | | X | X | X | X |
| File is banned | | | | X | X | X | X |
| File not found | | | | X | | | |
| FTP Session was closed because of error | | | X | | | | |
| FTP Session was closed by timeout | | | X | | | | |
| FTP Session was closed by user (QUIT) | | | X | | | | |
| Invalid password | | X | | | | | |
| IP address was banned | | | X | | | | |
| IP address was rejected | X | | | | | | |
| IP address was rejected and banned | X | | | | | | |
| Max incorrect password attempts reached | | | X | | | | |
| Protocol not supported | | X | | | | | |
| Quota exceeded | | | | | X | X | X |
| Restricted IP | | X | | | | | |
| TCP/IP connections was closed by peer | | | X | | | | |
| Too many connections per IP | X | X | | | | | |
| Too many connections per Site | X | X | | | | | |
| Too many connections per user | | X | | | | | |
| User was kicked by administrator | | | X | | | | |

# Appendix D: Which Actions are Available with Which Event Triggers?

*When EFT Server performs a copy/move Action, the folder from which the files are moved remains and is emptied, but not deleted.*

*Certain Actions (Execute Advanced Workflow, Copy/move (push) file to host, Download (pull) file from host, and AS2 Send file to host) are available only in EFT Server Enterprise. The Actions are visible, but unavailable (grayed out) in EFT Server SMB.*

("X" indicates the Action is available for that Event; gray indicates the Action is not available for that Event.)

The EFT Server service must be running for an Event Rule to fire.

Certain Actions are only available with certain triggers, as shown in the table below. For example, the **User Disconnected** Event trigger has no reason to trigger the **Cleanup Folder** Action.

| Event Triggers | Actions<br>The Actions Execute command in folder, Execute Advanced Workflow, Send notification email, and Stop processing more rules are available for every event. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Copy/move file to host | Download file from host | OpenPGP Encrypt, Encrypt + Sign, Decrypt | Cleanup folder | Generate Report | AS2 Send file to host | Backup Server Config | Write to WEL |
| **Scheduler (Timer)** | X | X | X | X | X | X | X | X |
| **Folder Monitor** | X | X | X | | | X | | X |
| **Folder Monitor Failed** | | X | | X | | | | X |
| **File Uploaded** | X | | X | | X | X | | X |
| **File Downloaded** | X | X | X | | X | X | | X |
| **Verified Upload Succeeded** | X | X | X | | X | X | | X |
| **Verified Download Succeeded** | X | X | X | | X | X | | X |
| **File Renamed** | X | X | X | | X | X | | X |
| **File Moved** | X | X | X | | X | X | | X |
| **File Deleted** | X | X | | | X | X | | X |
| **Folder Created** | X | X | | | X | X | | X |
| **Folder Deleted** | X | X | | | X | X | | X |
| **Folder Changed** | X | X | | | X | X | | X |
| **Upload Failed** | X | | | | X | X | | X |
| **Download Failed** | X | X | | | X | X | | X |
| **Verified Upload Failed** | X | | | | X | X | | X |
| **Verified Download Failed** | X | X | | | X | X | | X |
| **Before Download** | X | X | | | X | X | | X |
| **Service Stopped** | | | | | X | | X | X |
| **Service Started** | | X | | | X | | X | X |
| **Log Rotated** | X | X | X | | X | | | X |
| **Site Stop** | | | | | X | | | X |
| **Site Started** | | X | | | X | | | X |
| **IP Added to Ban List** | X | X | X | X | X | X | X | X |
| **User Account Enabled** | | X | | | X | | | X |
| **User Account Disabled** | | X | | | X | | | X |

| Event Triggers | Actions<br>The Actions Execute command in folder, Execute Advanced Workflow, Send notification email, and Stop processing more rules are available for every event. | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Copy/move file to host | Download file from host | OpenPGP Encrypt, Encrypt + Sign, Decrypt | Cleanup folder | Generate Report | AS2 Send file to host | Backup Server Config | Write to WEL |
| **User Account Locked** | | X | | | X | | | X |
| **User Quota Exceeded** | X | X | | | X | | | X |
| **User Logged Out** | X | X | X | | X | | | X |
| **User Logged In** | X | X | X | | X | | | X |
| **User Login Failed** | | X | | | X | | | X |
| **User Password Changed** | | X | | | X | | | X |
| **User Account Created** | | X | | | X | | | X |
| **User Account Deleted** | | X | | | X | | | X |
| **User Connected** | | X | | | X | | | X |
| **User Connect Failed** | | X | | | X | | | X |
| **User Disconnected** | | X | | | X | | | X |
| **AS2 Inbound Transaction Succeeded** | | X | | | X | | | X |
| **AS2 Inbound Transaction Failed** | | X | | | X | | | X |
| **AS2 Outbound Transaction Succeeded** | | X | | | X | | | X |
| **AS2 Outbound Transaction Failed** | | X | | | X | | | X |

# Appendix E: Event Rule Examples

This section describes how to create the following Event Rule examples:

- Scheduled Task
  - Cleanup old downloaded files
  - Download *.pdf from remote host
- Folder Monitor
  - Encrypt file
  - Push to remote host
  - Send email notification
- On File Upload
  - Decrypt file
  - If Failed send email notification
  - Write to Event Log

## Scheduled Task with Cleanup and Download Actions

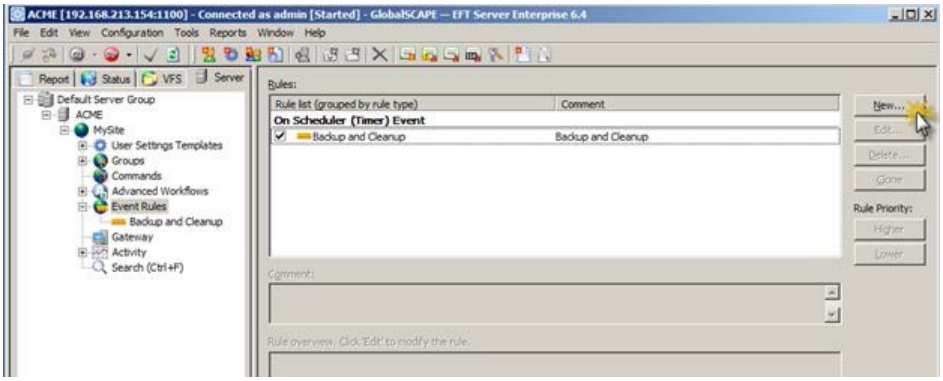
We want this Event Rule to run a task every 2 hours to delete all PDF files in a folder that are older than 7 days, and then download all PDF files from a folder on a remote host.

### Prerequisites

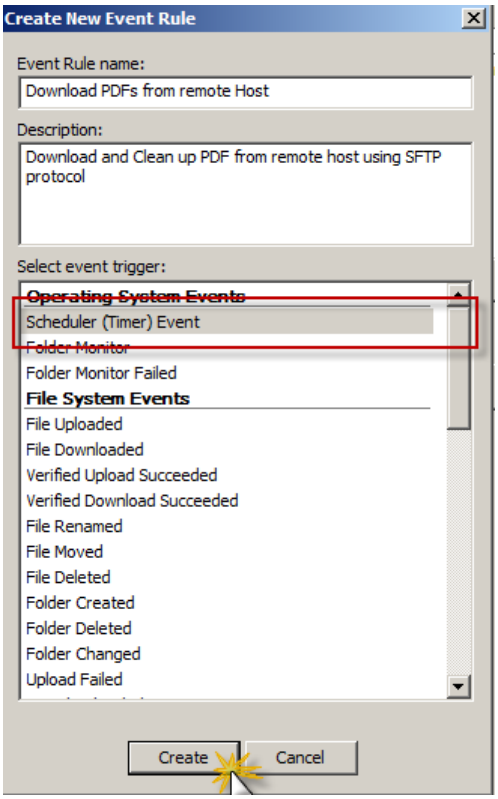
- Account with permissions on remote host
- Full control over local folder

**To create a Scheduled Task**

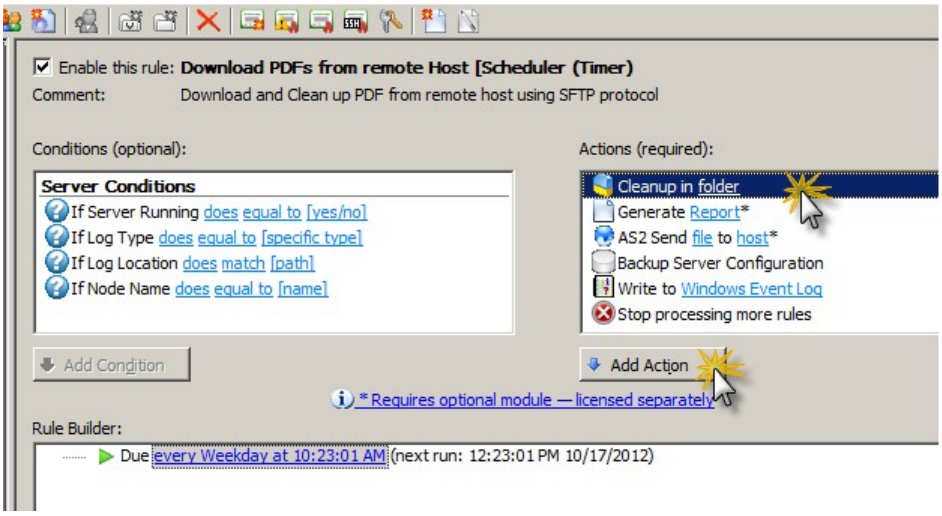
1. Create a new Event Rule.



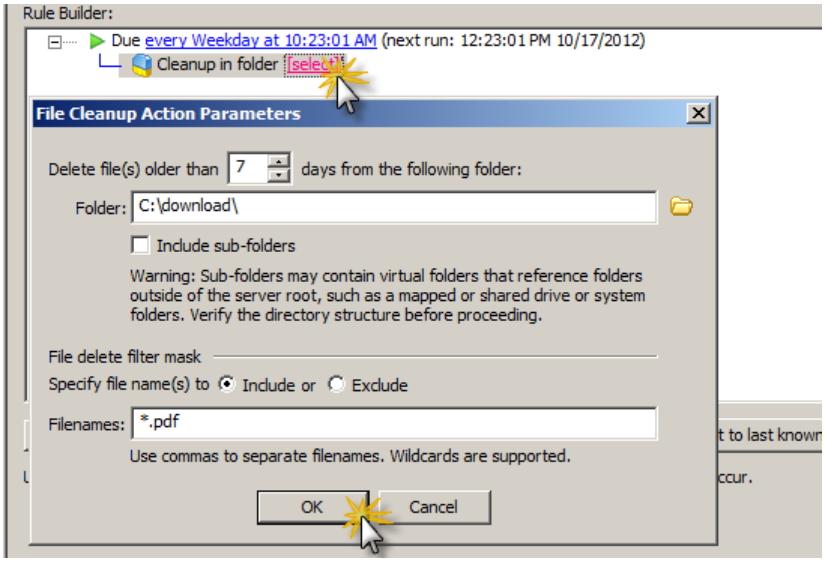
2. Select the **Scheduler (Timer) Event** trigger and name the Rule.



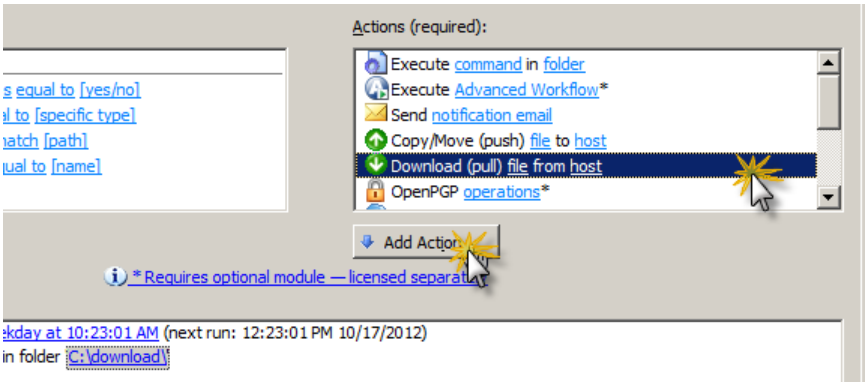

3. Add the **Cleanup in folder** Action.



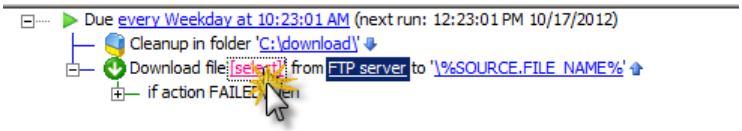
4. Configure the **Cleanup in folder** Action to specify the age of files to delete and which file names/types to delete.



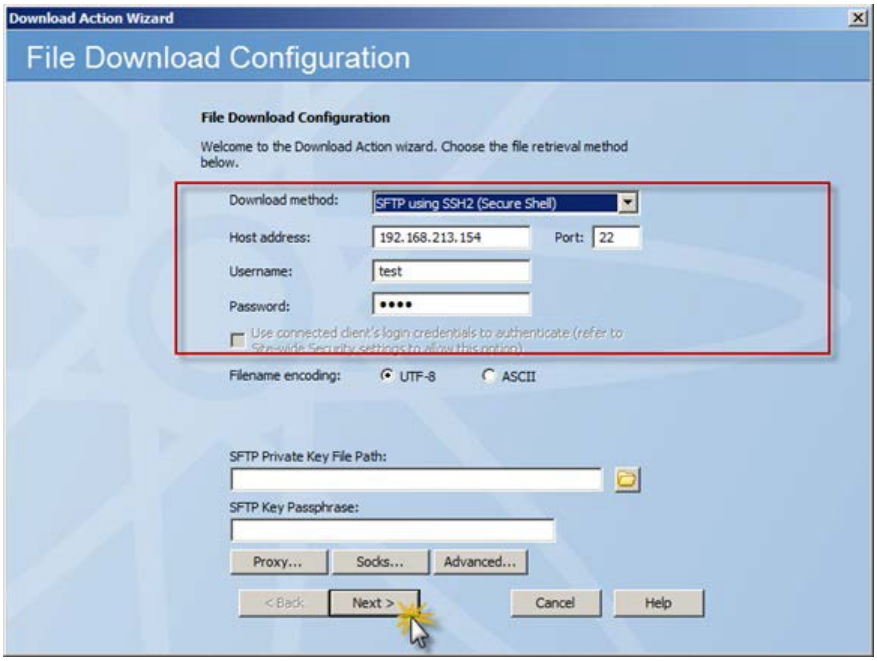

5. Add the **Download (pull) file from host** Action.



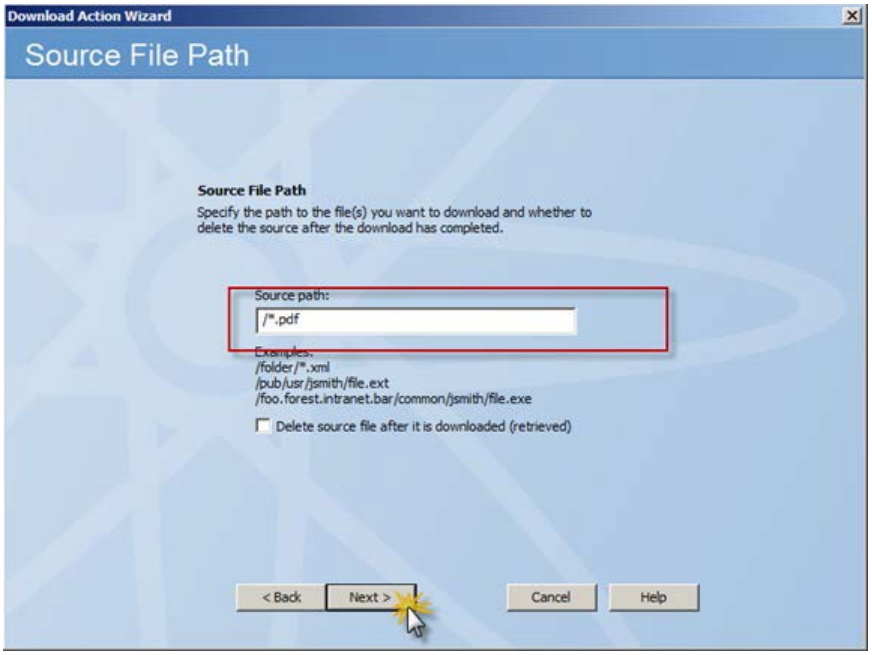

6. Click the Download Action in the Rule Builder to configure it.



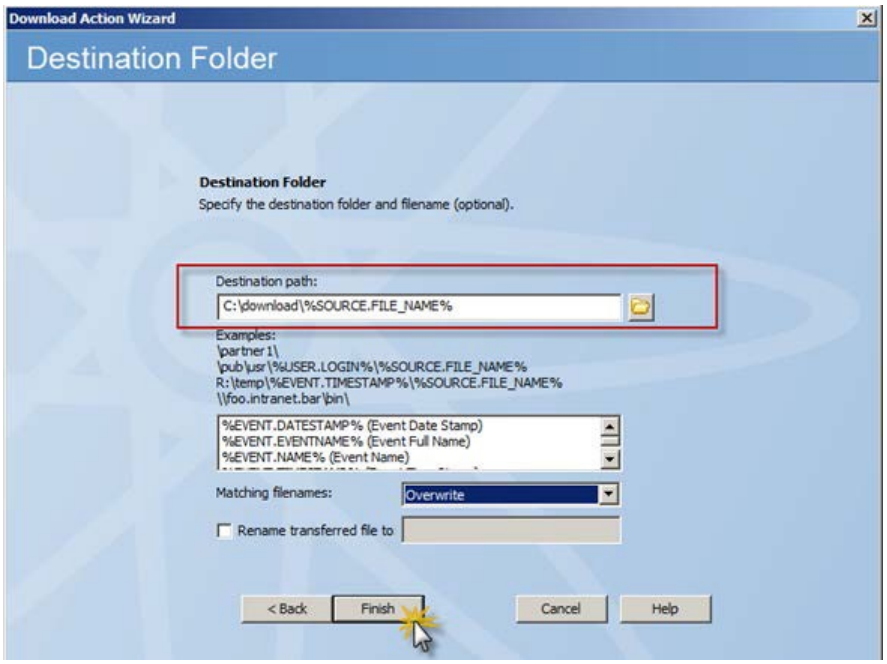
7. Configure the connection and login details.



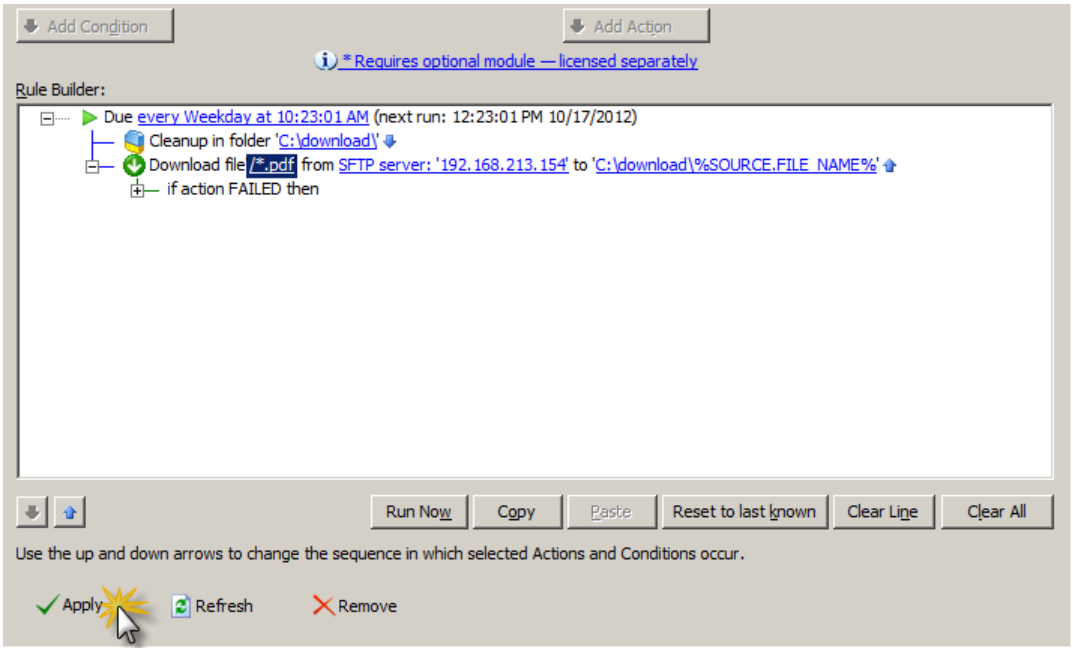

8. Specify the Source path for downloading.



9. Specify where to save the downloaded files.

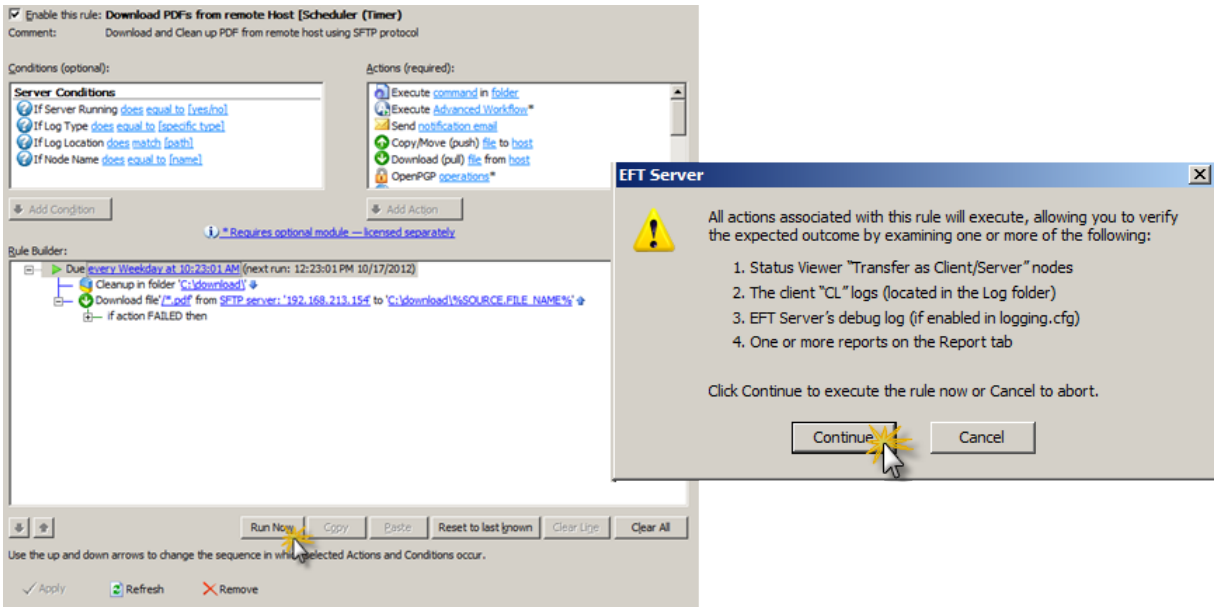



10. Remember to apply your changes!

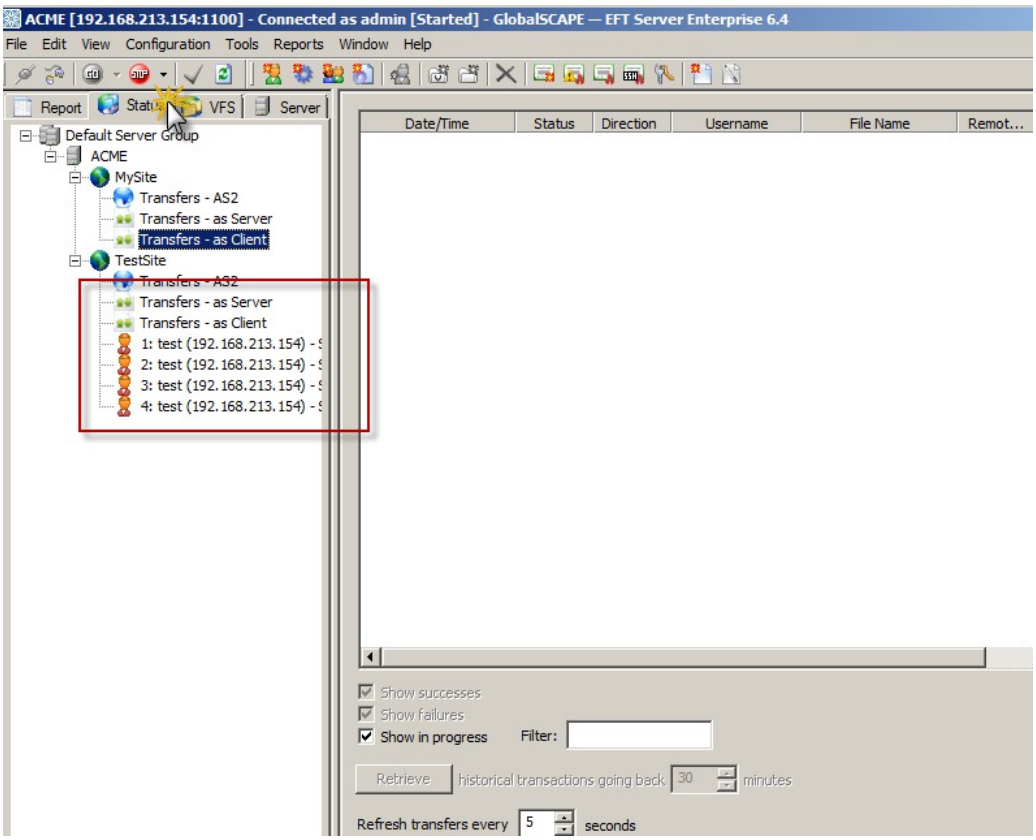



This Rule now reads, "Every Wednesday at 10:23:01 am, cleanup the files in C:\download, and then download all PDF files from this remote location."

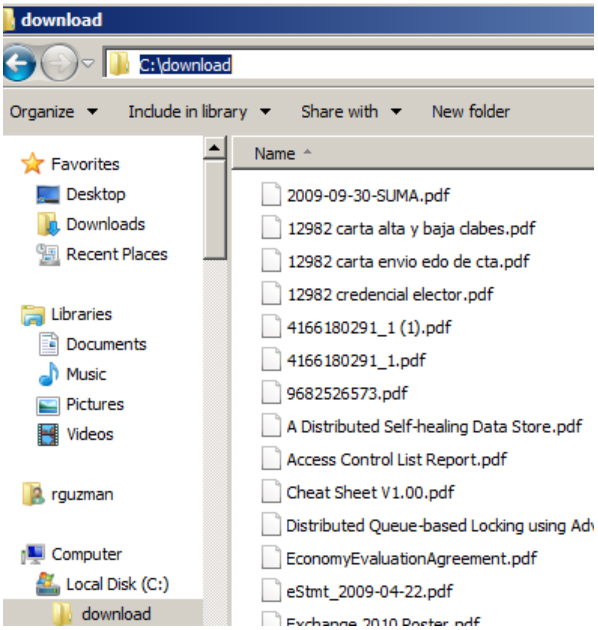
11. Click **Run Now** to run the task to verify success.




12. Click the **Status** tab to view the transfers in real time.



13. Look for expected files to have been downloaded locally to the folder specified in the Download Action (in this example, C:\download).



# Folder Monitor with OpenPGP, Copy, and Email Actions

We want this Event Rule to do the following:

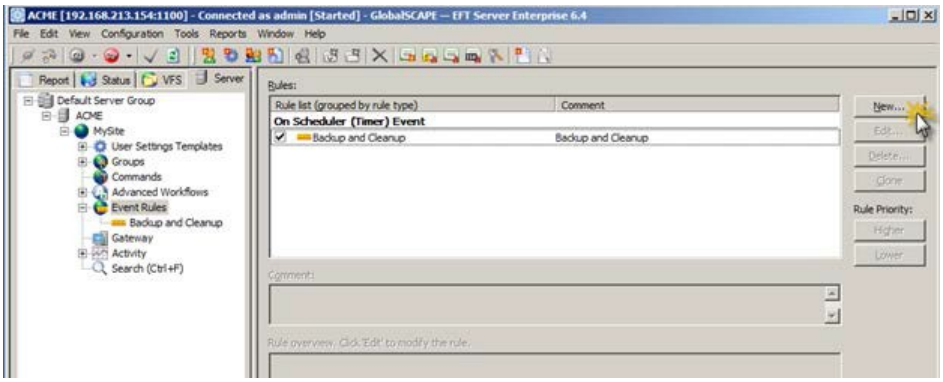
1. Monitor the folder C:\scans
2. Encrypt a file
3. Push the file to a remote host
4. Send an email notification

## Prerequisites

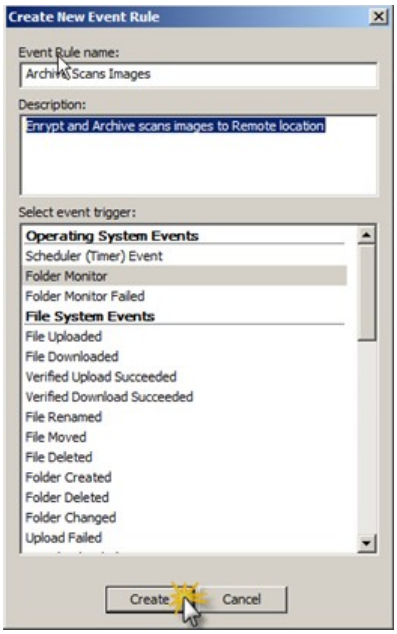
- Public PGP key imported from destination
- Account with permissions on remote host
- Email address for notification

**To create a Folder Monitor Event Rule**

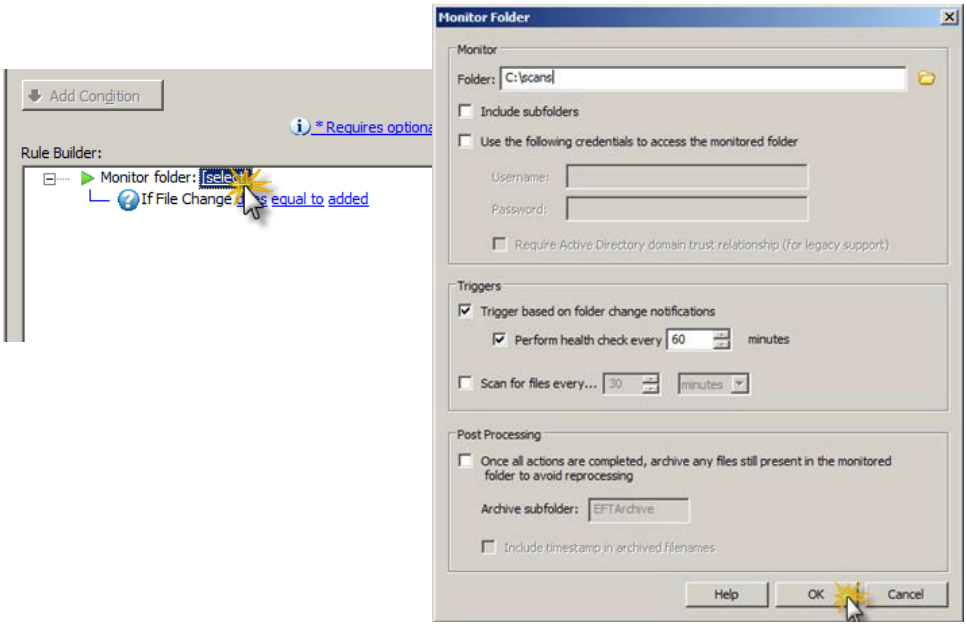
1. Create a new Event Rule.



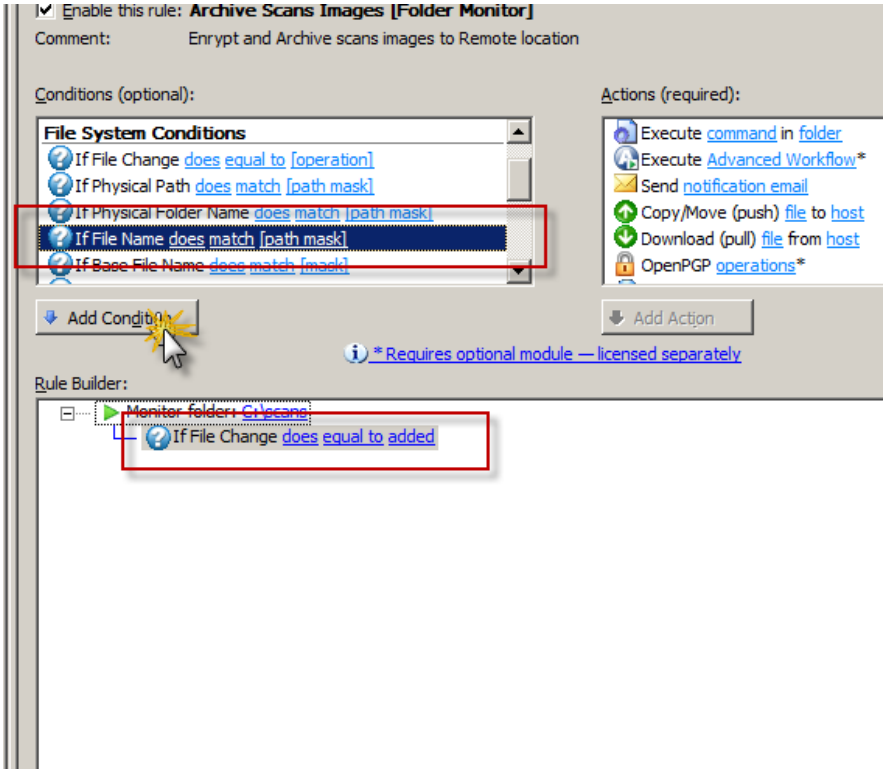

2. Select the Folder Monitor event trigger and name the Rule



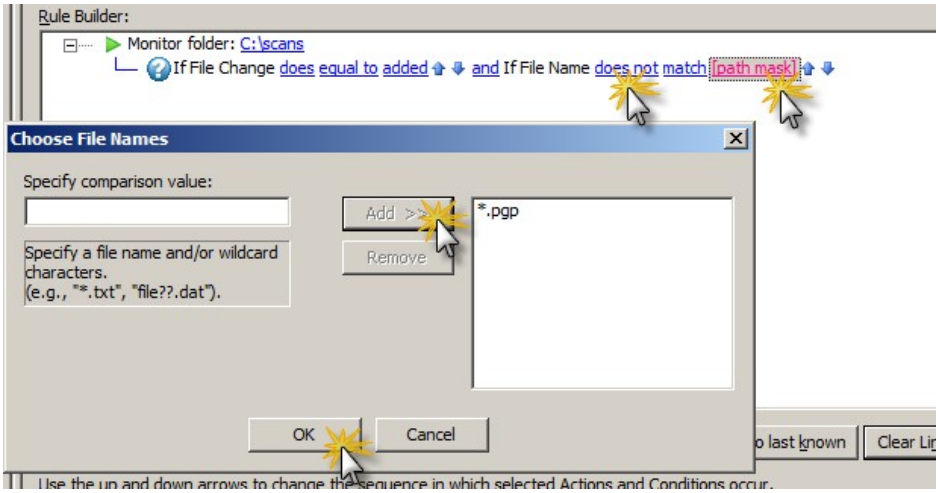
3. Configure the Folder Monitor settings.



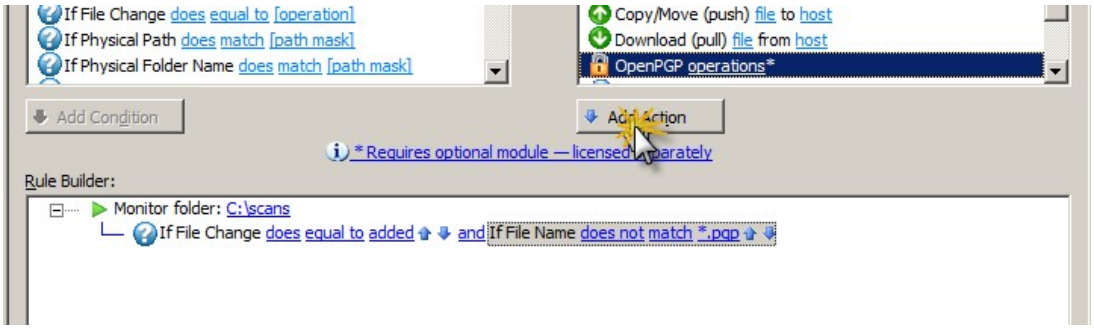

4. Notice that the **File Change** Condition is added automatically. Ensure that the Condition is highlighted in the Rule Builder, and then add the **File Name** Condition.



5. Configure the **File Name** Condition to look for non-PGP files, and click “does” to change it to “does not.”

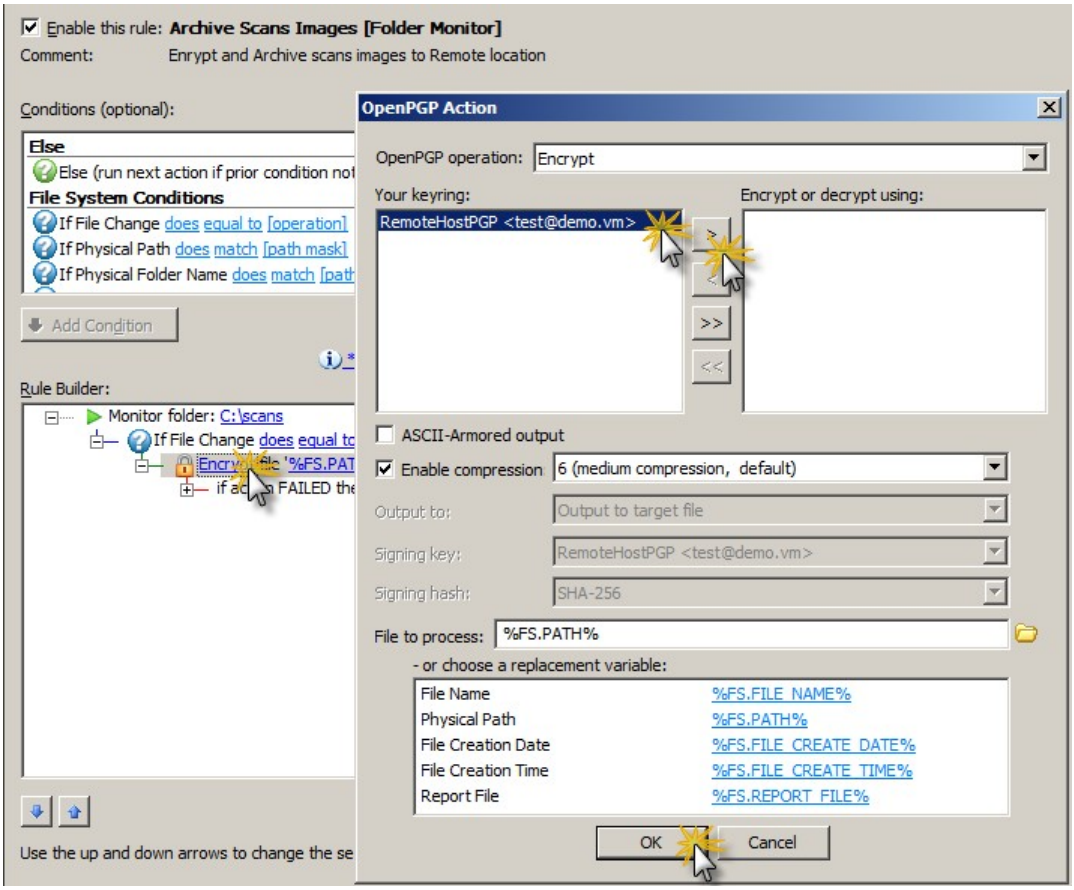



6. Add the **OpenPGP** Action after the Conditions. (Actions are added below the current selection.)

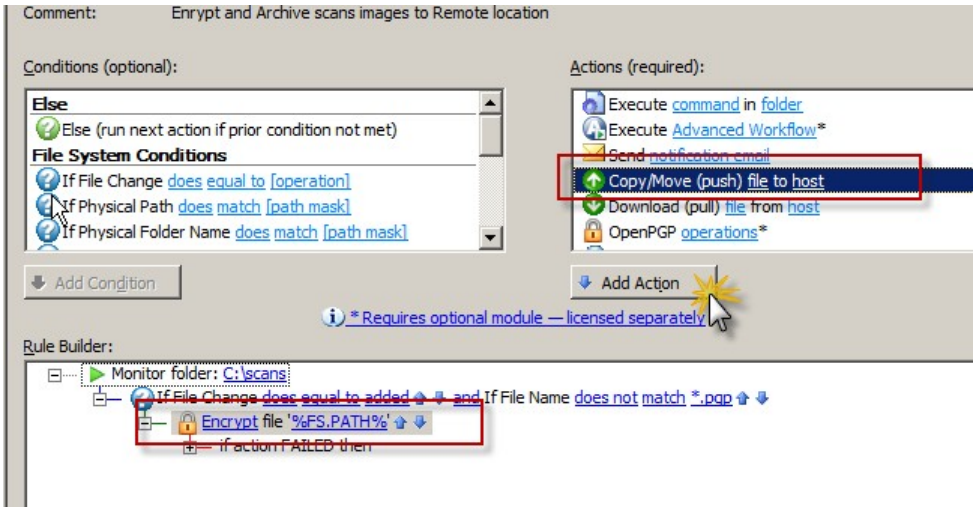


7. Read the reminder prompt about OpenPGP Actions in Folder Monitor Rules and click **OK** to continue.

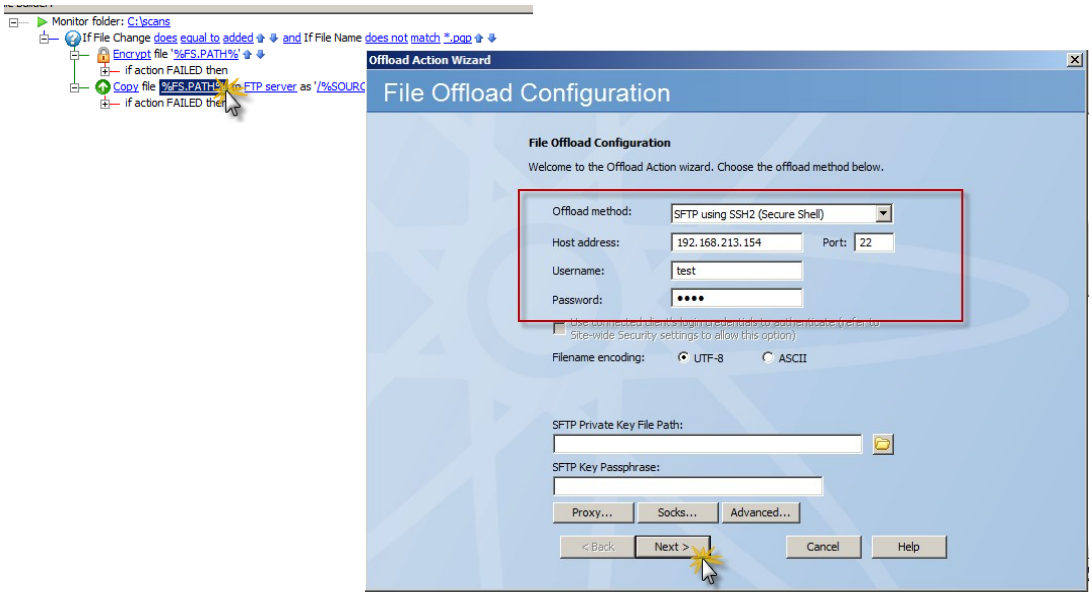
8. Configure the **OpenPGP** Action to Encrypt files.



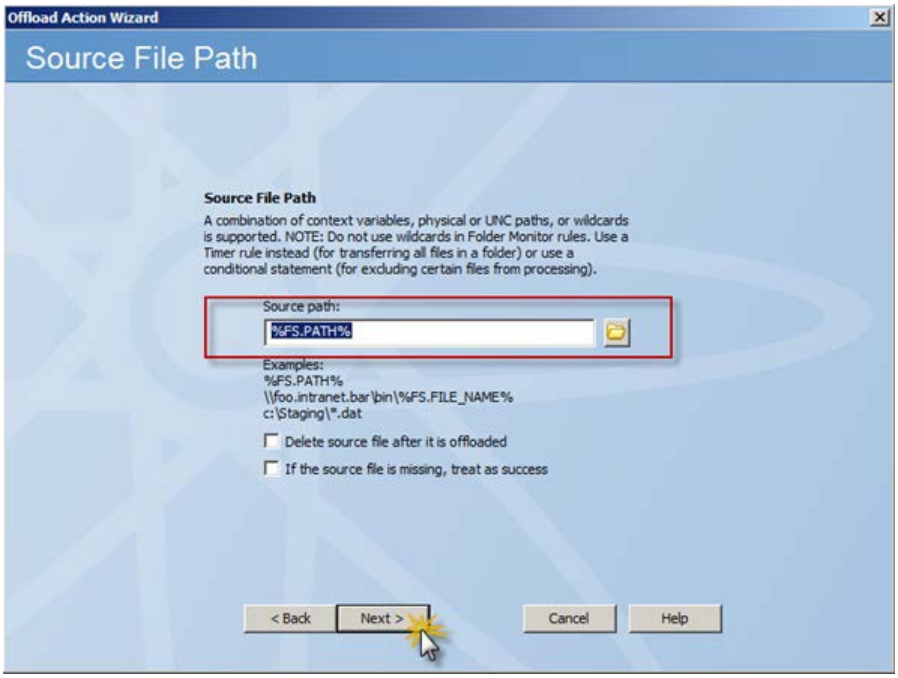

9. Add the **Copy/Move (push) file to host** Action.



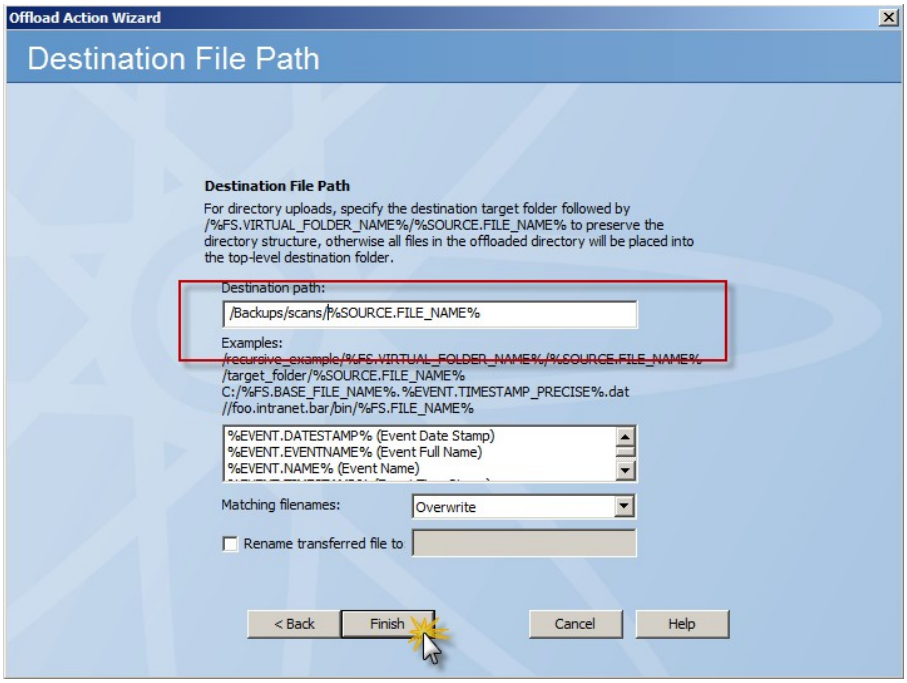
10. Click the Copy Action to configure the connection details.



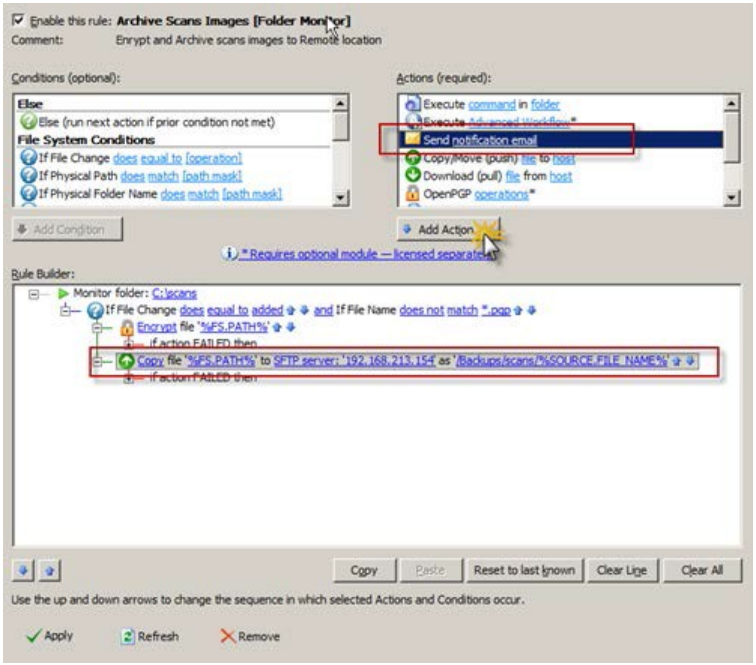

11. Specify which file(s) to upload. (The %FS.PATH% variable is the physical location of the file before it is moved/copied.)



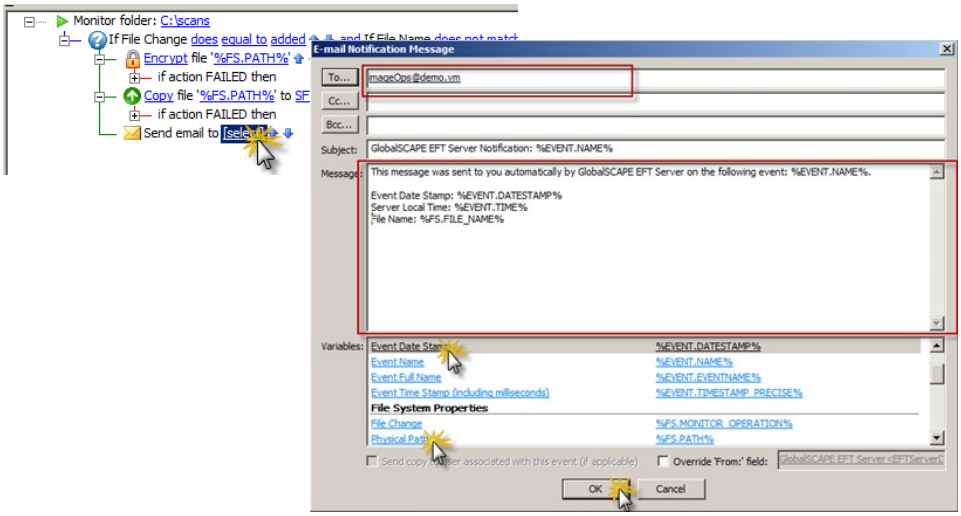
12. Specify where to upload the files. (%SOURCE.FILE_NAME% preserves the original name of the file, including the extension.)



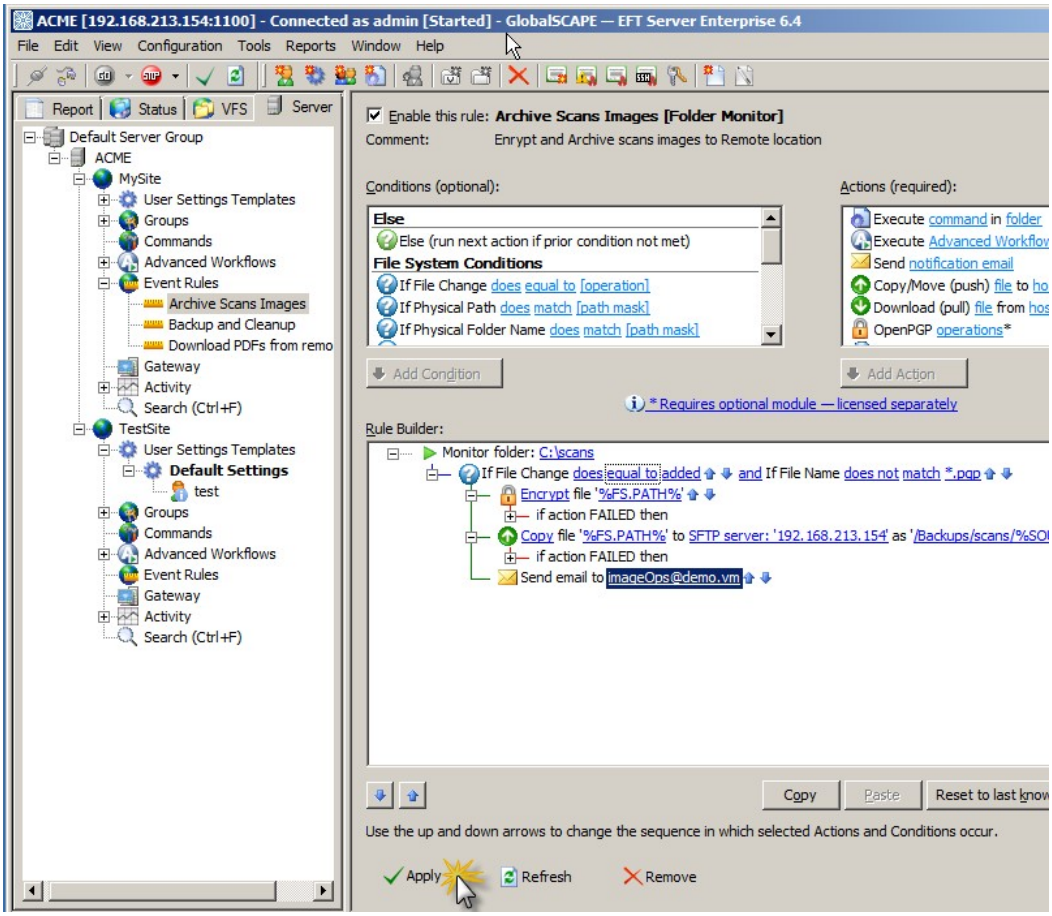

13. Add the **Send notification email** Action.



14. Specify the email recipient(s) and the variables that you want to appear in the **Message** box. Click the variable name in the left column (e.g., Event Date Stamp) if you want the variable name to appear in the email, as shown below. Otherwise, click the variable in the right column, and only the value of that variable appears (e.g., the date).

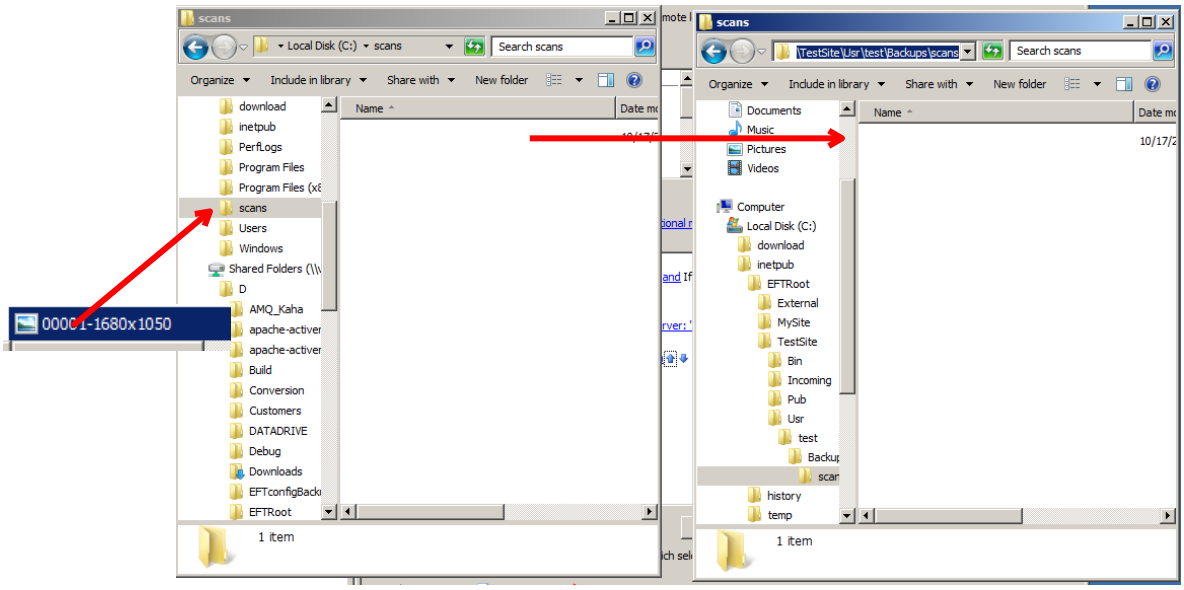



15. Apply your changes!




The Rule now reads, "If a file is added to C:\scans, and if the file does not have a PGP extension, encrypt the file in C:\scans, copy the file to this remote server, and then send an email to this recipient."

16. Test this Rule by uploading an unencrypted file to the monitored folder.



## On File Upload with OpenPGP, Email, and Windows Event Log Actions

For this example, we will create an Event Rule to trigger when a file is uploaded to the destination folder of the Folder Monitor Rule created in the previous example. We want this Event Rule to do the following:

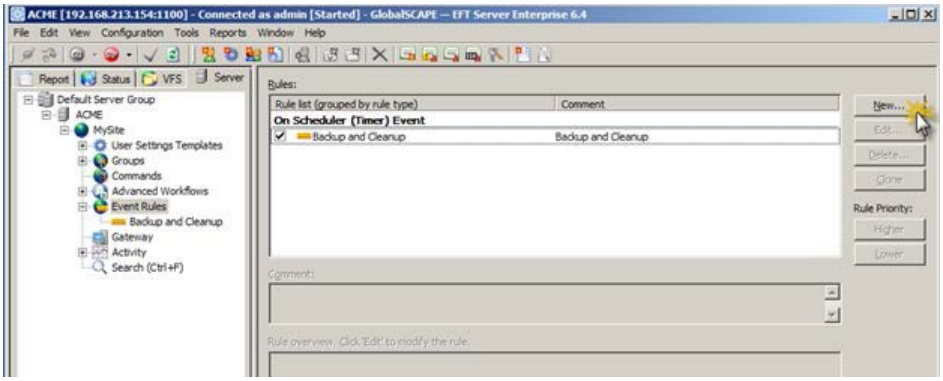
1. Decrypt the uploaded encrypted file
2. If the Action failed to decrypt the file, then:
    a. Send email notification
    b. Write to Windows Event Log

### Prerequisites

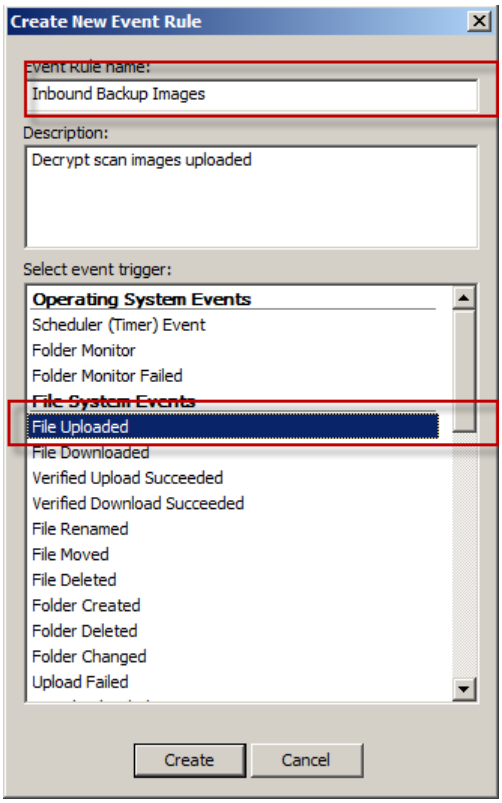
- Private PGP key (part of original key pair)
- Email address for notification

**To create a File Upload Event Rule**

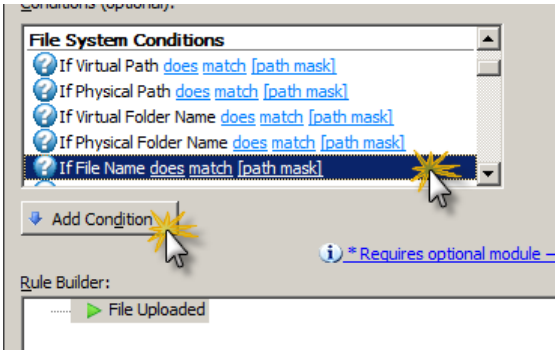
1. Create a new Rule.



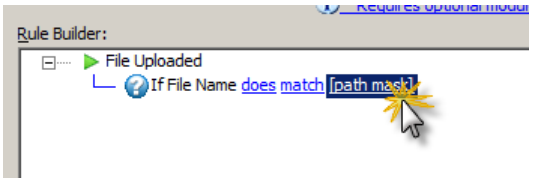
2. Select the File Uploaded event trigger and name the Rule.

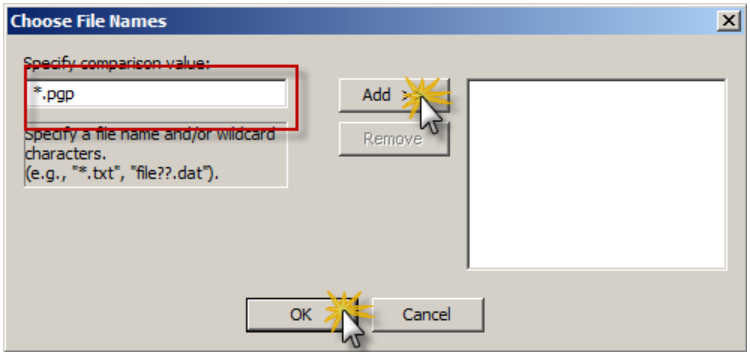



3. Add the **File Name** Condition to the Rule.

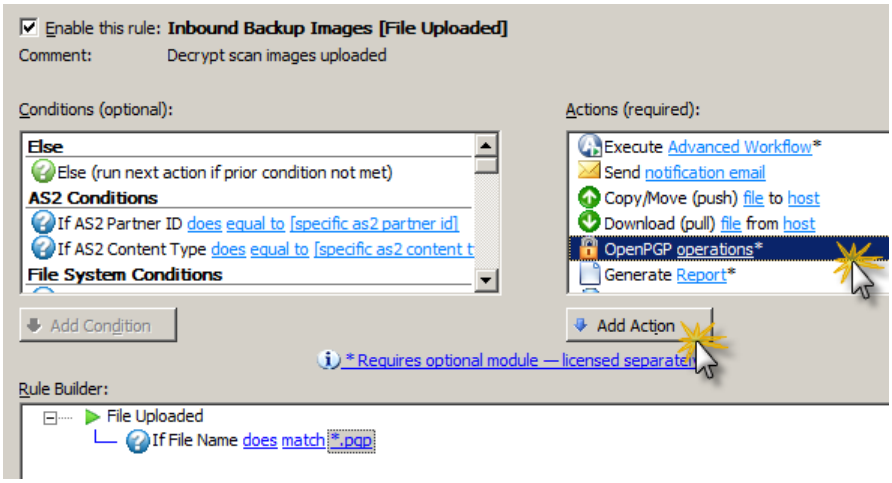


4. Configure the **File Name** Condition to trigger only on files with the PGP extension.

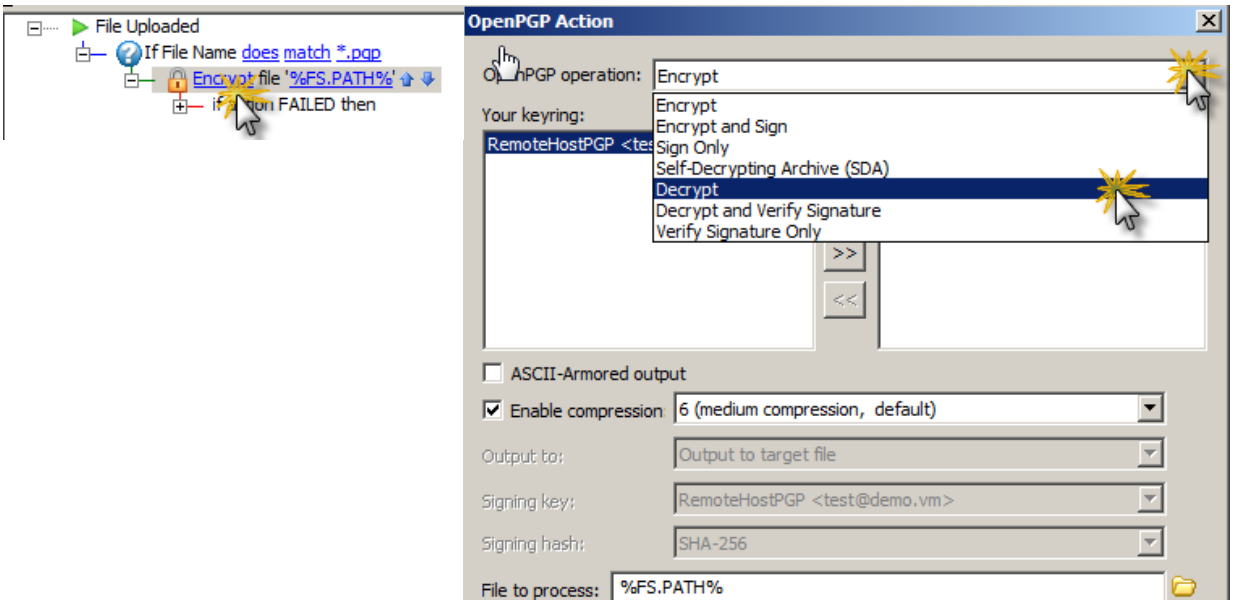


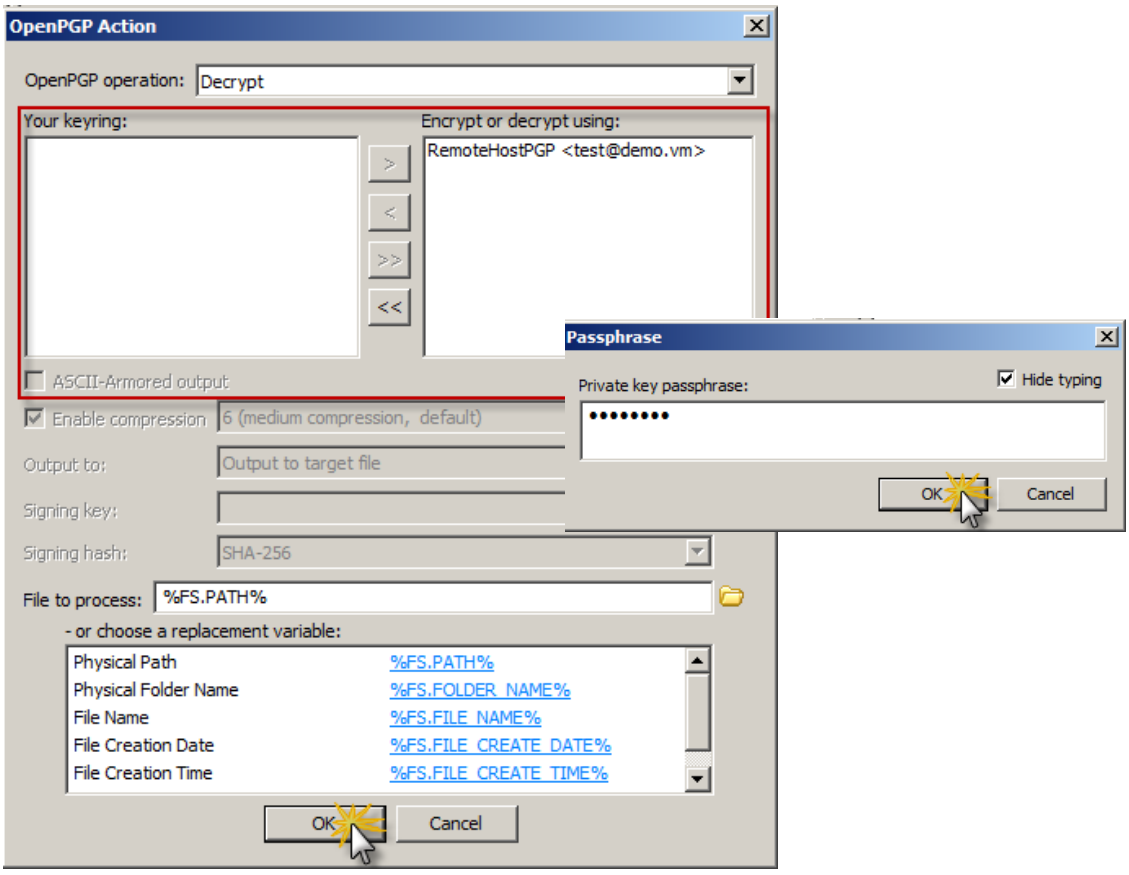




5. Add the **OpenPGP** Action.

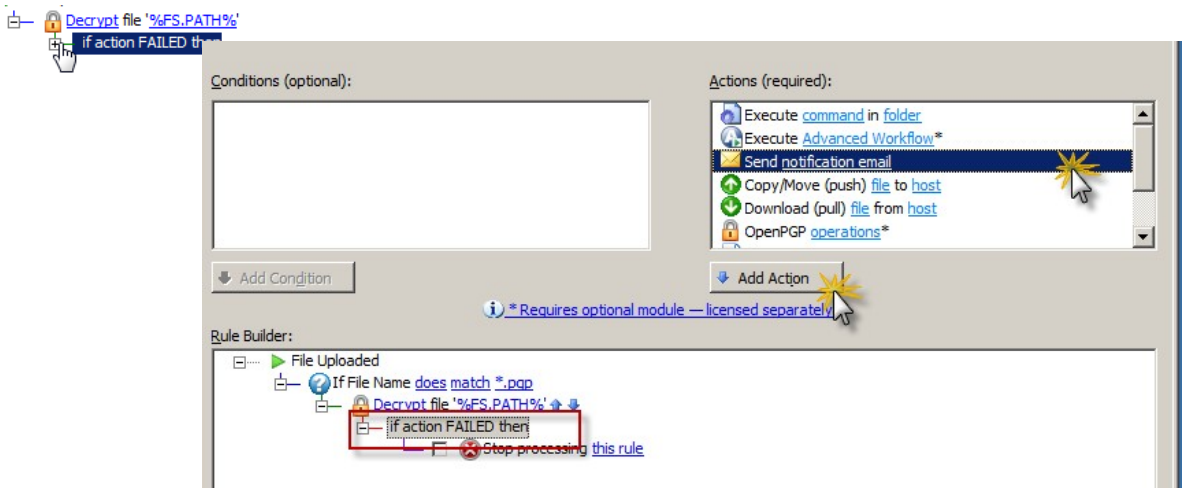


6. Configure the OpenPGP action to **Decrypt**.

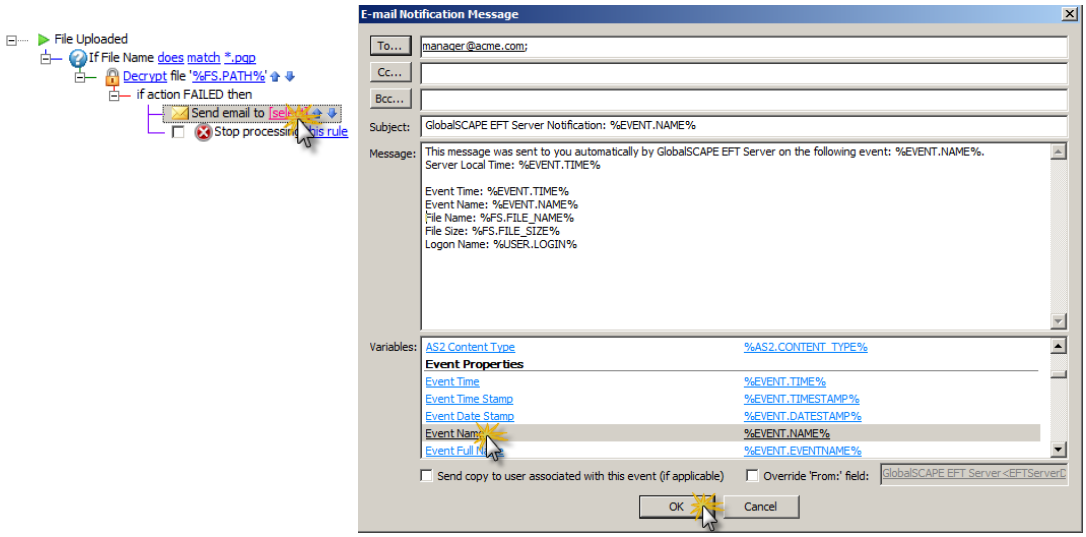


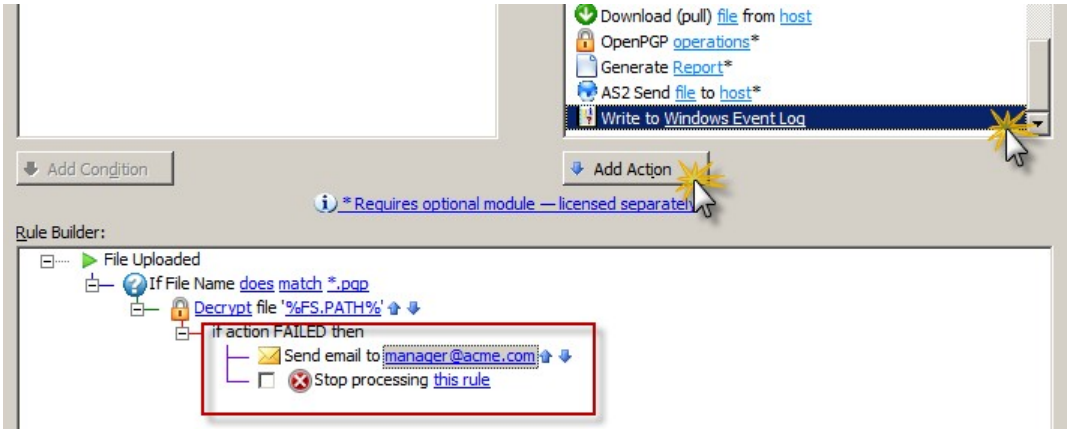
7. Add the **Send notification email** Action under the **if action failed** Condition.



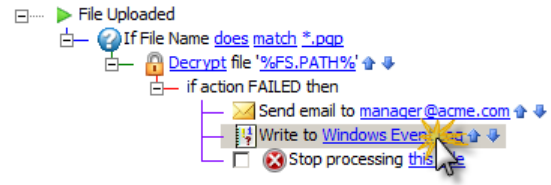

8. Configure the email as desired.

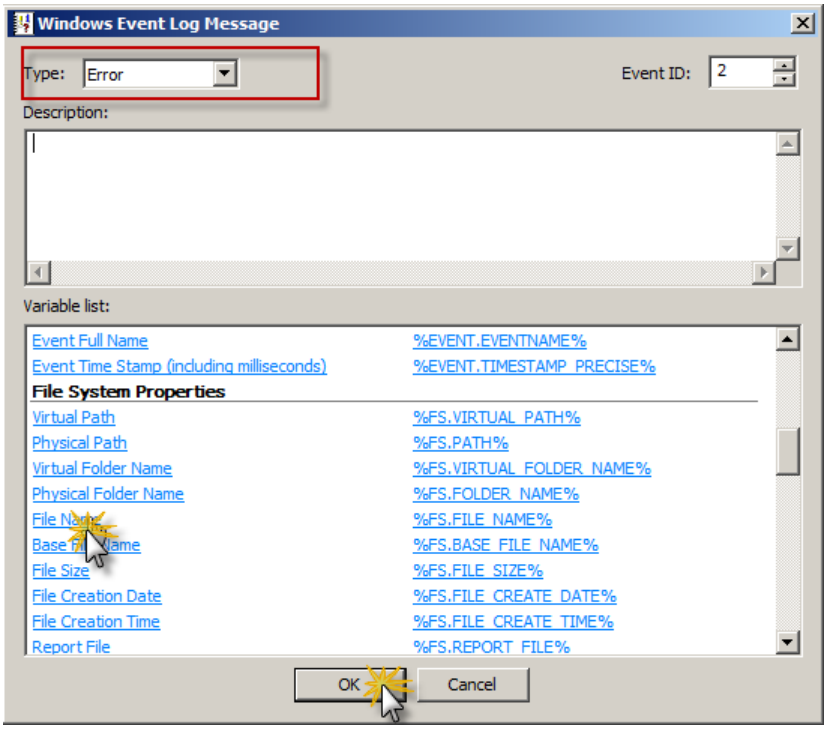



9. Add the **Write to Windows Event Log** Action.

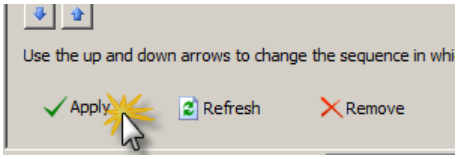


10. Specify which variables to write to the Event Log, such as the file name.




11. Click **Apply** to save the Event Rule.



# Index