FORTRA

Globalscape EFT v8.2
Event Rules Guide

202404020206

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 administration interface or with the COM API, you 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, you can set up an Event Rule that monitors that folder, and when someone puts a file into that folder, EFT can encrypt that file, move it into another folder, and then send emails 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, when the other administrator clicks **Apply**, he will get a message saying that the changes could not be saved because changes have been made by someone else. The administrator who receives that message will have to refresh (View > Refresh or press F5) 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'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). Refer to Events (Triggers) and Examples for examples of creating these rules in the Rule Builder.

(In the examples below, "ON FILE UPLOAD" is the Event trigger; the "if" statements are Event Rule Conditions; "PGP" and "MOVE" are 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" )
  {
    MOVE %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%
  }
  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 email TO %user.email%
}
```

Run the same Action more than once:

```
ON FILE UPLOAD
{
 SEND NOTIFICATION email TO serveradministrator@globalscape.com
 SEND NOTIFICATION email 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 email TO %user.email%
}
```

It is possible to configure Event Rules that create infinitely recursive cycles. 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.

Transferring Files with Event Rules

You can configure EFT'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 Protocol: Upload Action.

For details of downloading (pulling) a file from a specific server (host), refer to Protocol: Download Action.

Event Rules Modules

Certain Event Rules functions are available in the "core" EFT, while the rest require a licensed module. The Event Rule Change Log, Event Rule Folders, Event Rule import/export, and Event Rules Permissions are part of "core" EFT.

The following Event Rule features are available without a module:

- Connection Events (all)
- File Server Events (all)
- Server Events (all)
- Site Events (all)
- "IF" and "Else" Conditions
- Backup and Cleanup Actions
- Flow: Stop Processing Action
- Flow: Variable Action
- Protocol: Email Action
- System: Backup Action
- System: Cleanup Action

The following features require a module to be licensed and registered:

<table>
<tr><td>Enterprise Actions Module (EAM)
Compression Action
CSV: Export to Dataset Action
CSV: Import from Dataset Action
File: Operation Action
Flow: Subroutine Action
Folder: Operation Action
Loop: Break Action</td><td>Loop: Dataset Action
Protocol: Listing to Dataset Action
Script: Custom Command Action
Script: PowerShell Action
Event Rule Subroutine Event
REST Invocation Event</td></tr>
<tr><td colspan="2">File Transfer Client Module (FTC)
Protocol: Download Action
Protocol: Synchronize Action
Protocol: Upload Action</td></tr>
<tr><td colspan="2">Folder Monitor Module (FMM)
Folder Monitor Event</td></tr>
<tr><td colspan="2">Timer Event Module (TEM)
Scheduler Timer Event</td></tr>
<tr><td colspan="2">OpenPGP Module (PGP)
OpenPGP Actions (Encrypt, Decrypt, Sign, Verify, SDA)</td></tr>
<tr><td colspan="2">Cloud Object Monitor (CMM)
Cloud Object Monitor Event
Cloud: Download Action
Cloud: REST/Web Services Action
Cloud: Upload Action
Offload Secrets to cloud</td></tr>
<tr><td colspan="2">AS2 Module (AS2)
AS2 Events</td></tr>
<tr><td colspan="2">Workspaces Module (WSM)
Workspaces Events</td></tr>
</table>

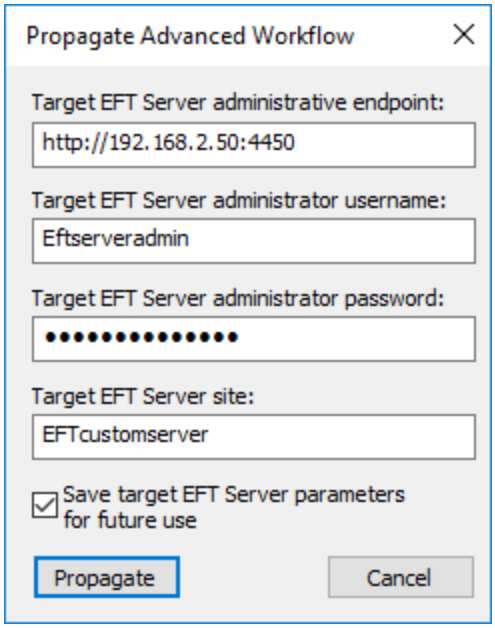
Propagating Event Rule Artifacts

Administrators can propagate (copy) individual items in Custom Commands, Advanced Workflows, and Connection Profiles to another server (for example, when adding a server to a cluster).

- Propagation is only available for EFT-managed administrator accounts
- Multiselect is not supported
- The target server must have remote administration and REST API/ web administration enabled on the **Server > Administration** tab

To propagate items

1. In the administration interface, on the **Server** tab, right-click the item to propagate (such as the Advanced Workflows node), then click **Propagate**. The **Propagate** dialog box appears.



2. In the **Propagate** dialog box, specify:
    a. **Target EFT Server administrator REST endpoint** in the form of http or htt://[host]:[port]
    b. **Target EFT Server administrator username**
    c. **Target EFT Server administrator password**
    d. **Target EFT Server Site name** to which you want to propagate the item

   a. Select the **Save target EFT Server parameters for future** use check box if you plan to propagate numerous items. All the parameters except for target server administrator password are preserved across administration interface restart.
3. Click **Propagate**. A prompt is displayed to the EFT administrator that action was successful or failed.

The result of successful propagation is that the artifact on the target EFT server is identical to the one propagated. The identity is provided by internal artifact ID.

- If target server's Site had no artifact with matching ID, it is created
- If target server's Site had the artifact with matching ID, it is replaced

Exceptions (not propagated) are:

- Custom Command's user-group assignment:
  - New Command has no user-group assignment
  - Replaced Command preserves its user-group assignment unchanged
- Advanced Workflow's Folder assignment:
  - New Workflow is placed outside any Folder
  - Replaced Workflow remains in its original Folder

> **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

- Admin ACL for all artifacts:
  - New artifact gets all admin permissions "inherited" from root container
  - Replaced artifacts preserves its permissions unchanged

When accepting the artifact, the target server performs all the standard activities, such as access control, name collision prevention, data validation, audit, logging, and so on.

- For creating new artifact, the ones performed when creating artifact via REST
- For replacing existing artifact, the ones performed when updating artifact via REST
- For name collision, no new validation was introduced, this functionality is dependent on REST API, i.e., if REST API allows it (even with case sensitivity) then propagate functionality will allow it

For artifact customization, some fields accept Run-Time Variables, which are:

- Custom Command:
    - Executable path
    - Log file path
- Advanced Workflow
    - Log directory path
- Connection Profile
    - All the fields that are Run-Time Variables-aware in Offload/Download/Cloud Actions
- Run-Time Variables are allowed to be specified in all EFT administrative interfaces (GUI, COM, and REST)
    - EFT validates incoming change and fails to accept if the fields contain unknown Run-Time Variables. In particular, it means that if the source server's artifact references the Run-Time Variable that is not defined in target server, propagation fails.

To support identity by artifact ID, EFT Administrative REST interface handles HTTP PUT requests on individual artifact endpoints.

- The new PUT REST endpoints are:
    - Custom Command: /Admin/v2/sites/<site-id>/custom-commands/<command-id>
    - Advanced Workflow: /Admin/v2/sites/<site-id>/awe-tasks/<workflow-id>
    - Connection Profile: /Admin/v2/sites/<site-id>/connection-profiles/<profile-id>
- The requests follow standard JSON:API model
- The semantics of the request is "create or replace":
    - If the endpoint corresponds to no existing artifact, EFT considers the request "create resource" one and serves it similar to POST to collection with the only difference that the artifact created has the specified (rather than random) id.
    - If the endpoint corresponds to existing artifact, EFT considers the request "replace resource" one and serves it similar to PATCH ("update resource") with the difference that, the body of PUT is considered full representation of the resource and all the missing fields are considered to have default (not "current" as for PATCH) values.

Effectively, when an artifact is propagated for the first time, target server creates its identical copy; for any subsequent propagation, target server replaces the copy with up-to-date value.

The Source server records propagation progress to EFT.log via COMMON logger (this is because the destination is not exercising REST API, its receiving incoming data).

Target server records propagation progress to EFT.log via standard REST Admin logger.

Artifact propagation is available via COM API Site interface new methods:

- ICISite::PropagateCommand
- ICISite::PropagateAdvancedWorkflow
- ICISite::PropagateConnectionProfile

Artifact propagation is available via REST Admin interface

POST REST API endpoints:

- Custom Command: /Admin/v2/sites/<site-id>/custom-commands/<command-id>
- Advanced Workflow: /Admin/v2/sites/<site-id>/awe-tasks/<workflow-id>
- Connection Profile: /Admin/v2/sites/<site-id>/connection-profiles/<profile-id>

Method name is “propagate” for all requests.

Example success case:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-
000000000001/custom-commands/00000000-0000-0000-0000-
000000000001 HTTP/1.1
{
   "jsonrpc": "2.0",
   "method": "propagate",
   "id": "1",
   "params":
   {
   "targetEndpoint": "http://target:4450",
   "targetSiteName": "targetSite",
   "targetAdminUsername": "targetAdminLogin",
   "targetAdminPassword": "targetAdminPassword"
   }
}
HTTP/1.1 200 OK
{
"jsonrpc": "2.0",
"id": "1",
```

```
"result": "success"
}
```

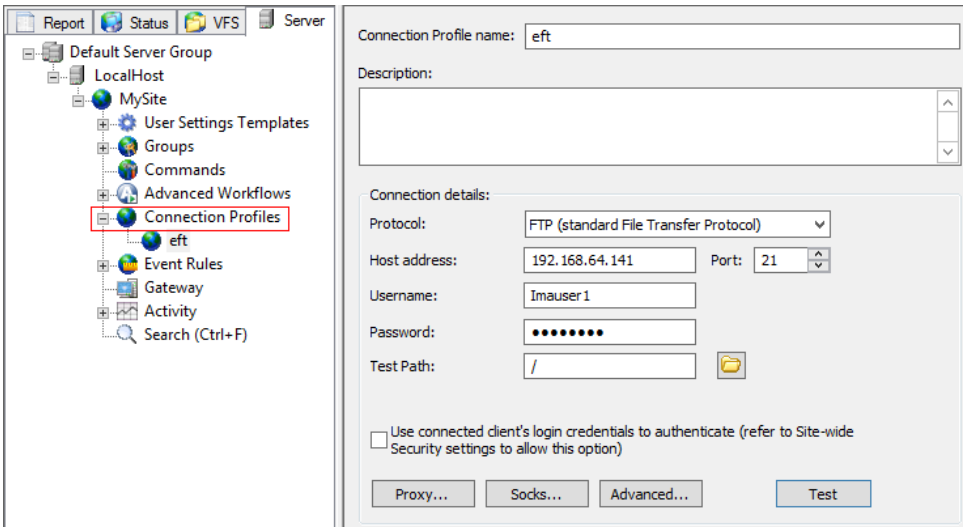
Example failure case:

```
POST /Admin/v2/sites/00000000-0000-0000-0000-
000000000001/custom-commands/00000000-0000-0000-0000-
000000000001 HTTP/1.1
{
  "jsonrpc": "2.0",
  "method": "propagate",
  "id": "1",
  "params":
  {
  "targetEndpoint": "http://target:4450",
  "targetSiteName": "targetSite",
  "targetAdminUsername":
   "targetAdminLogin","targetAdminPassword":
   "targetAdminPassword"
  }
}
  HTTP/1.1 404 Not Found
  {
  "jsonrpc": "2.0",
  "id": "1",
  "error": {
  "code": -32004,
  "message": "Not found: custom-command (00000000-0000-0000-
0000-000000000001)"
  }
}
```

Introduction to Connection Profiles

A Connection Profile is a connection settings template to be used in Event Rules that contains the server connection settings. A profile includes the Profile Name, Description, and Connection details such as protocol, host address, credentials, proxy, socks, and so on. A **Test** button is provided to verify the specified connection options. After you've created the profile on the Site, you can specify it in Copy/Move and Download Actions so that you don't have to define it every time you create a Copy/Move or Download Event Rule. (Connection Profiles require HTTPS, SFTP, or FTPS to connect as the server.)

Connection Profiles are defined on the Connection Profiles node. Refer to Defining a Connection Profile for details.



Defining a Connection Profile

Create a Connection Profile that you can reuse in Event Rules, rather than defining external servers every time you create a new rule.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

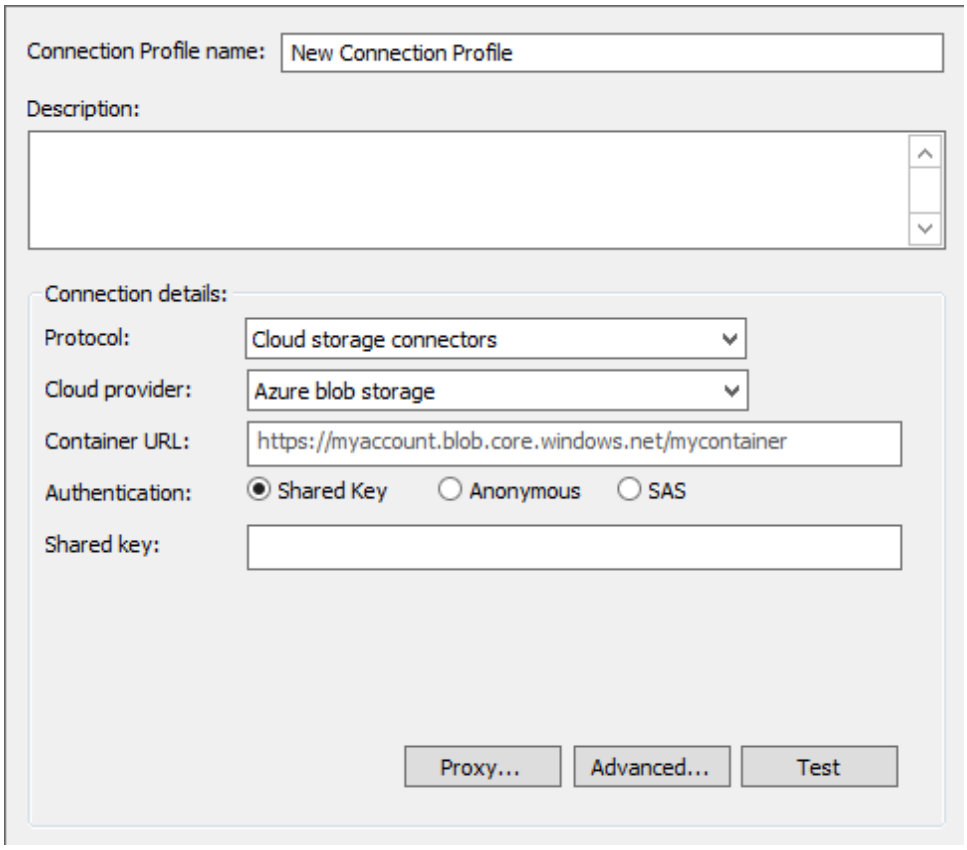
- Using the DMZ Gateway as a proxy is not available when using Cloud Connection profiles (Requires CCM). EFT uses the AWS SDK for cloud connections, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.
- Contact your system administrator for the proper host name, port, user name, password, and proxy type, as well as any required advanced authentication methods.

To define a Connection Profile

1. Right-click the **Connection Profiles** node, then click **New Connection Profile**.
2. In the **Connection Profile** name box, provide a name for the profile.
3. In the **Description** box, provide a description for the profile.
4. In the **Connection details** area, click the **Protocol** list to specify a protocol 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), FAST - Accelerated Transfer, Cloud storage connectors.
    - **Local /LAN:**

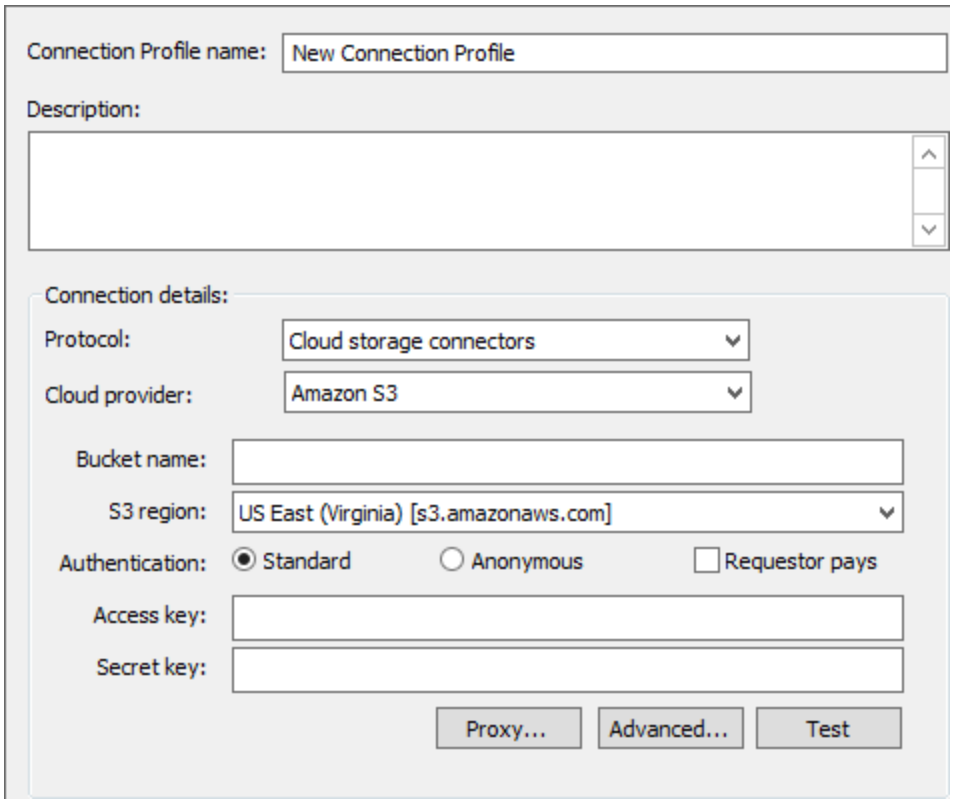
      If you selected Local (Local Files or LAN), provide the Windows account username and Password for connecting to remote shares (not local folders). These credentials are used only if/when a resource cannot be accessed using the credentials under which the EFT service is running. The **Optional credentials override** boxes allow you to specify an alternate set of logon credentials for accessing remote network shares to which the EFT service account may not have access (due to security constraints). If alternate credentials are specified, EFT will use its current security token (associated with the “Log on as” account specified in the EFT service settings) for local folder access and then new security token (associated with the alternate logon credentials) for the remote source folder accessed over network connections (e.g. network shares).

- **For Azure:**



  - Specify the **Container URL**, **Authentication** option, and **Shared key** or **SAS token**, and, if needed, Proxy and Advanced options.

- **For Amazon S3:**



- Specify the **Bucket name**, **S3 region**, **Authentication options**, **Access key**, and **Secret key**, then scroll down for Proxy and Advanced options.

  EFT does not perform any sort of validation on the Bucket name created. Be aware of the following AWS restrictions when creating the name:

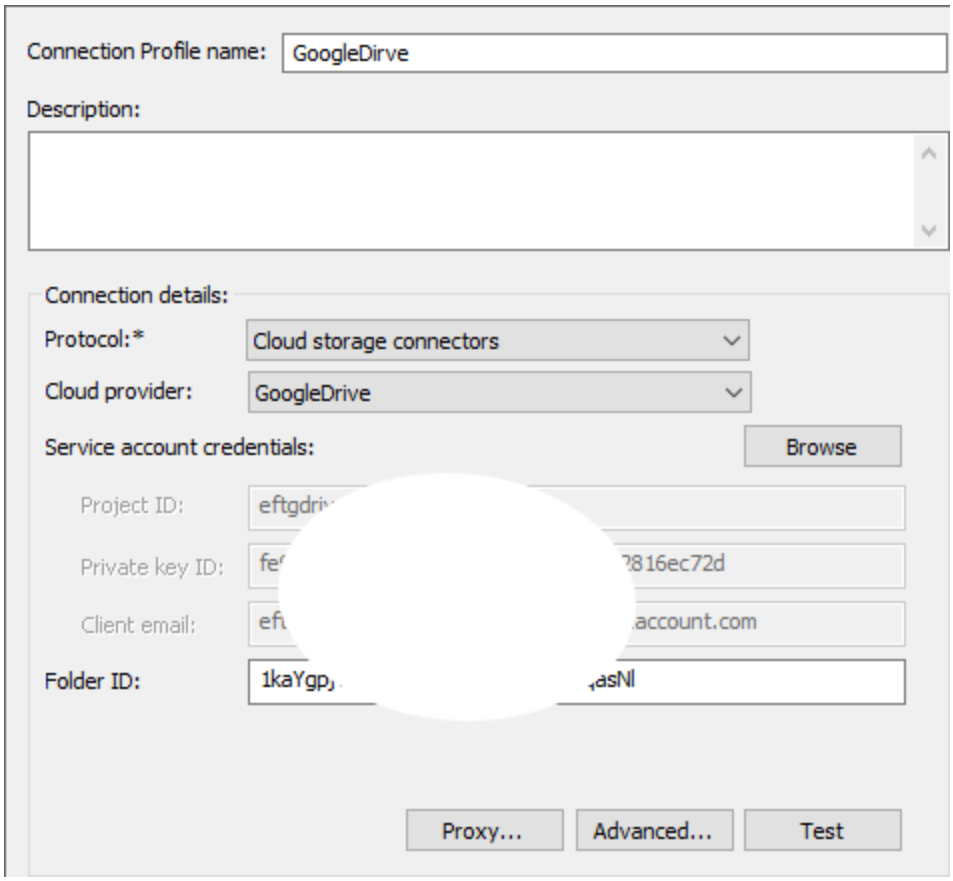
  - Bucket names can contain lowercase letters, numbers, and hyphens.
  - Each label must start and end with a lowercase letter or a number.
  - A Bucket name cannot start or end with a period.
  - Bucket names must be at least 3 and no more than 63 characters long.
  - Bucket names must not be formatted as an IP address (for example, 192.168.5.4).

- As a best practice, always use DNS-compliant bucket names regardless of the region in which you create the bucket. For example, MyAWSBucket is a valid bucket name, even though it contains uppercase letters. If you try to access this bucket by using a virtual-hosted-style request (http://MyAWSBucket.s3.amazonaws.com/yourobject), the URL resolves to the bucket myawsbucket and not the bucket MyAWSBucket. In response, Amazon S3 will return a "bucket not found" error.
- For more information regarding restrictions, limitations, and naming, refer to Creating object key names in the Amazon documentation.
- To see a list of AWS regions supported, click the **S3 region** list in the Connection profile.

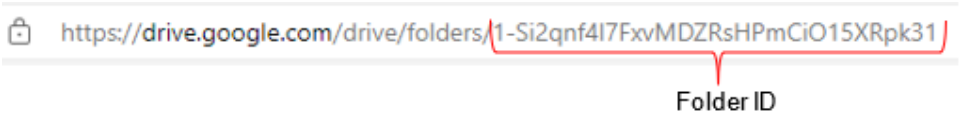
- **For Google Drive:**

  After setting up the Google service account, download and save the service account credentials file and the JSON file generated by Google, and place the JSON file in the EFT root folder (\Program Files\Globalscape\EFT Server). The JSON is formatted similar to this:

> **NOTE:** Refer to https://cloud.google.com/iam/docs/service-accounts for details of Google Service accounts.



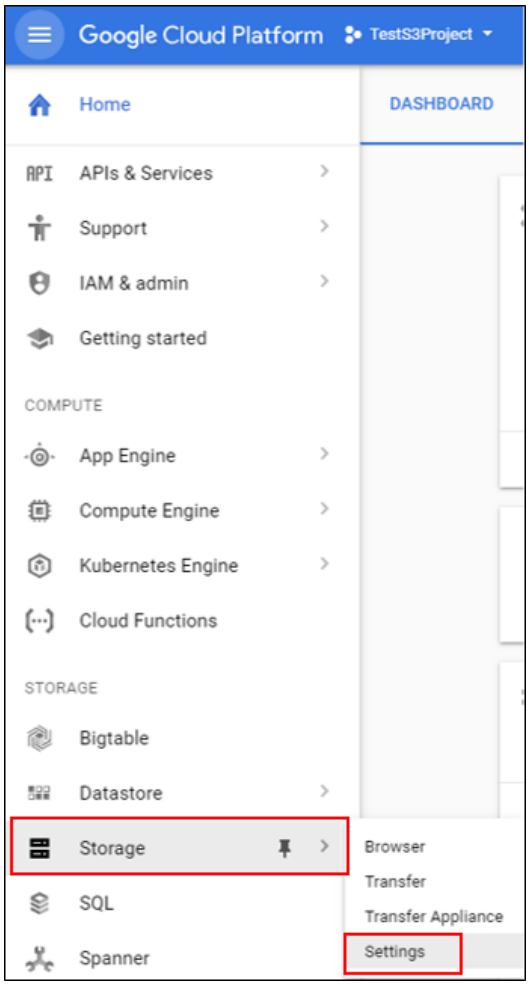
- For **Service account credentials,** click **Browse**, to find the service account credentials JSON file, downloaded from Google Cloud console. (The Google drive folder must be shared with this service account.)
- **Project ID**, **Private key ID**, and **Client email** are read-only and are completed with the service account credentials file.
- Provide the Google Drive **Folder ID**. You can get this ID by clicking on a folder in Google Drive, then copying everything after /folders/ from the URL.



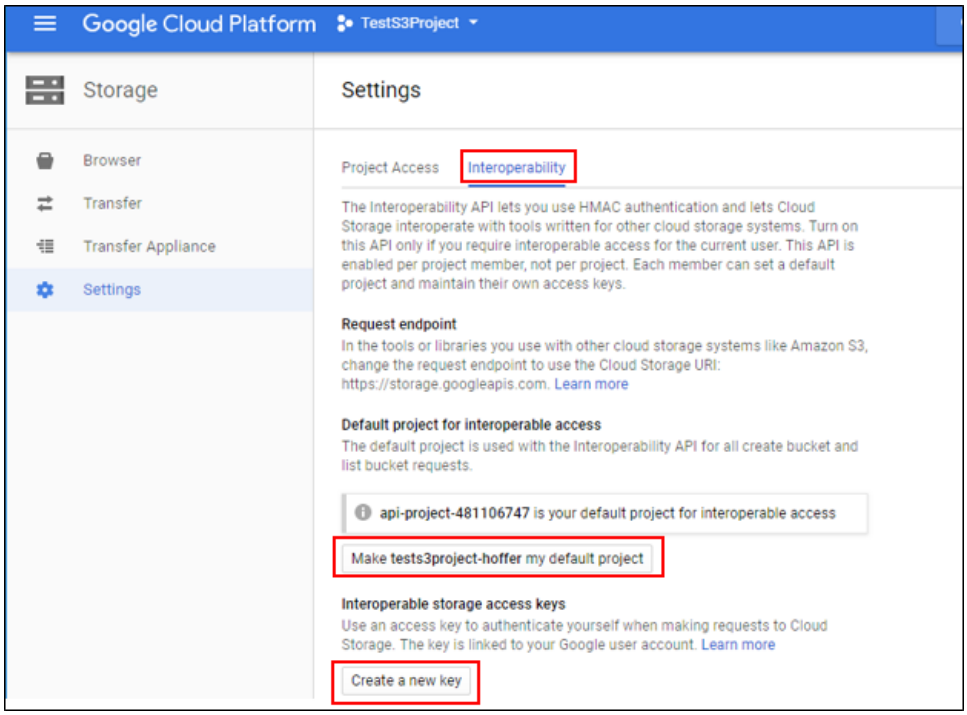
- **Alternatively, for Google Drive using Amazon S3:**

  Configure Google Cloud Storage access:

  a. Log in to Google Cloud, then click **Storage > Settings**.

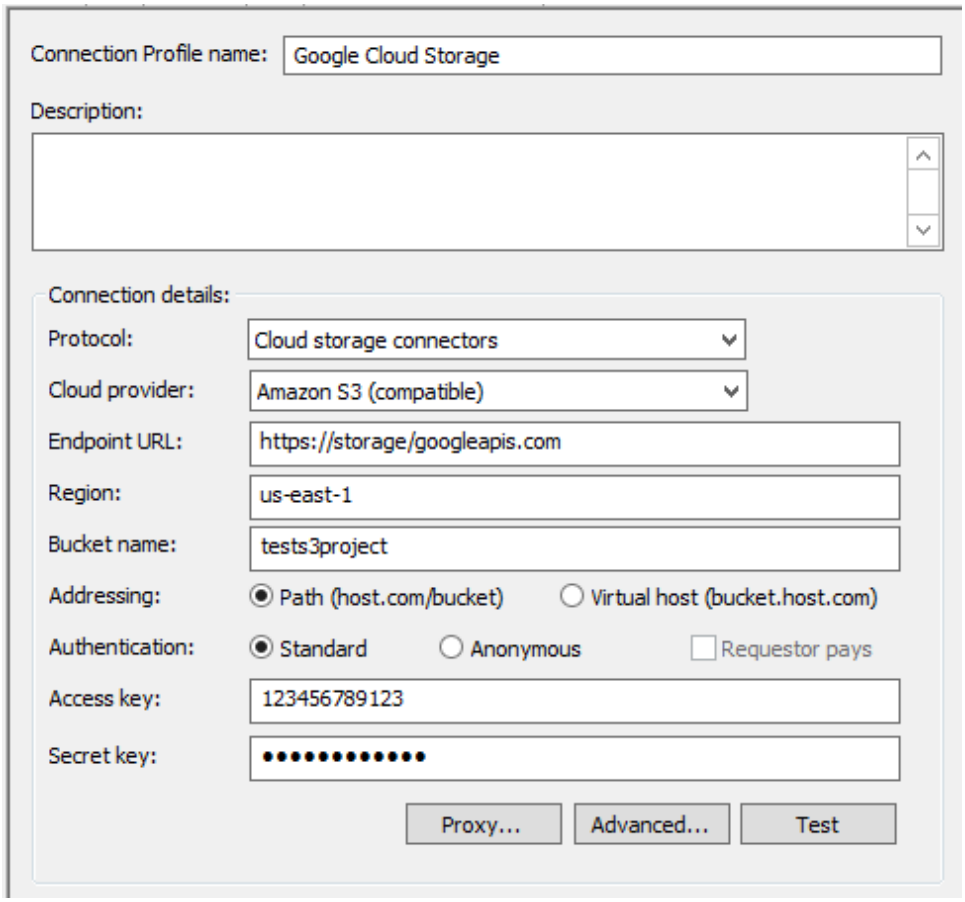


  b. In **Settings**, click **Interoperability**.



c. Under **Default project for interoperable access**, click the **Make <project name> my default project**, then click **Create a new key**.

d. In EFT, configure a Connection Profile to use the **AWS S3 (compatible)** connection:



e. Use the **Endpoint URL** https://storage/googleapis.com.

f. Specify the **Bucket name** you created in your Google Cloud Storage project

g. For **Addressing**, click Path (host.com/bucket).

h. Specify the **Access Key** and **Secret Key** as shown in your Google Cloud Storage console for "Interoperable storage access keys."

- **If you chose anything except Local or a cloud provider, do the following:**
  - In the **Host address** box, type the IP or host address of the EFT to which you want to connect.
  - The **Port** number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
  - In the **Username** and **Password** boxes, type the username and password used to authenticate.
  - In the **Test Path** box, type a path to the remote folder that you will access with this Connection Profile, such as root /.

    - If you chose a protocol that uses SSL (**FTPS** or **HTTPS**), provide the client and remote server's SSL certificate information.
    - If you chose **SFTP**, provide the client SFTP certificate information.
- (Optional) 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.
- (Optional) If you connect to EFT through a Socks server, click **SOCKS**. Refer to Using a SOCKS Proxy Server for details of configuring the SOCKS connection.
- (Optional) To configure advanced transfer options, click **Advanced**. The **Advanced Options** dialog box appears. Refer to Advanced Transfer Options for details.
- To verify the connection settings, click **Test**.

Defining Event Rules

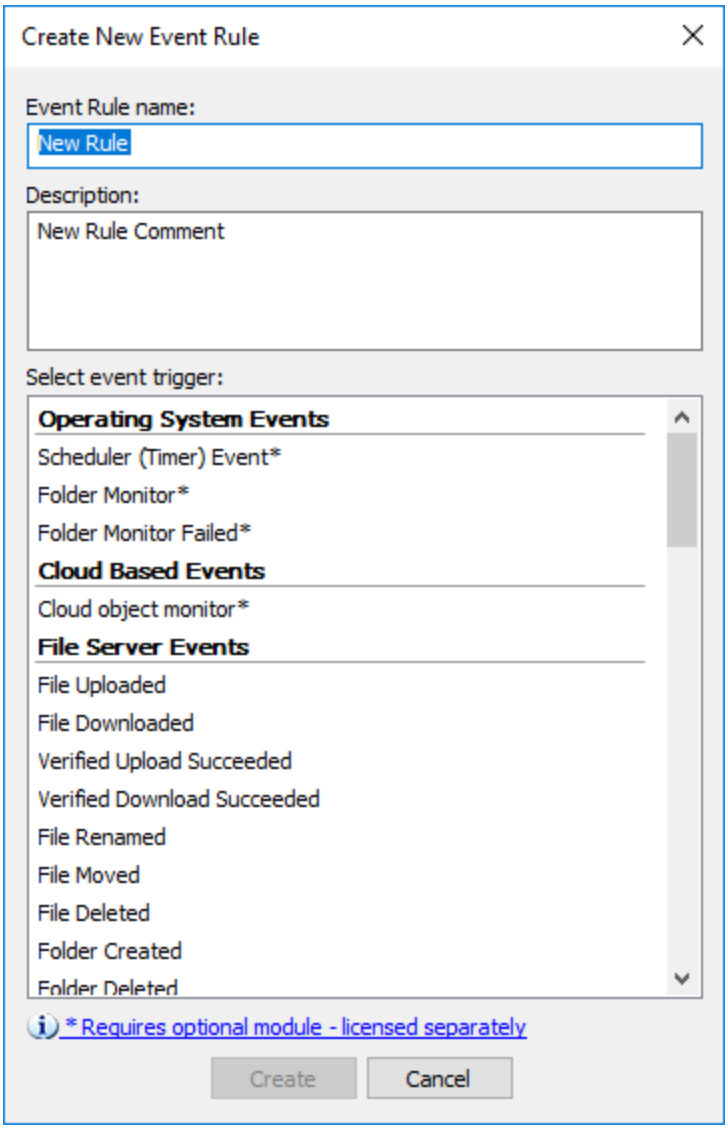
To define Event Rules in the administration interface, you begin with an Event you want to use as a trigger for the Event Rule. The Event could be when someone uploads a file, when a user quota is exceeded, when a change is detected in a folder, or many other Event triggers. Then you specify an Action to be taken when the Event occurs. The Action could be sending an email 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.

- While you can have two administrators working on Event Rules at the same time, if they are working on the same Rule at the same time, when they save their Rule, the second administrator to save will get a notice that the changes could not be saved because changes have been made by someone else. They then need to refresh to see the other changes, and then make their changes to the Rule again.
- The EFT log will display an error message when a file larger than 30 MB is attached to a Send notification email Action in an Event Rule.

To define an Event Rule

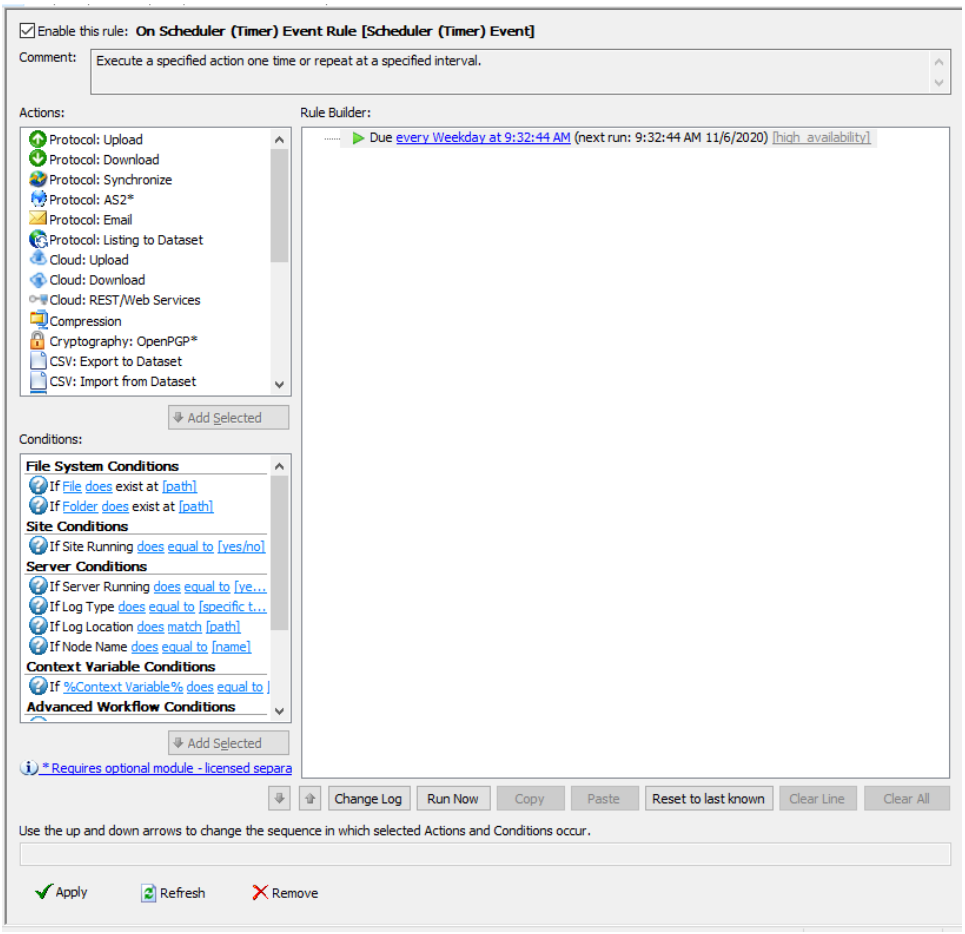
1. In the administration interface, connect to EFT and click the **Server** tab.
2. Do one of the following:
   - Right-click on the **Server** tab, and then click **New Event Rule**.
   - On the **Server** tab, expand the Site you want to configure, and then click **Event Rules**. In the right pane,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

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



NOTE: Event triggers marked with an asterisk require a module license.

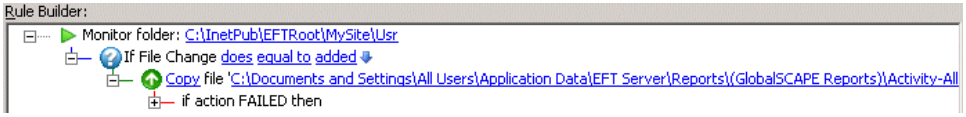
3. In the **Event Rule name** box, type a descriptive name for the Rule. This name will appear in the Event Rules node and in reports and logs. Therefore, name it something you will recognize, rather than something generic such as "Rule #24."
4. In the **Description** box, provide any notes about the 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 Rule Builder appears.



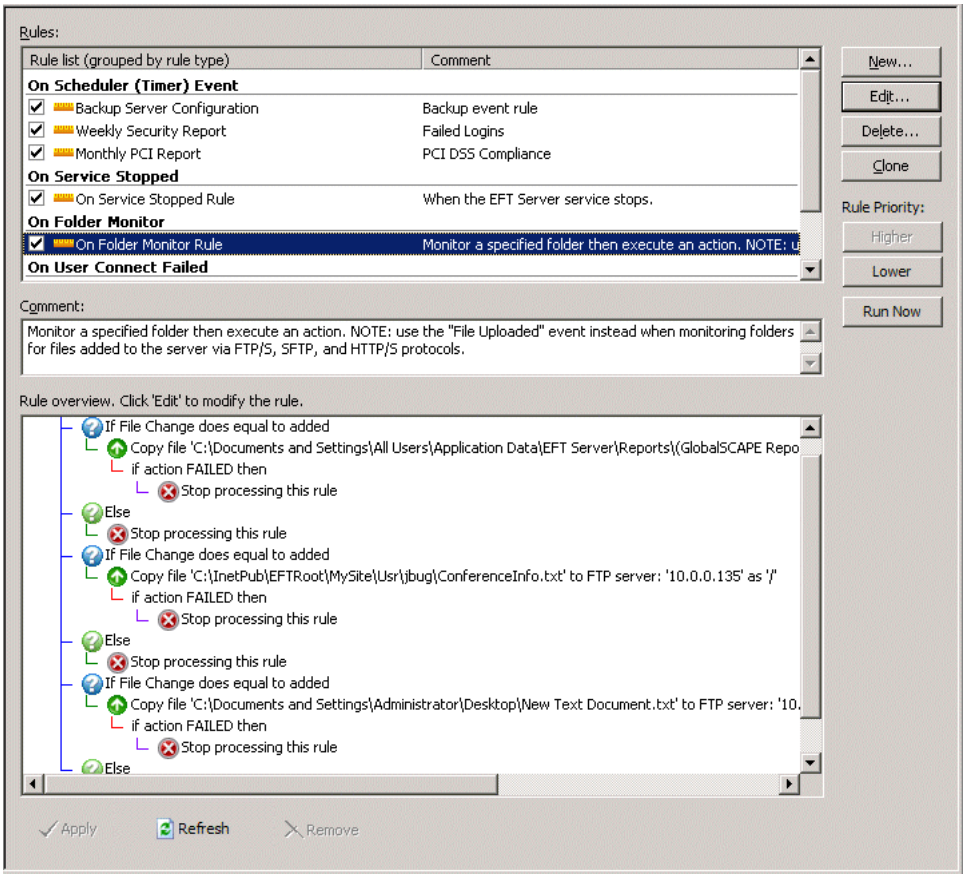
7. Actions and Conditions available for the specified event appear on the left of the Rule Builder. Conditions are optional. When applicable to the Event Rule, the Else option also appears. To add a Condition to the Rule, double-click the Condition, or click to select it, and then click **Add Condition**. Not all Conditions that EFT supports are available for every Event. To learn more about available Conditions, refer to Event Rule Conditions.

8. To add an Action to the Rule, double-click it or click the Action in the list, 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/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. EFT 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. If clicking **Remove** doesn't work (because you were in the process of creating or changing the rule), then click **Refresh**.

Event Rule Folders

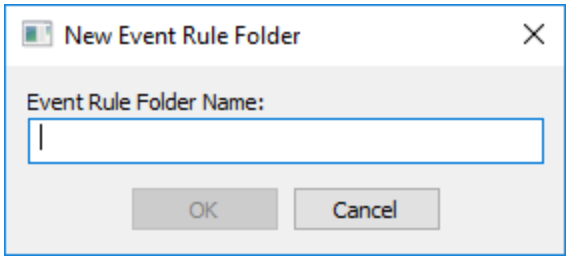
Event Rules can be organized into folders for easier management and organization.

You can:

- Apply permissions to an Event Rule folder that apply to all Event Rules in that folder.
- Create new Event Rules within a folder. (You cannot create subfolders in folders.)
- "Drag and drop" Event Rules into a folder
- Select multiple event rules and then drag them all to the new folder.

To create an Event Rule folder

1. Click the Event Rules node or an Event Rule, then click **New Event Rule Folder**. The **New Event Rule Folder** dialog box appears.



> **NOTE:** If you right-click an Event Rule and then click **New Event Rule Folder**, the selected Event Rule is NOT placed in that folder. You will have to move it if you want it to be added to the new folder.

2. Provide a name for the folder, then click **OK**.
3. Click **Apply**.
4. Now you can click and drag Event Rules into your new folder and apply any Event Rule Permissions.

Event Rules Change Log

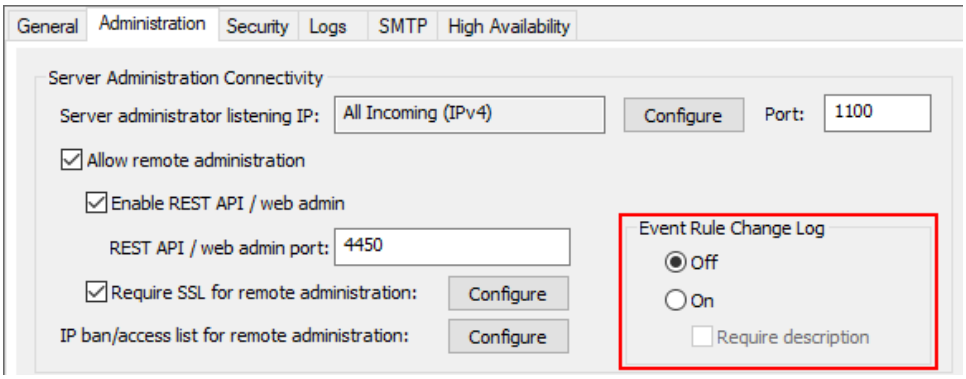
The Event Rules Change Log is used to record changes made to the Event Rules. For example, if three different administrators on three different shifts are making updates to the Event Rules or creating new Event Rules, logging these changes in the log ensures that all responsible parties are aware of the changes. Over time, this also creates a history of changes.

> **NOTE:** The Change Log only indicates changes made to existing Event Rules. It does not document the creation of an Event Rule. That is, if you've created a Rule and have never made any changes to it, it will not show up in the log.

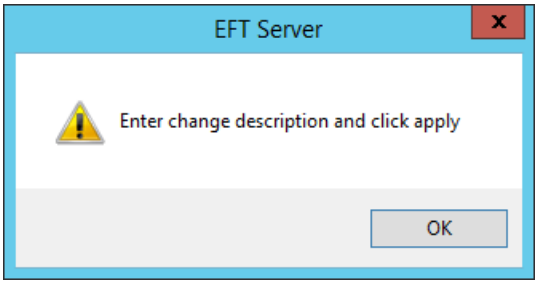
You must first enable the Change Log on the Server's **Administration** tab before changes can be recorded.

To enable and use the Change Log

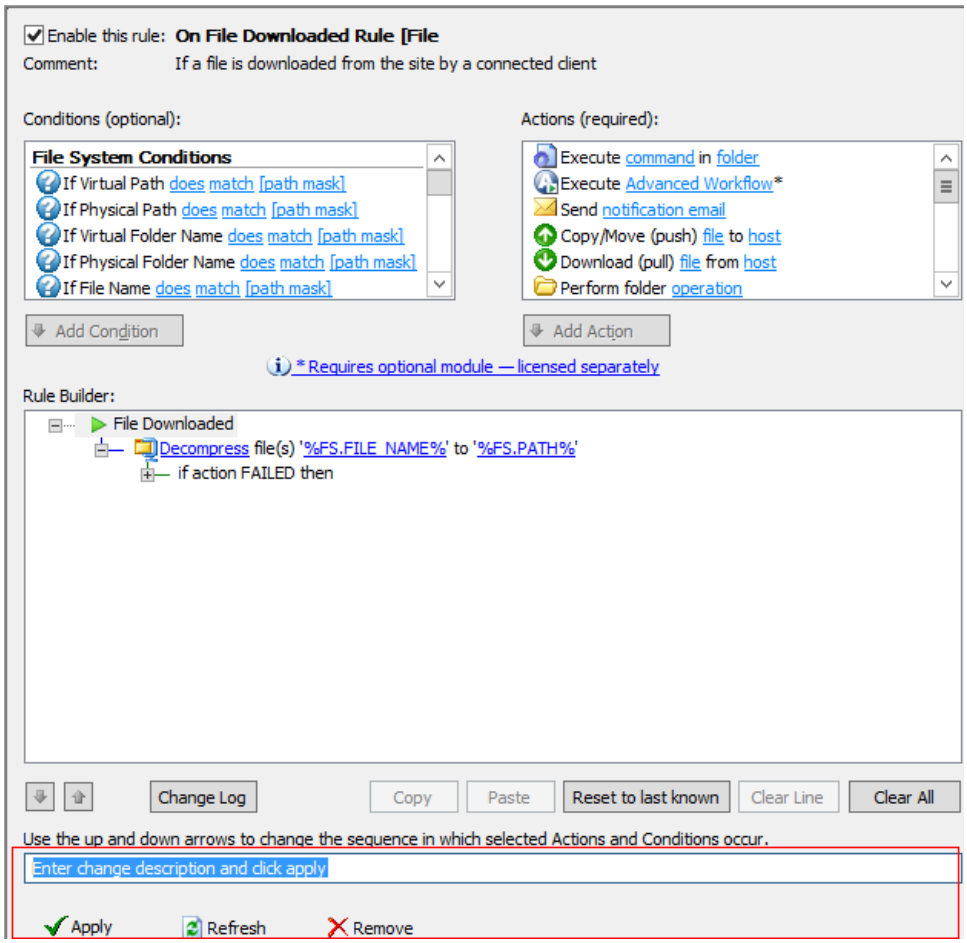
1. On the Server's **Administration** tab, under **Event Rule Change Log**, click **On**.
2. Select the **Require description** check box to require that changes contain descriptions. Without this check box selected, you can still add a description, but it is not required.



3. When the Change Log is enabled and you make a change to an Event Rule, a message appears that tells you to provide a change description.



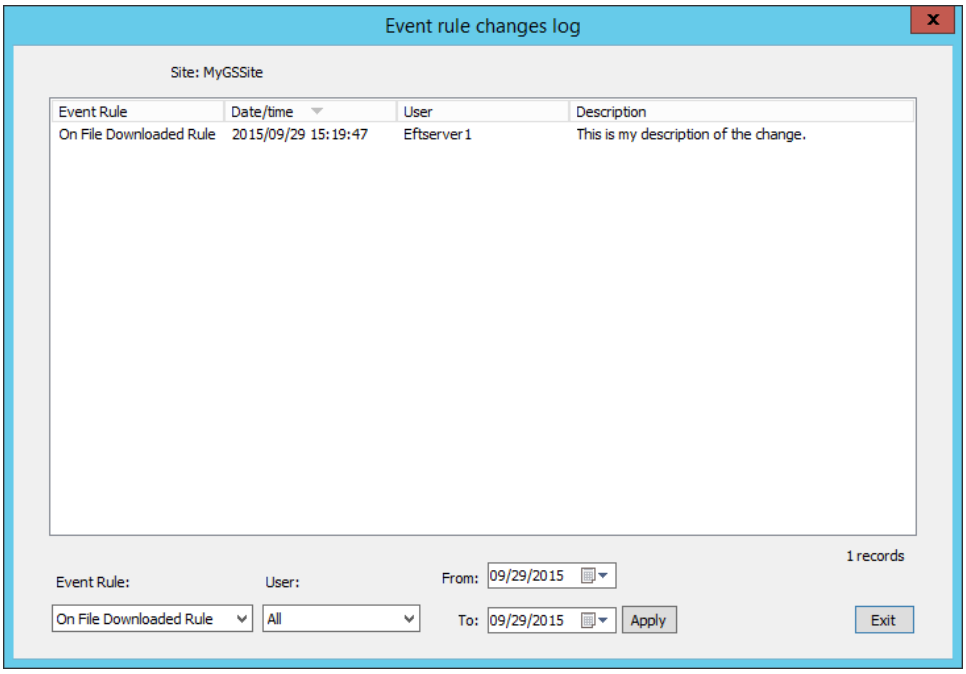
4. Click **OK**. The **Enter change description** box is enabled.



5. Provide a description of the change, then click **Apply**.

To view the Change Log

1. Open the Rule in the Rule Builder
2. Click **Change Log**. The log appears.



The log displays the name of the Event Rule, the date/time of the change, the name of the user who changed it, and the description if one was entered.

By default, only the selected Event Rule, all users, and changes on today's date are displayed. You can choose to show changes for all Event Rules, specific users, and a date range, then click **Apply**.

3. Click **Exit** when you're finished.

Using Virtual Paths In Event Rules

An EFT administrator can configure certain event rule actions using virtual paths that point to local/LAN object or cloud (AWS/Azure) objects. This allows you to configure Event Rule Actions using virtual paths that can point to local/LAN objects or cloud (AWS/Azure) storage objects. Below is a list of corresponding Event Rule Actions with paths that support the virtual path context variable (%FS.VIRTUAL_PATH%):

- Protocol: Upload,
  - Source path
- Protocol: Download
  - Destination path
  - Rename transferred file to

- Protocol: Synchronize
    - Mirror local - Source path
    - Mirror remote - Destination path
- Protocol: AS2
    - File(s) to upload
- Protocol: Email
    - Attach
- Cloud: Upload
    - Source path
- Cloud: Download
    - Destination path
    - Rename transferred file to
- Cloud: REST/Web Services
    - Save response to - File
    - Compression
- Compression
    - Source Path
    - Destination Path
- Cryptography: OpenPGP
    - File to process
- File: Scan
    - File Path
- File: Operation
    - Write operation - Destination Path
    - Read operation - Source Path
    - Rename operation - Source Path, Destination Path
    - Delete operation - Source Path
    - Concatenate operation - Source Path A, Source Path B, Destination Path
    - Checksum operation - Source Path

- Folder: Operation
  - Create action - Destination Path
  - Rename action - Source Path (Path), Destination Path (New Path)
  - Delete action - Source Path
- Script: Advanced Workflow
  - [Paths from custom parameters list] (Name/Value)

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 Protocol: Upload Action. This allows EFT 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 and click the **Server** tab.
2. On the **Server** tab, 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.

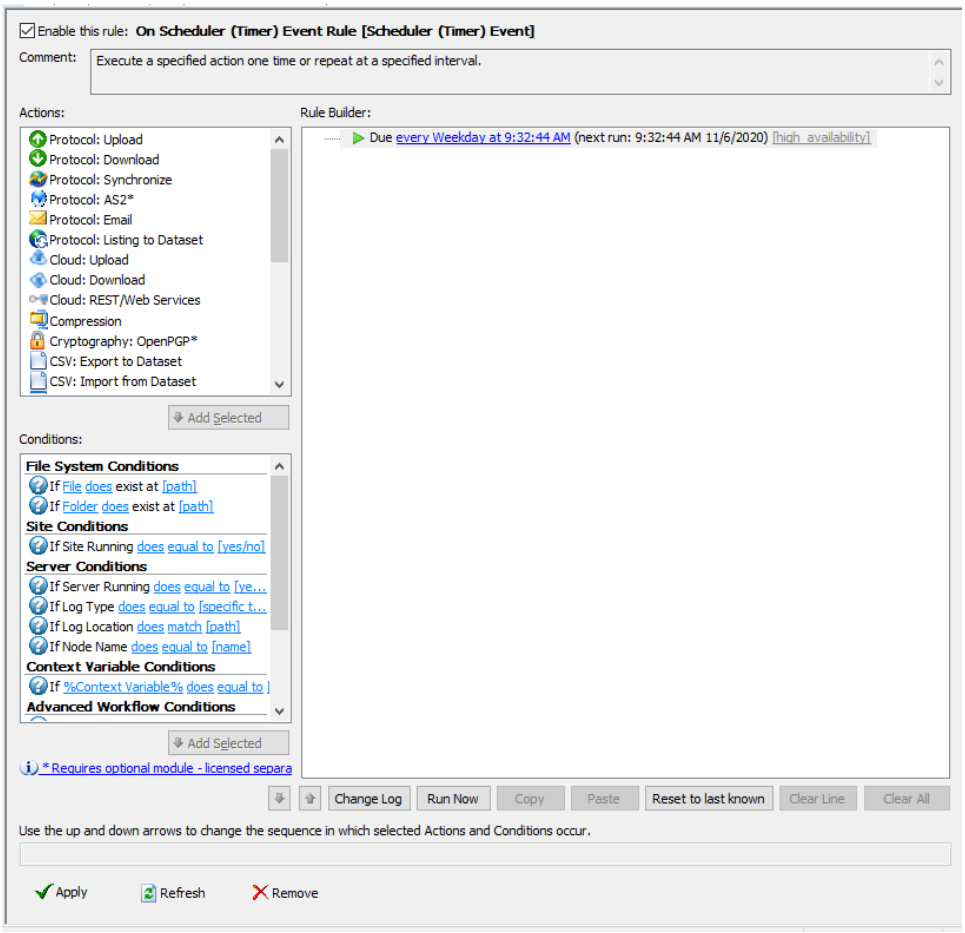
WARNING: Allowing user name and password replacement variables introduces a potential security vulnerability, because it allows passwords to reside in memory on EFT. The risk is low, but should be avoided unless you require the variables for an Event Rule.

Using Run Now to Test an Event Rule

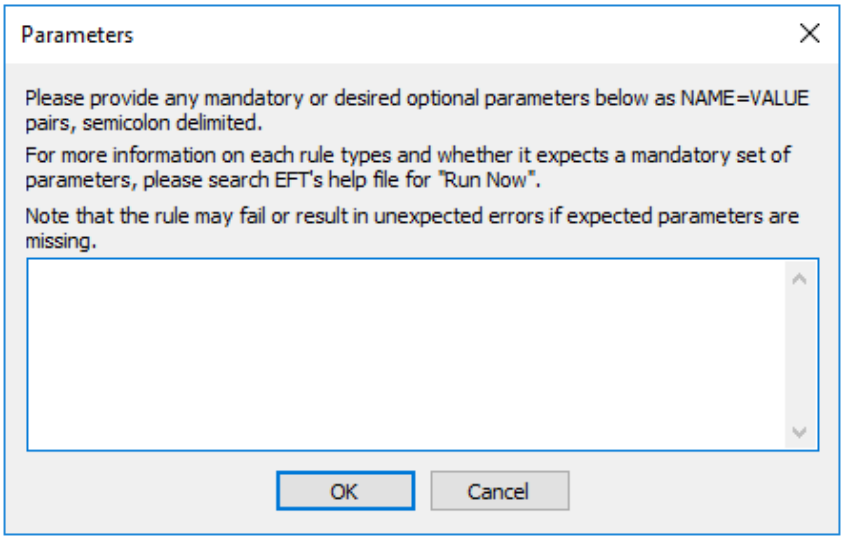
When defining Event Rules, you might want to run a quick test to verify the configuration.

To test an Event Rule

1. Define the Event Rule
2. At the bottom of the Rule Builder, click **Run Now**.



The **Parameters** dialog box appears.



3. In the **Parameters** dialog box, provide parameters that the rule is expecting, in NAME=VALUE pairs, such as USER LOGIN=lmauser1, or FS.PATH=c:\pathtomyfile\file.dot. To define multiple parameters, place a semicolon between each one.
    - Do not use percent signs % with the variables (that is, use FS.PATH, not %FS.PATH%).
    - For Folder Monitor rules, pass the following parameters when you use the "If File Change does equal to added" Condition:

      ```
      FS.MONITOR_OPERATION=added;
              FS.PATH=C:\dummyFile;
      ```

4. Click **OK**. The rule runs with the parameters used.
5. If you do not get the desired results, redefine the parameters or the rule itself and try again.

Exporting and Importing Event Rules

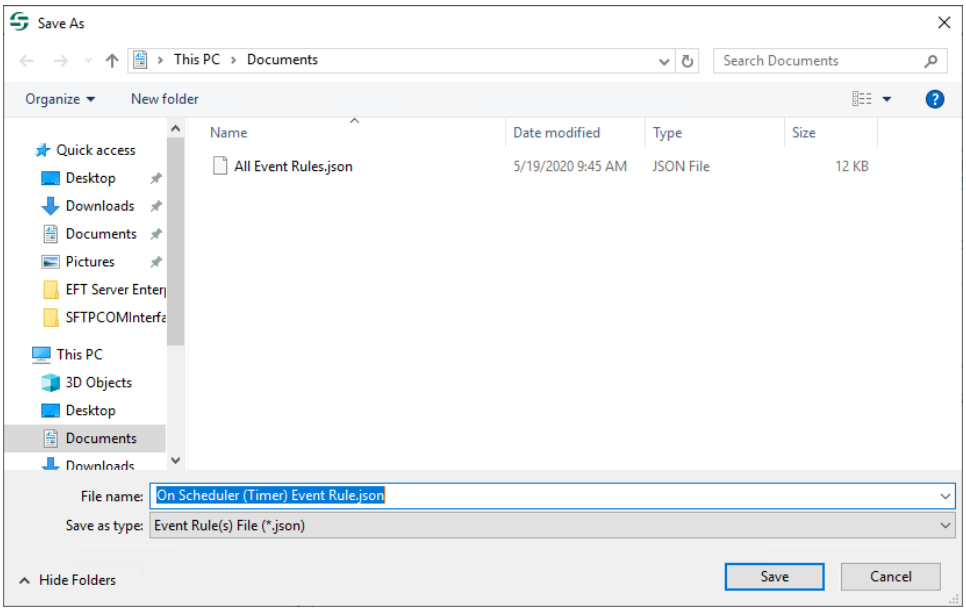
When moving an installation of EFT from staging to production, the biggest issue is moving the Event Rules.

When you do a Server Backup, all of the Event Rules are copied. Often, however, you don't want ALL of the Event Rules moved to production, just certain ones. With the import/ export feature, you can export just the Event Rules that you want as a JSON file, edit them, if needed, and import them into another EFT installation or Site. Or perhaps you want to send the rule to a colleague or technical support for assistance. You can send someone the file, that person can review and edit as needed, and then send it back to you, and then you can import it.

- You can only export and import event rules within the same version of EFT.
- You can import a JSON file of Event Rules that contain plain-text passwords. This change applies to all fields that use passwords. Plain-text passwords in the file must be bracketed by curly braces: `{"text"}` (like normal JSON values).
- You can export one or more Advanced Workflows. Refer to Exporting Advanced Workflows.
- If you are importing a "broken" Event Rule (for example, referring to an Advanced Workflows task that does not exist), the rule will not import.
- You can also export/ import Event Rules via COM and REST API
- You cannot import empty event rule folders.

To export Event Rules

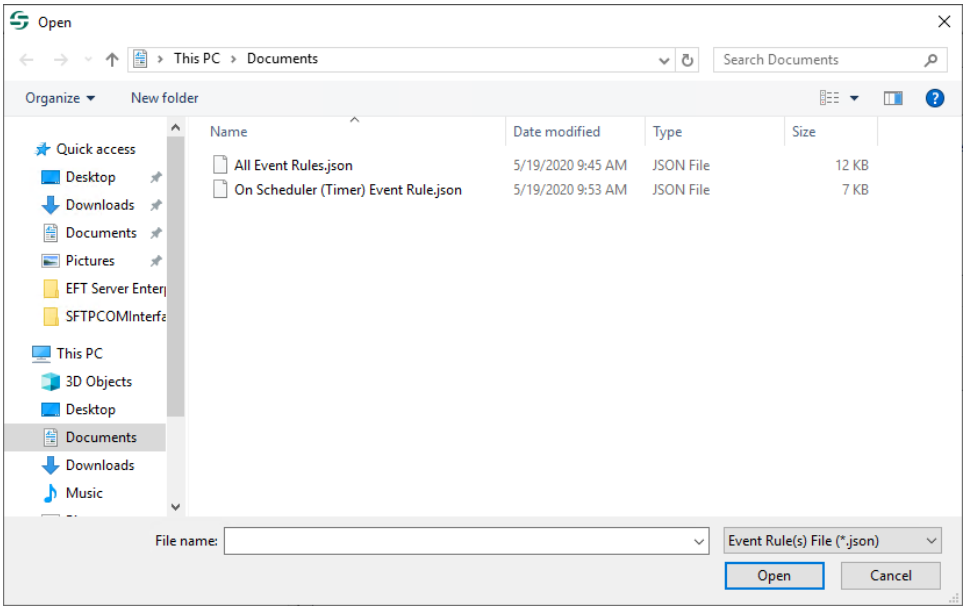
1. Right-click the Event Rule that you want to export (or the Event Rules node), then click **Export Event Rule**. The Windows **Save As** dialog box appears.



2. Click **Save**. The Event Rule is saved as a JSON file with the name you gave it. A message appears to confirm that it was saved.
3. You can view and edit JSON files in a text editor, such as Notepad.

To import Event Rules

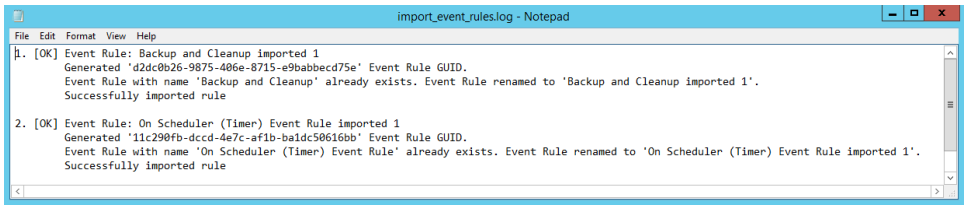
1. Right-click the Event Rule that you want to import, then click **Import Event Rule**. The Windows **Open** dialog box appears.



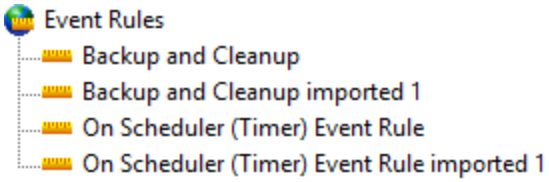
2. Click **Open**. The Event Rule is added to the Event Rules node.

   A message appears to confirm that it was imported and you are offered the option to view the log. The log file is saved to the logged-in user's

\Appdata\Local\Temp\EFT folder. The Event Rule GUID, the name of the Event Rule, and success or failure of import appears in the log.



3. If an Event Rule exists with the same name as the one being imported, a number is added to the name in the tree.



4. After the Event Rule is imported, you can drag and drop it into an Event Rule folder, edit it, and so on, just like any other Event 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.

While you can have two administrators working on Event Rules at the same time, if they are working on the same Rule at the same time, when they save their Rule, the second administrator to save will get a notice that the changes could not be saved because the system changed underneath them. They then need to refresh to see the other changes, and then make their changes to the Rule again.

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.

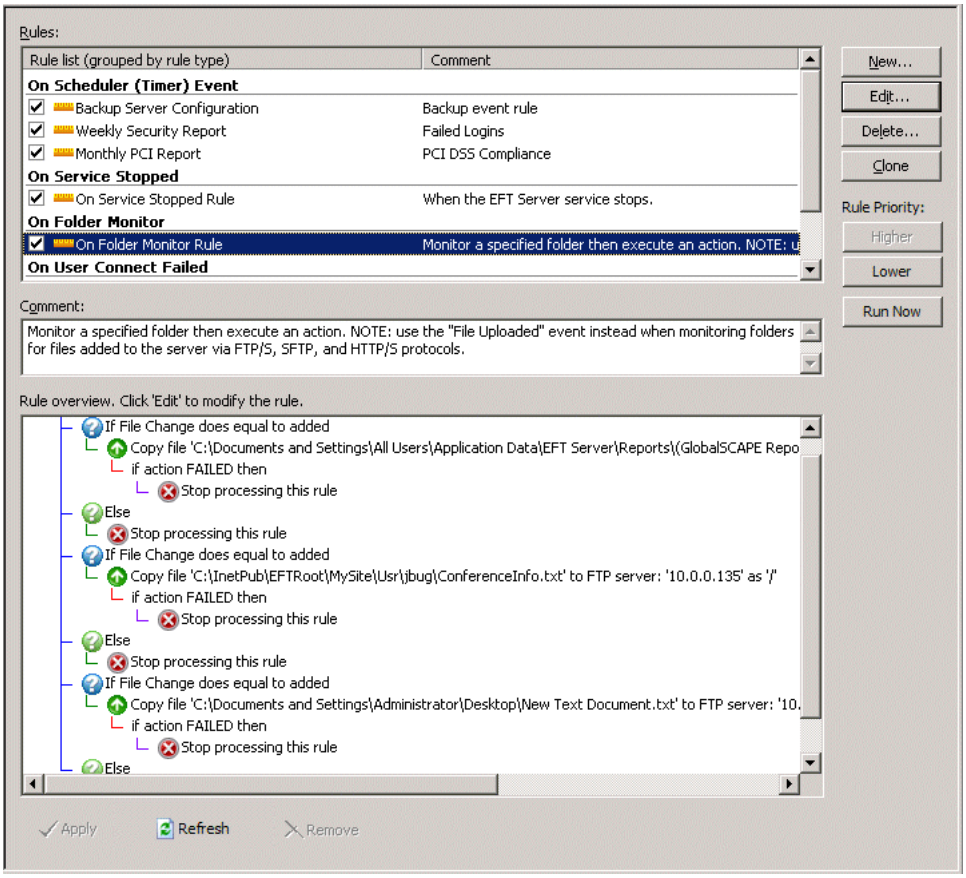
Prioritize - If you create more than one Rule for a single type of Event, EFT prioritizes the Rules in the order they appear on the Event Rules list. You can rearrange them using the **Rule Priority** buttons.

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 and click the **Server** tab.
2. On the **Server** tab, 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. Actions are indicated by their associated icons.

   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 .

To edit an Event Rule

a. 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.

b. 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.

c. Configure the Condition or Action by clicking the underlined variables (red or blue underlined text)

d. You can reorder Conditions and Actions by dragging them where you want them and using the up and down arrows.

e. Click **Apply** to save the changes on EFT.

To delete an Event Rule

a. In the right pane, click **Delete**. A confirmation message appears.

b. Click **Yes**. The Rule is deleted from the Site.

To clone an Event Rule

a. 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.

b. Edit the copy of the Rule as needed, and then click **Apply** to save the changes on EFT. Your new Rule appears in the Event Rules node with "Copy" appended to the name.

c. To rename the Rule, in the left pane, right-click the Rule, and then click **Rename**.

To change the priority of a Rule

a. In the right pane, click the Rule you want to move.

b. 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

a. In the right pane, clear the **Enable this rule** check box.

b. Click **Apply** to save the changes on EFT.

To re-enable an Event Rule

a. In the right pane, click the **Enable this rule** check box.

b. Click **Apply** to save the changes on EFT.

To rename an Event Rule

a. 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.)

b. Type the new name, then press ENTER or click away from the name. The name is changed.

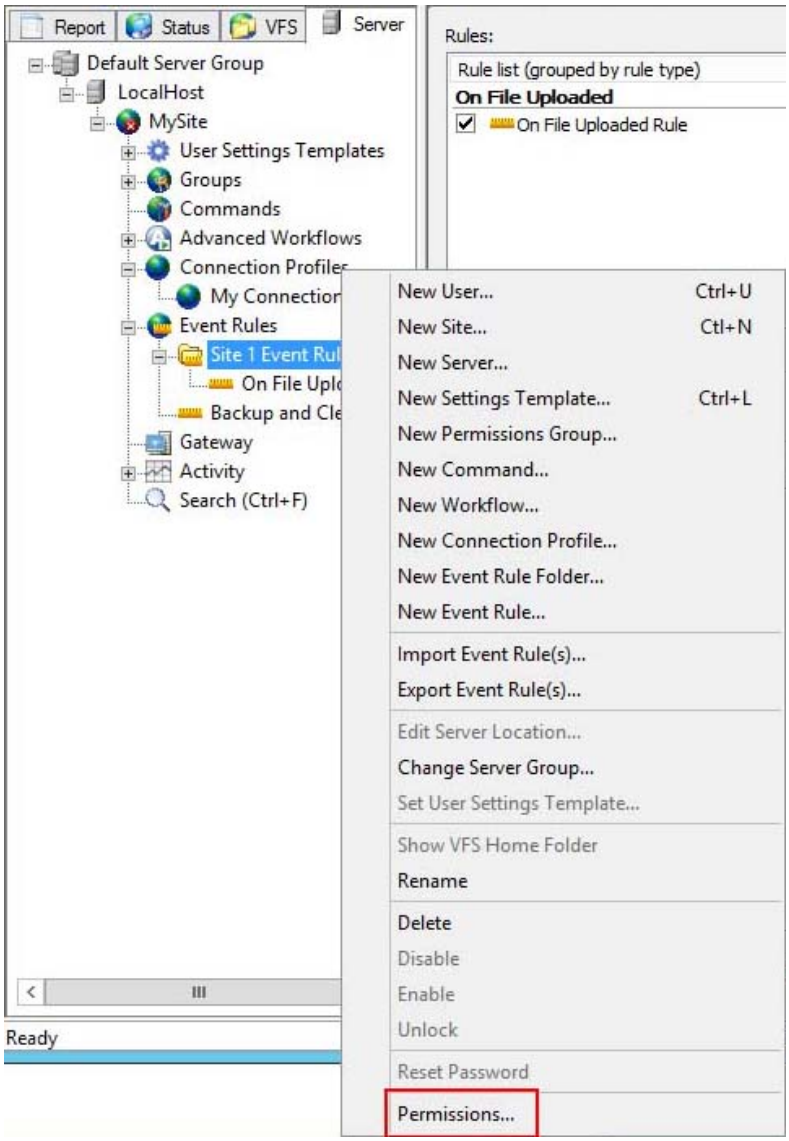
Event Rule Permissions

Permission to manage various aspects of the Event Rule system must be explicitly given to delegated administrators. Granular Event Rule permissions allow the EFT administrator to control which administrators have control over certain objects. If you change the Event Rule permissions for an administrator account while the administrator user is logged in to the administration interface, the user will have to log out and then log back in to effect the changes.

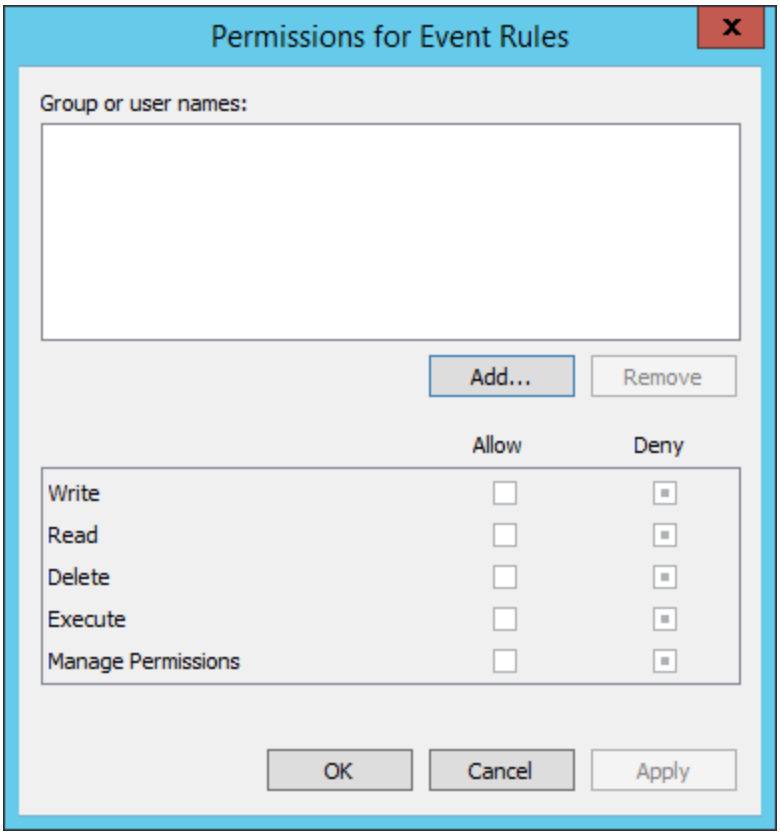
For delegated administrators to have **Allow** permission for ALL Event Rules, the Server administrator must configure permissions at the **Event Rules** node. To assign permissions only on certain Event Rule folders or only on certain Event Rules, right-click the folder or Event Rule, then click **Permissions**.

To manage permissions

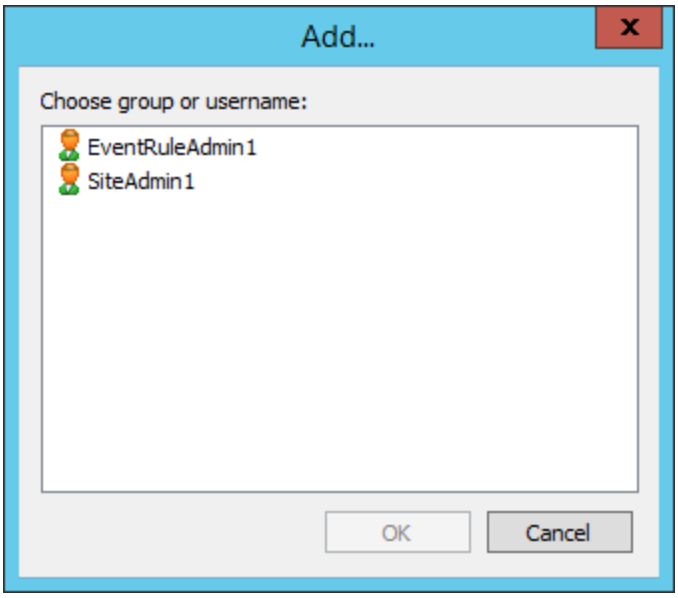
1. Log in as the **Server** administrator.
2. Right-click the Event Rules node, an Event Rules folder, an Event Rule, the Advanced Workflows node, or a Workflow, then click **Permissions**.



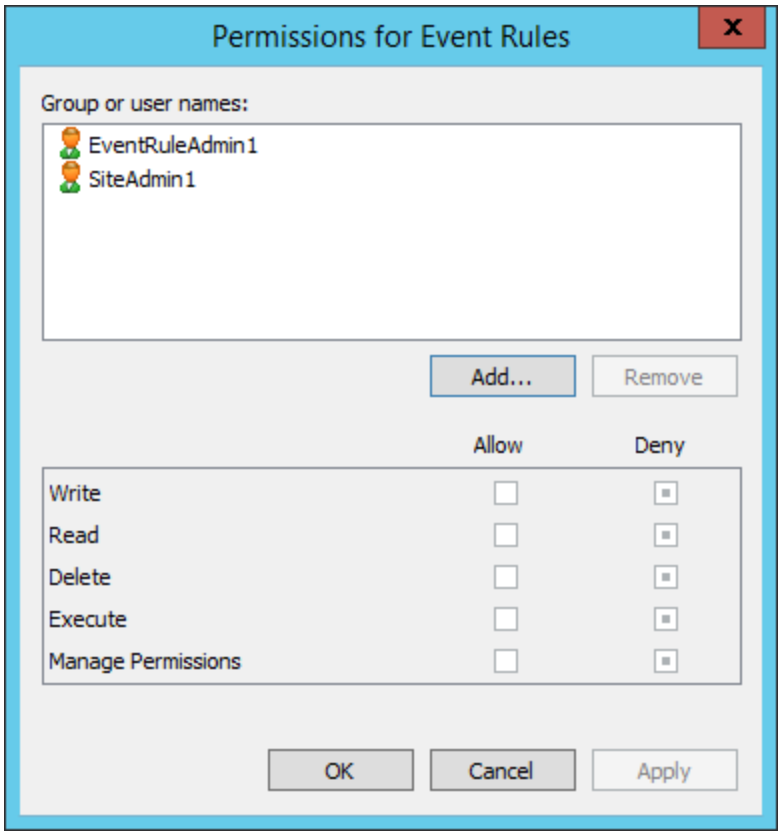
The **Permissions** dialog box appears. (The text in the title bar of the dialog box changes depending on which item in the tree you clicked.)



3. Click **Add**. Only Site and Event Rule administrators are present in the dialog box.



4. Click the administrator(s) for whom you want to add/edit permissions, then click **OK**.



5. The tristate check box for each permission has the following meanings:

Allow ☑ Deny ☐	Allowed
Allow ☐ Deny ☑	Denied
Allow ■ Deny ☐	Inherited (and allowed by inheritance)
Allow ☐ Deny ■	Inherited (and denied by inheritance)

6. Select the check boxes of the permissions that you want to **Allow** or **Deny**.
7. Click **OK**.
8. The permissions assigned at the node level and at the folder level are inherited by the items in the node or folder. You can then, as needed, edit the permissions for specific Event Rules, Workflows, or Event Rule folder.

Container Permissions

Permissions can be inherited from Container to Folder to Object. The table below describes the granular nature of these permissions.

Permission	Container	Folder	
Write	Create Folder or Object	Create Object	Update Object
Read	List	List + Show in Container List	Read + Show in Container or Folder List
Delete	None (inheritance only)	Delete this Folder	Delete this Object
Execute	None (inheritance only)	None (inheritance only)	• Execute Rule • Execute via Web-services
Manage permissions	Read and Write Permissions	Read and Write Permissions	Read and Write Permissions
Rename object requires	Write on Container or Folder + Delete on the Object		
Rename folder requires	Write on Container + Delete on the Folder		
Move rule requires:	Write on destination Container or Folder + Delete on the Rule		
Delete non-empty rule folder requires	• Delete Permission on each containing Rule • Administrator will receive “Need to Refresh” error when trying to remove/rename rules for which he/she has no Read Permission (e.g. when deleting non-empty folder containing “invisible” rules).		
Reordering rules	• Requires Delete + Manage Permissions on Container • Given an ordered set of Rules $\{R_1, R_2, \ldots, R_N\}$, of which an administrator sees $\{R_{i1}, R_{i2}, \ldots, R_{iM}\}$. If the administrator moves the Rule R_{ij} up, it will place the Rule in the complete list just before $R_{ij\text{-}1}$. Move the Rule R_{ij} down is interpreted as move the Rule $R_{ij\text{-}1}$ up.		
If an administrator has no Read permission on a Command, they will not be able to	• See the Command in Choose Command list of **Execute Command Action** dialog box • Assign the Command to the Rule (for example, when applying changes to the Event Rule with the Execute Command Action configured by other administrator)		
If an administrator has no Write permission in Command Container, they will not be able to	• Create Custom Command via Event Rules interface.		

Permission	Container	Folder
If an administrator has no Read permission on a Workflow, they will not be able to	• See the Workflow in **Choose Workflow** list of Advanced Workflow Action dialog box. • Assign the Workflow to the Rule (for example, when applying changes to the Event Rule with the Advanced Workflow Action configured by other administrator).	
If an administrator has no Read permission on a Profile, they will not be able to	• See the Profile in **Choose Profile list** of Offload/Download Action wizard. • Assign the Profile to the Rule (for example, when applying changes to the Event Rule with the Offload/Download Action configured by other administrator).	

Event Rules Client Log

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

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

For example:

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

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

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

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

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

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

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

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

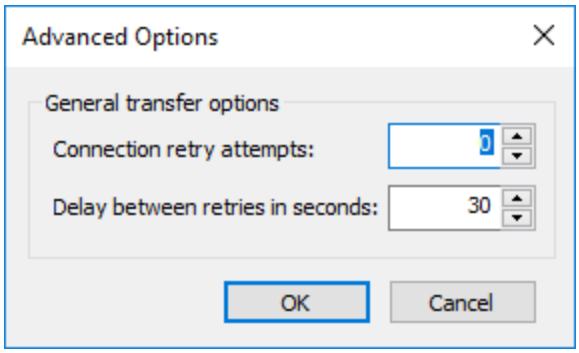
Advanced Transfer Options

The **Advanced Options** dialog box provides options for advanced transfer such as data port mode, connection retry attempts, filename encoding, time stamps, cloud transfers, and so on. These optional settings are available in the Connection Profile, File Offload configuration (Protocol Upload Action), File Download configuration (Protocol Download Action), Cloud: Upload and Download Actions, and the Web Services Action.

To configure advanced transfer options

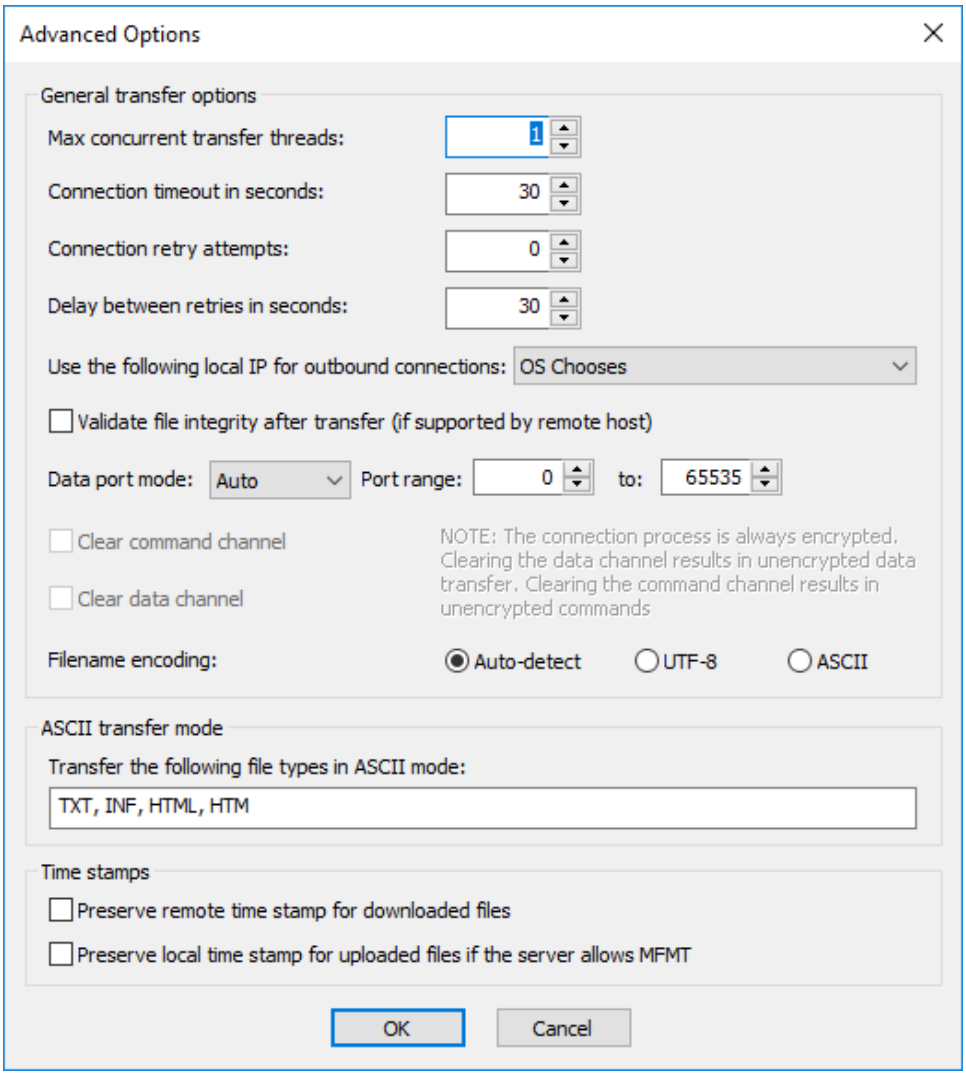
- Click **Advanced**. The **Advanced Options** dialog box appears.

For Local/LAN transfers:



- Specify the **Connection retry attempts** and **Delay between retries**. When files are being transferred with Event Rules (copy/move), if there are connection problems (for example, the network is unavailable), the server will attempt to establish a connection the number of times specified in **Connection retry attempts**. When EFT is able to re-establish the connection, it continues to transfer the file even if there are multiple interruptions.

Other protocols:



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 (for example, the network is unavailable), the server will attempt to establish a connection the number of times specified in **Connection retry attempts**. When EFT is able to re-establish the connection, it continues to transfer the file even if there are multiple interruptions.

b. Next to **Use the following local IP for outbound connections**, a list box contains an option labeled **OS Chooses** followed by a list of available IPv4 addresses and available IPv6 addresses (loopback addresses are not displayed). EFT only allows one physical IP to be selected at a time in an event rule, which cannot be replicated to the other HA nodes for obvious reasons. When the rule runs, the connection will fail on the second node with a 10038 failure, indicating that there is no IP or socket available. Click a single IP address from the list or let the operating system of EFT select the source IP based on the Site's listening IP settings. If the computer has multiple IP addresses available and/or both IPv4 and IPv6 addresses, you can specify an IP address to use or click **OS Chooses**.
    - (To specify an outbound IP address in an HA environment) In this drop-down list, you can specify a class C subnet for outbound connections. When the Event Rule executes, EFT performs a local check to see which IP addresses are available locally, and chooses the correct one based on the list selected.

c. Select the **Validate file integrity after transfer** check box to specify that EFT 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 initially makes connections in PASV mode. If the PASV connection fails, EFT attempts to connect in PORT mode automatically.
    - **Active**—When Active mode is selected, EFT 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 tells the remote server to provide <IP:PORT> to which EFT 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.

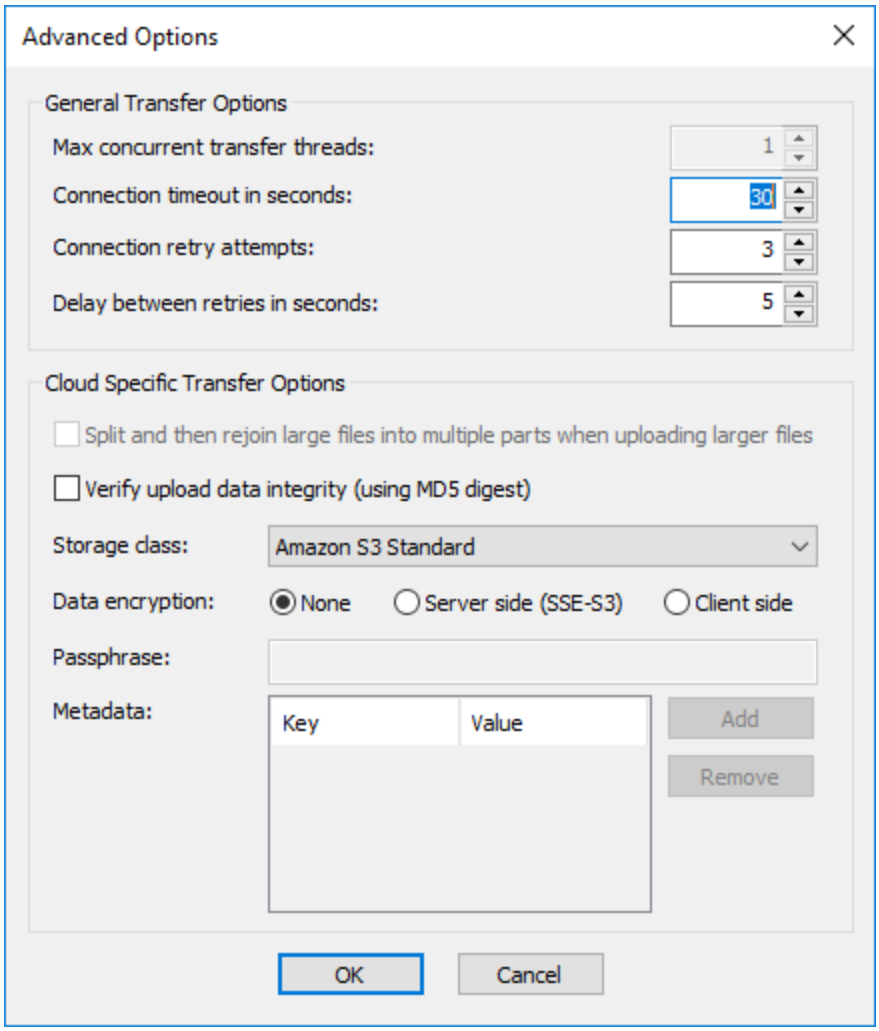
h. In the **ASCII transfer mode** area, specify the file types that can be transferred. Use a comma ***and a space*** between extensions. If you use only a comma with no space, then the Rule will not recognize the extension/file type. TXT, INF, HTML, and HTM are specified by default. If an asterisk (*) 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.)

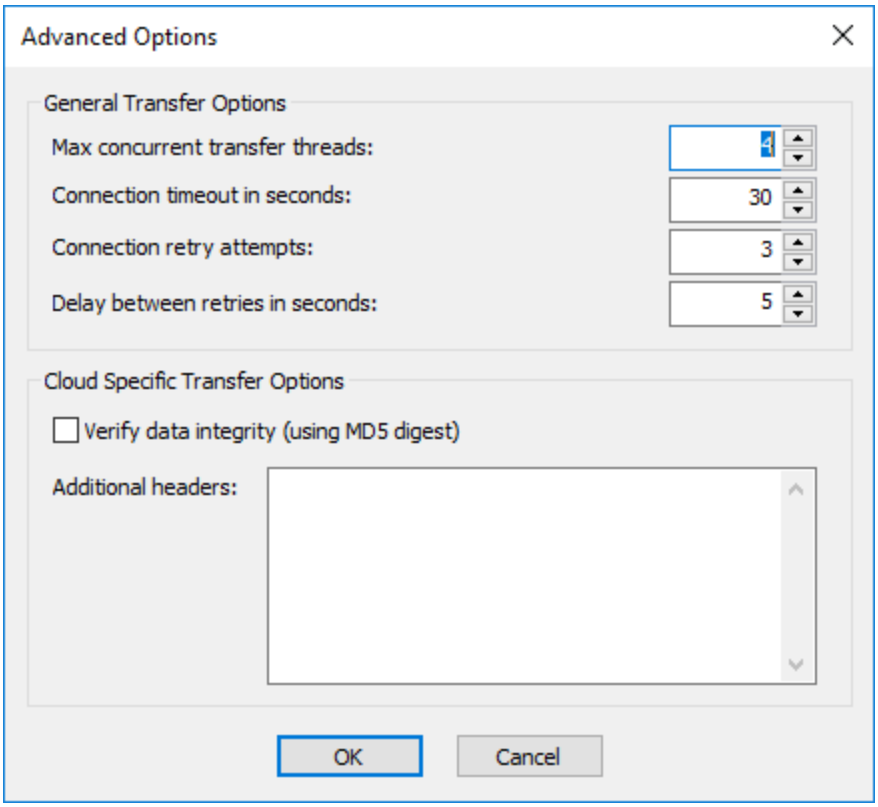
j. Click **OK**.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

Amazon Storage:



Azure Storage:



- **General Transfer Options** are the same as above.
- If you expect large file uploads (such as video), select the **Split and then rejoin large files into multiple parts when uploading larger file**s check box.
- Select the **Verify upload data integrity (using MD5 digest)** check box to assure file integrity
- **Amazon only:**
    - In **Storage class**, specify which cloud storage to use: **Amazon S3 Standard**, **Amazon S3 Standard - Infrequent Access**, **Amazon S3 Redunancy Storage (RRS)**,
    - Data encryption options include **None**, **Server side (SS3-S3)**, and **Client side**.
    - Provide the **Passphrase** to access the storage.
    - Add any **Metadata** to capture.
- **Azure only:**
    - Additional headers: Add header information as needed, in the format header:value
- Click **OK** to save the configuration.

FAQs:

- **Can I use context variables?**

  Context variables are supported for passphrase and Metadata.

- **What is the difference between Amazon S3 vs Amazon S3 (compatible)?**

  Amazon S3 (compatible) allows you to manually specify some of the fields (Endpoint URL, Region, host format). For example, for using with S3-compatible storage, such as Google or others. (refer to Defining a Connection Profile for details)

- **Are the values in metadata passed as custom headers in the request to S3?**

  Metadata are passed as a custom header, with a name that starts with "x-amz-meta-". For example:

  ```
  x-amz-meta-metadatakey: MetadataValue
  ```

Event Rule Load Balancing

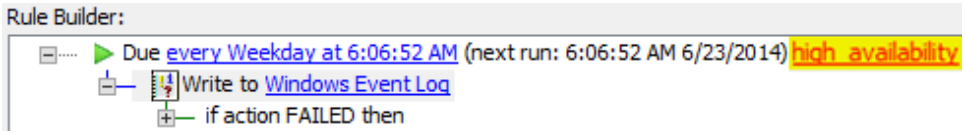
When two or more EFTs are configured in an active-active cluster, which of the EFT nodes executes a Timer or Folder Monitor Event Rule is determined by load balancing. Timer and Folder Monitor Event Rules have a "high availability" hyperlink with which you can specify if the rule will be load balanced. Clicking the hyperlink allows you to specify which node will run the Event Rule. The rule is load balanced based on which specified node is next available.

- If a specified node is offline, that node is skipped, and the rule is assigned to the next node specified in the node list. If none of the nodes specified in the list are online, an error is logged to the Windows Event Viewer.
- If you want to have a particular node handle more of the load, then you can enter that node more than once in the node list. For example, if the list is NODE1, NODE1, NODE2, NODE5, node 1 is sent Event Rules more frequently than nodes 2 or 5.
- Server Message Block (SMB) caching can cause load-balanced Folder Monitor events to fail to process files under an HA (active-active) clustered environment. To prevent this from happening, the installer creates an advanced property described in Knowledgebase article #11175: https://kb.globalscape.com/KnowledgebaseArticle11175.aspx.

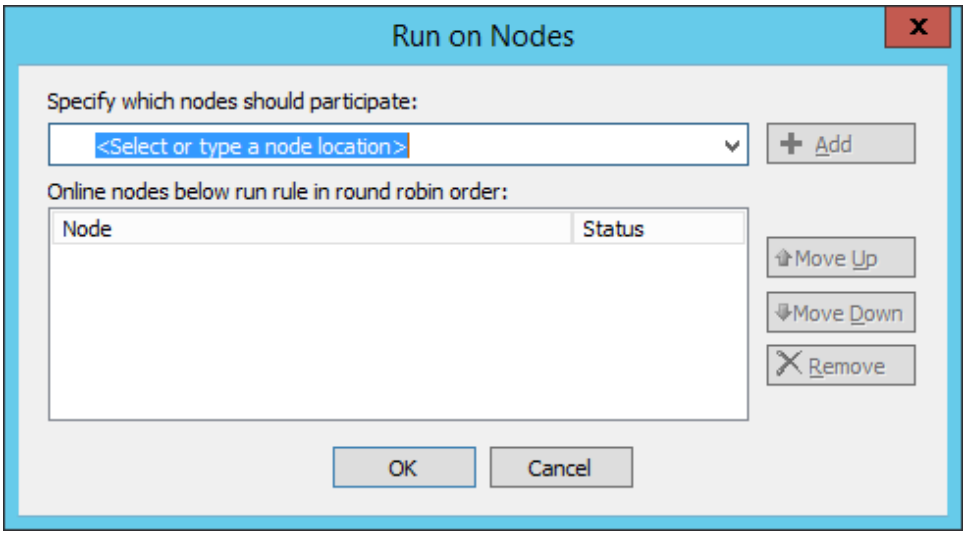
- **Define a default Event Rule load balancing list, as described below**. If no nodes are specified, the rule will run in non-HA (standalone) mode in which the event runs on ALL nodes and is not load balanced. For example, a Timer rule configured to run daily at 1 pm will run on ALL nodes of the cluster every day at 1 pm. You can specify default nodes on the High Availability Tab of the Server. You can override this default policy in individual Event Rules, as shown below.

To specify nodes for Event Rule load balancing

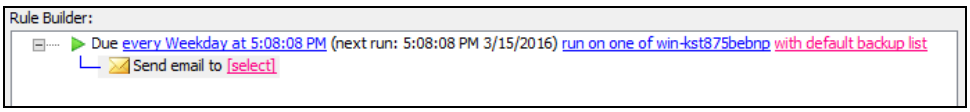
1. In the Rule Builder, in the Timer or Folder Monitor event, click the **high availability** link.



   The **Run on Nodes** dialog box appears.



2. Specify the nodes that are to run the rule (using the computer name), then click **Add**. Computer names are case sensitive. If you want a certain node to handle more of the load, list it more than once in the node list (for example, NODE1, NODE2, NODE2, NODE2, NODE 3...) You can specify nodes by IP Address (both IPv4 and IPv6).
   After you specify the nodes, the event expands to include "with default backup list."



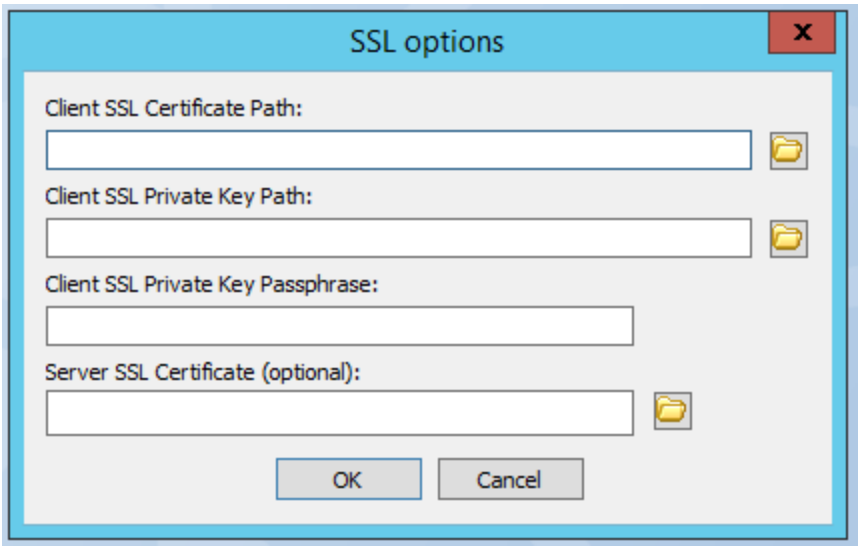
3. Click "with default backup list" to specify the default backup list.
4. Click **OK** to save your changes in the rule.

SSL Options Dialog Box

If you use a protocol that uses SSL (**FTPS** or **HTTPS**), you must provide the client and remote server's SSL certificate information in the Event Rule Action. The SSL options dialog box appears in the Connection Profile, File Offload configuration (Protocol: Upload Action), File Download configuration (Protocol: Download Action), and the Cloud: REST-Web Services Action Action.

To specify SSL options

1. In the Connection Profile or Event Rule, specify the protocol that uses SSL (**FTPS** or **HTTPS**).
2. Next to **SSL**, click **Configure**, or in the Invoke Web Service action, click **SSL**. The **SSL options** dialog box appears.



   a. In the **Client SSL Certificate Path** box, click the folder to specify the client SSL certificate path.
   b. In the **Client SSL Private Key Path** box, click the folder to specify the client SSL private key path.
   c. In the **Client SSL Private Key Passphrase** box, provide the passphrase for the client SSL certificate.
   d. In the **Server SSL Certificate** box, specify the remote server's certificate file. It is recommended, especially for production systems, that the EFT administrator obtain the remote server's SSL certificate and save it as a file in a place accessible by the EFT server service (such as the shared configuration path in HA mode or a local configuration path).

EFT will validate that the server side of any SSL-based connection made for that event action will match the server certificate. If you do not specify an SSL certificate in this box, EFT will accept any server-provided SSL certificate, which would leave the connection open to a man-in-the-middle attack.

3. Click **OK** to save the SSL options.

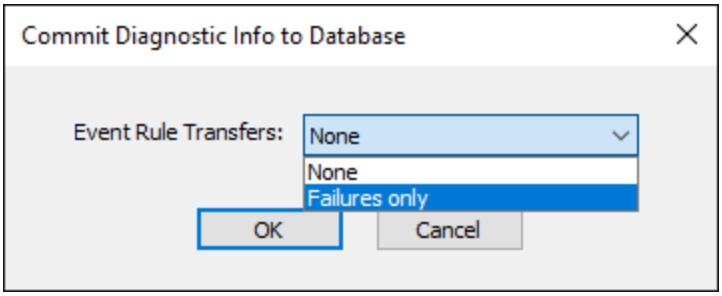
Logging Event Rule Transfer Failures

By default, and unless explicitly disabled, EFT will audit and retain all failed file transfer operations initiated by EFT's event rules to a flat file in EFT's /AppData/ directory. Optionally, you can instruct EFT to redirect its auditing of failed Event Rule-initiated transfer operations to the Auditing and Reporting (ARM) database. If enabled via this setting, those failed transfer logs will be stored in the tbl_EventRuleTransfers table in the database.

You can view a log of Event Rule transfer failures in our external business activity monitoring tool, BAM. To log more information about the failure, you must first enable the logging of failures on the **Logs** tab in EFT, as described below.

To enable and configure auditing and reporting

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Server node you want to configure.
3. In the right pane, click the **Logs** tab.
4. Next to **Audit event rule client outbound transfers,** click **Configure**, then specify whether to save Event Rule transfer failures to the database.



5. Click **Apply** to save the changes on the server.

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.

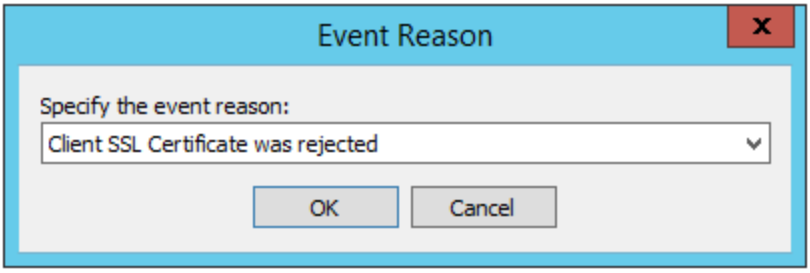
For details of overriding the default "concurrent threads" advanced property, refer to the Knowledgebase article, Changing the Number of Concurrent Threads Used by Event Rules.

Too Many Connections per Site

You can define an Event Rule to send you an email 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.

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**.

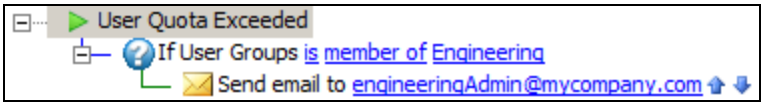
5. Click **OK**.
6. In the **Actions** list, double-click **Send notification email** (or click it, and then click **Add action**) to add it to the Rule.
7. In the **Rule Builder**, click the linked text **[select]** and configure an email to send yourself a notification (or link to your defined email template) then click **OK**.
8. Click **Apply** to save the changes on EFT.

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 specific Groups (By default, all Rules apply to all users.) For example, suppose the Engineering department has its own user administrator for EFT and you want the administrator to get an email when one of the user accounts exceeds its quota. You would set up a **User Quota Exceeded** Event with an **If User Groups** 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 email Action to the Rule and provide the email address of the user administrator and anyone else you want to receive the email.
6. Click **Apply**. The Rule appears similar to the following example:



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

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 (for example, `%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`.

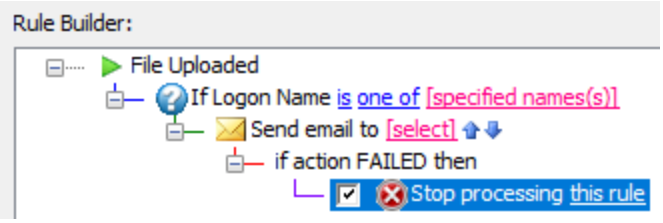
For details of the Copy/Move Action, refer to Copy or Move File to Host Action.

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.

Example: Send an Email Notification When a Certain User Uploads a File

To send an email notification when a user or group of users uploads a file

1. Create an event rule using the event trigger **File Uploaded**.
2. Add the Condition **If Logon Name is** and specify the username. You can specify one or more user names. (For a group of users, you could use the **If User is a member of specific group**, such as Administrators or Guests.)
3. Add the Action **Protocol: Email** and add user variables such as %USER.LOGIN% and file system variables such as %FS.FILENAME%. (You could also use variables for the home folder, physical folder, virtual folder, home IP, and so on.)



Example: Copy/Move and Download File Cloud Storage Actions

The **Upload** and **Download file to cloud storage** Actions are used when you want to copy, move, or download files to/from Amazon S3 or Azure Blob storage. The **Cloud Connector Configuration** page in the Action wizard allows you so specify the cloud provider storage and other details, based on whether you specify Amazon S3 or Azure Blob storage.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

Be aware of the following AWS restrictions when creating a bucket name:

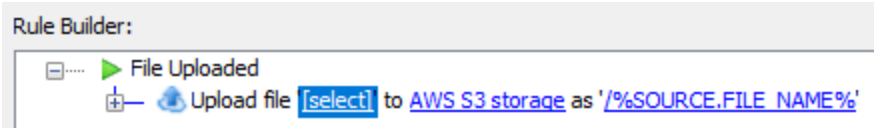
- Bucket names can contain lowercase letters, numbers, and hyphens.
- Each label must start and end with a lowercase letter or a number.
- A bucket name cannot start or end with a period.
- Bucket names must be at least 3 and no more than 63 characters long.
- Bucket names must not be formatted as an IP address (for example, 192.168.5.4).

- As a best practice, always use DNS-compliant bucket names regardless of the region in which you create the bucket. For example, MyAWSBucket is a valid bucket name, even though it contains uppercase letters. If you try to access this bucket by using a virtual-hosted–style request (http://MyAWSBucket.s3.amazonaws.com/yourobject), the URL resolves to the bucket myawsbucket and not the bucket MyAWSBucket. In response, Amazon S3 will return a "bucket not found" error.
- For more information regarding buckets restrictions, limitations, and naming, refer to http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html.
- Cloud transfers are performed in multi-part sequential files. You can configure an advanced property to revert to legacy behavior (chunked transfers in parallel).

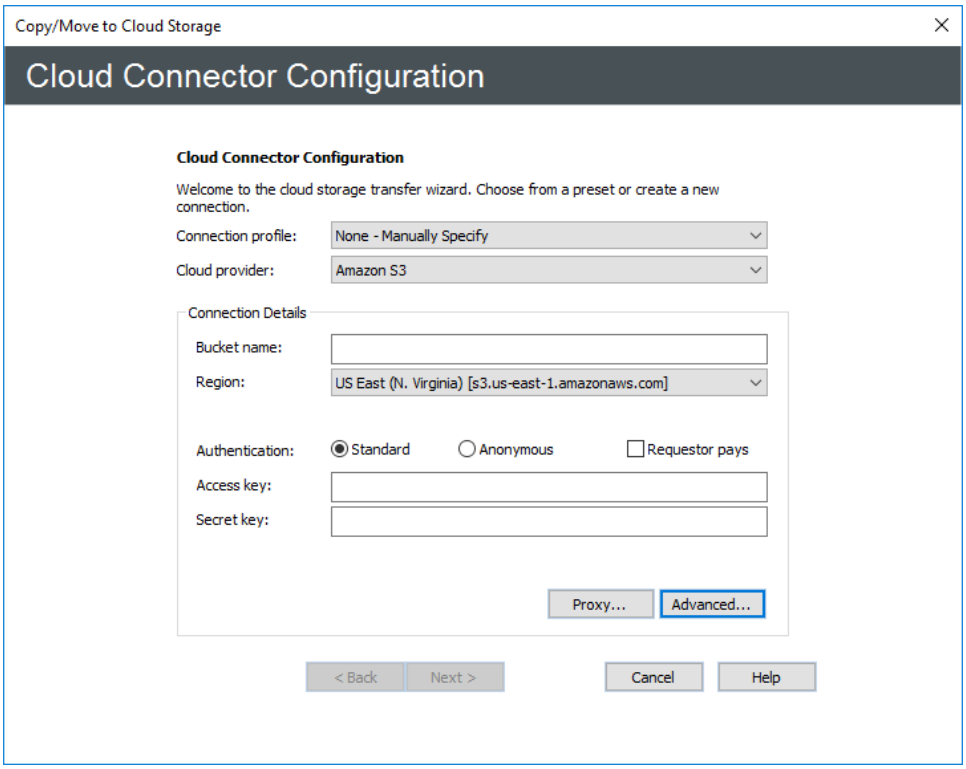
Refer to https://kb.globalscape.com/KnowledgebaseArticle11437.aspx for details of the advanced property.

To configure Copy/Move and Download file to cloud storage Event Rules

1. After specifying an event in the Rule Builder, in the **Actions** list, double-click **Copy/Move (push) to** or **Download file from cloud storage**.



2. In the Action that was added to the Event Rule, click **select**. The **Cloud Connection Configuration** page appears.



3. Specify the connection details. You could also configure a cloud provider in a Connection profile to avoid having to configure connection details for every Event Rule.
4. Click **Advanced** to specify **Cloud Specific Transfer Options**. Refer to Specifying Advanced Transfer Options for configuration details.
    - **Can I use context variables?**

      Context variables are supported for passphrase and Metadata.

    - **What is the difference between Amazon S3 vs Amazon S3 (compatible)?**

      Amazon S3 (compatible) allows you to manually specify some of the fields (Endpoint URL, Region, host format). For example, for using with S3 compatible storage such as Google drive and others.

    - **Are the values in metadata passed as custom headers in the request to S3?**

      Metadata are passed as a custom header, with a name that starts with "x-amz-meta-". For example:

      ```
      x-amz-meta-metadatakey: MetadataValue
      ```

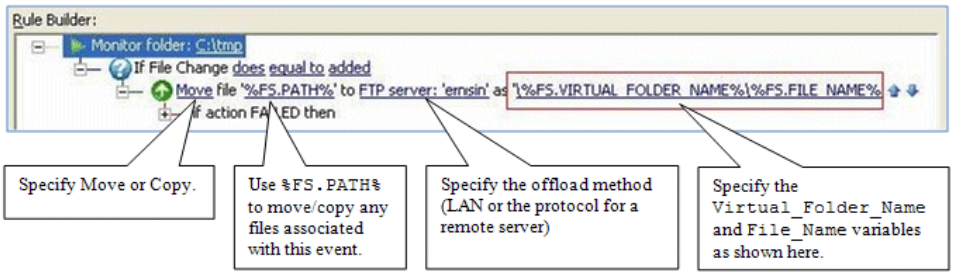
(For metadata details, refer to https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingMetadata.html.)

5. Click **Next**. In **Source File Path**, specify the source file. You can specify filenames, paths, or context variables.
6. Click **Next**. Specify the **Destination** for folder and filename (optional). Context variables can be used here also. Also in the **Destination** page of the wizard, you can specify what to do with matching filenames (Overwrite, Skip, or Numerate) and, can specify to rename the transferred file.
7. Click **Finish**.

Example: 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.



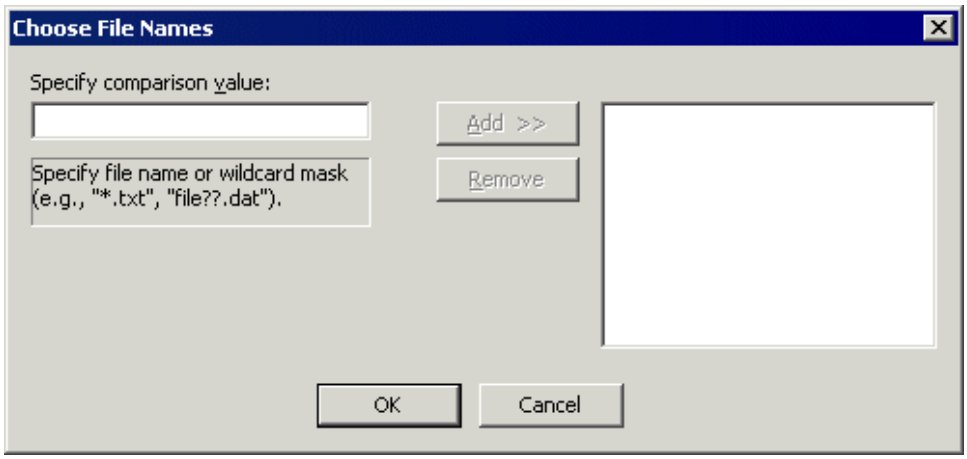
Refer to Monitoring Folders for details of creating a Folder Monitor Rule. Refer to Copy/Move (push) File to Host Action for details of using the **Copy/Move** Action.

Example: Moving an Uploaded File Based on Filename

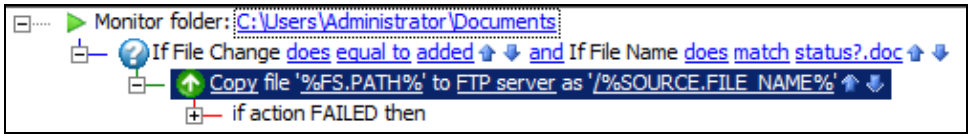
Suppose every Friday the manager of Engineering uploads a status report named `status<date>.doc` to EFT. You want the manager of Marketing to have access to that file, but not to any other files in the Engineering manager's folder. The example below describes how to create an Event Rule so that when a file with "status" in the name is uploaded to EFT, EFT 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 and click the **Server** tab.
2. On the **Server** tab, 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 Monitor Folder Rule. Note that if you create a Monitor Folder Rule to monitor a folder that is already being monitored by another Monitor Folder Rule, a warning message appears because the two Monitor Folder 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, 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 **Protocol: Upload**. The Action is added to the **Rule Builder**.



10. Click one of the undefined parameters (for example, '%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 ProtocolUploadAction 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.) In this example, we specified a user's folder.
17. Click **Finish** then click **Apply** to save the changes on EFT. (You could also add other Actions, such as email notifications.)

    Now when a user uploads a file called `status?.doc`, EFT 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.

> **WARNING:** Do ***not*** use `%EVENT.TIME%`, because the colon (for example, `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).

Proxy Settings

The topics below describe how to define and use a proxy for event rules.

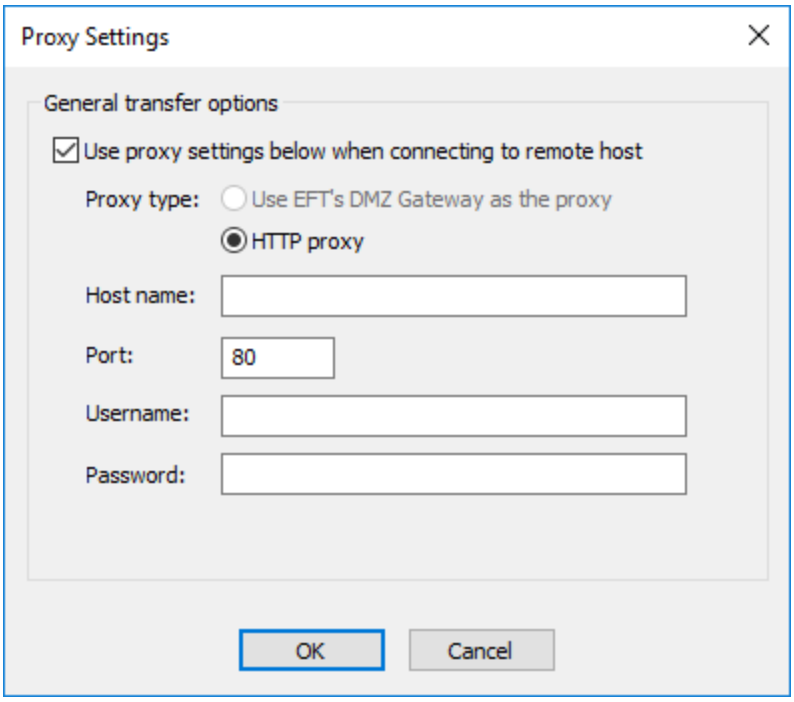
Defining a Proxy

If you connect to EFT through a proxy server, you must enable and define the proxy. The **Proxy Settings** dialog box appears in the Connection Profile, File Offload configuration (Copy/Move Action), File Download configuration (Download Action), and the Invoke Web Service from URL Actions.

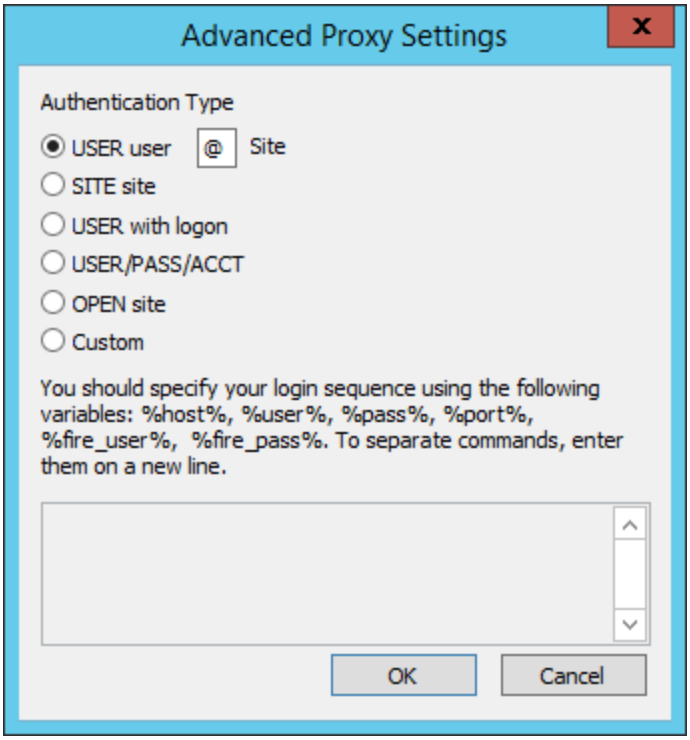
- Using the DMZ Gateway as a proxy is not available when using Cloud Connection profiles. EFT uses the AWS SDK, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.
- Contact your system administrator for the proper host name, port, user name, password, and proxy type, as well as any required advanced authentication methods.

To configure the proxy settings

1. In the profile or action that you are configuring, click **Proxy**.
2. Select the **Use proxy settings** check box.
3. Specify the **Proxy type**.
4. Specify the **Host name**, **Port**, **Username**, and **Password** used to access the proxy server.



5. Click **Advanced** to specify an authentication type or login sequence. You must have selected **FTP Proxy** in the **Proxy Settings** dialog box to specify advanced settings.



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**, 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.

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

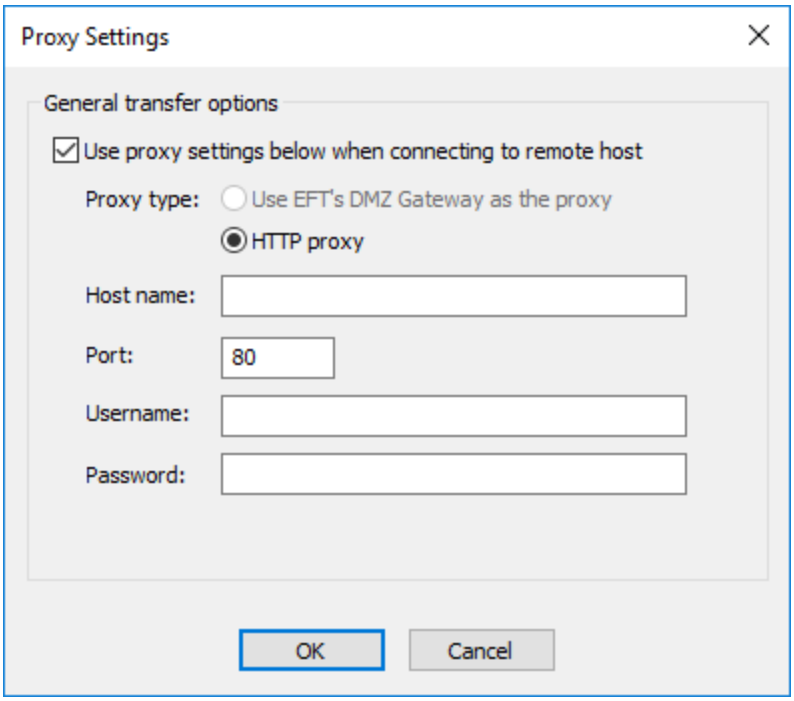
Configuring Advanced Proxy Settings

If you connect to EFT through a proxy server, you must enable and define the proxy. The **Advanced Proxy Settings** dialog box appears in the Connection Profile, File Offload configuration (Copy/Move Action), File Download configuration (Download Action), and the Invoke Web Service from URL Actions.

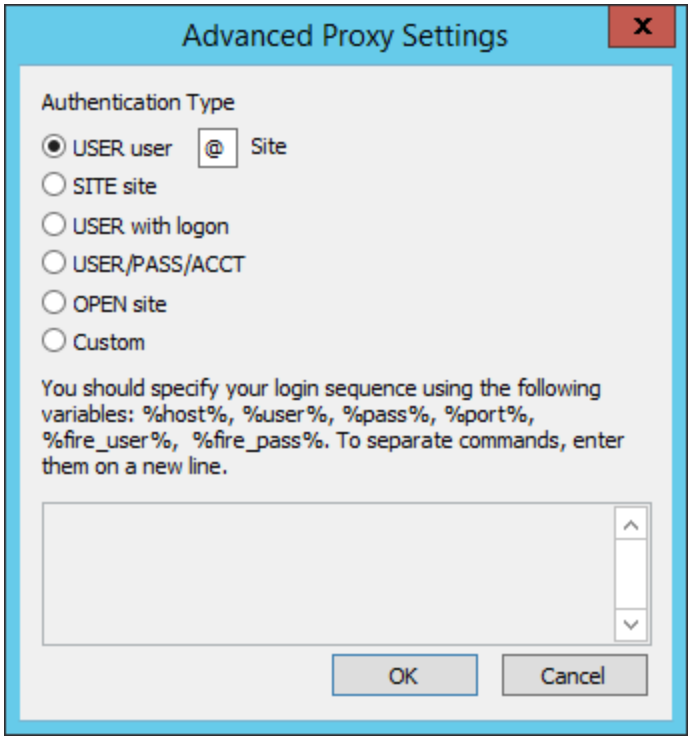
- Using the DMZ Gateway as a proxy is not available when using Cloud Connection profiles. EFT uses the AWS SDK, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.
- Contact your system administrator for the proper host name, port, user name, password, and proxy type, as well as any required advanced authentication methods.

To configure advanced proxy settings

1. In the profile or action that you are configuring, click **Proxy**.
2. Select the **Use proxy settings** check box.
3. Specify the **Proxy type**.
4. Specify the **Host name**, **Port**, **Username**, and **Password** used to access the proxy server.



5. Click **Advanced** to specify an authentication type or login sequence. You must have selected **FTP Proxy** in the **Proxy Settings** dialog box to specify advanced settings.



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**, 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.

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

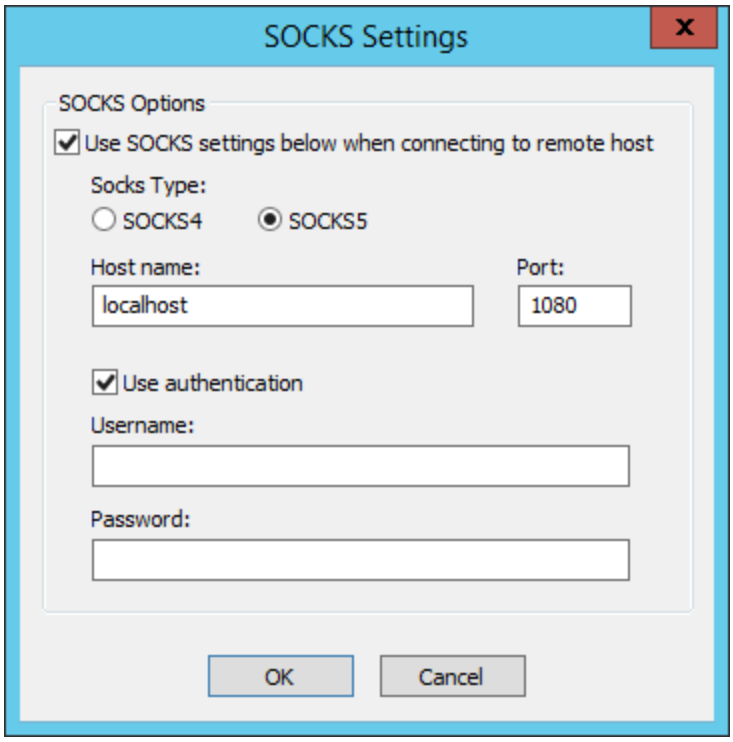
Using a SOCKS Proxy Server

When you create an Event Rule that requires the use of a SOCKS proxy server, you can specify settings in EFT for the connection to the SOCKS proxy server.

If you enable the use of DMZ Gateway as the proxy in the Proxy Settings dialog box, SOCKS options are disabled. EFT does not support the use of DMZ Gateway as a proxy and SOCKS settings in combination. For cloud connections, EFT uses the AWS SDK, which does not support the SOCKS protocol, which is required to proxy communications via the DMZ Gateway.

To use a SOCKS proxy server

1. Create an Event Rule.
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.

Routing Outbound Traffic through a Proxy

You can connect to EFT through an outbound 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 will route through normal network mechanisms to reach the destination. However, it is possible to configure 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.

EFT Variables

This section provides details of the EFT context variables. EFT uses *context variables* to pull data from the database. The variable contains specific information about an Event. You can use the variables in Event Rules, email notifications, and Advanced Workflows.

- How to Use EFT Context Variables
- Advanced Workflow Variables - Properties associated with Advanced Workflows, used when the Execute Advanced Workflow Action is added to an Event Rule.

  > **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

- AS2-Related Variables - Status of AS2 transfers (available only in AS2-related Event triggers)
- Cloud Variables - Used in the Download from Cloud Storage Action and Send Email Notification for Cloud Event Rules

  > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

- Connection Variables - IP address, port, etc. for connecting to EFT
- Event Properties 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
- Remote Agent Variables - Properties associated with Remote Agent activities, such as Remote Agent template name, status, last update, and so on.
- Scheduler (Timer) Rule Variables - Used for Scheduler (Timer) Rules (For file operation triggers, use File System Variables.)
- Server Variables - Server status, logs, and computer name
- Site Variables - Site URL and status
- Transfer Properties Variables - Properties associated with the transfer: Speed, size, and seconds to transfer
- User Variables - User name, login information, etc.
- Workspaces-Related Variables - Virtual/physical path, owner, and so on.
- Using Context Variables for Parameterized Event Rules

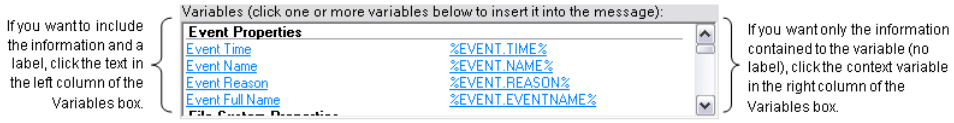
> **NOTE:** EFT can also use other variables as described in Context Variable Condition, Runtime Template Variables, Upload Forms, Flow: Variable Action, Flow: Subroutine Action, and Workspaces-Related Variables.

How to Use the Variables

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

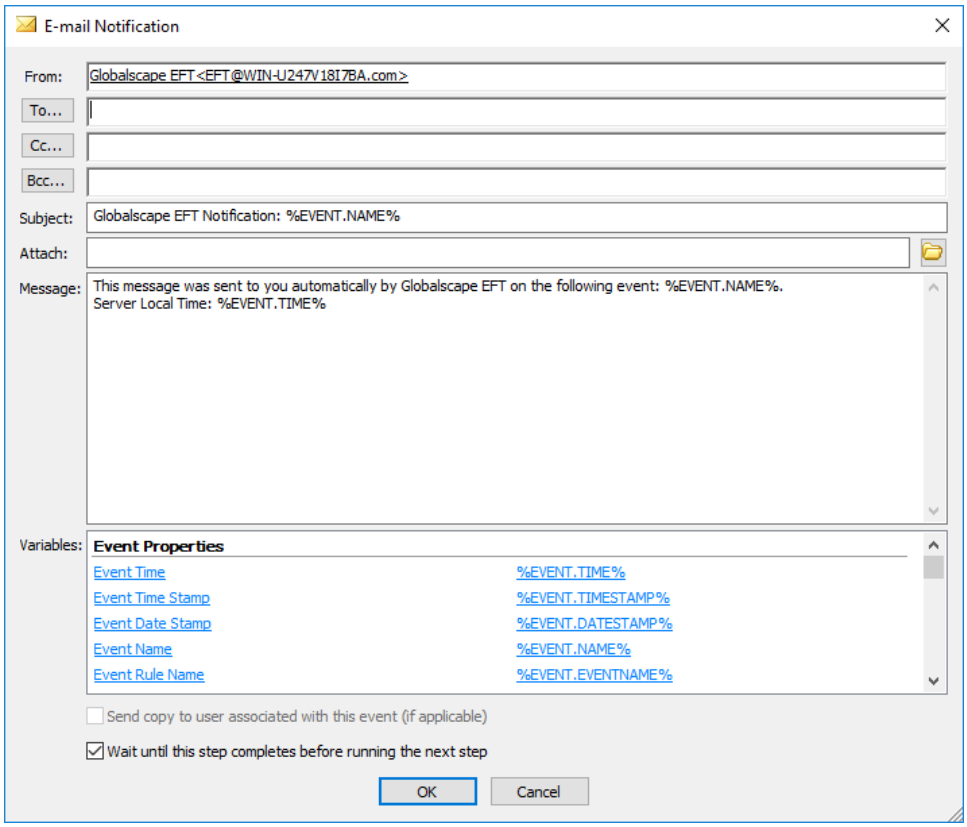
- If you just want the information contained to the variable, click the variable in the right column of the **Variables** box.
- If you want the information ***and*** a label, click the text in the left column of the **Variables** box.

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 email to be sent when the Event occurs. In the **Edit Mail Template** dialog box, you can send the default email or you can add one or more variables listed in the **Variables** box at the bottom of the email. Each of the variables defined in EFT is described in Connection Variables; however, not all of the variables described below are available in the email notification. In the email notification, you can specify to display the text along with the value of the variable (e.g., File Creation Date: 8/28/2022), or just the value of the variable (e.g., 8/28/2022).

Suppose you configured this email notification:



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

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

Event Time: 28 Aug 22 10:01:56

File Creation Date: 8/28/20202

File Creation Time: 10:01:56

Event Date Stamp: 20200828

Event Time Stamp: 100156
```

NOTE: In Event Rules and Commands with a defined path or file name, do not use variables that add invalid file name 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 email 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
```

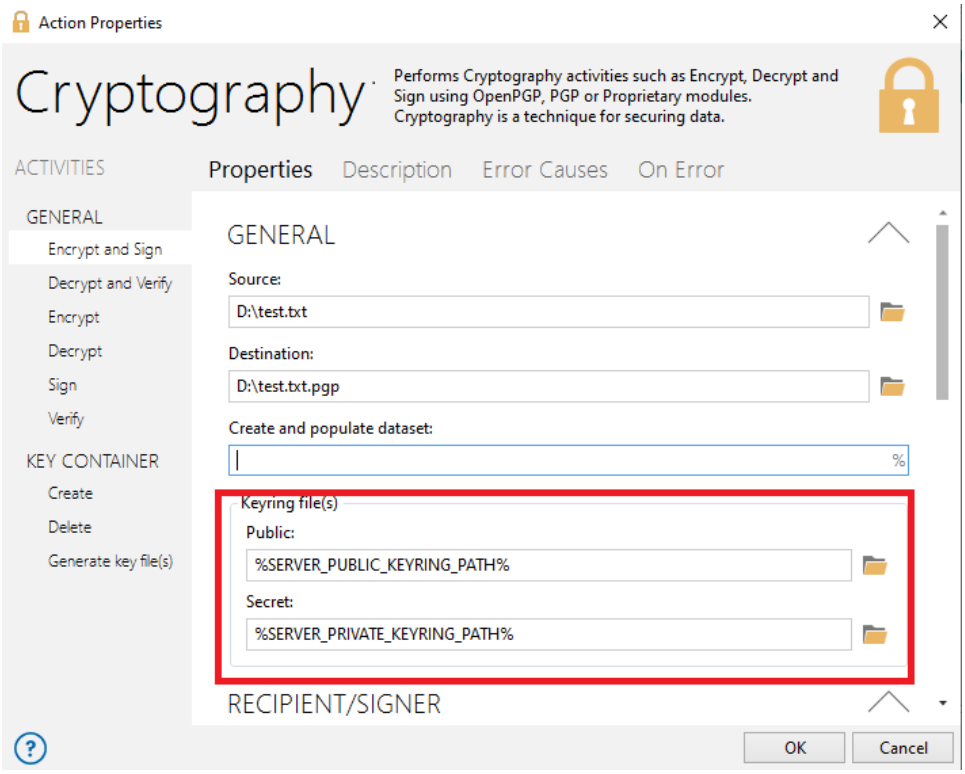
Advanced Workflow Variables

Used when the Execute Advanced Workflow Action is added to an Event Rule.

Text Displayed	Variable	Description
Advanced Workflow Name	%AWE.TASK_NAME%	Workflow name
Advanced Workflow Log Path	%AWE.LOG_PATH%	Workflow log path
Advanced Workflow Error Code	%AWE.ERROR_CODE%	Workflow error code
Advanced Workflow Error Description	%AWE.ERROR_DESCRIPTION%	Workflow error description
Advanced Workflow Error Line	%AWE.ERROR_LINE%	Workflow error line
Advanced Workflow Result Code	%AWE.RESULT_CODE%	Workflow result code displayed in the Windows Event Log and others
Advanced Workflow Result Description	%AWE.RESULT_DESCRIPTION%	Workflow result description displayed in the Windows Event Log and others

Advanced Workflow Execution Time (ms)	%AWE.EXECUTION_TIME_MS%	Workflow execution time (ms)

You can also pass other EFT variables into the Advanced Workflow Actions. For example, the path to the OpenPGP keyring files can be passed to the workflow with the %SERVER_PUBLIC_KEYRING_PATH% and %SERVER_PRIVATE_KEYRING_PATH% variables.



AS2 Variables

Status of AS2 transfers (**available only in AS2-related Event triggers**)

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 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)

Text Displayed	Variable	Value Contained in Variable
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

Cloud Variables

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

Used in the **Download from Cloud Storage** Action and **Send Email Notification** for Cloud Event Rules

Text Displayed	Variable	Description
Cloud Object Content Length	%CLOUD.OBJ_META_CONTENT_LENGTH%	Object's size in bytes
Cloud Object Content MD5	%CLOUD.OBJ_META_CONTENT_MD5%	Base64-encoded 128-bitMD5 digest of the object
Cloud Object Date	%CLOUD.OBJ_META_DATE%	Object's date from meta data
Cloud Object Last Modified	%CLOUD.OBJ_META_LAST_MODIFIED%	Object's date last modified
Cloud Object Version ID	%CLOUD.OBJ_META_VERSION_ID%	From x-amz-version-id, which is the object version
Cloud Object Key Name	%CLOUD.OBJ_KEY_NAME%	Exact object name (e.g., 4my$-organization, or my.great_photos-2014/jan/myvacation.jpg

Text Displayed	Variable	Description
File Change	%CLOUD.MONITOR_ OPERATION%	Operation of file change (create, delete, and rename)

Connection Variables

IP address, port, etc. for connecting to EFT

Text Displayed	Variable	Description
HTTP Query String	%CONNECTION.HTTP.QUERY_ STRING%	HTTP header string
HTTP Headers List	%CONNECTION.HTTP.HEADERS_ LIST%	HTTP header list
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 Properties Variables

Name, date, time, reason, etc. for Event trigger

Text Displayed	Variable	Description
Event Date Stamp	%EVENT.DATESTAMP%	Date that the Event was triggered, e.g., `20070828` (suitable for file naming)
Event Rule Name	%EVENT.EVENTNAME%	User-defined name for the Event Rule (e.g., My File Renamed Event Rule)
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

Text Displayed	Variable	Description
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 Time Stamp in ISO8601 format	%EVENT.DATE_TIME_ISO8601%	Date and time that the Event Was triggered in ISO8601 format: 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
Event Timestamp	%EVENT.TIMESTAMP%	Time that the Event was triggered, e.g., `100156` (suitable for file naming)
Event Transaction ID **(EFT Enterprise only)**	%EVENT.TRANSACTION_ID%	The Transaction ID as logged by the database EFT is connected to (with ARM). This ID can be used to backtrack and find it in the database manually or to generate queries to the database.
Folder Monitor Failure Reason	%EVENT.MONITORFAILUREREASON%	Reason why the Folder Monitor Rule failed.
Folder Monitor Health	%EVENT.MONITORHEALTH%	Health of network share
Event Rule Failure Reason	%EVENT.ACTION_FAILURE_REASON%	Set to a string that represents the failure cause for event rule actions.

File System Variables

File name, date, size, path, etc. that was transferred; also report name and content

Text Displayed	Variable	Description
Report File	%FS.REPORT_FILE%	The full path of the report generated by the Generate Report Action, including the file name. This variable can be used in copy/move, OpenPGP, and custom commands that have a failure Event defined, but should not be used for custom command actions that do not have a failure Event defined.) 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 stops processing the Event Rule, **do not use this variable in email notifications**; use %FS.REPORT_CONTENT% instead.
Report Content	%FS.REPORT_CONTENT%	Contents of the report generated by the Generate Report Action. This variable is typically used after creation of an HTML report, in an email notification action, where it is desirable to embed the HTML contents of the report as the email body.
Report File Name	%FS.REPORT_FILENAME%	The name of a report file created by a Generate Report action. This variable is typically used after creation of a PDF report file, in an email notification, to provide the destination path for the report file after a Copy/Move action deposits it in a more permanent location.
Virtual Path	%FS.VIRTUAL_PATH%	Virtual location of the file (See a list of uses for this variable below.)
Physical Path	%FS.PATH%	Physical location of the file
File Change	%FS.MONITOR_OPERATION%	File change that triggered the Event (added, removed, etc.) Used in Folder Monitor rules
Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%	The structure of the virtual folders
Physical Folder Name	%FS.FOLDER_NAME%	Name of the physical folder
Virtual Directory Name	%FS.VIRTUAL_DIR_NAME%	Name of virtual directory, without the whole path
Base File Name	%FS.BASE_FILE_NAME%	Name of the file without the extension

Text Displayed	Variable	Description
File Extension	%FS.FILE_EXTENSION%	File extension; Takes anything after the last dot (before the extension) and places it into this context variable. (e.g., for `document.docx`, `docx` is the value of the variable.) This variable can be used anywhere %FS.BASE_FILE_NAME% can be used.
File Name	%FS.FILE_NAME%	Name of the file with the extension
File Size	%FS.FILE_SIZE%	Size of the file involved in the Event
File CRC	%FS.FILE_CRC%	This variable is only applicable for "Verify Uploaded" events using HTTP and HTTPS protocols.
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 Creation Date in ISO8601 format	%FS.FILE_CREATION_DATETIME_ISO8601%	File Creation Date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
File Modification Date in ISO8601 format	%FS.FILE_MODIFICATION_DATETIME_ISO8601%	File Modification Date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
Virtual Destination Path	%FS.DST_VIRTUAL_PATH%	Virtual destination path of the file involved in the Event
Physical Destination Path	%FS.DST_PATH%	Physical destination path of the file
Physical Destination Folder Name	%FS.DST_FOLDER_NAME%	Physical destination folder
Destination File Name	%FS.DST_FILE_NAME%	Destination file name
Compressed File Physical Path	%FS.COMPRESSED_PATH%	Physical path to the compressed file
Compressed File Name	%FS.COMPRESSED_FILE_NAME%	Name of the compressed file with the extension

Text Displayed	Variable	Description
Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%	Name of the compressed file without the extension

The following Event Rule Actions with paths can support the virtual path context variable (%FS.VIRTUAL_PATH%):

- Protocol: Upload
  - Source path
- Protocol: Download
  - Destination path
  - Rename transferred file to
- Protocol: Synchronize
  - Mirror local - Source path
  - Mirror remote - Destination path
- Protocol: AS2
  - File(s) to upload
- Protocol: Email
  - Attach
- Cloud: Upload
  - Source path
- Cloud: Download
  - Destination path
  - Rename transferred file to
- Cloud: Rest/Web Services
  - Save response to - File
- Compression
  - Source Path
  - Destination Path
- Cryptography: OpenPGP
  - File to process
- File: Scan
  - File Path

- File: Operation
  - Write operation - Destination Path
  - Read operation - Source Path
  - Rename operation - Source Path, Destination Path
  - Delete operation - Source Path
  - Concatenate operation - Source Path A, Source Path B, Destination Path
  - Checksum operation - Source Path
- Folder: Operation
  - Create action - Path (Destination of the path to be created)
  - Rename action - Path (Source Path), New Path (Destination Path)
  - Delete action - Path (Source Path)
- Script: Advanced Workflow
  - [Paths from custom parameters list] (Name/Value)

Remote Agent Context Variables

The Remote Agent Context Variables can be used in RAM Event Rules. Each of the variables is described below.

Text Displayed	Variable	Description
Remote Agent Name	%AGENT.NAME%	Computer name of remote system running the Remote Agent, enumerated if there is more than one Agent with that name.
Remote Agent Version	%AGENT.VERSION%	Version of Remote Agent update
Remote Agent Last Update Time Stamp	%AGENT.LAST_ UPDATE_TIMESTAMP%	Date of last Remote Agent update
Remote Agent Next Update Time Stamp	%AGENT.NEXT_ UPDATE_TIMESTAMP%	Date of next scheduled Remote Agent update
Remote Agent NetBIOS Name	%AGENT.COMPUTER_ NAME%	Computer name of remote system running the agent
Remote Agent Template	%AGENT.TEMPLATE%	Template name associated with the Agent
Remote Agent Status	%AGENT.STATUS%	Status of Remote Agent (e.g., Active, Pending, Approved, Denied, Banned)

Scheduler (Timer) Rule Variables

The %SOURCE.FILE_NAME% variable is available in the list box of **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

Server status, logs, and computer name

Text Displayed	Variable	Description
Log Location	%SERVER.LOG_LOCATION%	Location of the log file
New Log File Name	%SERVER.LOG_NEW_NAME%	New name of the log file
New Log File Path	%SERVER.LOG_NEW_PATH%	New path of the log file
Old Log File Name	%SERVER.LOG_OLD_NAME%	Old name of the log file

Text Displayed	Variable	Description
Old Log File 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 is running
Server Running	%SERVER.STATUS%	Indicates whether the EFT 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 Advanced Workflows module
Public Key ring path	%SERVER_PUBLIC_KEYRING_PATH%	Pass the location of the private key ring to the Advanced Workflows module
Install Directory	%SERVER.INSTALL_DIRECTORY%	Directory in which the server is installed

Site Variables

Site URL and status

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 Running	%SITE.STATUS%	Indicates whether the Site was running when the Event was triggered. (Yes or No)
Data Protection Officer email	%SITE.PRIVACY_DPO_EMAIL%	Displays the email of the Data Protection Officer (DPO) that you specify in the GDPR dialog box on the Site > Web tab.
DMZ Gateway Address	%SITE.DMZ_ADDRESS%	Displays the IP address of the DMZ Gateway
DMZ Gateway Port	%SITE.DMZ_PORT%	Displays the port of the DMZ Gateway

Transfer Properties Variables

Properties associated with the transfer: Speed, size, and seconds to transfer

Text Displayed	Variable	Value Contained in Variable
Transfer Rate	%TRANSFER.RATE_ KBPS%	Average speed of transfer (total bytes transferred/total seconds to transfer) Displayed in kilobytes per second (KBps).
Transferred Bytes	%TRANSFER.BYTES%	Total number of bytes in the transfer. **NOTE**: By default FTP uses built-in compression (MODE Z); therefore, it is possible for transferred bytes to be less than the file size. Moreover, the values for FTPS, SFTP, and HTTP could differ from file size due to internal compression and protocol overheads.
Transfer Seconds	%TRANSFER.SECONDS%	Total number of seconds it took to transfer

User Variables

User name, login information, etc.

Text Displayed	Variable	Description
Using Remote Agent	%USER.AGENT%	Indicates whether the user is using a Remote Agent (Yes or No)
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)
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
DUNS Number	%USER.DUNS%	A user's organization's "DUNS number"; (The Data Universal Numbering System, DUNS, is a proprietary system developed and regulated by Dun & Bradstreet that assigns a unique numeric identifier to a single business entity.)
email Address	%USER.EMAIL%	email address of the user, if defined in the **User Account Details** dialog box. You can pass multiple addresses to the Advanced Workflow Engine using this variable.

Text Displayed	Variable	Description
Account Enabled	%USER.ENABLED%	User account is enabled:(Yes or No
Account Expiration Date	%USER.EXPIRATION_DATE%	Date in the default system locale when user account expired: Date , or `Never`
Account Expiration Date in ISO8601 format	%USER.EXPIRATION_DATETIME_ISO8601%	Displays the account expiration date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
(GDPR) User EU data subject status	%USER.EU_DATA_SUBJECT_STATUS%	User is an EU data subject: Yes, No, or Unknown
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
(GDPR) Reason given	%USER.GDPR_REASON_Given%	Reason the user exercised privacy rights (used with "Right exercised" variable)
(GDPR) Right exercised	%USER.GDPR_RIGHT_EXERCISED%	User has exercised the "right to be forgotten": Yes, No, or Unknown
(GDPR) Right exercised per Article ID	%USER.GDPR_RIGHT_EXCERCISED_ ARTICLE_ID%	Article ID is applicable to the right exercised by the user (used with "Right exercised" variable)
Groups	%USER.GROUPS%	Lists groups of which the user is a member
Home Folder	%USER.HOME_FOLDER%	User's home folder, for example, \asmith
Home Folder	%USER.HOME_FOLDER_PATH%	Entire path to a user's home folder (for example, C:\InetPub\EFTRoot\MySite\Usr\asmith)
Home IP	%USER.HOME_IP%	IP address of the user
Home Folder is Root	%USER.HOME_IS_ROOT%	**Treat Home Folder as Root** check box is selected: Yes or No

Text Displayed	Variable	Description
Invalid login attempts	%USER.INVALID_LOGINS%	Number of invalid login attempts by the user
User is locked out	%USER.IS_LOCKED_OUT%	Indicates whether user account is locked
Last Login Date	%USER.LAST_LOGIN%	Provides the date and time (in the default system locale) the user last logged in to EFT
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 date/time in the default system locale when the user account is set to expire, or `Never`
Password Expiration Date in ISO8601 format	%USER.PASSWORD_EXPIRATION_DATETIME_ISO8601%	Password Expiration Date in ISO8601 format 2019-01-14T20:10:19Z 2019-01-14T20:10:19+0500
Phone Number	%USER.PHONE%	Phone number of the user, if defined in the **User Account Details** dialog box
Consent status	%USER.PP_CONSENT_STATUS%	Returns the status of the Privacy Policy: Unknown, Granted (implicit), Granted (explicit), Denied, Rescinded
(GDPR) User consent to privacy policy	%USER.PP_CONSENT_STATUS%	User consented to the privacy policy: Unknown, Agreed (implicit), Agreed (explicit), Disagreed, or Withdrawn.
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).
Settings Template	%USER.SETTINGS_LEVEL%	Settings Template of the user

Text Displayed	Variable	Description
(GDPR) User agreement to terms of service	%USER.TOS_AGREEMENT_STATUS%	User agreed to the terms of service: Unknown, Agreed (implicit), Agreed (explicit), Disagreed, or Withdrawn.

Workspaces-Related Variables

The variables below are for use in Event Rules for virtual/physical path, owner, and so on. The Workspaces notifications use different variables than these, as shown below.

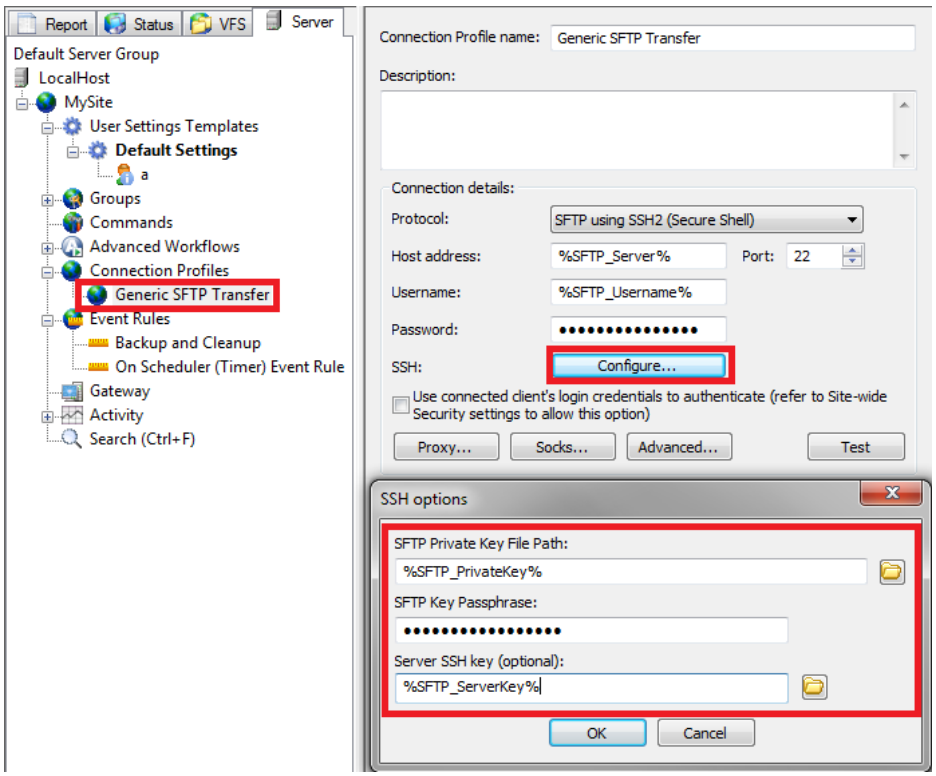
Text Displayed	Variable	Value Contained in Variable
Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%	Virtual path of the Workspace
Workspace Physical Path	%WORKSPACE.PATH%	Physical path of the Workspace
Workspace Name	%WORKSPACE.NAME%	Name of the Workspace Folder
Workspace Participants List	%WORKSPACE.PARTICIPANTS%	Participants sharing the Workspace
Workspace Subject	%WORKSPACE.SUBJECT%	Subject line of the email sent via Workspaces
Workspace Message	%WORKSPACE.MESSAGE%	Message sent via Workspaces
Workspace Owner	%WORKSPACE.OWNER%	Owner of the Workspace
Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%	Email address of the owner of the Workspace; the variable is case sensitive when used in the To, Cc, or Bcc fields of email notifications.
Workspace User	%WORKSPACE.USER_NAME%	Username of the Workspace participant
Workspace User Permissions	%WORKSPACE.USER_ PERMISSIONS%	User permissions of the Workspace
Workspace User Email Address	%WORKSPACE.USER_EMAIL%	User email of the participant

Text Displayed	Variable	Value Contained in Variable
Workspace User Account Exists	%WORKSPACE.USER_ACCOUNT_EXISTS%	Identifies whether the user account exists (or needs to be created)

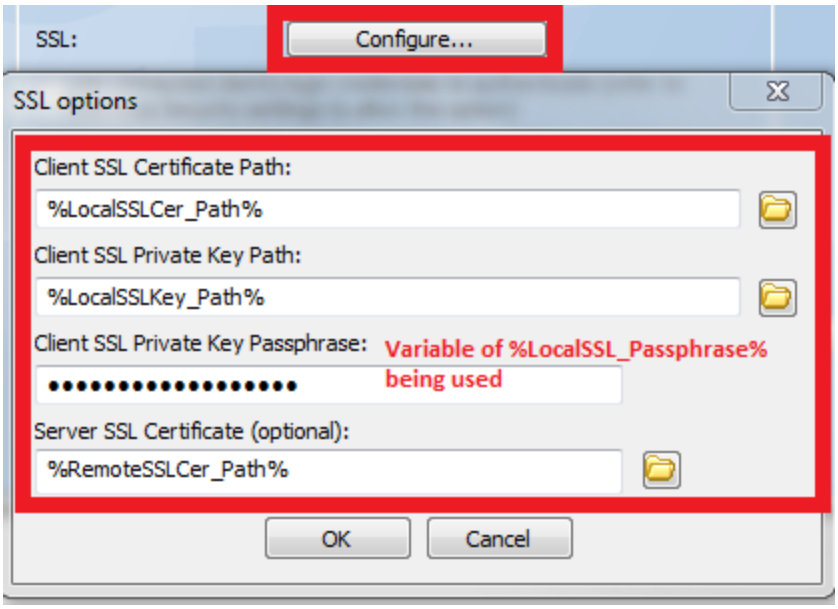
Using Context Variables for Parameterized Event Rules

Some EFT administrators have a need for "parameterized" event rules to do SFTP and FTPS transfers. When defining a Connection Profile or a connection directly within a Protocol: Upload Action or Protocol: Download Action, the administrator can use arbitrary Context (%...%) variables in the following dialog box fields:

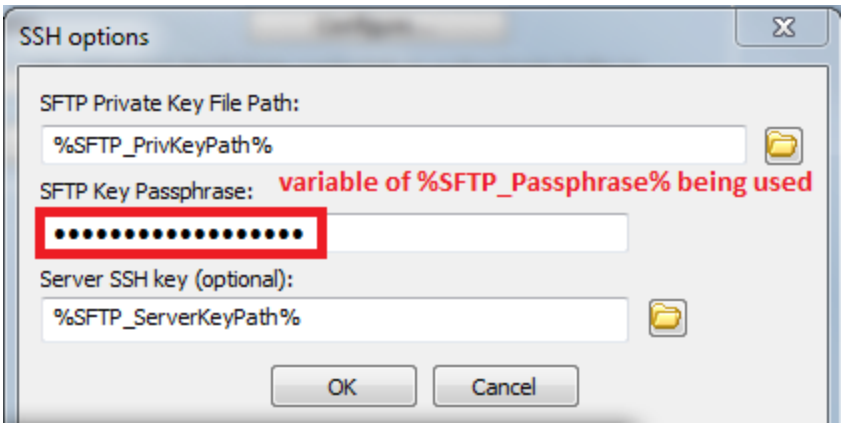
- SFTP Private Key Path
- SFTP Key Passphrase
- Server SSH Key
- Client SSL Certificate Path
- Client SSL Private Key Path
- Client SSL Private Key Passphrase
- Server SSL Certificate
- Connection Profile (SFTP and FTPS/HTTPS):



- Client SSL Certificate/Key/Passphrase Path and Server SSL Certificate Path:



- SFTP Private Key File Path/Passphrase/Key and Server SSH Key Path:



Events (Triggers)

The topics below provide examples of some common uses of Event Rules.

EFT includes more than 25 different event triggers, based on the following event types:

- Operating System-related events, such as a folder's contents changed or a recurring Timer has executed
- Cloud object monitor is similar to Folder Monitor, but is used to monitor folders in your cloud storage

  > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

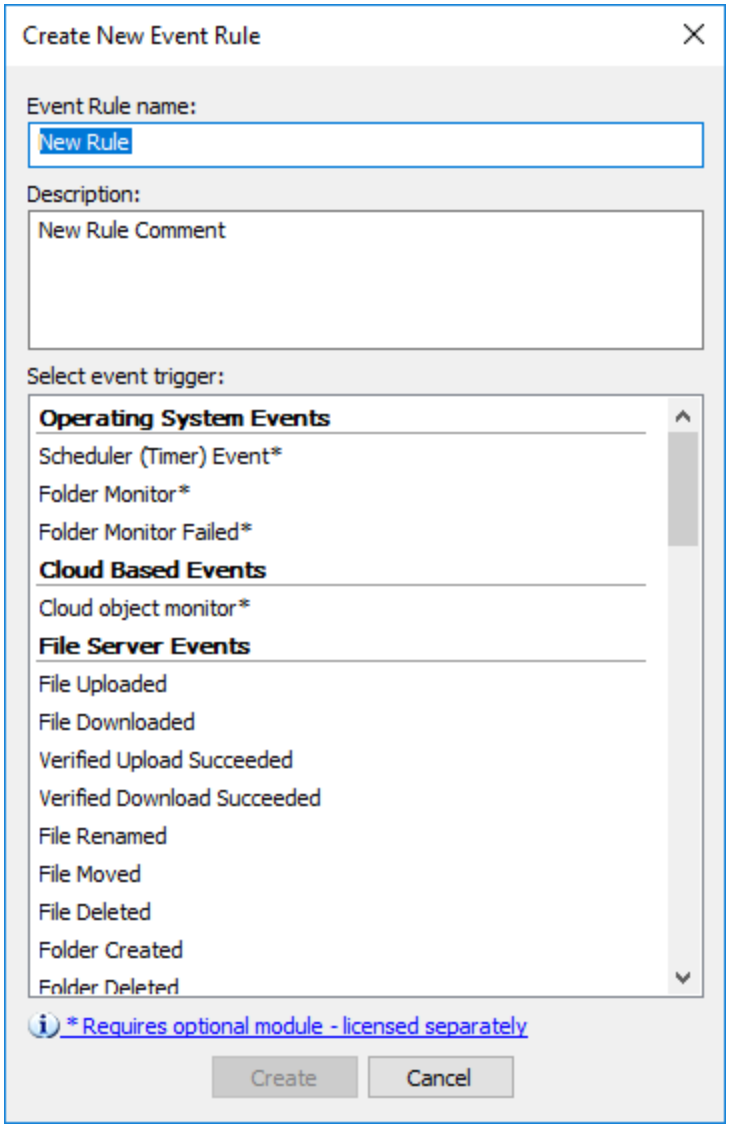
- File server-related events, such as file uploaded or file deleted
- Workspaces-related events, such as User Invited
- Secure File Send events, such as Message Not Sent
- Server-related events, such as Server stopped or started
- Site-related events, such as Site stopped or started
- User-related events, such as User Account Locked
- Connection-related events, such as a user connections failed
- AS2-related events, such as the transfer was successfully completed
- Event Rule Subroutine - The **Event Rule Subroutine** event is used to call another rule from the current rule to create more modular "functional" style of rules. With the **Event Rule Subroutine** event, you can build an event rule that calls a Call Event Rule Subroutine Action asynchronously, thus letting the target rule handle the burden of processing, while returning a reply immediately to the client.
- REST Invocation- The REST Invocation event is used to call up a specific REST endpoint, such as a remote webhook, or for non-administrative users to execute an event rule for inbound traffic.

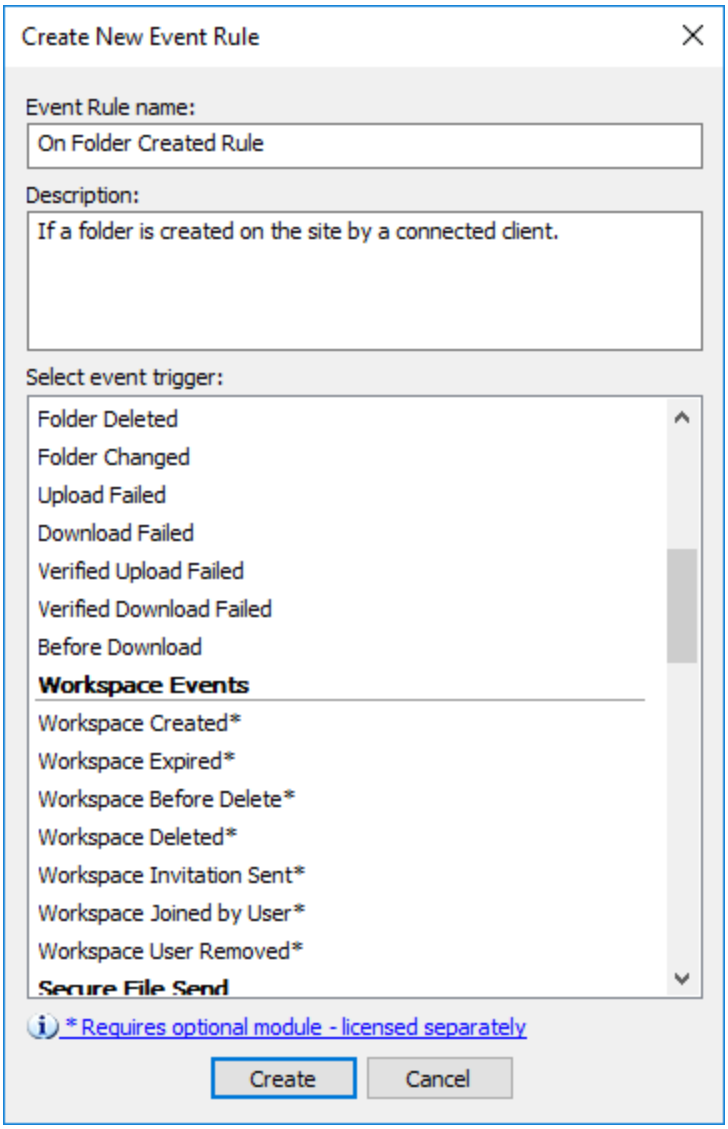
Not all variables are available with every Event trigger. For example, it does not make sense to use the %EVENT.REASON% variable with a File Downloaded Event, but it does make sense with the Upload Failed Event, because EFT can determine the reason for the failure.

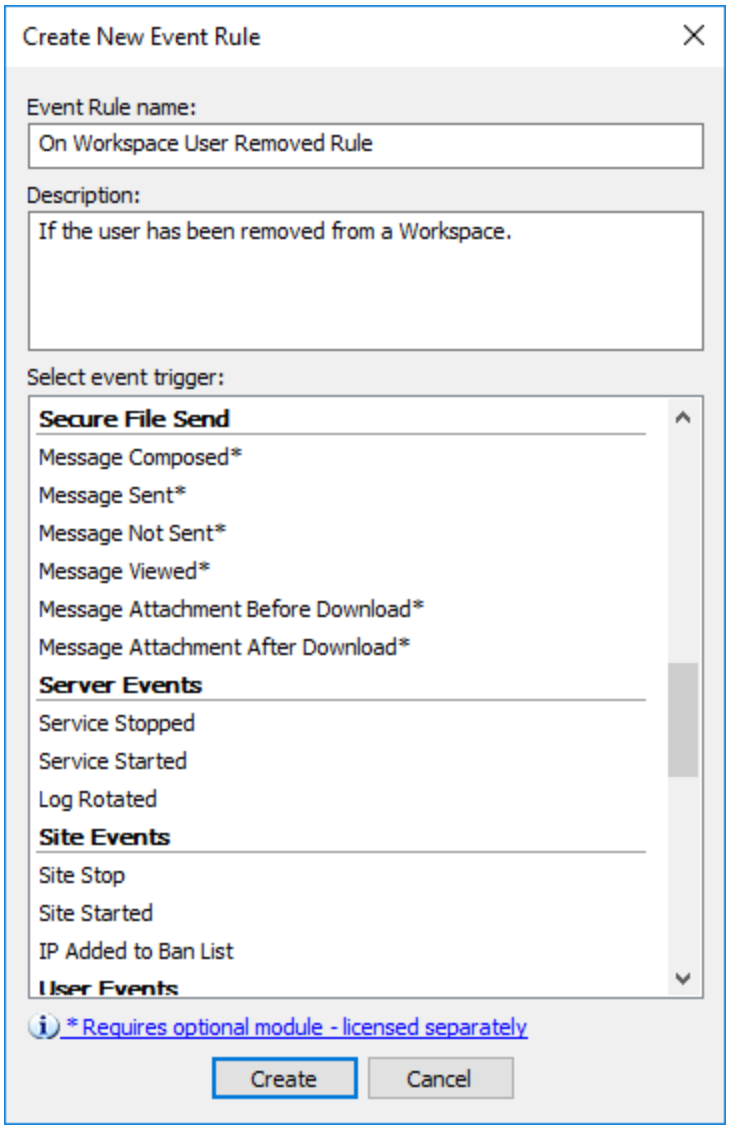
Refer to Variables for a description of each variable and caveats (for example, %EVENT.TIME% is not suitable for file naming and %FS.REPORT_FILE% should not be used in email notifications).

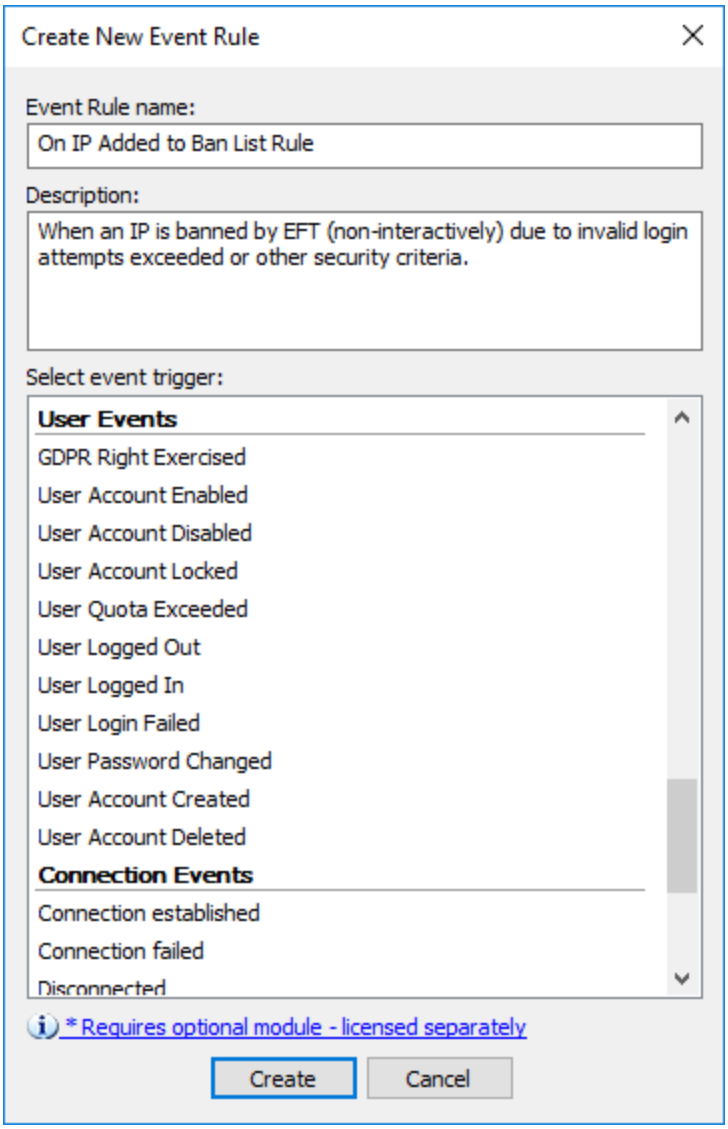
Refer to Which Actions can be Added to which Events for details of added Actions to Events.

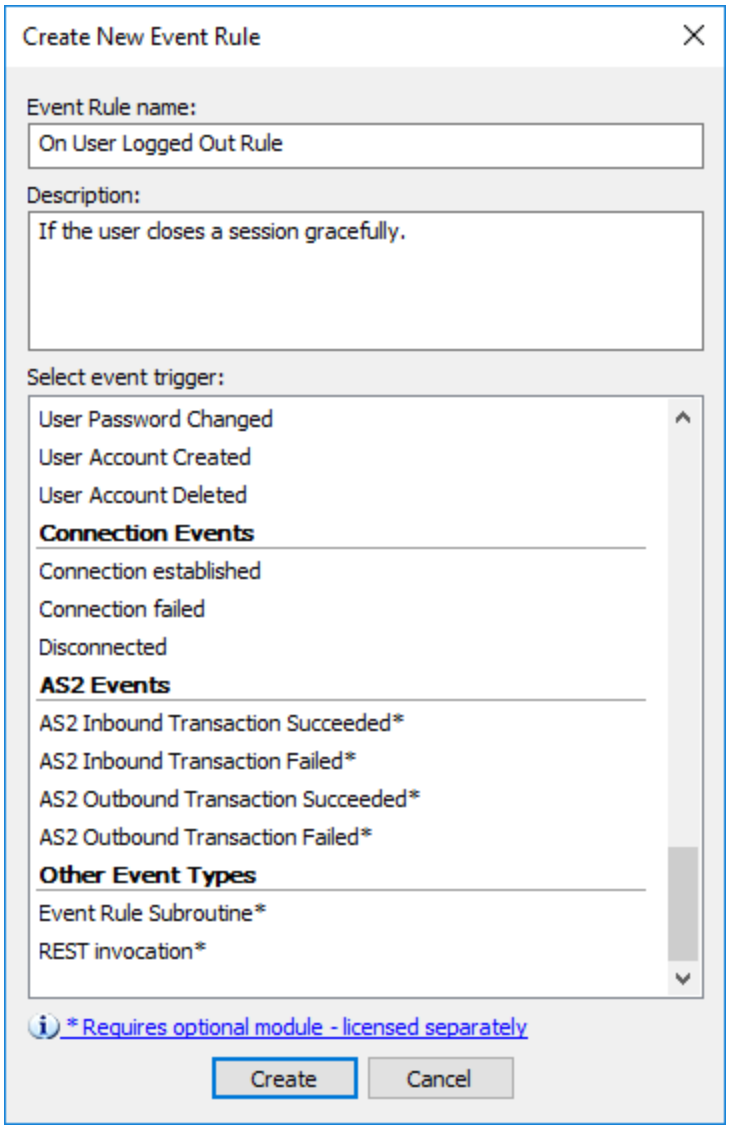
> **NOTE:** Event triggers marked with an asterisk in the **Create New Event Rule** dialog box require a module license. (See below.)




Create New Event Rule
Event Rule name:
On Folder Created Rule
Description:
If a folder is created on the site by a connected client.
Select event trigger:
Folder Deleted
Folder Changed
Upload Failed
Download Failed
Verified Upload Failed
Verified Download Failed
Before Download
Workspace Events
Workspace Created*
Workspace Expired*
Workspace Before Delete*
Workspace Deleted*
Workspace Invitation Sent*
Workspace Joined by User*
Workspace User Removed*
Secure File Send
* Requires optional module - licensed separately
Create
Cancel


Create New Event Rule
Event Rule name:
On Workspace User Removed Rule
Description:
If the user has been removed from a Workspace.
Select event trigger:
Secure File Send
Message Composed*
Message Sent*
Message Not Sent*
Message Viewed*
Message Attachment Before Download*
Message Attachment After Download*
Server Events
Service Stopped
Service Started
Log Rotated
Site Events
Site Stop
Site Started
IP Added to Ban List
User Events
* Requires optional module - licensed separately
Create
Cancel


Create New Event Rule
Event Rule name:
On IP Added to Ban List Rule
Description:
When an IP is banned by EFT (non-interactively) due to invalid login attempts exceeded or other security criteria.
Select event trigger:
User Events
GDPR Right Exercised
User Account Enabled
User Account Disabled
User Account Locked
User Quota Exceeded
User Logged Out
User Logged In
User Login Failed
User Password Changed
User Account Created
User Account Deleted
Connection Events
Connection established
Connection failed
Disconnected
* Requires optional module - licensed separately
Create
Cancel



AS2 Events

(Requires AS2) 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.
- **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.

- **AS2 Outbound Transaction Succeeded**—Triggers if EFT has offloaded a file to a remote partner, and that partner replied with a receipt over HTTP/S, indicating that the transfer was successfully completed.
- **AS2 Outbound Transaction Failed**—Triggers if the expected MDN receipt was not received in the expected time or the receipt signature or MIC failed.

Type	Label (can appear in email 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 Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%

Type	Label (can appear in email notification)	Variable
User Properties	User (Group)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%
Connection Properties	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%

Type	Label (can appear in email notification)	Variable
Site Properties	Site name	%SITE.NAME%
	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%
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%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

Cloud Object Monitor Event

The Cloud Object Monitor Event is used when you want to download files from Amazon S3, Azure blob storage, or Google Drive.

> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

- Files arriving at EFT can be automatically copied/moved to cloud storage.
- Timer rules can download files from cloud storage at set intervals
- Download always uses TLSv1.2 protocol

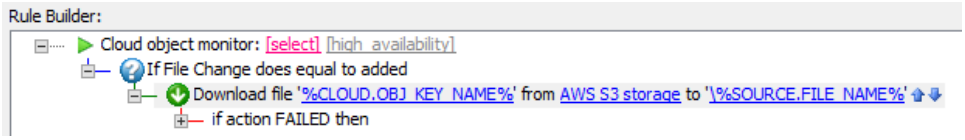
With the Cloud object monitor Event, EFT administrators can:

- Connect natively to cloud storage without scripting, manual browsing, or complexity in setting up connections
- Integrate natively with cloud storage through EFT without the need for outside integration

The Cloud Object Monitor Event does not support cloud-to-cloud (S3 to S3, Azure to S3, or S3 to Azure) direct file transfers. Currently, it can only download from the cloud to EFT, and then upload from EFT to the cloud. Timer Event Rules are also capable of downloading files from the cloud.

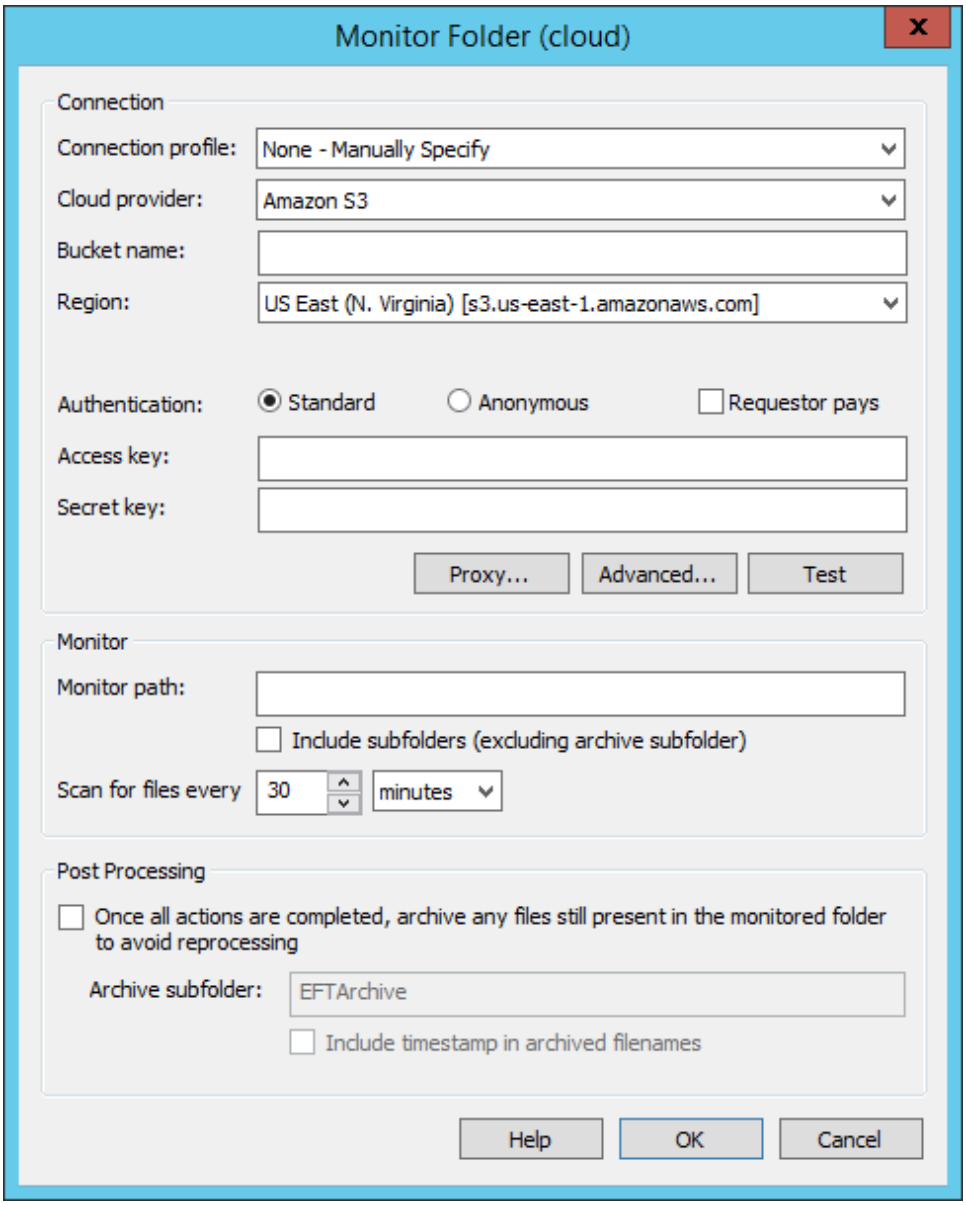
To configure a Cloud object monitor Event

1. Follow the procedure in Defining Event Rules, and to add the **Cloud object monitor** event to the Rule Builder.



   When you add the **Cloud object monitor** event to the Rule builder, an **If Change** Condition and **Download** Action are added automatically.

2. Next to **Cloud object monitor**, click **select**. The **Monitor Folder (cloud)** dialog box appears.



3. Specify the connection and authentication options described in Cloud Storage Actions.
4. If you are creating this rule on a high availability node, click **high availability** to specify the load balancing options.
5. Specify the options for the If File Change condition and the Download Action, then click **Apply** to save the event rule.

Connection Events

- **User Connected**—When a user connects to the Site (this occurs before log in).
- **User Connect Failed**—When a user attempts to connect and fails (this can occur before log in).
- **User Disconnected**—When a user disconnects from the Site (this can occur before log in).

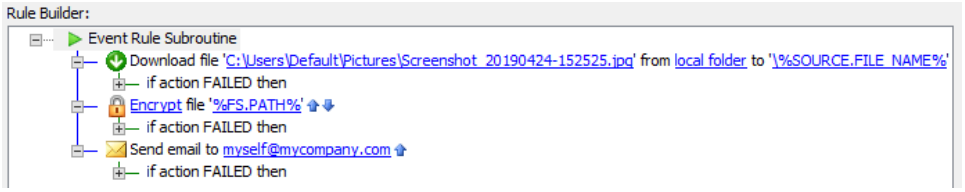
Event Rule Subroutine Event

(Requires EAM) The **Event Rule Subroutine** event is used to call another rule from the current rule to create more modular "functional" style of rules. With the **Event Rule Subroutine** event, you can build an event rule that calls a Call Event Rule Subroutine Action asynchronously, thus letting the target rule handle the burden of processing, while returning a reply immediately to the client.

Subroutines do not have conditions; when you call them, if you have multiple steps, they will all run.

To create an Event Rule Subroutine Event

1. Create an Event Rule using the **Event Rule Subroutine** event.
2. Add desired actions to the subroutine. For example, you could add a **Download file from host** action, **OpenPGP** action to encrypt the downloaded file, and a **Send Email notification** action to notify you when the action is complete.



3. Click **Apply**. You have created the subroutine.
4. Now you can call this subroutine in a Call Event Rule Subroutine action.

Related Topic

File System Events

- File Uploaded—File is uploaded to the Site.
- File Downloaded—File is downloaded from the Site.
- Verified Upload Succeeded—Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.
- Verified Download Succeeded—Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.
- File Renamed—File on the Site is renamed by a connected client.
- File Moved—File is moved from one folder in the VFS to another by a connected client.
- File Deleted—File is deleted from the Site by connected client
- Folder Created—Folder is created on the Site by a connected client.
- Folder Deleted—Folder is deleted from the Site by a connected client.
- Folder Changed —User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")
- Upload Failed—Upload fails to transfer successfully.
- Download Failed—Download fails to transfer successfully.
- Verified Upload Failed—Integrity check of uploaded file fails when transferred using the Web Transfer Client.
- Verified Download Failed—Integrity check of downloaded file fails when transferred using the Web Transfer Client.
- Before Download—If a download is requested, perform the Action(s) defined in this Event, then continue with the download.

Available Variables

The events above can take the following variables:

Type	Label (can appear in email 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 Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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%

Type	Label (can appear in email notification)	Variable
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Type	Label (can appear in email notification)	Variable
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%
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	Triggers when file is downloaded from the Site.	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

File Downloaded	Triggers when file is downloaded from the Site.	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

File Downloaded	Triggers when file is downloaded from the Site.	
Type	**Label (can appear in email notification)**	**Variable**
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%
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.	
Verified Download Succeeded	**Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

Verified Upload Succeeded	Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.	
Verified Download Succeeded	**Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Verified Upload Succeeded	Integrity check of uploaded file succeeds when transferred using the Web Transfer Client.	
Verified Download Succeeded	**Integrity check of downloaded file succeeds when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
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.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

File Renamed	**File on the Site is renamed by a connected client.**
File Moved	**File is moved from one folder in the VFS to another by a connected client.**
File Deleted	**File is deleted from the Site by connected client**
Folder Created	**Folder is created on the Site by a connected client.**
Folder Deleted	**Folder is deleted from the Site by a connected client.**
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**

Type	Label (can appear in email notification)	Variable
User Properties	Groups	%USER.GROUPS%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
	Logon Name	%USER.LOGIN%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
	Logon Password	%USER.PASSWORD%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

File Renamed	**File on the Site is renamed by a connected client.**	
File Moved	**File is moved from one folder in the VFS to another by a connected client.**	
File Deleted	**File is deleted from the Site by connected client**	
Folder Created	**Folder is created on the Site by a connected client.**	
Folder Deleted	**Folder is deleted from the Site by a connected client.**	
Folder Changed	**User navigates to a new folder on the Site. (Applies to FTP/S only, as HTTP/S and SFTP have no concept of "current directory.")**	
Type	**Label (can appear in email notification)**	**Variable**
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
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.	
Type	**Label (can appear in email 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 Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	Event Reason	%EVENT.REASON%

Upload Failed	Upload fails to transfer successfully.	
Type	**Label (can appear in email 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%
	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

Upload Failed	Upload fails to transfer successfully.	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Upload Failed	Upload fails to transfer successfully.	
Type	**Label (can appear in email notification)**	**Variable**
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

Download Failed	Triggers if download fails to transfer successfully.	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	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%

Download Failed	Triggers if download fails to transfer successfully.	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Download Failed	Triggers if download fails to transfer successfully.	
Type	**Label (can appear in email notification)**	**Variable**
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	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%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
Transfer Properties	Transfer Rate	%TRANSFER.RATE_KBPS%
	Transfer Bytes	%TRANSFER.BYTES%
	Transfer Seconds	%TRANSFER.SECONDS%

Verified Upload Failed	Integrity check of uploaded file fails when transferred using the Web Transfer Client.	
Verified Download Failed	**Integrity check of downloaded file fails when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	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%

Verified Upload Failed	**Integrity check of uploaded file fails when transferred using the Web Transfer Client.**	
Verified Download Failed	**Integrity check of downloaded file fails when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

Verified Upload Failed	**Integrity check of uploaded file fails when transferred using the Web Transfer Client.**	
Verified Download Failed	**Integrity check of downloaded file fails when transferred using the Web Transfer Client.**	
Type	**Label (can appear in email notification)**	**Variable**
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%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site	Site name	%SITE.NAME%
	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%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%

Before Download	If a download is requested, perform the Action(s) defined in this Event, then continue with the download.	
Type	**Label (can appear in email notification)**	**Variable**
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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%

Before Download	If a download is requested, perform the Action(s) defined in this Event, then continue with the download.	
Type	**Label (can appear in email notification)**	**Variable**
User Properties	User (Groups)	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Account Enabled	%USER.ENABLED%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%
	Custom Field 1, 2, 3	%USER.CUSTOM1%, %USER.CUSTOM2%, %USER.CUSTOM3%

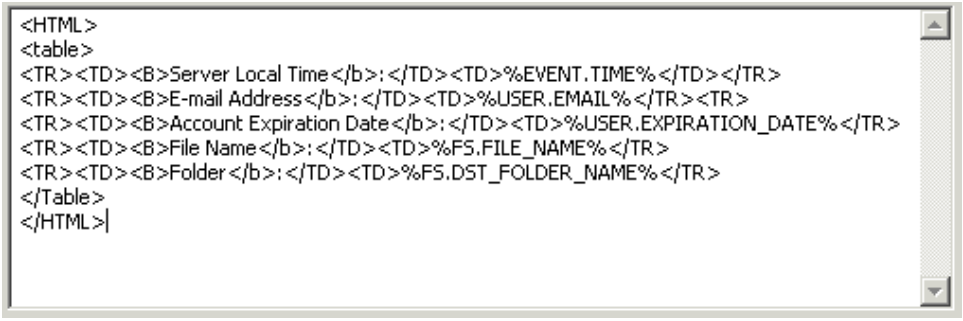
Before Download	If a download is requested, perform the Action(s) defined in this Event, then continue with the download.	
Type	**Label (can appear in email notification)**	**Variable**
Connection Properties	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Local Port	%CONNECTION.LOCAL_PORT%
	Protocol	%CONNECTION.PROTOCOL%
	Using Web Transfer Client	%CONNECTION.USING_WEB_TRANSFER_CLIENT%
	HTTP Query String	%CONNECTION.HTTP.QUERY_STRING%
	HTTP Headers List	%CONNECTION.HTTP.HEADERS_LIST%
Site Properties	Site name	%SITE.NAME%
	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%
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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%

File Uploaded Event

Suppose you want to be sent an email each time any user uploads a file to EFT, 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 email Notification Action.
3. In the Message of the email, 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 email is sent whenever ***any*** user uploads a file to EFT. 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 Logon 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 Groups" and select the Group.

Defining the Email with User Details

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

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

> This message was sent to you automatically by EFT on the following Event: File Uploaded.
>
> **Server Local Time**: 12/5/2007 14:00:00
> **email Address**: jbite@mycompany.com
> **Account Expiration Date**: 12/1/2008 11:59:59
> **File Name**: file.txt
> **Folder**: C:\InetPub\EFTRoot\Standard\Usr\jbite

Folder Monitor Event

(Requires FMM) If you are attempting to monitor a user's home folder or one if its sub-folders, the following warning message appears:

"It appears you are attempting to monitor a user's home folder or one if its sub-folders. For detecting protocol-based file uploads, we strongly encourage the use of the File Upload trigger, rather than a Folder Monitor trigger. The Folder Monitor trigger relies on Window's notification events, which will occur as chunks of the file are uploaded. The resulting downstream effect is a race condition where actions associated with this event rule may fire BEFORE the file has been completely uploaded. We recommend only using Folder Monitors for monitoring LAN file copy events."

The EFT **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 via the FTP/S, SFTP, and HTTP/S protocols, use File Uploaded, File Downloaded, and other File Server 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 Module, 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 (for example, due to network errors), so files added to the monitored folder are missed and not processed (for example, 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:
	  ◦ If folder sweep is on, show frequency, time units, and archive subfolder name.
	  ◦ If RDCW* is on, show whether health check is on and its frequency.
	• When a monitored folder is polled for its contents with special indication for the first poll.
	• Log which mechanism, RDCW notification or folder polling, triggers the processing of a file.
	• Log when file has been archived.
	• Log when file is still in folder after Event Rule Actions have completed and user chose not to archive.
	• Record trigger collisions by logging if Event is being ignored because file is already in process.
	• For folder sweep, log when folder contents have been received and are about to be processed.
	
	*RDCW = ReadDirectoryChangeWrite function; Retrieves information that describes changes within a specified directory.

Error	• Log reason for archive folder creation failure. • Log reason for file archive Action failure.

Risks associated with Folder Sweep include:

- EFT creates a handle for EVERY file polled (when **Scan for files every *n*** is selected). You can use an "If File Name" or "If Base File Name" Condition to include or exclude file name or extension or wildcard characters (for example, "*.txt" or "File??.dat"). Using the Condition prevents EFT from opening a file handle for each of the excluded files, which provides a slight performance improvement.
- 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 be reprocessed in the next Folder Sweep cycle.
- If the Health Check fails, it is possible to see duplicate Folder Monitor errors in the log.
- 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.
- Folder Monitor does not trigger when Unicode filenames are added to the monitored folder; however, Folder Sweep archives them. Refer to Unicode Support in EFT for more information.
- EFT must have permission to access the folder (see note below). If the folder specified is not accessible by EFT, an error message appears.
  (For information about system error codes, refer to https://docs.microsoft.com/en-us/windows/win32/debug/system-error-codes--0-499-)
- If you are sending files to an ICAP server in batches for scanning using the Content Integrity Control Action, you might not get consistent results. It is not recommended to use the Folder Monitor event for scanning files with the Content Integrity Control Action. Instead, use the File Uploaded event.

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 Stop processing 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 keeps track of the number of active threads over time and periodically calculates the average number of concurrent active threads during that time. 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 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 starts with 3 threads in the pool per Site, and can grow to a maximum of 32 threads.

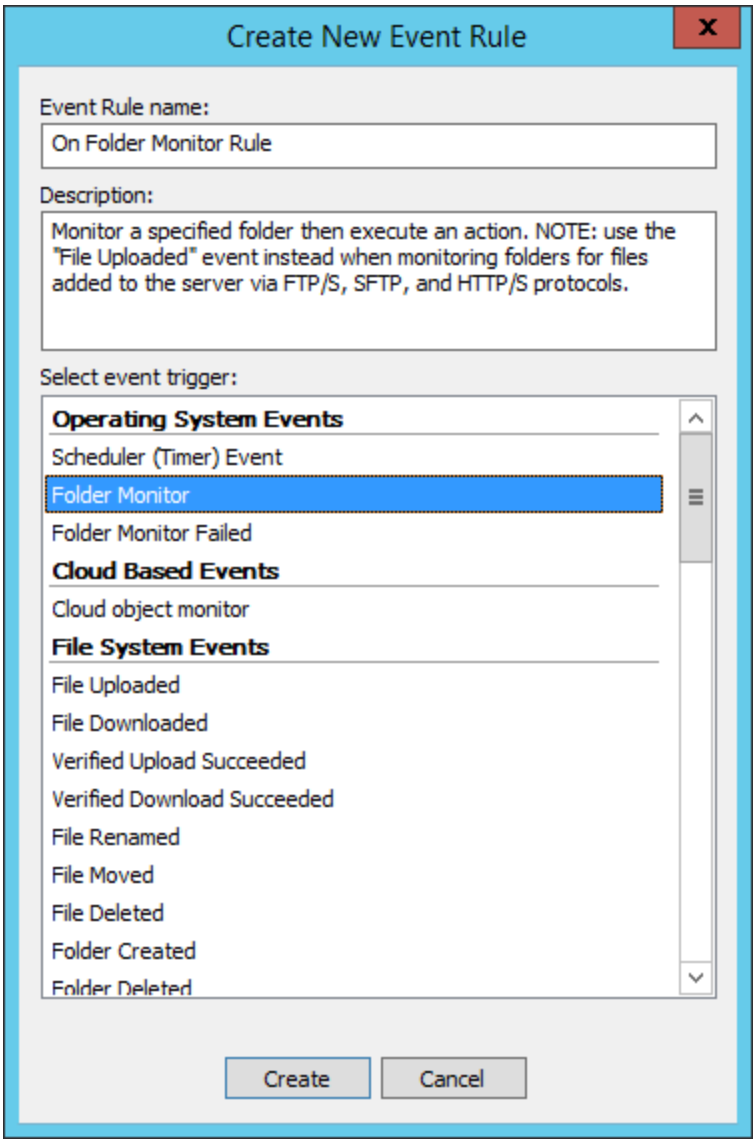
EFT will only reset affected (modified) folders when applying configuration changes to an Event Rule, rather than resetting all folders.

When monitoring a folder, EFT watches for any file being added to, removed from, or renamed in the monitored folder. Moving a file, performing OpenPGP 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**.

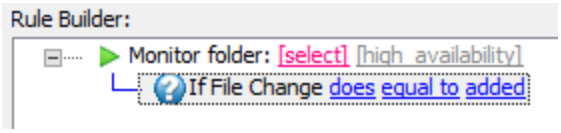
The **Require Active Directory domain trust relationship** check box is cleared by default for new installs and selected by default during upgrades if the advanced property **FolderMonitorUseNonInteractiveLogon** is present during the upgrade. The **Scan for files every** check box is not selected and 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

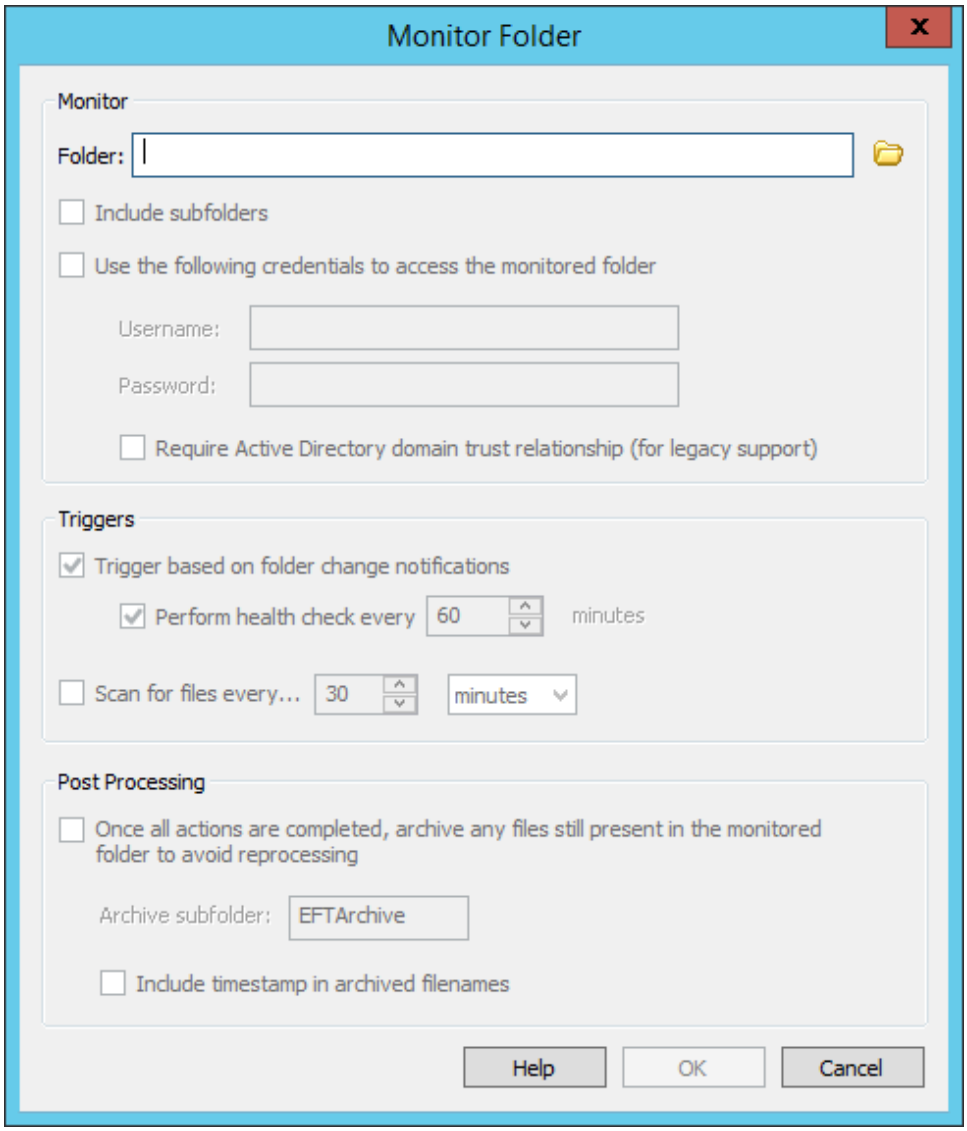
1. Open the Create New Event Rule dialog box.
2. In the **Create New Event Rule** dialog box, click **Folder Monitor**, and then click **Create**.



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



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



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

To monitor a folder on a remote, non-EFT file 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 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 service to run as a domain account, or specify a dedicated “run as” account in the **Monitor Folder** dialog box.

Wildcards are not supported; however, you can use an "If File Name" or "If Base File Name" Condition to include or exclude file name or extension or wildcard characters (for example, "*.txt" or "File??.dat"). Doing so prevents EFT from opening a file handle for each of the excluded files, which provides a slight performance improvement.

4. 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.
5. If login credentials (other than the EFT server service account) are required to access the folder and subfolders, select the **Use the following credentials to access the monitored folder** check box, 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 computers on a network without having to re-enter logon information for each computer.” In this case, EFT 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.

   The **Require Active Directory domain trust relationship** check box specifies how the Folder Monitor 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.)

6. 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.
7. 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.

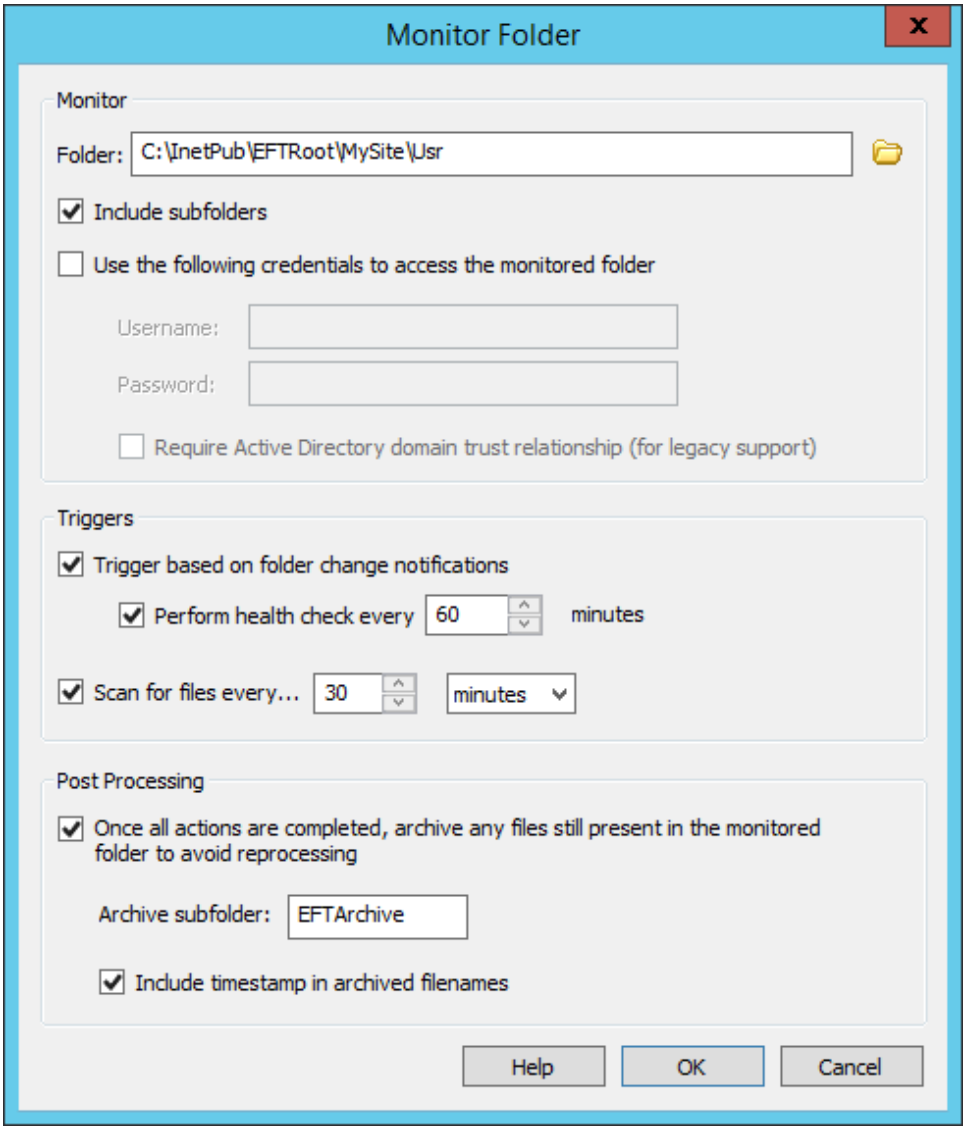
   When the check box is selected, EFT periodically writes a special file to the folder specified and then waits for the "file added" notification to verify that it can receive notifications of changes within the folder. When there is a loss of connectivity, EFT attempts to re-establish a link to the folder and triggers the Folder Monitor Failed Event internally.

- If you want to receive email 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 email** Action to it.

  The time EFT waits for the notification from Windows when a Folder Monitor health check file is created can be controlled by an advanced property described in https://kb.globalscape.com/KnowledgebaseArticle10682.aspx.

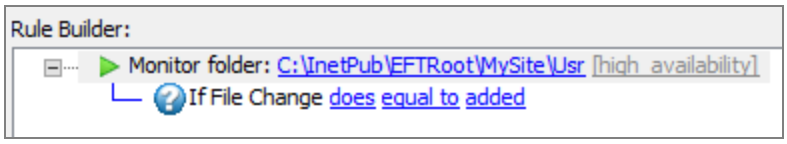
8. To enable Folder Sweep, select the **Scan for files every** check box and specify the frequency. The default is 30 minutes. A value between 1 and 9999 can be specified with units of seconds, minutes, or hours. The timer for the next sweep cycle is not started until all the files for the current sweep 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 email notification, those Actions will be triggered. (This check box is not selected by default.) Selecting the **Scan for files every** check box causes the Event Rule's **If File Change** Condition to be set to **does equal to added**.
9. 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.



10. 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.

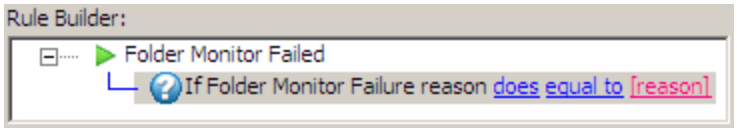
11. The **If File Change** Condition is added automatically to restrict the triggering of the Rule. Click the links in the **If File Change** Condition to specify whether the Rule should trigger when a file in the folder is or is not renamed, added, or removed. If Folder Sweep (the **Scan for files every** check box) 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.
12. Specify any Action/Conditions to occur when this Event is triggered, such as:
    - Add an email notification. (Refer to email 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.)



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

Folder Monitor Failure

To audit failures of Folder Monitor Rules, use the **Folder Monitor Failed** Event, 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.

GDPR Right Exercised

The **GDPR Right Exercised** event is triggered based on the **If Event Reason** Condition specified. You can specify that the Event Reason "does" or "does not" equal one of the following behaviors:

- The user has rescinded consent
- The user has accessed (viewed) their personal data
- The user has had rectified (modified) their personal data
- The user has asked to be forgotten
- The user has asked to restrict the use of their personal data
- The user has asked to restrict the use of their personal data
- The user's personal data has been modified by someone other than the user
- The user has ported (exported) their personal data
- The user has objected to the use of their personal data

For example, you could define an Event Rule to send an email notification when a user's personal data is modified by someone other than the user, such as an administrator.

IP Added to Ban List Event

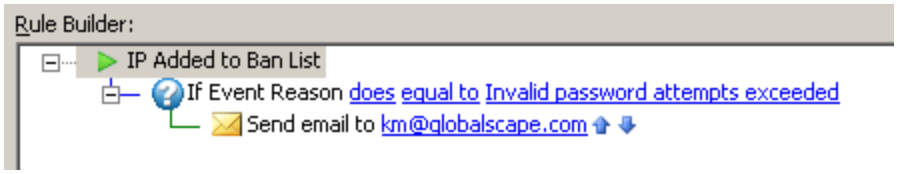
This Event is triggered when an IP address is added to the ban list by the system (not manually by an administrator). Administrators can configure Event Rules to capture this Event and send notifications or write to logs.

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 (for example, If Event Reason, If Remote IP, If Server Running, etc.) and one or more Actions (for example, Send notification email).

- The possible Event Reasons include DoS/Flood prevention trigger (permanent or temporary), Invalid password attempts exceeded, and Invalid username attempts exceeded.

4. Click **Apply** to save the Rule. The Rule appears similar to the Rule below.



IP Access-related Event Rules are limited to 50,000 rules. This can be increased with the advanced properties IPRulesLimit and AutobanLimit, however, you could experience performance issues at higher limits.

If the limit is reached, rather than not adding the IP, EFT performs a FIFO operation, adding the newly banned IPs, and removing the oldest banned IP (ONLY for auto-banned IPs; manually added IPs cannot be automatically removed.)

If an IP had to be removed, a WARNING is sent to the eft.log, indicating that a new IP has been added, and oldest IP has been dropped as the list is full. The DMZ Gateway has a correspondingly large list to handle any IPs passed to it by EFT.

Refer to the Knowledgebase article https://kb.globalscape.com/Knowledgebase/10877/Adjust-IP-Access-Rule-Count-Limit-and-IP-Auto-Ban-List-limit for more information.

Operating System Events

The operating system events below are available in EFT:

- Scheduler (Timer)—Execute a specified Action one time or repeat at a specified interval. (Requires TEM)
- Folder Monitor—Monitor a specified folder, then execute an Action whenever a change is detected. (Requires FMM)
- Folder Monitor Failed—Monitor a specified folder, then execute a specified Action whenever a failure is detected. (Requires FMM)

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

Available Variables

Scheduler (Timer)

Execute a specified Action one time or repeat at a specified interval. (Requires TEM)

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
	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%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%

Type	Label (can appear in email notification)	Variable
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_ MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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, then execute an Action whenever a change is detected. (Requires FMM) Use the **File Uploaded** file system Event to notify you when a file is uploaded to the Site.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%

Type	Label (can appear in email notification)	Variable
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	File Change	%FS.MONITOR_OPERATION%
	Physical Path	%FS.PATH%
	Physical Folder Name	%FS.FOLDER_NAME%
	Base File Name	%FS.BASE_FILE_NAME%
	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%
	Virtual Path	%FS.VIRTUAL_PATH%
	Virtual Folder Name	%FS.VIRTUAL_FOLDER_NAME%
	Virtual Destination Path	%FS.DST_VIRTUAL_PATH%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
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, then execute a specified Action whenever a failure is detected. (Requires FMM)

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Folder Monitor Health	%EVENT.MONITORHEALTH%
	Folder Monitor Failure Reason	%EVENT.MONITORFAILUREREASON%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	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%
Workspaces Properties	Workspace Physical Path	%WORKSPACE.PATH%
	Workspace Virtual Path	%WORKSPACE.VIRTUAL_PATH%
	Workspace Name	%WORKSPACE.NAME%
	Workspace Participant List	%WORKSPACE.PARTICIPANTS%
	Workspace Owner	%WORKSPACE.OWNER%
	Workspace Owner Email Address	%WORKSPACE.OWNER_EMAIL%
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%

REST Invocation Event

(Require EAM and HTTPS) The REST Invocation event is used to call up a specific endpoint, such as a remote webhook, or for non-administrative users to execute an event rule for inbound traffic.

> **NOTE:** You do NOT need the REST API enabled to use this event trigger

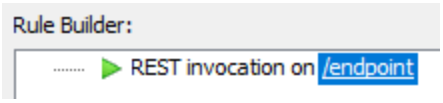
If you are using a PowerShell script for the authentication or verification, The PowerShell authentication script has to set the HTTP.AuthSuccess variable to "true." The PowerShell script for signature checking has to set the HTTP.SignatureValid variable to true.

This new feature has nothing to do with the internal REST API functionality, but instead allows EFT administrators to expose or create "endpoints" that when accessed will trigger defined actions within the event rule. Additionally, the requests will go through either the HTTP or HTTPs protocol and NOT via our REST API protocol.

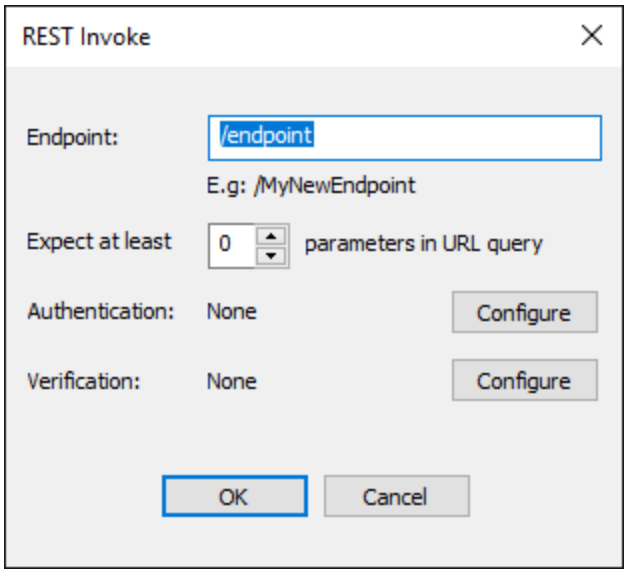
See also the sample PowerShell action for REST invocation, EFT response, and The list of variables EFT populates below.

To use the REST Invocation Event

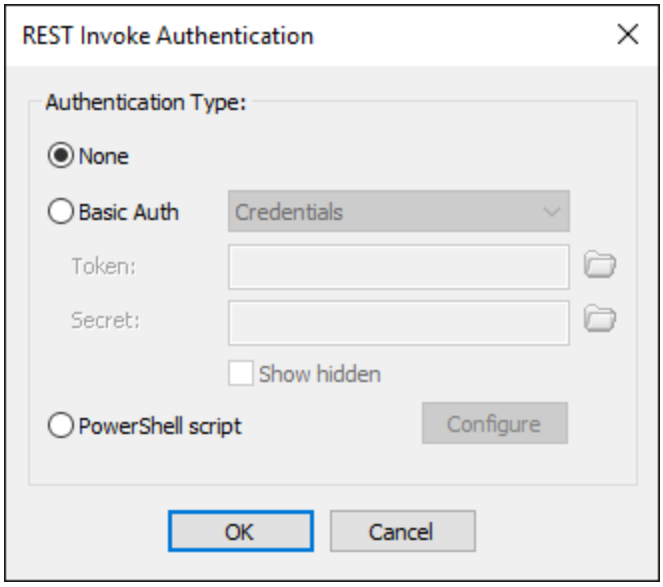
1. Ensure HTTPS or HTTP is enabled. If neither port is enabled, the event rule cannot be created and a warning or err
2. Define an Event Rule using the **REST Invocation** Event trigger. The Event trigger appears in the Rule Builder.



3. Click the linked text, /endpoint, to open the **REST Invoke** dialog box.

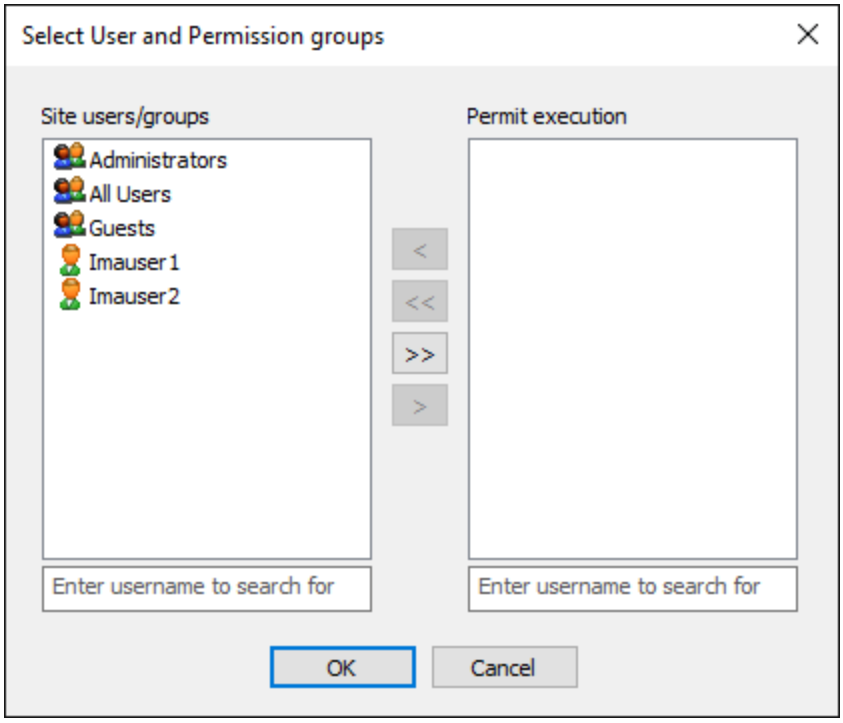


4. In the **Endpoint** box, provide the name of the endpoint.
5. In the **Expect at least** box, provide the number of parameters required in the URL query. When this is defined, the Invoke would only trigger if the set amount of URL parameters are passed, For example https://192.168.100.165/endpoint?Value&Value2&Value3 is passing three parameters in the URL. If **Expect at least** is set to 2, then this would trigger the event rule because it at least 2 parameters are passed (but you can pass as many as you need).
6. For **Authentication** options, click **Configure**. The **REST Invoke Authentication** dialog box appears.



7. Under **Authentication Type**, click an option:

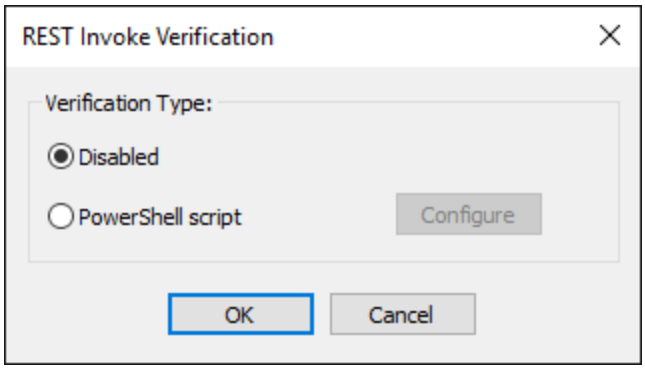
- **None** - No authentication is required. When configured for None, any call to the EFT server that contains the endpoint will trigger the event rule.
- **Basic Auth** - Use Basic authentication:
  - **Credentials**, provide the **Token** and **Secret**. (Copy and paste the token and secret generated by the provider, such as Twilio. They are case sensitive.) When using token/secret you must pass the defined token/secret within the URL request to the EFT server.
  - **Clients and Permission Groups**, click the folder icon, then move the **Site user/groups** that you want to **Permit Execution**. User/Group supports EFT users or groups defined in EFT.



- **PowerShell script** - Click **Configure** and then point to a PowerShell script. The PowerShell script has to set the HTTP.AuthSuccess variable to "true":

  $EFT_CONTEXT.SetVariable("HTTP.AuthSuccess", "true")

8. For signature **Verification** options, click **Configure**. The **REST Invoke Verification** dialog box appears.



9. The default is **Disabled**. To specify a different verification type. click **PowerShell script**, click **Configure** to select your script. then click **OK**. (The PowerShell script for signature checking has to set the HTTP.SignatureValid variable to "true." See the sample below.
10. Add Conditions (optional) and Actions (for example, Send email or write to a file), then click **Apply**.

EFT Response

The response includes an HTTP response code, and optionally, JSON payload with modified context variables.

By default, EFT responds with "200 OK." To modify the response code, set the `HTTP.Response.Code` variable. The body goes to `HTTP.Response.Body`.

EFT populates the following context variables

URL query:

- HTTP.Request.Url.Query -- Raw query
- HTTP.Request.Url.Query.Count -- number of items in the query
- HTTP.Request.Url.Query[1] -- the first item (e.g file=untitled.txt)
- HTTP.Request.Url.Query[1].Key -- the first item name (eg "file")
- HTTP.Request.Url.Query[1].Value -- the value of the first item (e.g. "untitled.txt")
- HTTP.Request.Url.Query[file] -- the value of the item named "file"

For the query items in the body (for POST requests with the content-type: application/x-www-form-urlencoded)

- HTTP.Request.Body.Query
- HTTP.Request.Body.Query.Count

- HTTP.Request.Body.Query[1]
- HTTP.Request.Body.Query[1].Key
- HTTP.Request.Body.Query[1].Value
- HTTP.Request.Body.Query[file]
- HTTP.Request.Raw -- the whole request
- HTTP.Request.Verb -- HTTP verb (GET, PUT, POST etc)
- HTTP.Request.Url -- full path including query string
- HTTP.Request.Url.Endpoint only endpoint path (e.g up to the '?' character if present)
- HTTP.Request.Headers.Count -- total number of headers
- HTTP.Request.Headers.Raw -- all headers separated by newline character
- HTTP.Request.Headers[content-type] -- a header value by name
- HTTP.Request.Headers[1] -- the first header name and value
- HTTP.Request.Headers[1].Key -- the first header name
- HTTP.Request.Headers[1].Value -- the first header value
- HTTP.Request.Body.Raw -- raw body of the request
- HTTP.Request.Body.Json.user.name -- value of the JSON payload (if present) by name. here you access the user.name field. Array fields are accessible via brackets like in javascript (e.g userrs[3])

Sample PowerShell action

Below is a sample PowerShell action that retrieves all context variables and outputs them back as a JSON, which you can use for testing.

```
$urlquery = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query")

$urlqueryCount = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query.Count")

$urlfirstQueryItemByNymber = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query[1]")

$urlfirstQueryItemByNumberKey = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query
[1].Key")

$urlfirstQueryItemByNumberValue = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query
[1].Value")

$urlfirstQueryItemByName = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Query[a]")

$bodyquery = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query")
```

```
$bodyqueryCount = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query.Count")

$bodyfirstQueryItemByNymber = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query[1]")

$bodyfirstQueryItemByNumberKey = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query
[1].Key")

$bodyfirstQueryItemByNumberValue = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query
[1].Value")

$bodyfirstQueryItemByName = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Query[c
 x]")

$HttpRequestRaw = $EFT_CONTEXT.GetVariable("HTTP.Request.Raw")

$Verb = $EFT_CONTEXT.GetVariable("HTTP.Request.Verb")

$Url = $EFT_CONTEXT.GetVariable("HTTP.Request.Url")

$Endpoint = $EFT_CONTEXT.GetVariable("HTTP.Request.Url.Endpoint")

$headersCount = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers.Count")

$headersRaw = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers.Raw")

$ContentType = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[content-type]")

$FirstHeader = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[1]")

$FirstHeaderKey = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[1].Key")

$FirstHeaderValue = $EFT_CONTEXT.GetVariable("HTTP.Request.Headers[1].Value")

$BodyRaw = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Raw")

$BodyJsonFirstItem = $EFT_CONTEXT.GetVariable("HTTP.Request.Body.Json.first")

$response = @{

    urlQuery=$urlQuery

    urlFirstQueryItemByNumber=$urlFirstQueryItemByNymber

    urlFirstQueryItemByNumberKey=$urlFirstQueryItemByNumberKey

    urlFirstQueryItemByNumberValue=$urlFirstQueryItemByNumberValue
```

```
    urlFirstQueryItemByName=$urlFirstQueryItemByName

    bodyQuery=$bodyQuery

    bodyFirstQueryItemByNumber=$bodyFirstQueryItemByNymber

    bodyFirstQueryItemByNumberKey=$bodyFirstQueryItemByNumberKey

    bodyFirstQueryItemByNumberValue=$bodyFirstQueryItemByNumberValue

    bodyFirstQueryItemByName=$bodyFirstQueryItemByName

    HttpRequestRaw=$HttpRequestRaw

    Verb=$Verb

    Url=$Url

    Endpoint=$Endpoint

    Headers=$Headers

    ContentType=$ContentType

    FirstHeader=$FirstHeader

    FirstHeaderKey=$FirstHeaderKey

    FirstHeaderValue=$FirstHeaderValue

    BodyRaw=$BodyRaw

    BodyJsonFirstItem=$BodyJsonFirstItem

}

$json = $response | ConvertTo-Json

$EFT_CONTEXT.SetVariable("HTTP.Response.Body",
 $json)
```

Examples

In development testing and QA, we used curl to make HTTP or HTTPs calls to the EFT Server.

Making an HTTP REST request using curl:

HTTPs: When using HTTPs and a self signed certificate, curl will be unable to accept the certificate; therefore, you will need to add --insecure to the request, as shown below.

```
curl.exe --insecure
https://<username>:<password>@<IP>:<PORT>/<endpoint>

curl.exe --insecure https://Ivan:test@192.168.100.165:443/QA
```

HTTP:

```
curl.exe http://<username>:<password>@<IP>/<endpoint>

curl.exe http://Ivan:test@192.168.100.165/QA
```

Passing parameters via the request:

In order to pass multiple parameters, the endpoint needs to include them: Multiple query string parameters via curl - Squirrel Code - Electric Imp Forums

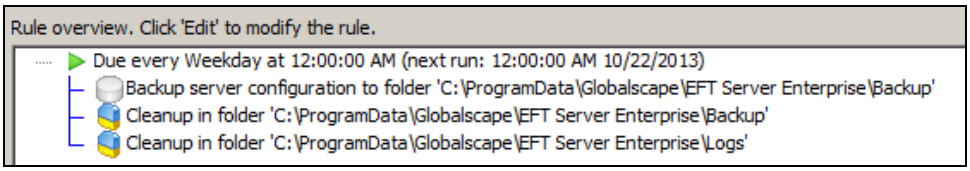
For example if you set EFT to expect at least 5 URL requests, then the curl request would be as follows:

```
curl --insecure
"https://192.168.100.166:443/QA?One&Two&Three&Four&Five"
```

Scheduler (Timer) Event

(Requires TEM) The **Scheduler (Timer) Event** allows you to execute a specified Action (e.g. send an email or a report) only one time or to repeat 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 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 **Clean-up** Action to delete files matching the expressions you specify. You can also choose to define it in the administration interface on existing Sites.

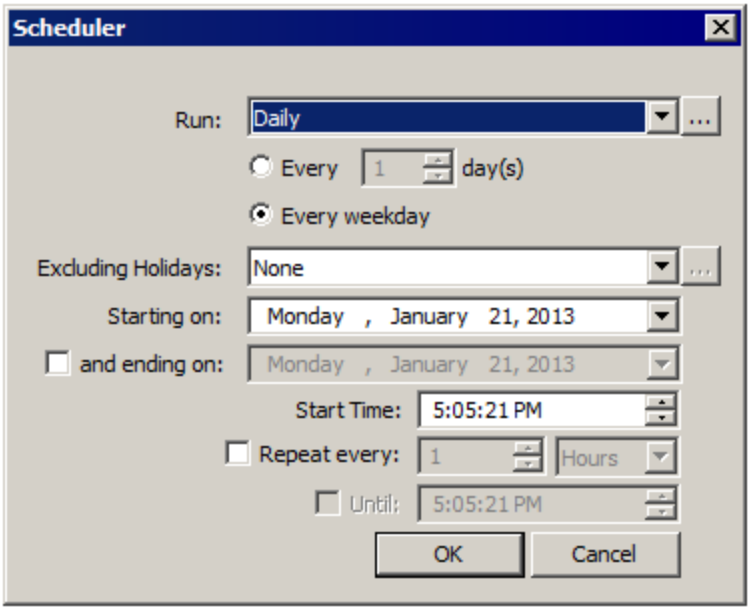


A recurring Timer does not stop recurring if the Rule Actions fail; it will recur as scheduled until you disable or delete the Rule. For example, suppose you want to download a file from a remote server, delete the file from the remote location after transfer, then send yourself an email. If the file 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 (for example, 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 email), 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).

The "Run On One of" feature in Event Rules currently only supports computer (NetBIOS) names. Refer to Event Rule Load Balancing for more information about the "Run On One of" feature.

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. The **Scheduler** dialog box appears.



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.)

   The **Run** options include the following frequencies. The dialog box options change depending on your selection in the Run box.

   - **Once**—The event runs one time at a specified date and time, and never repeats. (for example, 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**. (for example, 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. (for example, 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. (For example, 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. (for example, 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. (for example, 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 not available.)
    - 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; 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, 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 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.

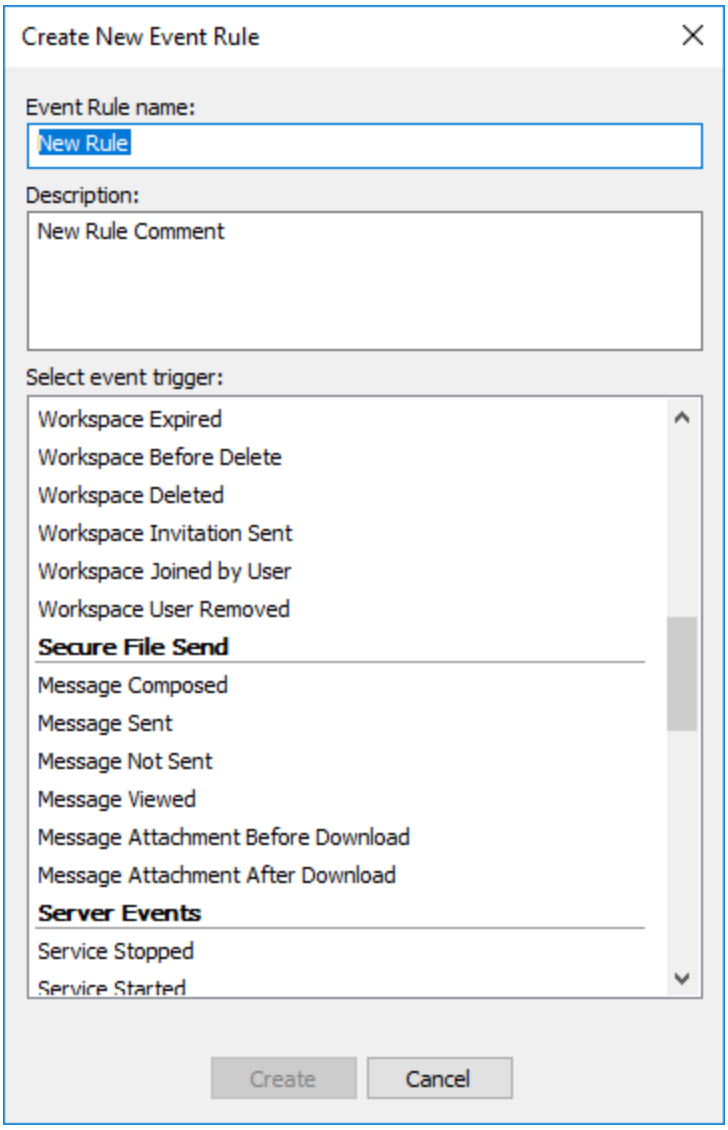
   When you create a Timer Rule, the **Run Now** button appears at the bottom of the **Rule Builder**. When you click **Run Now**, EFT executes any actions associated with the event, and any Rule construction errors are identified. You cannot perform any other operations in the EFT administration interface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

   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.

8. Click **Apply** to save the changes on EFT.

Secure File Send Events

Secure File Send events are "ad hoc" triggers used in event rules for secure file send with Outlook Add-In, Send Portal, Reply, Drop Off, and Request File-related events.



Message Composed- Send has been pressed and basic validation done, but before Workspaces creation

Message Sent - The message is sent after the Workspace has been created.

Message Not Sent - Triggers on any error during validation and preprocessing steps

Message Viewed - Recipient visited pickup page

Message Attachment Before Download - If a download is requested, perform the Action(s) defined in this Event, then continue with downloading the attachment

Message Attachment After Download - Attachment is downloaded from the Site

Server Events

- **Service Stopped**—When the EFT service stops.
- **Service Started**—When the EFT service starts.
- **Log Rotated**—When the current activity log closes and EFT opens a new log file.

Service Stopped- Triggers if the EFT service stops.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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- Triggers when the EFT service starts.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
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%
Site Properties	Site name	%SITE.NAME%

Log rotated - Triggers when the current activity log closes and EFT opens a new log file.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_ PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%

Type	Label (can appear in email notification)	Variable
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
	Compressed File Physical Path	%FS.COMPRESSED_PATH%
	Compressed File Name	%FS.COMPRESSED_FILE_NAME%
	Compressed File Base Name	%FS.COMPRESSED_BASE_FILE_NAME%
Site Properties	Site name	%SITE.NAME%
	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%
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%
	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**—When the Site stops.
- **Site Started**—When the Site starts.
- IP Added to Ban List—This Event will trigger when an IP address is banned by EFT (non-interactively) due to invalid login attempts exceeded or other security criteria.

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
Site Properties	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%
Connection Properties (for **IP Added to Ban List** event)	Remote IP	%CONNECTION.REMOTE_IP%
	Local IP	%CONNECTION.LOCAL_IP%
	Protocol	%CONNECTION.PROTOCOL%

User Events

- **GDPR Right Exercised**—The **GDPR Right Exercised** event includes an "If Event Reason [does] equal to [specific reason]" condition in the Rule Builder. This event is triggered when one of the following events are initiated:
    - When a user's personal data has been modified by someone other than the user

      or

    - Within the Web Transfer Client, when a user has:
        - Rescinded consent to the use of their personal data ("ungranted" consent to privacy policy)
        - Accessed their personal data
        - Rectified their personal data
        - Asked to restrict the use of their personal data
        - Exported their personal data
        - Objected to the use of their personal data
        - Asked to be forgotten
- **User Account Enabled**—When an administrator enables a user account on the Site. (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)
- **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. (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)
- **User Account Locked**—The user account has been locked out by the server (for example, invalid login attempts). (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)
- **User Quota Exceeded**—The user has taken too much disk space on EFT. (This applies ONLY to allotted disk space, not to file size.)
- **User Logged Out**—The user closes a session gracefully.
- **User Logged In**—The user logs in to EFT.
- **User Login Failed**—The user attempted an incorrect username or password.
- **User Password Changed**—The user or administrator changes a user's password.

- **User Account Created**—The administrator has created a new user. (On an Active-Active (HA) cluster configuration, add the "If node name" Condition to avoid multiple actions, such as email notifications)

  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 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.

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

  User events can take these variables:

Type	Label (can appear in email notification)	Variable
Event Properties	Event Time	%EVENT.TIME%
	Event Time Stamp	%EVENT.TIMESTAMP%
	Event Date Stamp	%EVENT.DATESTAMP%
	Event Name	%EVENT.NAME%
	Event Rule Name	%EVENT.EVENTNAME%
	Event Time Stamp (including milliseconds)	%EVENT.TIMESTAMP_PRECISE%
	Event Transaction ID	%EVENT.TRANSACTION_ID%
File System Properties	Report File	%FS.REPORT_FILE%
	Report Content	%FS.REPORT_CONTENT%
	Report File Name	%FS.REPORT_FILENAME%
User Properties	(GDPR) User EU data subject status	%USER.EU_DATA_SUBJECT_STATUS%
	(GDPR) User consent to privacy policy	%USER.PP_CONSENT_STATUS%
	(GDPR) User agreement to terms of service	%USER.TOS_AGREEMENT_STATUS%
	(GDPR) Right exercised	%USER.GDPR_RIGHT_EXERCISED%
	(GDPR) Right exercised article id	%USER.GDPR_RIGHT_EXERCISED_ ARTICLE_ID%
	DUNS Number	%USER.DUNS%

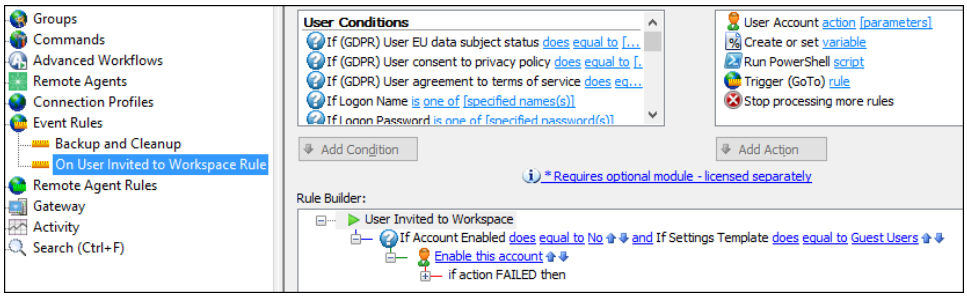
Type	Label (can appear in email notification)	Variable
	Groups	%USER.GROUPS%
	Logon Name	%USER.LOGIN%
	Logon Password	%USER.PASSWORD%
	Settings Template	%USER.SETTINGS_LEVEL%
	Full Name	%USER.FULL_NAME%
	Description	%USER.DESCRIPTION%
	Comment	%USER.COMMENT%
	Email Address	%USER.EMAIL%
	Phone Number	%USER.PHONE%
	Pager Number	%USER.PAGER%
	Fax Number	%USER.FAX%
	Partner_Id	%USER.PARTNER_ID%
	Custom Field 1	%USER.CUSTOM1%
	Custom Field 2	%USER.CUSTOM2%
	Custom Field 3	%USER.CUSTOM3%
	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%
	Account Locked Out	%USER.IS_LOCKED_OUT%

Type	Label (can appear in email notification)	Variable
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	Site name	%SITE.NAME%
	Account Management URL	%SITE.ACCOUNT_MANAGEMENT_URL%
	Site Running	%SITE.STATUS%
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%

Workspaces Events

(Requires Workspaces module) Use Workspaces Events in Event Rules if you want to be notified or cause other Actions to occur when a Workspace is create or deleted, when a use is invited to join or joins a Workspace, or when a user is removed from a Workspace. In EFT v8.5.0.8, some of the Workspaces events were renamed. The old and new names are noted below.

- **Workspace Created** - Perform actions based on a Workspace being created, such as sending an email.
- **Workspace Expired** - Perform actions based on a Workspace expiring, such as sending an email.
- **Workspace Deleted** - Perform actions based on a Workspace being deleted, such as sending an email.
- **Before Workspace Deleted/ Workspace before Delete** - Perform actions to occur before a Workspace is deleted, such as copy/move actions.
- **User Invited to Workspace/Workspace Invitation Sent** - If an account has been disabled due to expired Workspaces links, you can configure an Event Rule to re-enable the account automatically when they are sent a Workspaces invitation.



- **User Joins Workspace/Workspace Joined by User** - Perform an action when a user joins a Workspace. You could create an Event Rule using the **User Joins Workspace** Event, and add the **Email Notification Message**. In the email, you could add the variables Workspace Physical Path, Workspace Name, Workspace Participants List, and Workspace Owner. Then, whenever a user joins a Workspace, you would get an email telling you all the information you would need to know about the Workspace, including the information about the user who joined the Workspace. You could also create a custom report and define the Event Rule to generate a report automatically once per month that lists each of the Workspaces and their participants.
- **User Removed from Workspace/Workspace User Removed**- Perform actions based on a user being removed from a Workspace.

Actions

The topics below provide information regarding defining and using Event Rule Actions.

Available Actions

Once an Event Rule is triggered, assuming all Conditions are met, EFT can launch one or more of the following user-definable Actions. Some Actions require a specific module.

- Protocol: Upload (formerly "Copy/Move (push) file to host") - The designated file is automatically moved to another location.
- Protocol: Download (formerly "Download (pull) file from host") - Downloads a specified file.
- Protocol: Synchronize - Synchronize local and remote folders
- Protocol: AS2 (formerly "AS2 Send file to host" Action) - You can send files via AS2 to a partner that does not have inbound access defined in EFT's account management system.
- Protocol: Email (formerly "Send notification email") - An email message is sent to the address specified.
- Cloud: Download; Cloud: Upload (formerly Cloud Storage actions) - Supports transfers from/to Amazon S3 and Azure containers including advanced settings like multi-part, encryption, requestor-pay, and others. GET, POST, PUT, DELETE at a specific URL and save the response to a specific file.

  > **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

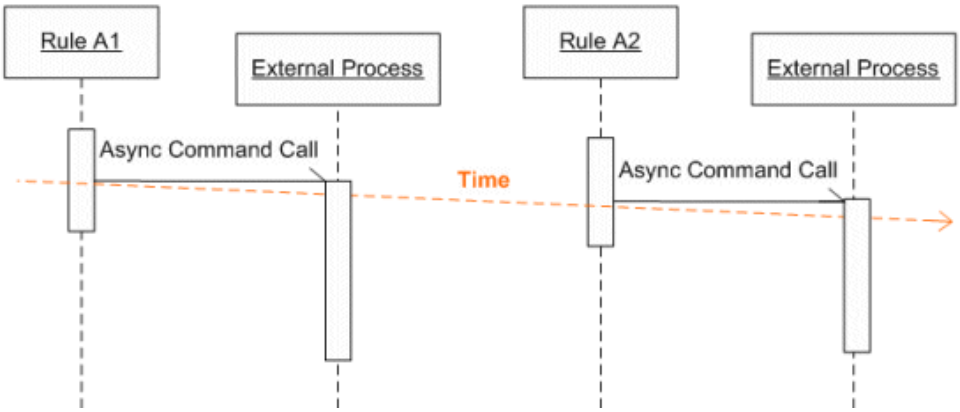
- Cloud: REST/Web Services (formerly "Invoke Web Services") - GET, POST, PUT, DELETE at a specific URL and save the response to a specific file.
- Compression - Compress or decompress file in the format of Zip, 7Zip, Gzip, Bzip2, Tar, Tar and Gzip, or ZCompress. You can also add context variables to the Action.
- Cryptography: OpenPGP (formerly "OpenPGP operations") - **(Requires OpenPGP module)** The designated cryptographic action is performed on the file.
- CSV: Export to dataset - Used in conjunction with Protocol: Listing to Dataset and Loop: Dataset Action (or with an existing dataset) to create a CSV file, which can then be used in other applications.
- CSV: Import from dataset - Reads data from a comma-separated values (CSV) file, and populates the specified dataset with those values.

- File: Scan (formerly Scan file using Content Integrity Control) - Used to send a file to an antivirus or data loss prevention scanner for processing.
- File: Operation - Create, rename, or delete specified file. Optionally use specified credentials.
- Folder: Operation - Create, rename, or delete specified folder. Optionally use specified credentials.
- Flow: Abort User Operation - Used after the File: Scan Action for a Message Composed event in case a file is attached to the message that did not pass the ICAP scan.
- Flow: Subroutine (formerly "Call Event Rule subroutine") - Allows you to call an Event Rule Subroutine event (a sub task) from the current rule
- Flow: 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.
- Flow: Variable (formerly "Create or set variable") - Used to create or modify a variable to be used in Event Rules
- Loop: Dataset (formerly "Loop through Dataset") - Used to read from a remote directory listing to create a dataset or read from a CSV file to create a dataset. reads through ("parses") a dataset until the end of the dataset is reached or a Loop Break is used to stop the loop.
- Script: Advanced Workflow (formerly "Execute Advanced Workflow") - An Advanced Workflow is triggered.
- Script: Custom Command (formerly "Execute command in folder") - The custom command in a specific location is triggered.
- Script PowerShell (formerly "Run PowerShell script") - Used in Event Rules to execute a PowerShell script
- System Backup - Automatically backs up EFT configuration for use in disaster recovery or EFT migration.
- System Cleanup - Cleans up a specified folder
- System: Report (formerly "Generate Report") - **(Requires database and Auditing and Reporting module)** A report is generated and emailed or saved to a file at a specific date and time.
- User: Action- Lock, disable, ban, delete, or kick user account
- User: Create - Added to an event rule when you want a certain event to trigger the creation of a new user. (This action is available to any event trigger.)

- Windows Event Log - Defines the parameters to display in the Windows Event Log when the Event is triggered.

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

Order in which Actions are Executed



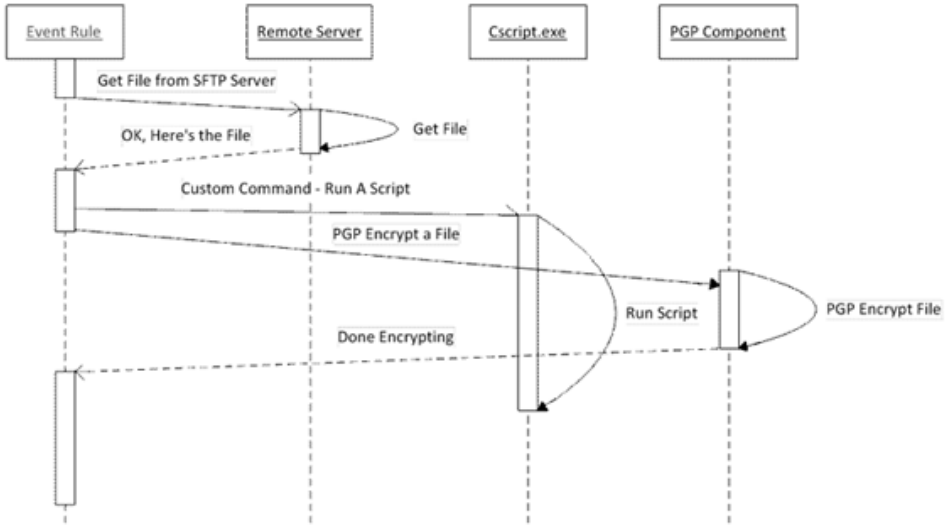
For **Execute Command** Actions and **Execute Advanced Workflow** Actions, EFT does not wait for a reply before returning control to the Event Rule thread, *unless* an "if failed" Condition is specified, such as **Stop Processing this Rule**. If an "if failed" Condition is specified, regardless of whether 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

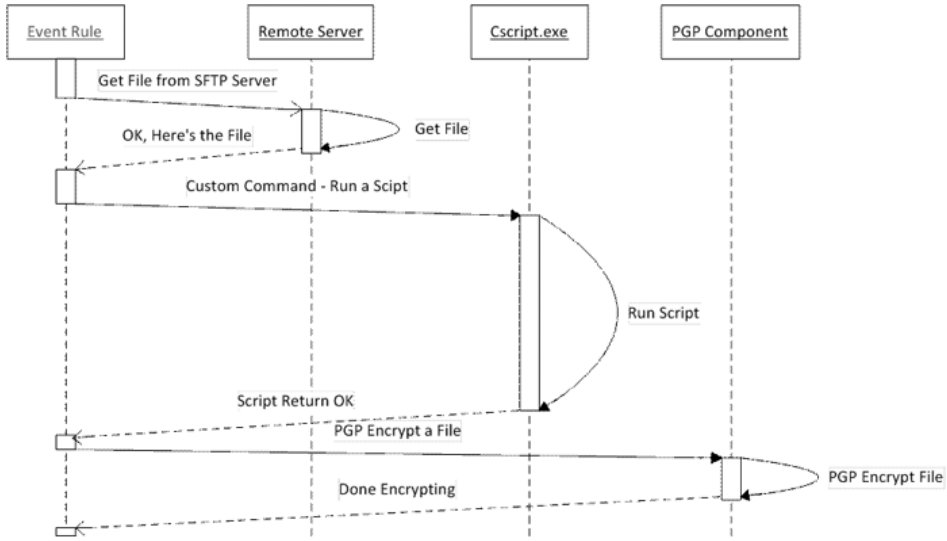
A common Event Rule scenario is downloading a file, running a script against that file (either with an **Execute Command** Action or an **Execute Advanced Workflow** Action), then encrypting or decrypting the file.

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 an **OpenPGP** 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 OpenPGP operation, the potential risk is that there will be a race condition and likely OpenPGP will lose; that is, the pre-transformed file will be encrypted 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.



Related Topic

- Event Rule Order of Execution

Order in which Event Rules are Executed

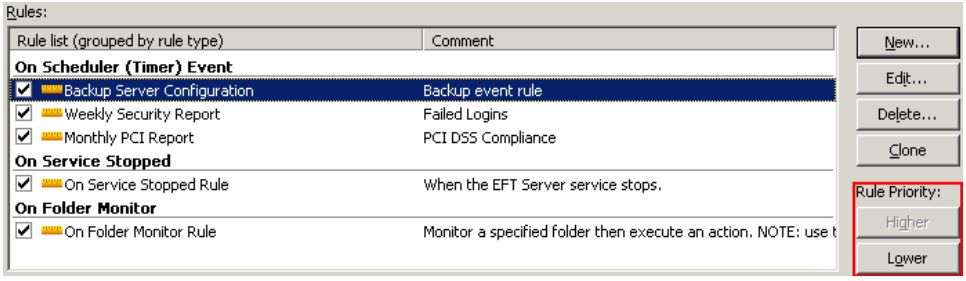
Almost all of EFT's Event Rule Actions are executed one after the other *(for example, execute 1, wait until it finishes, execute 2, wait until 2 finishes, execute 3 … etc.)*, because there may be Actions that follow that depend on the prior Action completing successfully. Each Action is completed before continuing to the next, with a few

exceptions, which are described below (Timer Rules, Monitor Folder Rules, and Rules that use the Execute Command Action or Advanced Workflow Action).

If you create more than one Event Rule for a single type of Event trigger (for example, Monitor Folder), EFT prioritizes the Rules in the order they appear in 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 (for example, place one Timer Event to occur before another Timer Event).

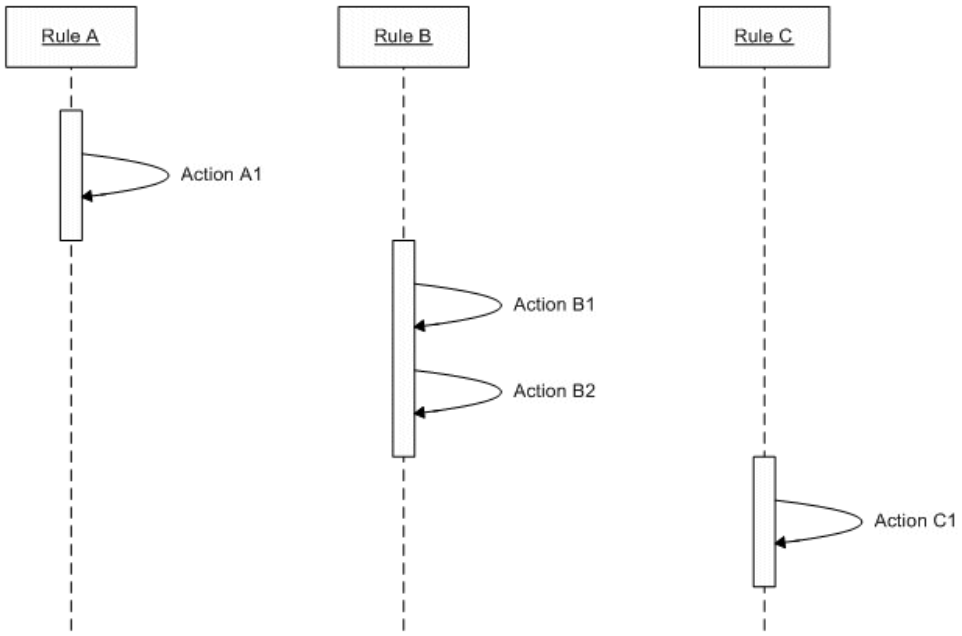
To change the priority of a Rule

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure, 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**.



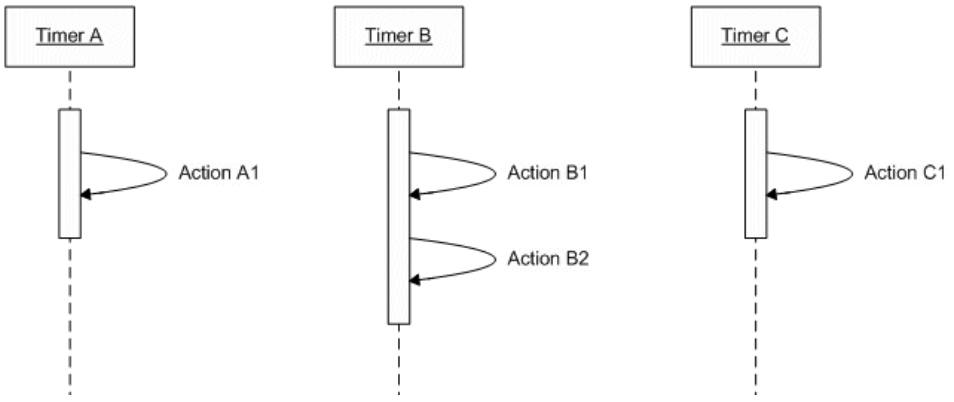
Event Rule Sequence for Matching Event Rules

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

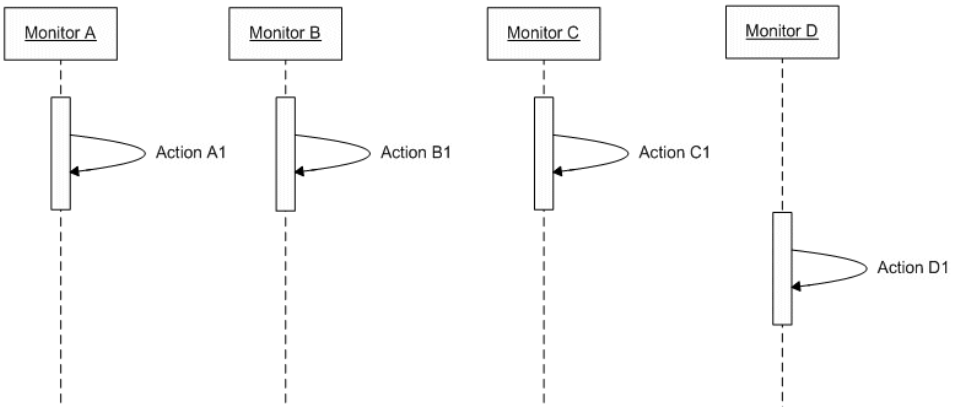
This sequential firing of duplicate Event Rules applies to almost all of EFT's supported Events. However, the Monitor Folder and Timer Event Rules are not executed at the same time. When you stop the Site or the Server service, EFT breaks all existing connections and waits until all socket threads die. 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.



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.



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 Builder**.
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.

Which Actions are Available with Which Event Triggers?

Some actions are only available with certain Events. The following actions can be used with any Event: Protocol: Email, Protocol: Listing to Dataset (Requires EAM), Flow: Subroutine (Requires EAM), Flow: Stop Processing, Flow: Variable, Loop: Dataset (Requires EAM), Script: Advanced Workflow (Requires AWM), Script: Custom Command (Requires EAM), Script: PowerShell (Requires EAM), and Cloud: Rest/Web Services (Requires CCM).

IMPORTANT: During the trial, all event triggers and actions are available for you to try. Any event rules that you created during the trial will no longer be available if you do not activate a license for the events and actions used in the event rules that require a license. In the EFT administration interface, event triggers and actions that require a license have an asterisk (*) next to them. Also refer to Introduction to EFT Managed File Transfer

Actions and Events Chart

Events	Protocol: Upload	Protocol: Download	Protocol: Synchronize	Protocol: AS2	Cloud: Upload	Cloud: Download	Compression	Cryptography: OpenPGP	CSV: Import from Dataset	CSV: Export to Dataset	File: Scan	File: Operation	Folder: Operation	Flow: Abort User Operation	System: Cleanup	System: Backup	System: Report	User: Action	User: Create
Operating System Events																			
Scheduler (Timer)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y
Folder Monitor	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N
Folder Monitor Failed	N	Y	N	N	N	Y	N	N	Y	Y	N	N	N	N	Y	N	N	N	N
Cloud-Based Events																			
Cloud Object Monitor	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y
File Server Events																			
File Uploaded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
File Downloaded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Verified Upload Succeeded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Verified Download Succeeded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
File Renamed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
File Moved	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
File Deleted	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Folder Created	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Folder Deleted	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Folder Changed (FTP/S only)	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Upload Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Download Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Verified Upload Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Verified Download Failed	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Before Download	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Workspace Events																			
Workspace Created	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Workspace Expired	Y	N	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y
Workspace Before Delete	Y	N	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y
Workspace Deleted	Y	N	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y
Workspace Invitation Sent	Y	N	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y
Workspace Joined by User	Y	N	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y
Workspace User Removed	Y	N	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y
Secure File Send																			
Message Composed	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Sent	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Not Sent	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Viewed	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Attachment After Download	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Message Attachment Before Download	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
Server Events																			
Service Stopped	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	Y
Service Started	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	Y	Y	N	Y
Site Created	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	Y
Site Events																			
Site Stop	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	N	Y
Site Started	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	N	Y
IP Added to Ban List	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y
User Events																			
GDPR Right Exercised	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
User Account Enabled	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Account Disabled	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Account Locked	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Quota Exceeded	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
User Logged Out	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
User Logged In	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y
User Login Failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Password Changed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Account Created	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
User Account Deleted	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
Connection Events																			
Connection established	N	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y
Connection Failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
Disconnected	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	N	Y	Y
AS2 Events																			
AS2 Inbound Transaction Failed	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
AS2 Inbound Transaction Succeeded	N	Y	Y	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
AS2 Outbound Transaction Failed	N	Y	N	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
AS2 Outbound Transaction Succeeded	N	Y	N	N	N	Y	N	N	Y	Y	N	N	N	N	N	N	Y	Y	Y
Other Event Types																			
Event Rule Subroutine	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y
REST Invocation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y

Cryptography: OpenPGP Configuration

The topics in chapter provide information regarding using OpenPGP with EFT.

OpenPGP and EFT

EFT employs industry-standard OpenPGP (based on the open source implementation of Pretty Good Privacy) technology to safeguard data at rest. In contrast to symmetric encryption technologies that rely on a single password or shared secret for encryption and decryption, OpenPGP uses a public/private key pair and a password. Although widespread, dual-factor encryption technologies such as OpenPGP are not universally employed throughout the industry, because of the complexities involved in key creation, management, and distribution, as well as the application of public-key infrastructure technologies. Another drawback is the fact that the entire file must be present for OpenPGP encryption to work, resulting in a very brief period of time whereby data is stored "in the clear," until the encryption process is completed and the source (unprotected) file is deleted.

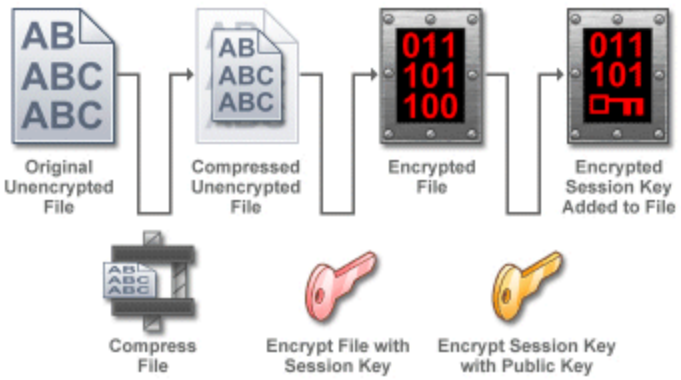
EFT supports encrypting, decrypting , signing, verifying OpenPGP messages in the format specified by RFC 4880. Refer to http://cdn.nsoftware.com/help/IG9/cs/OpenPGP.htm for more information.

For details of using OpenPGP in Event Rules, refer to OpenPGP Encryption/Decryption Action.

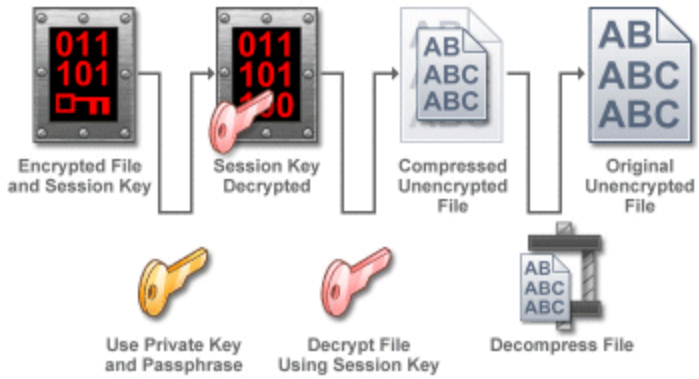
How OpenPGP Encrypt/Decrypt Works

Below are illustrations of how OpenPGP encryption and decryption works.

Encryption:



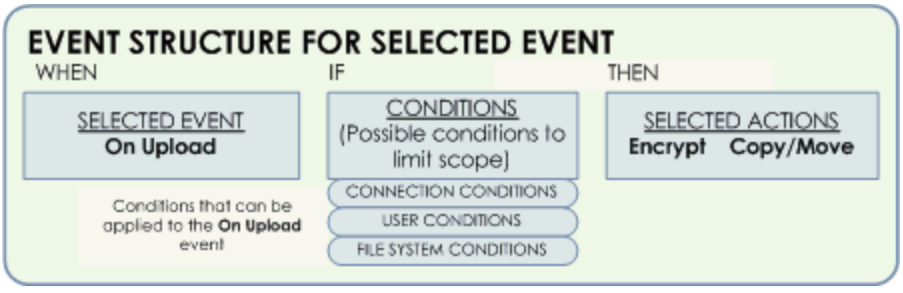
Decryption:



In EFT, the OpenPGP data encryption (or decryption) process is directed by Event Rules that specify how data files are treated in a particular context. OpenPGP uses a public key and a private key to encrypt data and maintain security. These two components are considered a key pair and are associated with a particular Site. The key pair is stored on the **OpenPGP Keyring**, which is the management tool for public keys and key pairs. The **OpenPGP Keyring** contains all key information and allows import, export, creation, and deletion of keys.

New key pairs are created using the **OpenPGP Key Generation** wizard. The wizard prompts you for key parameters and creation of a passphrase. Once the new key pair is generated, you must determine if the new key pair will be the default for the entire Site. Allowing assignment of a default key pair will automatically select this key when configuring an Event Rule using OpenPGP encryption.

The example below shows how a trigger Event (On Upload) is used to initiate OpenPGP encryption.

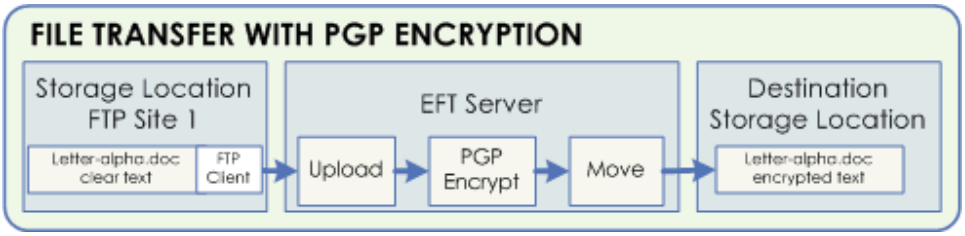


In an Event Rule, when a selected event occurs (for example, a file is uploaded to EFT), if the specified Condition exists (for example, user is member of group A), then the selected actions occur (for example, encrypt the file).

OpenPGP encryption is only available for certain Events:

- **On Upload** - when a file is uploaded to a location.
- **On Rotate Log** - when a log file is closed out and a new log initiated.
- **On Timer** - an Event that occurs once or according to a schedule.

Below is a simplified example of the file transfer process in which EFT uses OpenPGP to encrypt uploaded data and the off-load capabilities of EFT to move the file to another location.



OpenPGP Encryption Algorithms

The table below lists the encryption algorithms available for EFT OpenPGP. It is up to you to determine which settings to use in your environment.

EFT uses IP*Works! OpenPGP libraries. Refer to EFT Specifications for the version of the library used in this version of EFT.

Ciphers – Encryption Algorithms	Message Authentication Code (MAC) – Hashing algorithms
• AES256 • AES192 • AES128 • Twofish • 3-DES • CAST 5 • IDEA	• SHA512 • SHA384 • SHA256 • MD5 • SHA1 • RIPEMD-160

Creating Key Pairs for OpenPGP

You can create new key pairs for OpenPGP encryption using the **OpenPGP Key Generation Wizard**. The key pair file is saved in **SiteConfig<GUID>.db**. Note that the **\PGP** folder does not exist until you create or import a key pair.

EFT can create the following types of keys for OpenPGP:

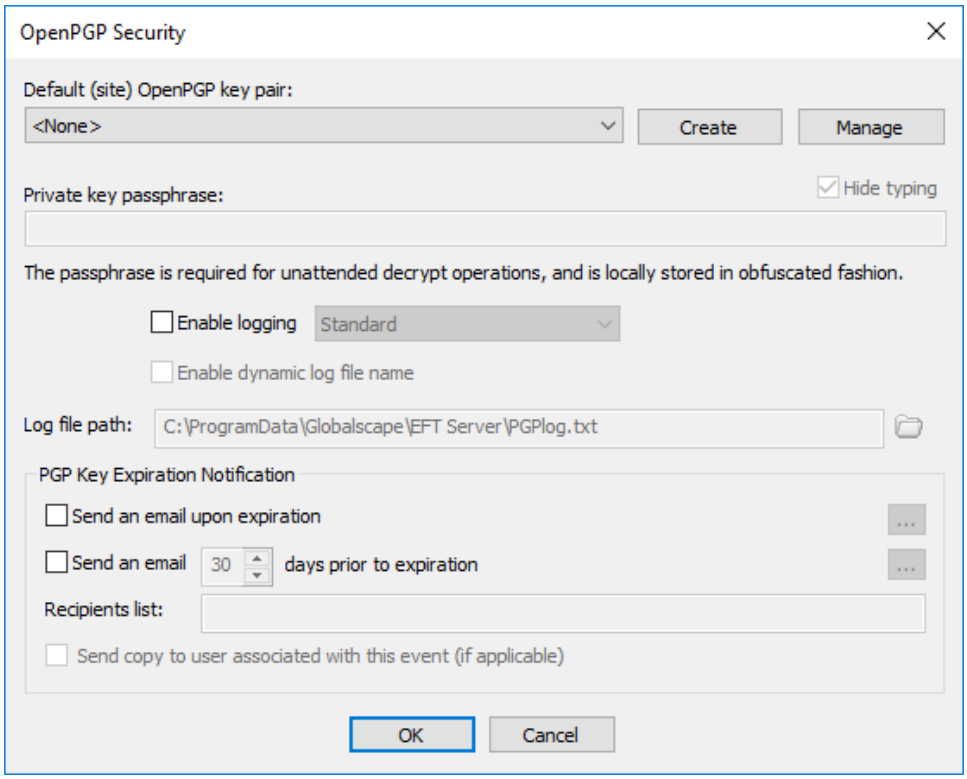
RSA: If you select RSA, the library generates the new standard RSA key pair format by default--keys that are compatible with newer OpenPGP clients. The new RSA key format supports features previously available only to DSS/DH keys. The new RSA key format enables you to have a primary key for signing and a subkey to encrypt data. In addition, the encryption key (the subkey) can be revoked or have a different expiration date as its primary key. A new subkey can always be added to a primary key and be used for encrypting data. New RSA keys are compatible with newer versions of OpenPGP. The library generates the new and improved RSA key format by default. These keys are not compatible with older OpenPGP clients that are not compliant with RFC 2440 such as OpenPGP 2.6.x.

RSA Legacy: In EFT, the OpenPGP library gives you the option to generate RSA Legacy keys that are compatible with older versions of OpenPGP. Old OpenPGP clients are compliant with RFC 1991 only, not RFC 2440.

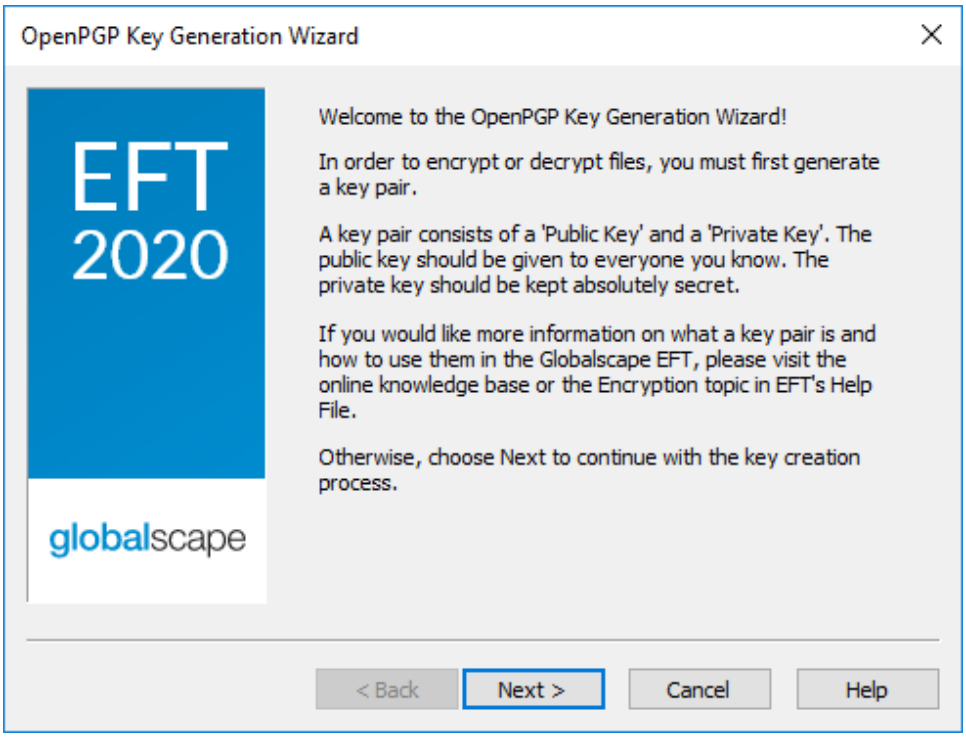
- For information about Diffie-Hellman key exchange, refer to http://en.wikipedia.org/wiki/Diffie-Hellman.
- For information about RSA, refer to http://en.wikipedia.org/wiki/RSA.
- If you have made any configuration changes, click **Apply** and/or **Refresh** before creating the key pair; otherwise, key creation will fail.
- If you attempt remote management of keys, you may encounter unexpected behavior.

To access the Key Ring Manager and use the OpenPGP Key Generation Wizard

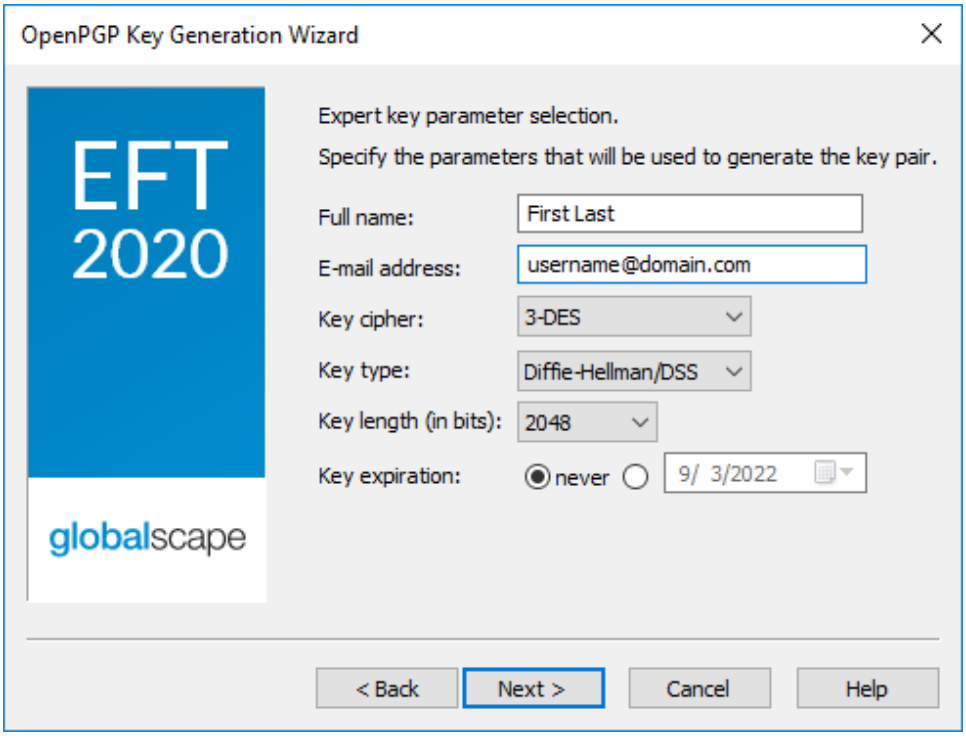
1. In the administration interface, connect to EFT and click the **Server** tab.
2. Click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area at the bottom of the tab, next to **OpenPGP security**, click **Configure**. The **OpenPGP Security** dialog box appears.



5. Click **Create**. The **OpenPGP Key Generation Wizard** appears. (Or you can click **Tools > Create OpenPGP Key**.)

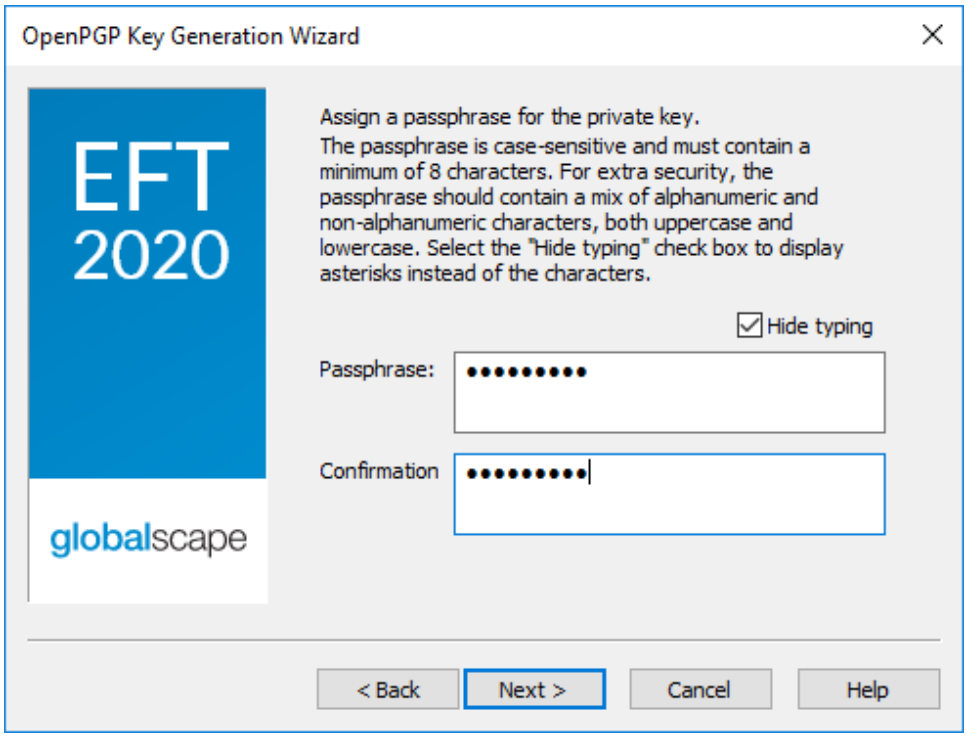


6. Read the instructions on the welcome page, and then click **Next**. The **Parameters** page appears.

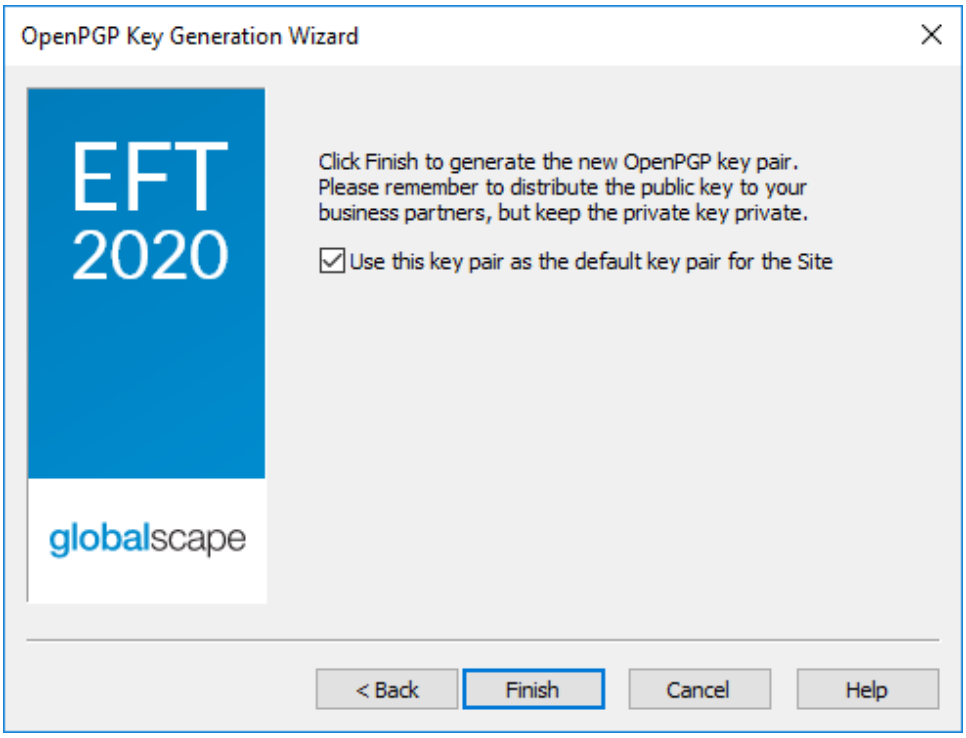


7. In the **Full name** box, provide your name or another contact's name.

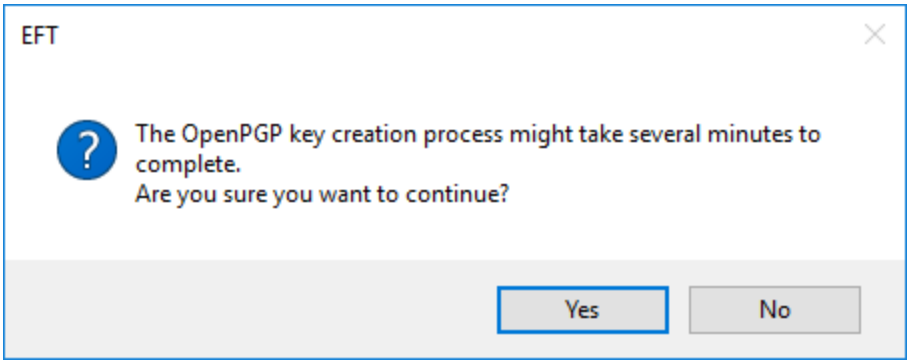
8. In the **email address** box, provide an email address.
9. In the **Key cipher** box, click the list to specify a cipher to use: IDEA, 3-DES (the default), CAST5, AES128, AES192, AES256, or TWOFISH.
10. In the **Key type** box, click Diffie-Hellman/DSS, RSA, or RSA legacy.
11. Specify the **Key length** (1024, 2048, 3072, or 4096). Larger bit sizes increase security, but increase encryption time.
12. Specify the **Key expiration** date, or never.
13. Click **Next**. The passphrase page appears.



14. Type your passphrase in the **Passphrase** and **Confirmation** boxes. The passphrase is case sensitive and must contain a minimum of 8 characters. For better security, the passphrase should contain a mix of alphanumeric (both upper and lower case) and non-alphanumeric characters. Select the **Hide typing** check box to display asterisks instead of the passphrase.
15. Click **Next**. The Site page appears.



16. Click **Finish** to generate the key pair. A message appears informing you that it might take several minutes to generate the key pair.



17. Click **Yes** to create the key. If you click **No**, the key is not created.
18. After the key is created and added to the Site keyring, click **OK** to close the notification dialog box.
19. **To specify a logging Level and the Log file path,** select the **Enable logging** check box.
20. **To specify a dynamic log file name**, select the **Enable dynamic log file name** check box, and specify an extension in the Log file path. The date and time will be added to the file name (e.g., PGPlog20190415.txt).
21. Click **OK** to save your changes and close the **OpenPGP Security** dialog box.

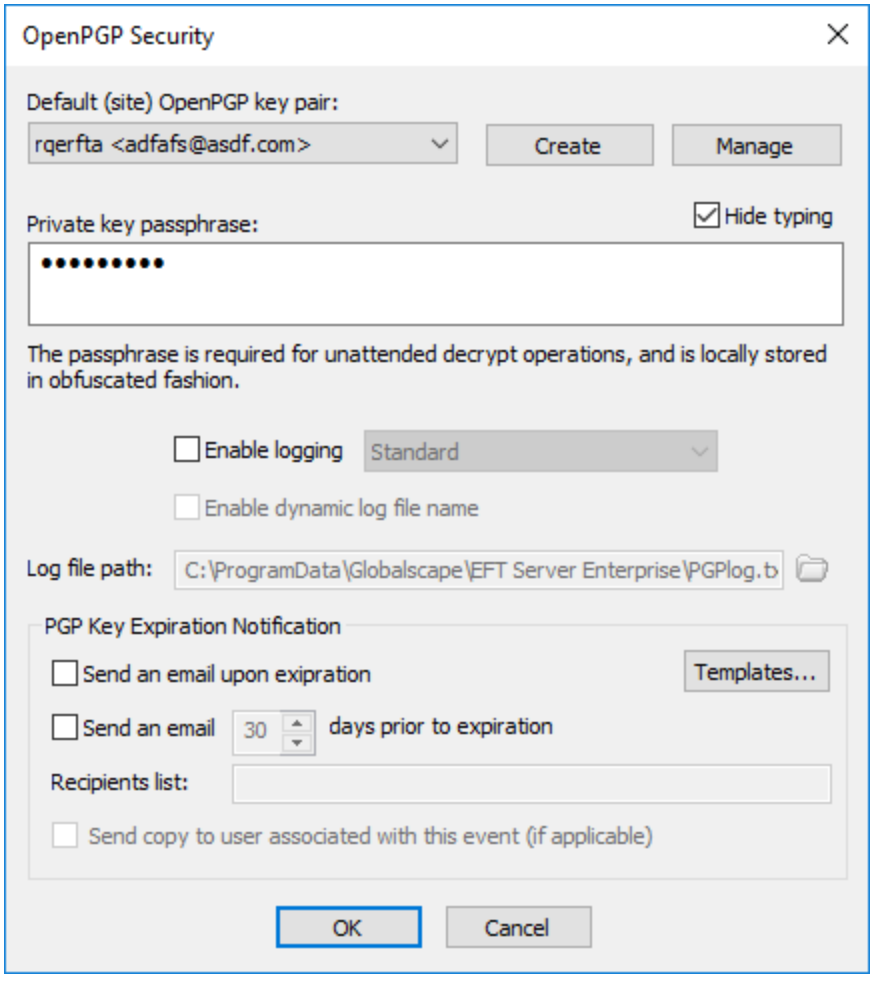
22. Click **Apply** to save the changes on EFT.

Setting OpenPGP Security for the Site

This procedure describes setting OpenPGP security for the Site.

To set OpenPGP security

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Site you want to configure.
3. In the right pane, click the **Security** tab.
4. In the **Data Security** area, next to **OpenPGP security**, click **Configure**. The **OpenPGP Security** dialog box appears.



5. If an OpenPGP key pair is defined on EFT, click the **Default Site key pair** drop-down menu and click the key. Otherwise, click **Create** and follow the instructions in Creating Key Pairs for OpenPGP or click **Manage** and following the instructions in Importing and Exporting Key Pairs for OpenPGP.

6. In the **Private key passphrase** box, provide the passphrase for the selected key. Select the **Hide typing** check box if you do not want the passphrase to be viewable.
7. Select the **Enable debug logging** check box if you want to log errors, and then click the drop-down menu to specify the level of logging: 0 (minimum logging), 1, or 2.
    - If you select the **Enable debug logging** check box, you can select the **Enable dynamic log file name** to add the date to the file name.
8. In the **Log file path** box, specify where to save the log file.
9. Under **PGP Key Expiration Notification** select the **Send an email upon expiration** check box. (EFT does a daily check at midnight.)
10. Select the **Send an email *n* days prior to expiration** check box, and specify the number of days. (The email is sent daily when nearing expiration. Acceptable values are 1 -90 days; 30 days is the default.)
11. Specify who is to receive the email. You can list multiple recipients separated by semicolons or a commas.

    The EFT log and Windows Event Viewer are updated with the same content as the template, even if email notification is disabled. The templates are stored in **C:\ProgramData\Globalscape\EFT Server\Template**s (by default). Click the buttons to the right to edit the files, if needed.

12. Click **OK** to save the changes.
13. Click **Apply** to save the changes on EFT.

The OpenPGP Keyring Manager

Use the **OpenPGP Keyring** manager to create, delete, import, and export OpenPGP key pairs.

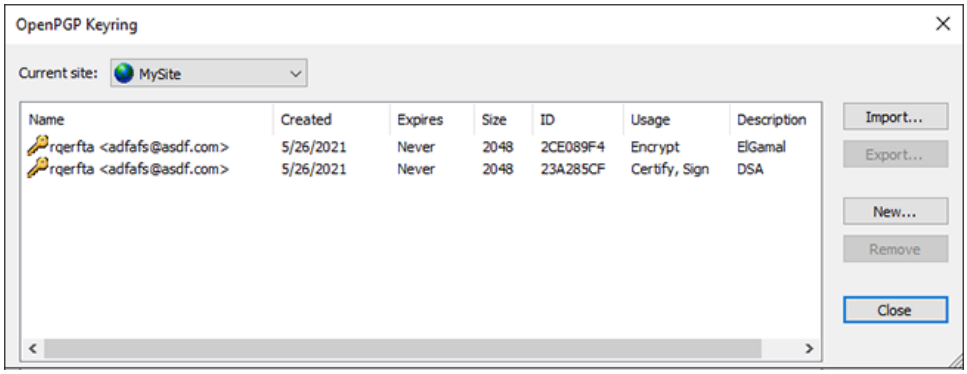
Some keys imported into EFT are dual keys: a master key used for signing, and a sub-key typically used for encrypting. When viewed in the EFT event rules PGP action, you see both keys, and it is not easy to identify which is which, as the key's email parameter is the same. EFT displays both the hex ID and that key's usage attribute (certify, sign, encrypt), to make it easier for you to choose the right key to add to the decryption set of keys.

Some PGP tools (Kleopatra, GoAnywhereOpenPGP tool suite) will display the KEY ID as a long. EFT displays the KEY ID as a short. If a KEY is imported into EFT that was created in one of these other tools, you will just see the bottom 8 hexadecimal characters in the **ID** field.

To open the OpenPGP Keyring manager

1. In the administration interface, connect to EFT.
2. Do one of the following:
   - On the toolbar, click the **Open OpenPGP Keyring** icon  .
   - On the main menu, click **Tools > Manage OpenPGP Keys**.
   - On the **Server** tab, click the Site you want to configure, then in the right pane, click the **Security** tab. In the **Data Security** area, next to **OpenPGP Security**, click **Configure**. The **OpenPGP Security** dialog box appears. Click **Manage**. The **OpenPGP Keyring** manager appears.

   The **OpenPGP Keyring** manager appears.



   For each keyring, the **OpenPGP Keyring** manager displays its name, the date it was created, the expiration date, the size, a hexadecimal ID number, and a description.

   The **Current site** list displays the selected Site name.

3. For instructions for each of the features of the **OpenPGP Keyring** manager, refer to the following topics:
   - **Import** and **Export**: Importing and Exporting Key Pairs for OpenPGP
   - **New**: Creating Key Pairs for OpenPGP
   - **Remove**: Deleting Key Pairs for OpenPGP
4. Click **Close** to close the dialog box.

- After you make any configuration changes, always click **Apply** and/or **Refresh** before creating a key pair; otherwise, key creation will fail.
- If you attempt remote management of keys, you may encounter unexpected behavior.

Removing OpenPGP Key Pairs

To delete a key pair

1. Open the OpenPGP Keyring dialog box.
2. Select the key pair that you want to delete, then click **Remove**. A confirmation message appears.
3. Click **Yes**.
4. Click **Close** to exit.

Importing and Exporting Key Pairs

To use public key cryptography, connecting clients must have a copy of your public key. (Do not share your private key.) Export the contents of your PGP keys and store them in key files to have a backup of your keys or to share your public key with someone. You will need to import keys that you receive, or import them from storage.

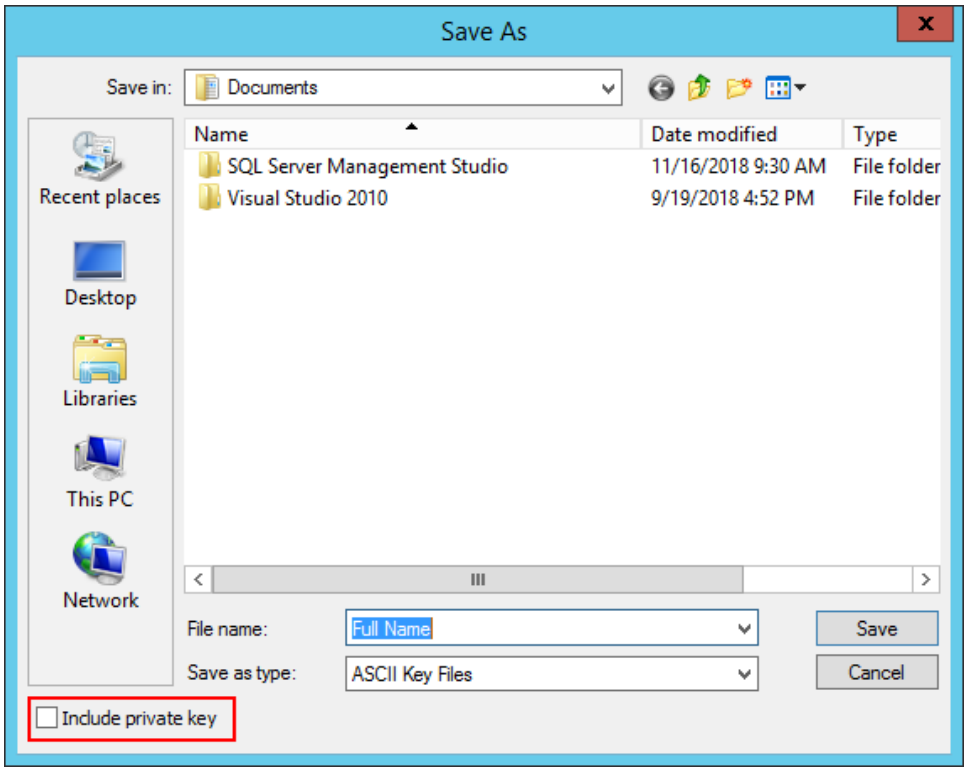
The **OpenPGP KeyRing** manager can be used to **Import** and **Export** keys. You can also sort the keyring by clicking the column headers.

To import a key

1. Open the OpenPGP Keyring dialog box.
2. Click **Import** to begin the key import process. (You can only import one key at a time.)
3. Click the file containing the key to be imported (***.asc**) then click **Open**. The **Import OpenPGP Key** dialog box closes, the imported file is added to the keyring list, the imported key is highlighted in the list, and a message box appears with the key details.
4. Click **OK** to dismiss the message box.

To export a key

1. Open the OpenPGP Keyring dialog box.
2. Select the file to be exported, and then click **Export**. The **Save As** dialog box appears.



3. Click the folder in which you want to save the new key file.
4. Select the Include private key check box to include the private key in the export. ***If you are exporting the key to provide to a client, do not select the check box.***
5. Click **Save** to export the file.

Cryptography: OpenPGP Action

You can configure EFT'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 Server 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 OpenPGP keys must be generated.

Using the OpenPGP 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 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.

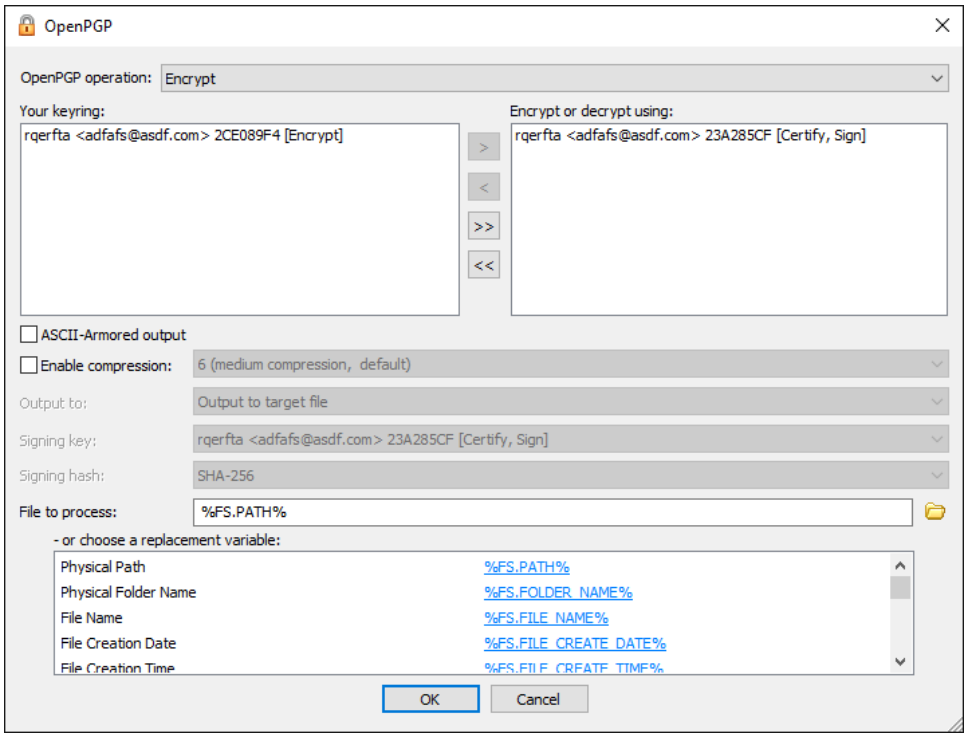
- When encrypting a file: "If File Name does not match *.pgp"
- When decrypting a file: "If File Name does match *.pgp"
- When verifying the signature: "If File Name does match *.sig"
- When signing a file "If File Name does not match *.sig'"
- When verifying signature only: "If File Name does match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

OpenPGP Source	OpenPGP Receiver
Encrypt+Sign	Decrypt+Verify
Encrypt+Sign	Decrypt
Sign Only	Verify Only

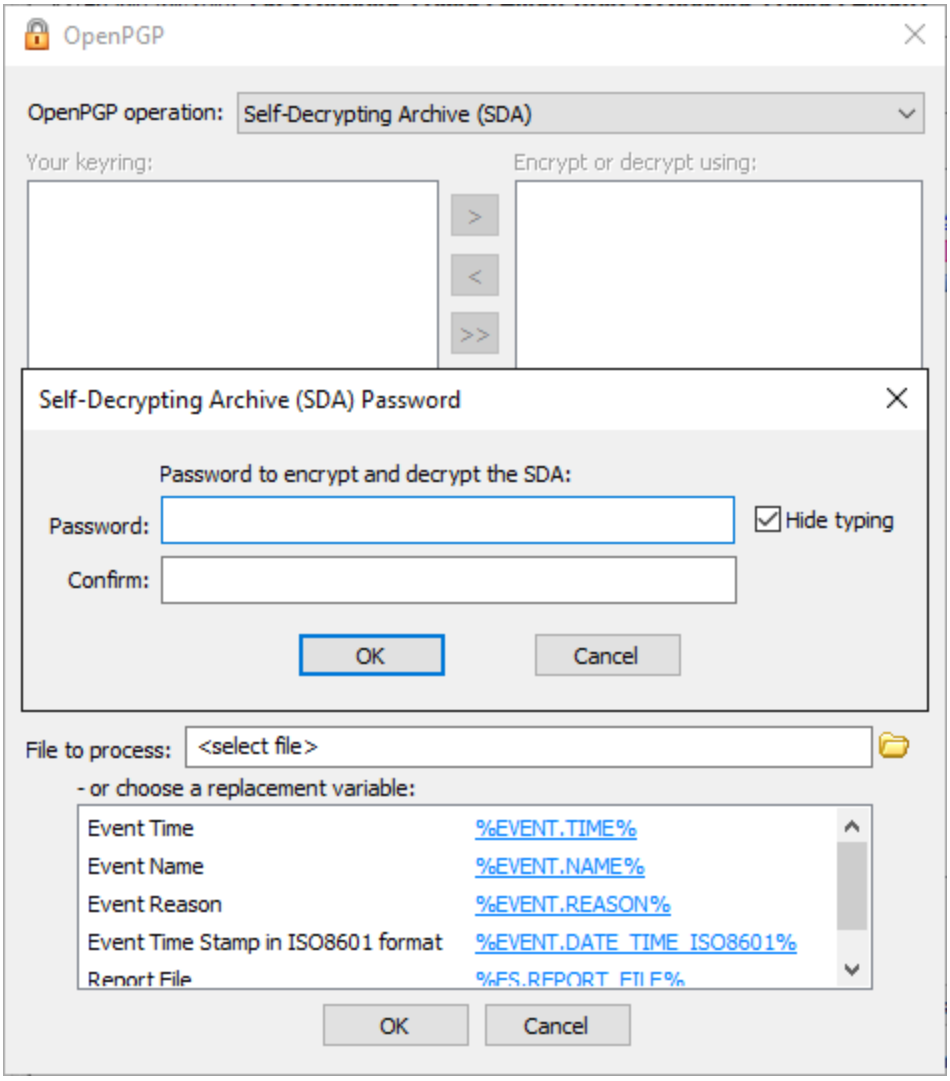
To set up EFT to use OpenPGP for particular Event Rules

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 **Cryptography: OpenPGP**. The Action appears in the Event in the **Rule Builder**.
3. In the **Rule Builder**, select either of the underlined elements (links). The **OpenPGP** 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).

   When **Self-Decrypting Archive** is selected, none of the encryption settings are available. The SDA Class uses a Deflate algorithm specified in RFC 1951 for compression, and then creates a self-decrypting executable archive. It doesn't use encryption in the standard sense like AES, etc. Therefore, it is not considered secure when matched up against OpenPGP. After you click **OK**, a password dialog box appears. Create and confirm a password, click **OK**, then send the password to the recipient. Use a different OpenPGP operation if you want to use encryption.



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. The encryption method and compression method are both chosen by the ciphers that are used/chosen when the key was created. These ciphers are stored in the metadata of the key. EFT reads this metadata and uses that cipher for encryption/compression process.

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.

OpenPGP on File Upload Event Rule

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.

We want this Event Rule to decrypt the uploaded encrypted file, then:

- If the Action failed to decrypt the file, then:
  a. Send email notification, and
  b. Write to Windows Event Log.

Prerequisites

- Private OpenPGP 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 **Cryptography: OpenPGP** Action.
6. Set the OpenPGP action to **Decrypt**. (Only private keys added to the keyring will show in the list when choosing to decrypt.)
7. Add the **Protocol: Email** Action under the **if action failed** Condition.
8. Configure the email as desired.
9. Add the Windows Event Log Action, and specify which variables to write to the Event Log, such as the file name.
10. Click **Apply** to save the Event Rule.

Cryptography: OpenSSL Action

You can configure an OpenSSL action in an event rule to sign or verify a file.

The OpenSSL action is supported on HTTPS and SFTP and can be used for the following triggers:

- Scheduler (Timer)
- Folder monitor
- File Uploaded
- Verified Upload Succeeded events

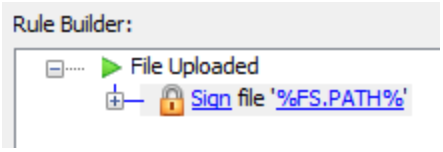
EFT can only create detached signature files; however, it can verify signatures for non-detached, detached, and XML Enveloped signature files.

The signing certificate formats include:

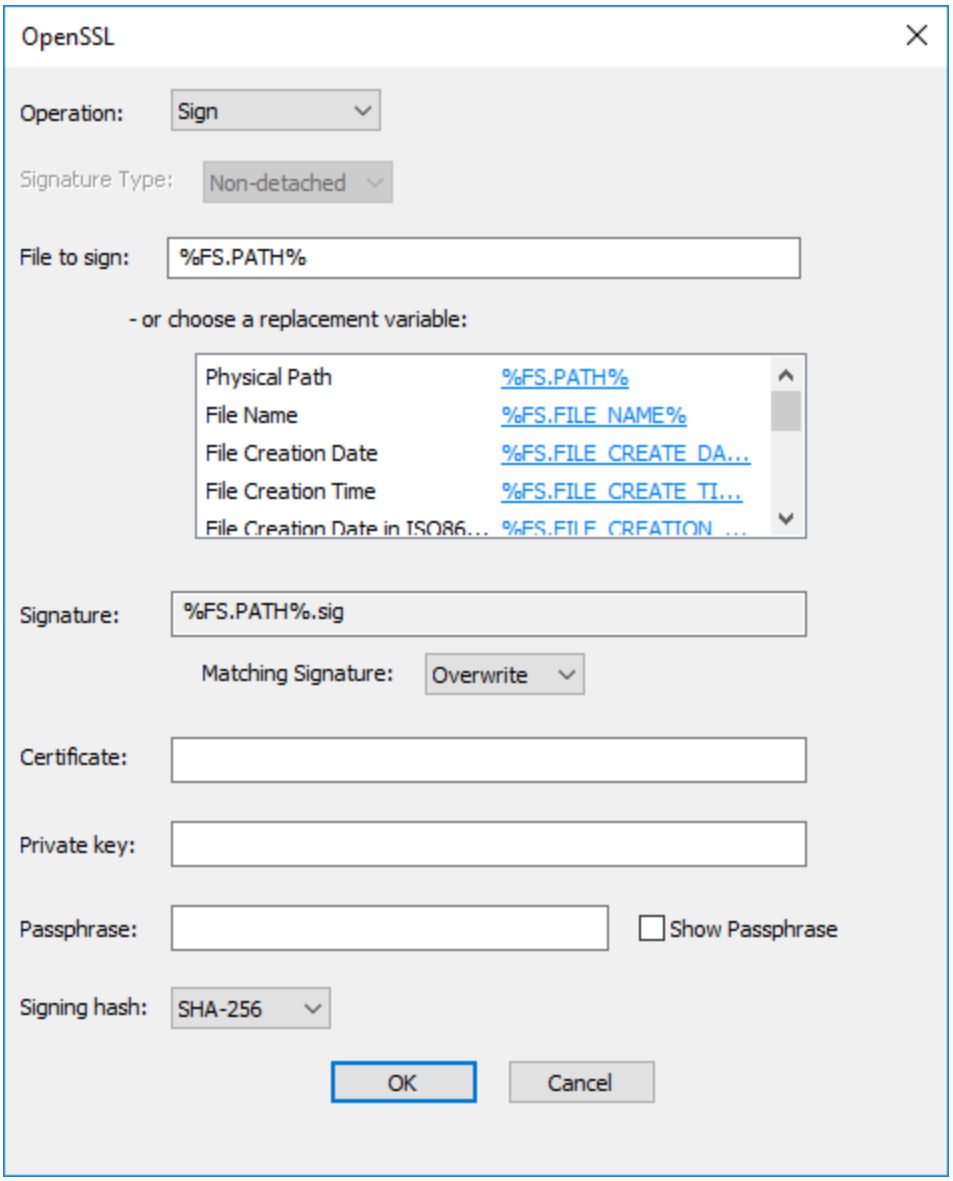
- .pem
- .cer, .crt, .der – in binary DER form only
- .p7b, .p7c – PKCS#7 SignedData structure without any data, just the certificate
- .p12 – PKCS#12, may contain certificate(s) (public) and private keys (password protected)
- .pfx – PFX, predecessor of PKCS#12 (usually contains data in PKCS#12 format, e.g., with PFX files generated in IIS)

To use the Cryptography: OpenSSL action

1. Create an event rule (or use existing rule) and add the action to the event.



2. Click one of the linked items. The **Open SSL** dialog box appears.



3. In **Operation**, click the drop-down list and click **Sign** or **Verify Signature**. The available fields change depending on whether you choose **Sign** or **Verify Signature**.
4. If you clicked **Sign**, the **Signature Type** field is read-only.

> **NOTE:** EFT can only create detached signature files, however, it can *verify* signatures for non-detached, detached, and XML-Enveloped signature files.

- In the **File to sign** box, The File System variable %FS.PATH% is the default. You can chooses a replacement variable instead.

- The **Signature** field is read-only and displays the filename of the signature file path used, which is the same as the file to process, with ".sig" appended to the filename. This text box is auto-filled and non-editable.
- In **Matching Signature**, specify what to do if a duplicate signature is found: **Overwrite**, **Skip**, or **Fail**.
- In the **Certificate**, **Private Key**, and **Passphrase** fields, provide the associated certificate information.

  > **NOTE:** You cannot browse for the certificate or private key location. Instead you must copy and paste the path to the certificate and private key. EFT server must have access to the location.

- The **Show Passphrase** check box allows you to verify the passphrase was typed correctly.
- In **Signing hash**, click the applicable algorithm: **SHA-256**, **SHA-384**, **SHA-512**.

5. If you clicked **Verify Signature**, in **File to sign**, specify the file path, or click another variable in the list of replacement variables. Then specify the **Certificate** path and click **OK**.
6. Add additional actions or conditions as needed, then click **Apply** to save the Event Rule.

> **NOTE:** A context variable, EVENT.EVENT_ACTION_FAILURE_REASON, can be used to convey error information returned from the OpenSSL library to any downstream actions.

Cloud Download and Upload Actions

Cloud storage actions are used in Event Rules to copy and move files to cloud storage and/or download files from cloud storage. Clicking the cloud storage link in those actions allows you to specify the storage. When you use a Cloud Object Monitor event, the **Cloud: Download** action is added automatically. Then you can add the **Cloud: Upload** action (or other actions).

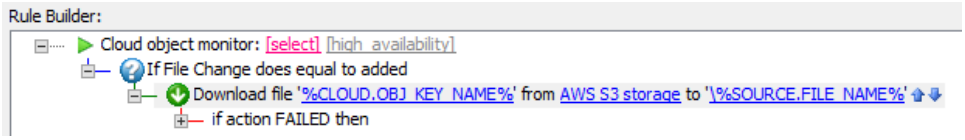
> **NOTE:** The Cloud Connector Module (CCM) is required for all cloud-based activities.

These instructions assume you have already created your cloud storage and know the connection details to provide to EFT. It is recommended that you configure your cloud connector first in a Connection Profile.

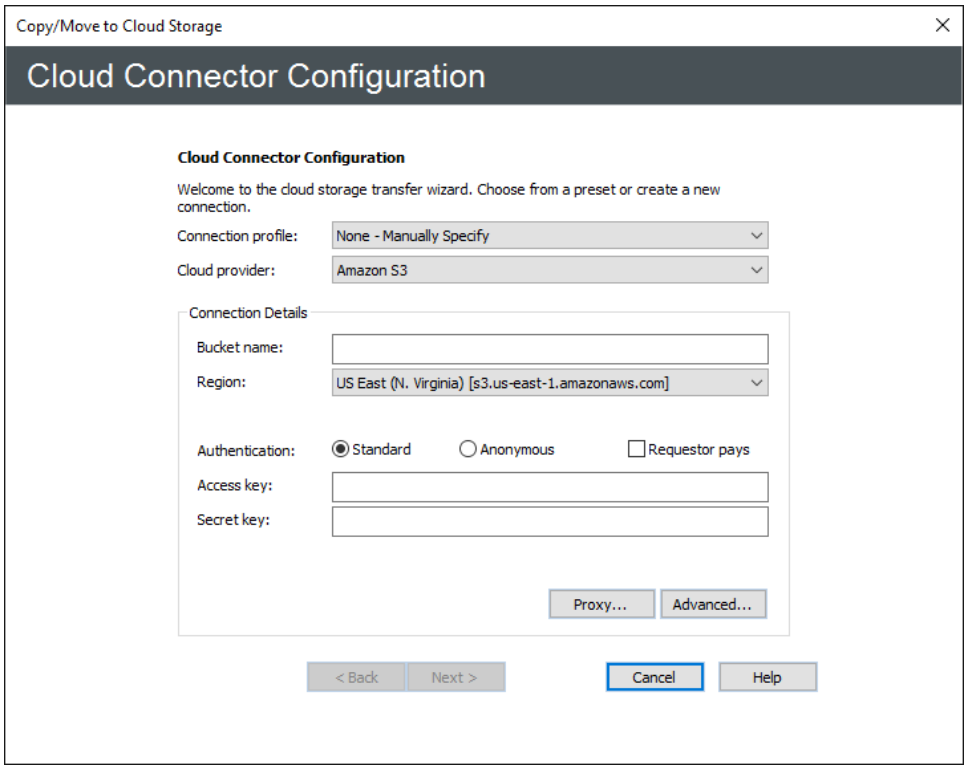
> **NOTE:** Do not confuse cloud Actions with the File Transfer module, which provides copy, move, upload, and download from non-cloud storage.

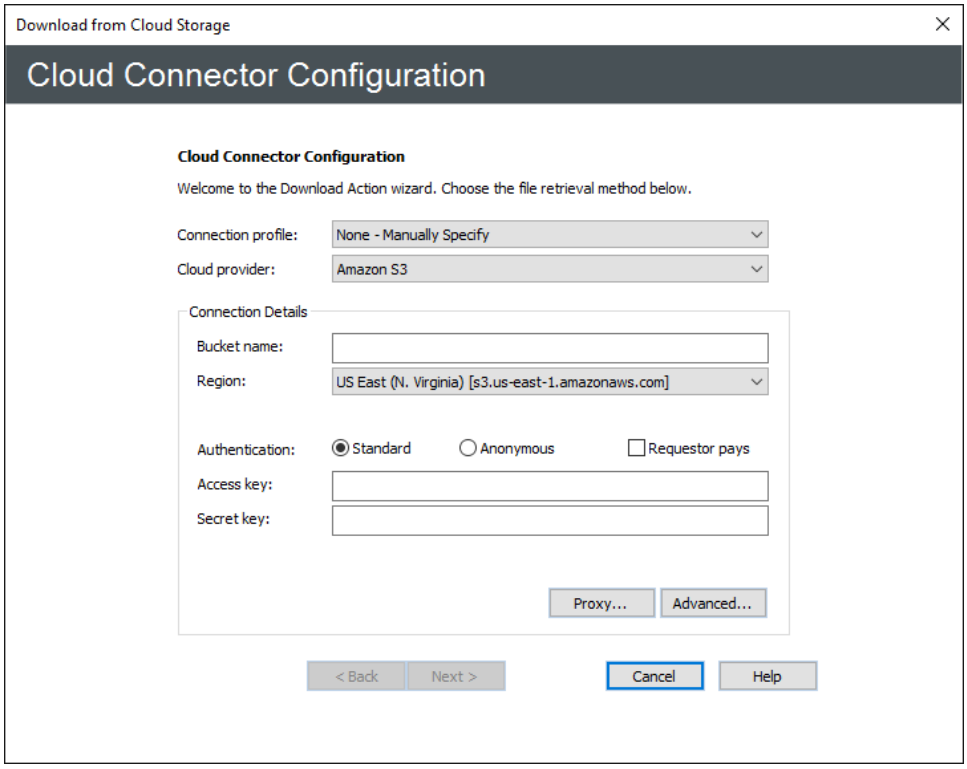
For Upload and Download actions, configure the Rule as described below

1. Follow the procedure in Defining Event Rules to add an event to the Rule Builder and then add the **Cloud: Download** or **Cloud: Upload** Action.



2. In the Rule Builder, click in the **Cloud: Download or Cloud: Upload** action. The configuration wizard appears.





3. In the **Copy/Move** and **Download** wizards, configure the **Cloud Connector Configuration** page to specify the cloud provider storage and other details, based on which cloud provider you specify. (You could configure a cloud provider

in a Connection profile to avoid having to configure connection details for every Event Rule. Refer to Defining a Connection Profile for details of connecting to cloud storage.)

4. In the **Source Object** page of the wizard, specify the source **Object name**. You can specify file names, paths, or context variables, and specify whether to **Delete object file after it is downloaded** and **If the source file is missing, treat as success**.

   > **NOTE:** You cannot browse for files in cloud storage.
   > In the **Cloud: Download Action** wizard (**Download from Cloud Storage**) on the **Source Object** page, the browse button  in the **Object name** field is not available.
   > In the **Cloud: Upload Action** wizard (**Copy/Move to Cloud Storage**) on the **Destination** page, the browse button  in the **Object name** field is not available.

5. Specify the **Destination path** for folder and filename (optional). Context variables can be used here also. You can also specify what to do with **Matching filenames** (**Overwrite**, **Skip**, or **Numerate**) and **Rename transferred file**.

Refer to the following topics for information about creating EFT Event Rules:

- Defining a Connection Profile
- Introduction to Event Rules
- Defining Event Rules
- Advanced Transfer Options

Cloud: REST-Web Services Action

(Requires CCM) The **Invoke Web Service from URL** Action can be used to integrate with an external server or application, such as auditing external systems.

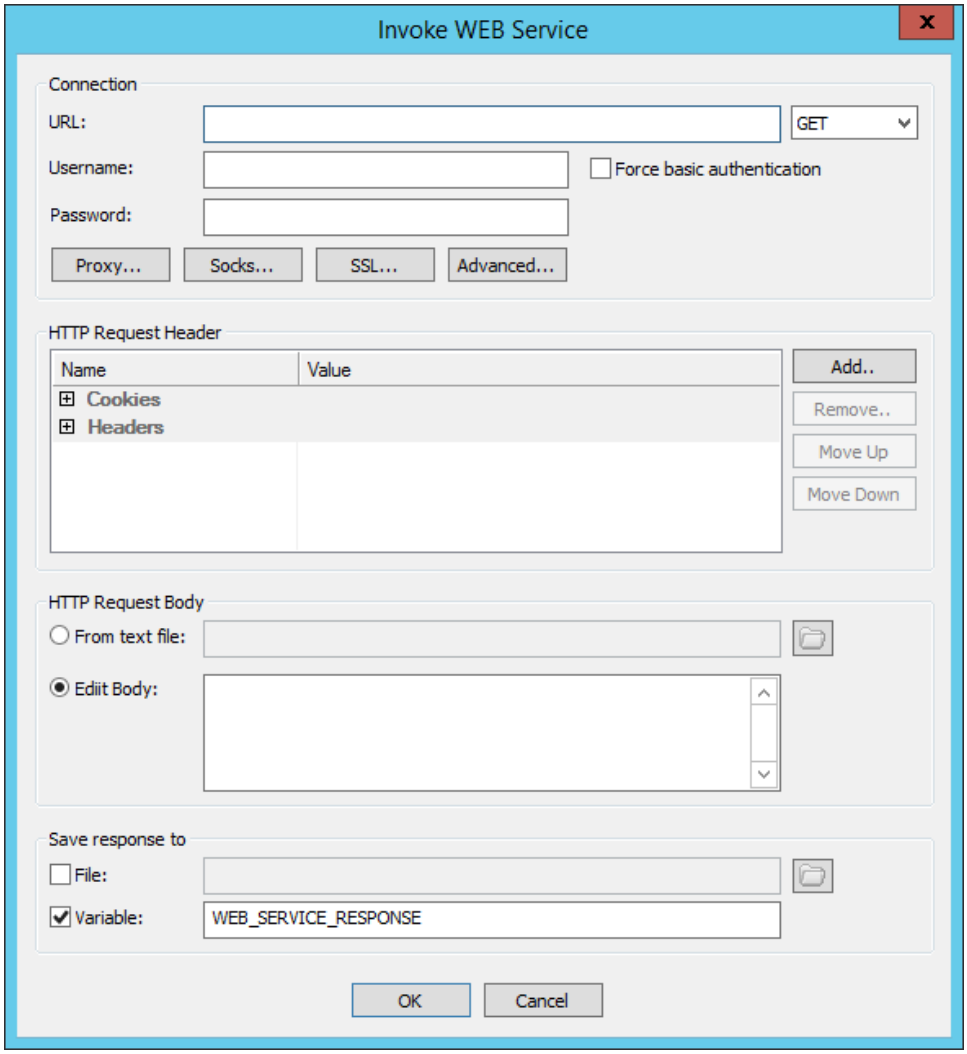
Refer to EFT Web Service for information about enabling the Web service in EFT.

The Web Service allows you to initiate an Event Rule from an external application, such as an enterprise scheduler. After the Event Rule finishes dispatching, the Web service responds with an XML document that consists of a single "Result" element. Adding an advanced property/ registry setting described in the Knowledgebase article linked below will modify the original response to add context variables that are in the XML document, from which you can then parse out values with another application.

https://kb.globalscape.com/Knowledgebase/11441/Add-Context-Variables-and-Values-to-Web-Services-XML-Response

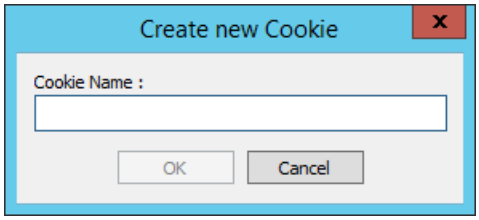
To define the Invoke Web Service Action

1. Add the Event to the Event Rule (for example, File Downloaded).
2. Add any (optional) Conditions.
3. Add the **Cloud: REST-Web Services** Action.
4. Click any links in the Action to open the **Cloud: REST-Web Services** dialog box.

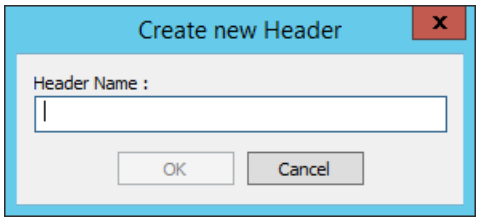


5. In the **URL** box, provide the URL on which to perform the **Invoke Web Service** Action.
6. Select the drop-down list to specify **GET**, **POST**, **PUT**, or **DELETE**.
7. In the **Username** and **Password** boxes, provide the credentials needed to log in to the URL.
    - Select the **Force basic authentication** check box, if needed.

8. (Optional) If you connect to the URL through a proxy server, click **Proxy** and then specify the **Proxy type**, **Host name**, **Port**, **Username**, and **Password**. Refer to Proxy Settings Dialog Box for details.
9. (Optional) To specify an **Authentication Type** and login sequence, in the **Proxy Settings** dialog box, click **Advanced**. The **Advanced Proxy Settings** dialog box appears. Refer to Advanced Transfer Options for details.
10. (Optional) If you connect to the URL through a Socks server, click **SOCKS**. Refer to Using a SOCKS Proxy Server for details.
11. (Optional) If you chose a protocol that uses SSL (**FTPS** or **HTTPS**), provide the client and remote server's SSL certificate information. Refer to SSL Options Dialog Box for details.
12. In the **Invoke Web Service** dialog box, in the **HTTP Request Header** area, do the following:
    - Click **Cookies**, then click **Add** to create a new cookie, provide a name for the cookie, then click **OK**.



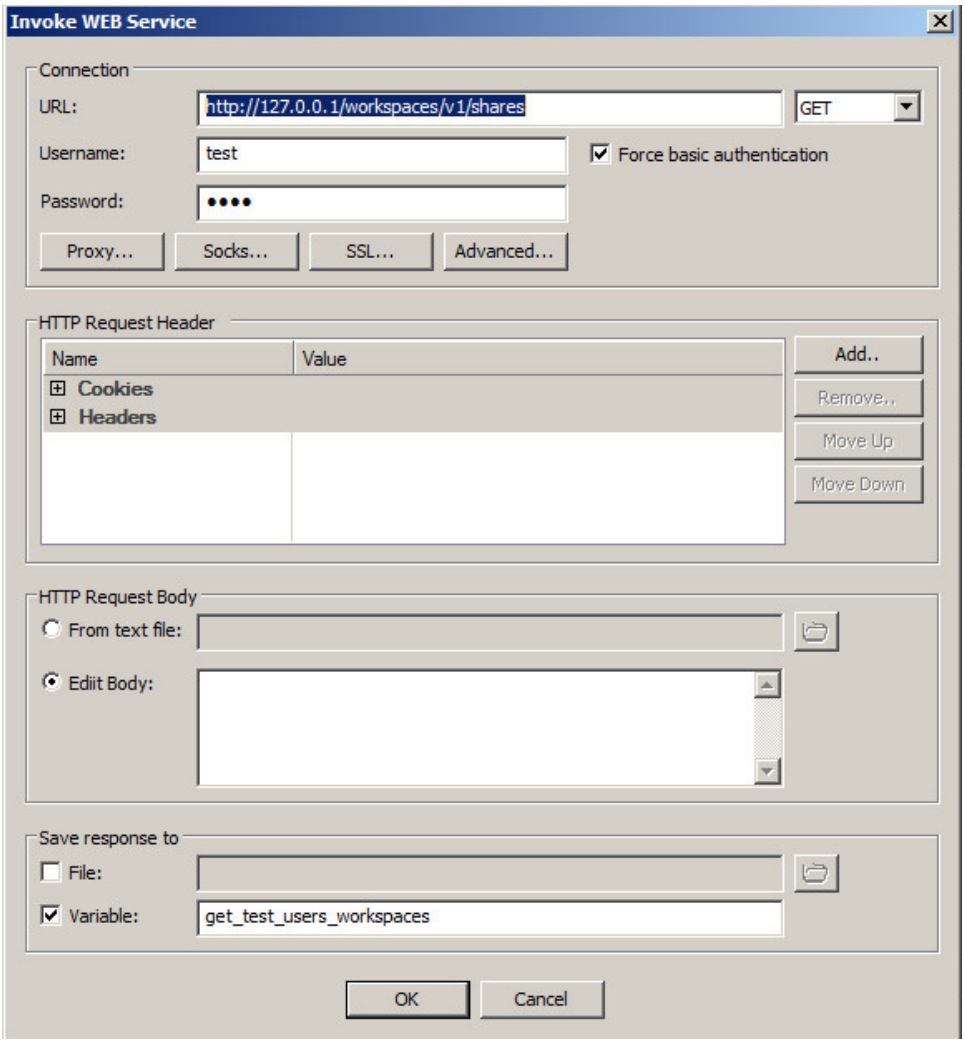
    - Click **Headers**, then click **Add** to create a new header, provide a name for the header, then click **OK**.



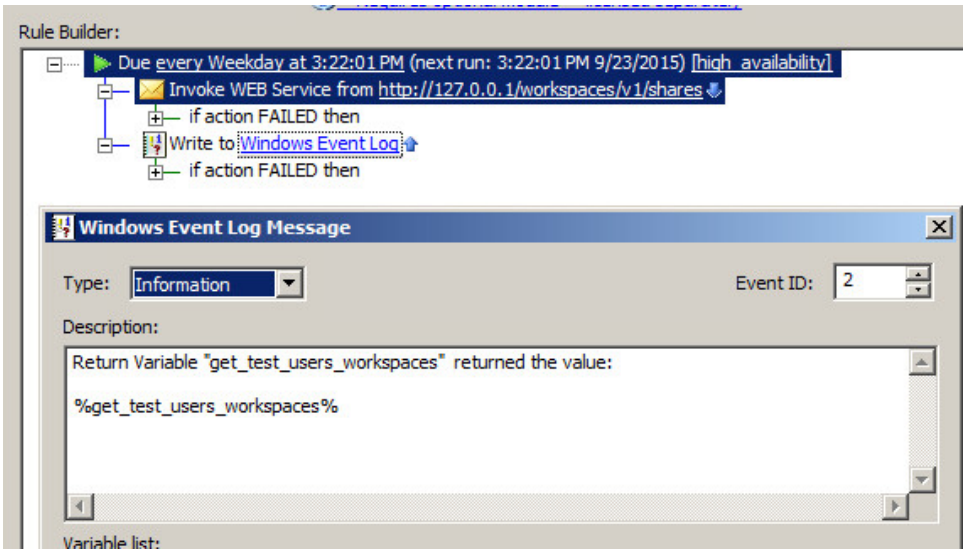
13. In the **HTTP Request Body** area, do one of the following:
14. Select **From text** file, then specify the text file from which to use the text.
15. Select **Edit Body**, then specify the text to use in the body of the HTTP Request.
16. In the **Save response to** area:
    - Select the **File** check box, then specify the name and path to the file, or click the folder icon to specify it.
    - Select the **Variable** check box, then specify the variable in the box. This variable can be anything you want, to be used in other places, such as the Windows Event Log.
17. Click **OK**.

Example:

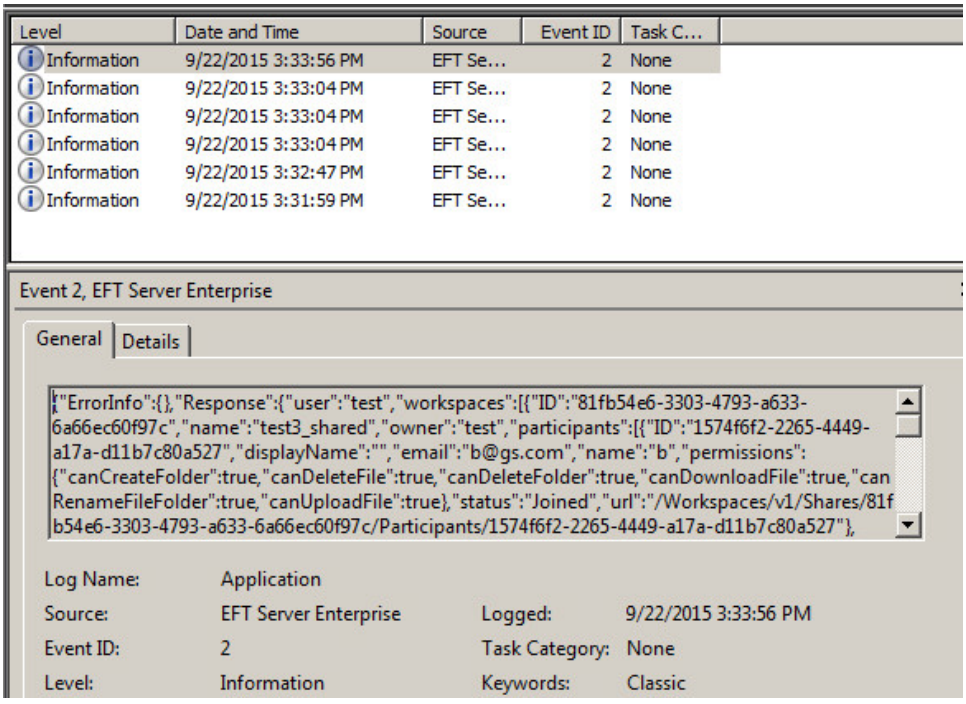
Below, the default value of `WEB_SERVICE_RESPONSE` is changed to `get_test_users_workspaces`.



You can use this variable within the same Event Rule call, such as to write to the Windows Event Log:



As shown below, when the Event is triggered, the Log reports the value of the response variable `get_test_users_workspaces`.



Azure Data Lake Storage

Azure Data Lake Storage is a highly scalable and cost-effective data lake solution for big data analytics. Data Lake Storage Gen2 extends Azure Blob Storage capabilities and is optimized for analytics workloads. EFT Event Rules allow you to store files in or monitor for added files in Azure's Data Lake generation 2 (ADLSg2), so that you can reduce cost when compared with saving files into a standard blob storage.

Containers created with ADLSg2 support can be monitored by a Folder Monitor Event as long as the Azure container credentials and Active Directory domain trust relationship is enabled.

To use a Folder Monitor Event to monitor an Azure file share, be sure to enable the VFS override and create a virtual folder that points to the Azure file share path.

EFT Secrets Primer (Knowledgebase)

From https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction:

The following are the equivalent entities, as described by different concepts. Unless specified otherwise these entities are directly *synonymous*:

Concept	Top Level Organization	Lower Level Organization	Data Container
Blobs – General purpose object storage	Container	Virtual directory (SDK only – does not provide atomic manipulation)	Blob
Azure Data Lake Storage Gen2 – Analytics Storage	Container	Directory	File

EFT Web Service

The Web Service allows administrators to initiate EFT 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.

The procedures below provide instructions to:

Enable the Web Service in EFT

Use the Invoke Web Service Action

- Access to Web Service requires authentication with a COM-enabled Server administrator account; without proper authentication and COM privileges, EFT returns a `401 Unauthorized HTTP error` to the requestor.
- An SSL certificate is required to use Web Service, because EFT sends the HTTP Web Services requests via HTTPS. (Specify SSL versions and ciphers before enabling SSL connections. SSL must first be enabled on EFT and the Site.)
- The Web Service is enabled in the Site's **Listener Settings** area. EFT 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.
- EFT 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 service that is hosting the web service.
- Requests to any /WebService URL is logged to the text log and ARM system just as any other HTTP request.
- The Web Service timeout is set to 60 seconds. You can change the timeout value with the advanced property described in https://kb.globalscape.com/KnowledgebaseArticle10553.aspx.

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. This page is generated from an HTML page in EFT installation folder, in a subfolder called **WebService**.

By default, the following files are installed in: **C:\Program Files\Globalscape\EFT Server\Web\WebServices**

- **\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.

- **\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.)

How EFT Supports the Web Service

EFT 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." 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 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.

HTTP GET

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

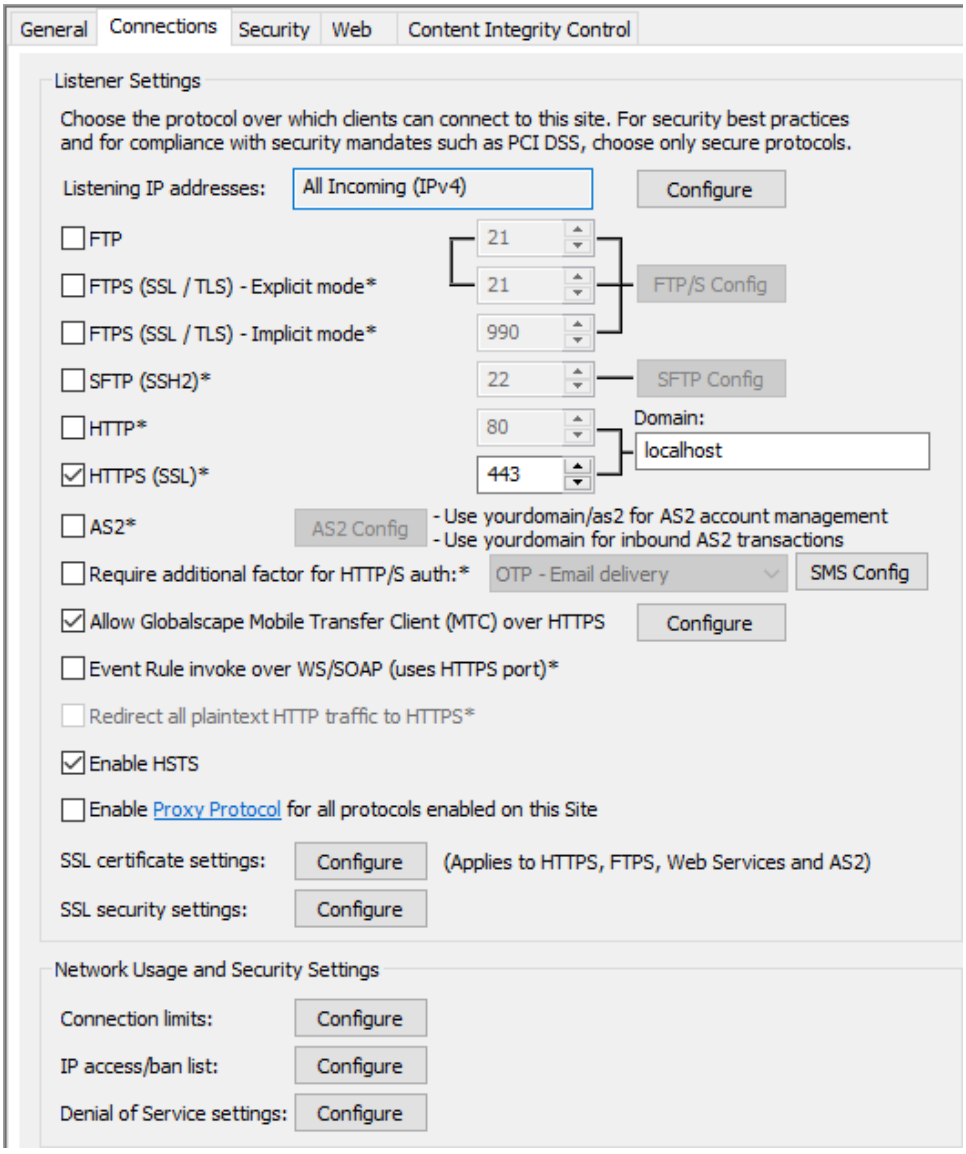
```
POST /WebService/InvokeEventRule HTTP/1.1 Host: localhost
Content-Type: application/x-www-form-urlencoded Content-Length:
length EventRuleName=string&EventParams=string

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>
```

To enable the Web service in EFT

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



4. Select the **Event Rule invoke over WS/SOAP (uses HTTPS port)** check box.

IMPORTANT: If this is not enabled, you will not be able to log in to the Web

> Service.

5. Click **Apply** to save the changes on EFT.

To use the scripts for testing Web Service

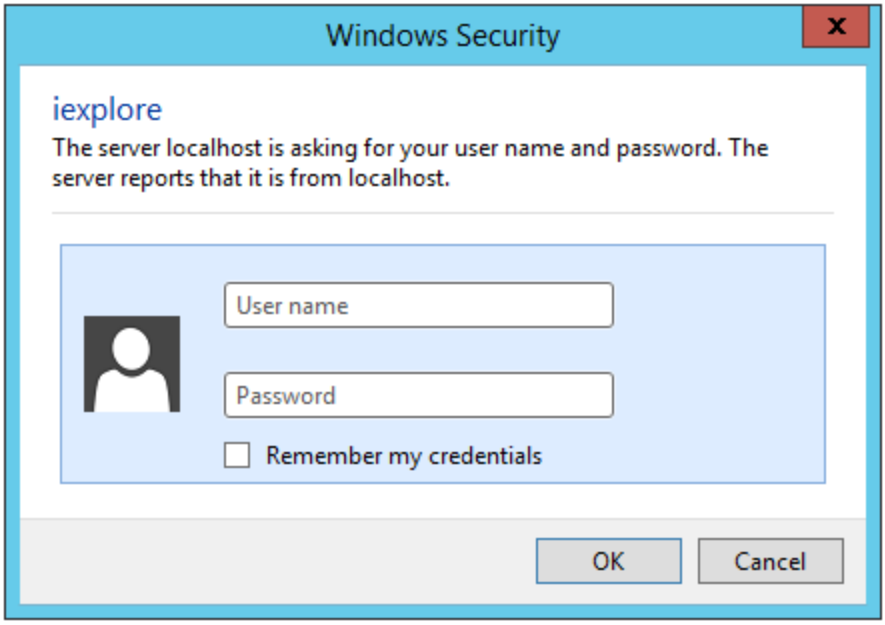
- **EFT.InvokeEventRule.ps1** uses regular output -1, 0 or 1 (classic SOAP)
  - Change the various strings at the top for host, administrator username, password, and event rule name.
- **InvokeEventRule.ps1** returns all context variables from the rule (behaves a bit more REST like, even though the response is XML, not json).
  - Add the advanced property "EventWebServiceResponseAddContextVariables" to the AdvancedProperties.JSON file. You must set this property to get the payload from EFT in response showing the context variables.
  - Change the administrator username and password various strings at the top of the script.
  - Modify the Invoke-WebRequest method, including the host, event rule name, and optional parameters.

To execute an Event Rule using Web Service

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

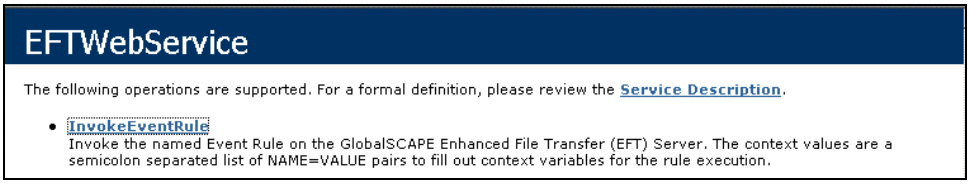
   > **IMPORTANT:** You must change the URL of the Site and the port number if you are not using "localhost" and port 443, as shown below!

2. A login prompt appears. Provide a COM-enabled Server administrator account login credentials. If the **Event Rule invoke over WS/SOAP (uses HTTPS port)** check box is not enabled on the Connections tab of the Site, you will not be able to log in to the Web Service.

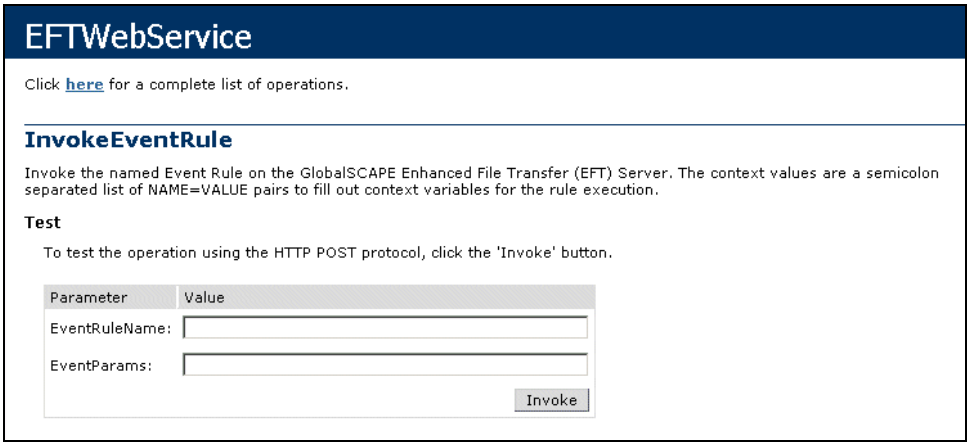


IMPORTANT: EFT leverages the USER https port (443 by default); however, WebService uses the Server administrator account login credentials, not USER credentials!

3. The EFTWebService interface appears.



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



5. In the **EventRuleName** box, type the name of the Event Rule.
6. In the **EventParams** box, type one or more variables, separated by semicolons.

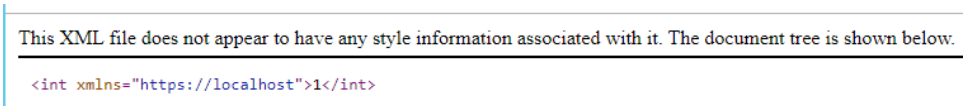
7. Click **Invoke**. The Event Rule is executed.

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

   For example, in the **EventRuleNameValue** box, type `Backup and Cleanup`. Leave **EventParams** blank, and then click **Invoke**. The browser returns the following string:

   ```
   <int xmlns="HTTPS://localhost:443/">1</int>
   ```

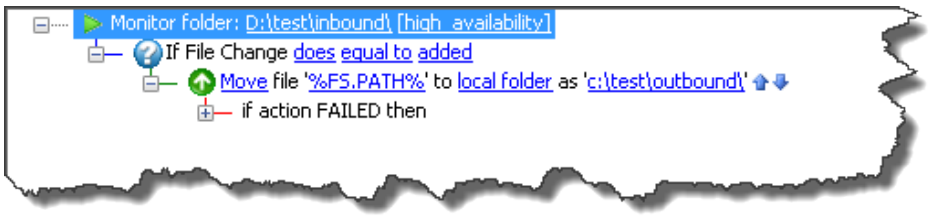
   - 0 indicates failure
   - 1 indicates success
   - -1 indicates EFT could not find the Event Rule (for example, the requested EventName does not exist or was not typed correctly.)

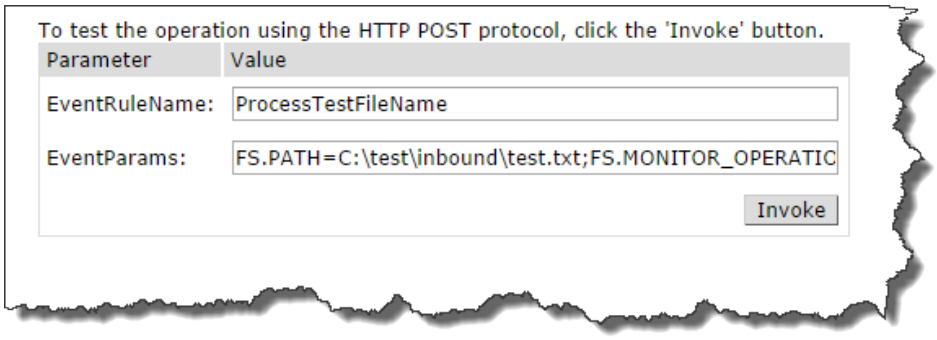
   

   For this example, you can open the **/Backup/** folder and see that a backup file was created (for example, **C:\ProgramData\Globalscape\EFT Server\Backup**).

Using Web Service Examples

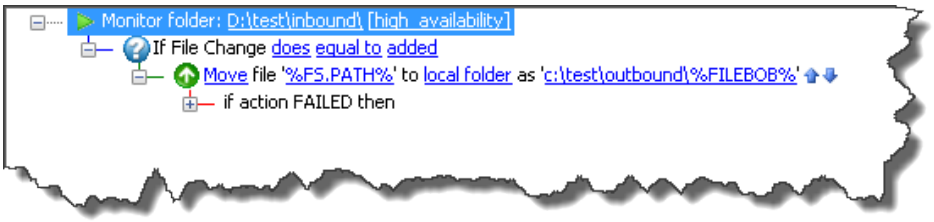
Folder Monitor






```
EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
OPERATION=added
```

As you can see, the FS.MONITOR_OPERATION is part of the Condition and must be passed along with the variable of choice; in this case it is FS.PATH or any other variable that is created.




```
EventParams=FS.PATH=C:\test\inbound\test.txt;FS.MONITOR_
OPERATION=added;FILEBOB=test.filebob.txt
```

As you can see above, the variable is a custom variable applied to this event rule, outside of the EFT variables.

Timer Event

EventParams=FILEBOB=test.filebob.txt

The Timer Event is the least used Event Rule in EFT to download files, move them, or to automate an Advanced Workflow Script/custom command. Using the Web Services allows you to manipulate custom variables for the specific environment or file that needs to be processed. In the case above, the Timer event is being used as a transmission only, triggered by a remote process using “wget”.

Passing the URL to WebServices

As the HTTP GET states:

```
GET
/WebService/InvokeEventRule?EventRuleName=string&EventParams=str
ing
 HTTP/1.1
```

Based on this information, the URL should contain the following:

- **EventRuleName**=ProcessTestFileName
- **EventParams**=FS.PATH=C:\test\inbound\test.txt;
- **FS.MONITOR_OPERATION**=added

Combine the parameters:

```
http://localhost/WebService/InvokeEventRule?EventRuleName=Proce
ssTestFileName&EventParams=FS.PATH=C:\test\inbound\test.txt;FS.
MONITOR_OPERATION=added
```

> **NOTE:** The ampersand “&” is used to separate the **EventRuleName** and **EventParams**, but you will use the semi-colon (;) to separate more than 1 **EventParams** that is required to make the Event Rule work correctly.

Compression Action

(Requires EAM) Occasionally, users might upload or download files that need to be compressed (for example, zipped) or decompressed (for example, unzipped) before transferring. The Compress/Decompress Action can be used to compress and decompress files. You can compress/decompress the following formats: ZIP, 7Zip, GZip, BZip2, Tar, Tar and GZIP, and ZCompress. You can also enable/disable compression for files older than a defined time in days to meet PCI DSS compliance on retention and accessibility of logs.

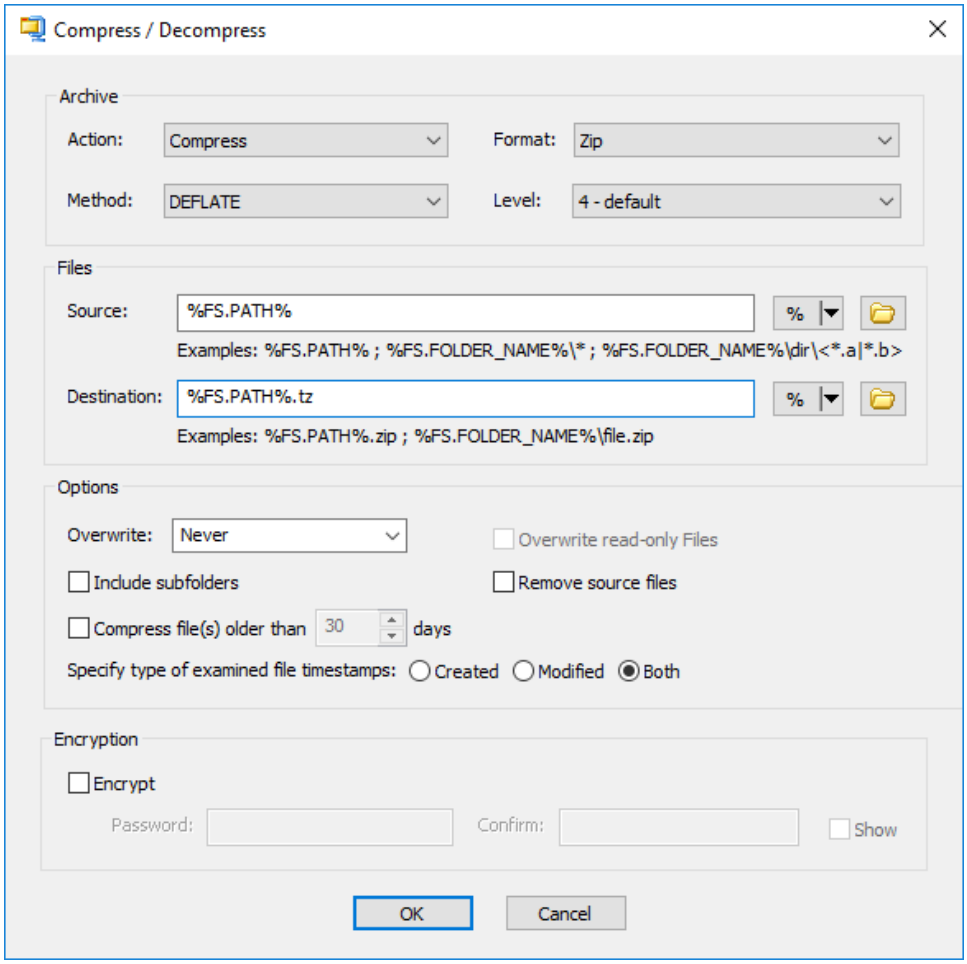
- To ensure maximum compatibility with third-party archival tools, Unicode passwords should be avoided.
- The **Source** and **Destination** file path specifications are limited to physical paths only – **virtual paths will not work for these fields**.
- For GZip format, add a trailing slash to the **Destination** path to make it explicitly clear that the destination is to be interpreted as a folder. If **Overwrite** is set to never, no error occurs, and the Action completes by removing the original GZip file.
- **Decompress Action Destination Paths and Trailing slashes (\):**

  If a user wants to decompress an entire archive and place it into a folder, using a destination path with a trailing slash (\) will always accomplish this. This is the typical use case and is shown in the example below the destination field. The only exception is if ZCompress is used, in which case the behavior is the same as for Zip, Tar, and 7zip as described below. If the trailing \ is missing, the behavior depends on the decompression format used:

  - For Zip, Tar, and 7zip archive formats it doesn't matter if the trailing \ is there, because the path will always be treated as the folder in which to decompress the entire archive. The exception to this is if the "< >" syntax is used where individual archive files and their destinations paths can be specified.
  - For Gzip, Bzip2, and "Tar and Gzip" (and ZCompress with or without trailing \) archive formats, only a single file whose name is the last part of the destination path will be extracted, decompressed, and saved into the parent folder specified in the destination path. So, if the destination path is given as "c:\myFolder\myFile", then a file named "myFile" will be extracted from the specified source archive, decompressed, and placed in "c:\myFolder" (with the same name).

To compress or decompress files using Event Rules

1. Add the Event to the Event Rule (for example, File Downloaded).
2. Add any (optional) Conditions.
3. Add the **Compression** Action.
4. Click any links in the action to open the **Compress/ Decompress** dialog box.



5. In the **Action** list, click the desired Action: **Compress** or **Decompress**.
6. In the **Format** box, specify the format in/from which to compress or decompress the file: ZIP, 7Zip, GZip, BZip2, Tar, Tar and GZIP, and ZCompress.
7. If the **Compress** Action is specified, in the **Method** list, specify the **Method**: Deflate or PPMd.
8. If the **Compress** Action is specified, in the **Level** list, specify a level of compression to apply, from **0 - fastest** to **6 - densest**.
9. If the **Decompress** Action is specified, the **Method** and **Level** lists are unavailable.

10. In the **Files** area, specify the **Source** and **Destination** paths. (As noted above, only physical paths should be specified; virtual path will not work.)
    - Select the variable drop-down list (percent sign **%**) to specify a context variable. You can specify more than one and use wildcards, as shown in the examples.
    - Select the folder icon to browse to a folder. Add a trailing slash to the **Destination** path to make it explicitly clear that the destination is to be interpreted as a folder.
11. In the **Options** area, the **Overwrite** options (Never, **Always**, **If Newer**). **If Newer** is available when the Decompress Action is specified.
12. Select the check boxes to specify whether to **Include subfolders** (for Compress Action), **Overwrite read-only files** (for Decompress Action), and/or **Remove source files** after decompressing or compressing the file.
13. To compress files based on age, select the **Compress file(s) older than <n> days** check box and provide the number of days (default is 30 days), and next to **Specify type of examined file timestamps**, specify **Created**, **Modified**, or **Both** (the default is Both).

    > **NOTE:** The purpose of compressing older files is to move the compressed files to an archive folder (in a subsequent action or event rule) to meet PCI DSS 10.7 to retain audit trail history.

14. If encryption is desired, select the **Encrypt** check box and then specify and confirm the password. Select the **Show** check box to see if you've entered the password correctly.

Also refer to the following properties the ICICompressActionParams interface in the COM API

- Property **AllowOperationForOldFiles** As Boolean
- Property **KeepOldFilesInDays** As Long
- Property **TimestampTypeForOldFiles** as CompressTimestampType
- Enum **CompressTimestampType**

In the Backup and Cleanup event rule in EFT:

- Compress file action is added to the beginning of the event rule
- Compress files option is enabled with a default value of 90 days
- Type of examined file timestamps is set to “Both” by default
- “Cleanup in folder” is in EFT logs
- Number of days after which the file will be deleted in Cleanup action is only for the Logs folder. The default value is 275 days (previously 30 days)

Export to Dataset and Import CSV from Dataset Action

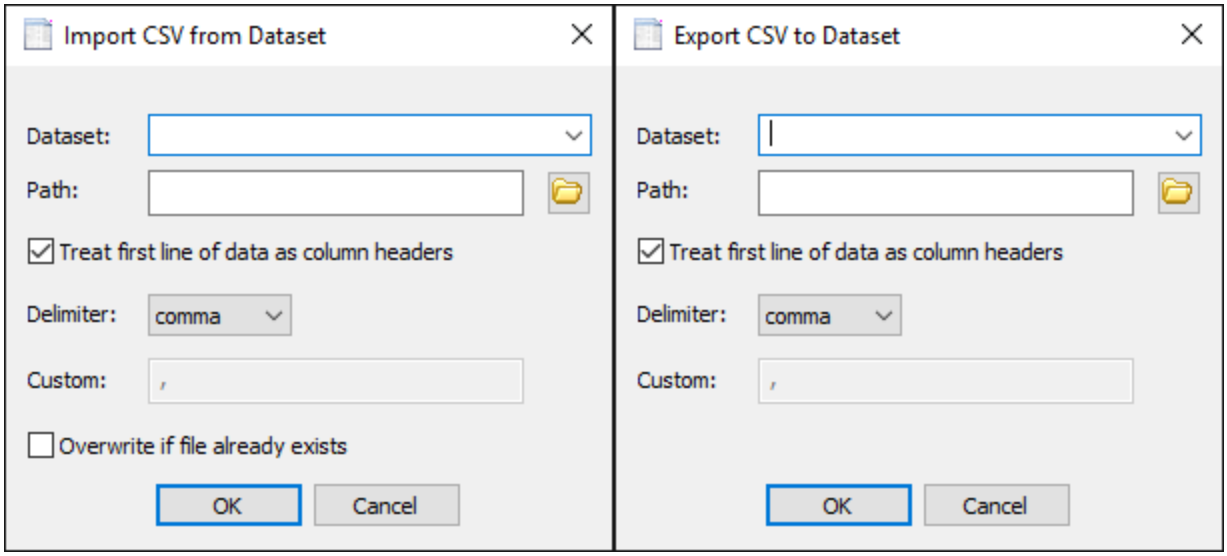
(Requires EAM) These CSV import/export actions can be used to move tabular data between programs that operate on incompatible, proprietary formats.

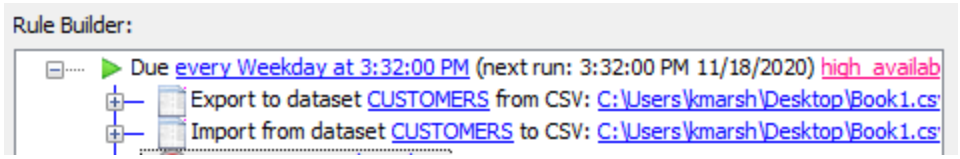
The **CSV: Import from Dataset** Action reads data from a comma-separated values (CSV) file, and populates the specified dataset with those values.

The **CSV: Export to Dataset** Action can be used in conjunction with Protocol: Listing to Dataset Action and Loop: Dataset (or with an existing dataset) to create a CSV file, which can then be used in other applications.

Refer to Datasets in Event Rules for information about using datasets in Event Rules.

In the **Dataset** drop-down in the **Export CSV** Action, do not specify a non-existent dataset, especially if you do not plan to dynamically create that dataset in the script via other means (such as PowerShell). If you specify a non-existent dataset, the action will fail and an error will appear in the EFT log (Export failed. Error: Dataset does not exist.)





CSV file format is not standardized; EFT allows multiple-character delimiter without any length limit. If the **Treat first line of data as column headers** check box is cleared, the dot notation for referencing the fields in records will be: Column0, Column1, Column2, and so on. For example, %Customer.CurrentRow.Column0%.

File Operation Action

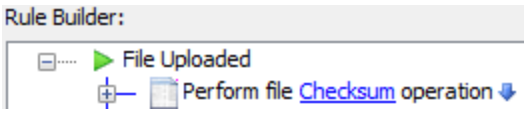
(Requires EAM) The File Operation Action is used to read, write, rename, delete, concatenate, or perform a checksum on files.

The COM API has been modified to address the changes to the File Operation Action. As a result, some COM objects are no longer supported as of version 8.0.5: ICIFileActionParams: Operation, Path, IncludeSubdirsFlag, Contents, Encoding, OverwriteOption, NewNameMask, ExclusionMasks, and UseExclusionMasksFlag.

Refer to the COM API reference for details.

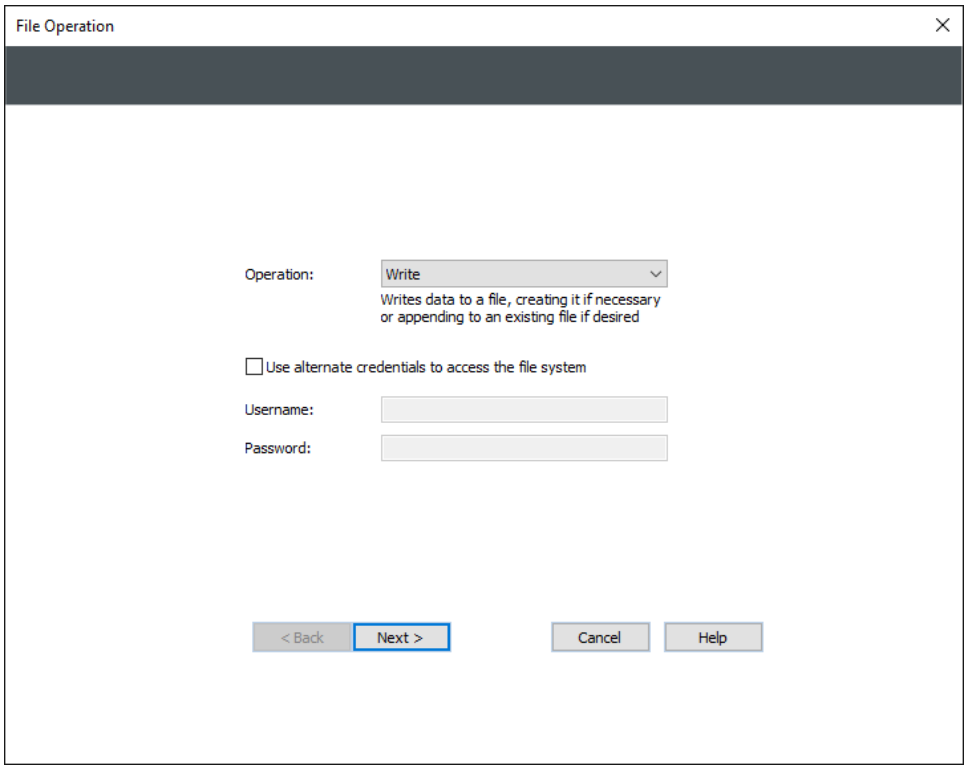
To define the File Operation Action

1. In the right pane, in the **Actions** list, add the **File: Operation** Action to the rule, then click the link in the rule to open the **File Action** dialog box. The Action appears in the Event in the **Rule Builder**.



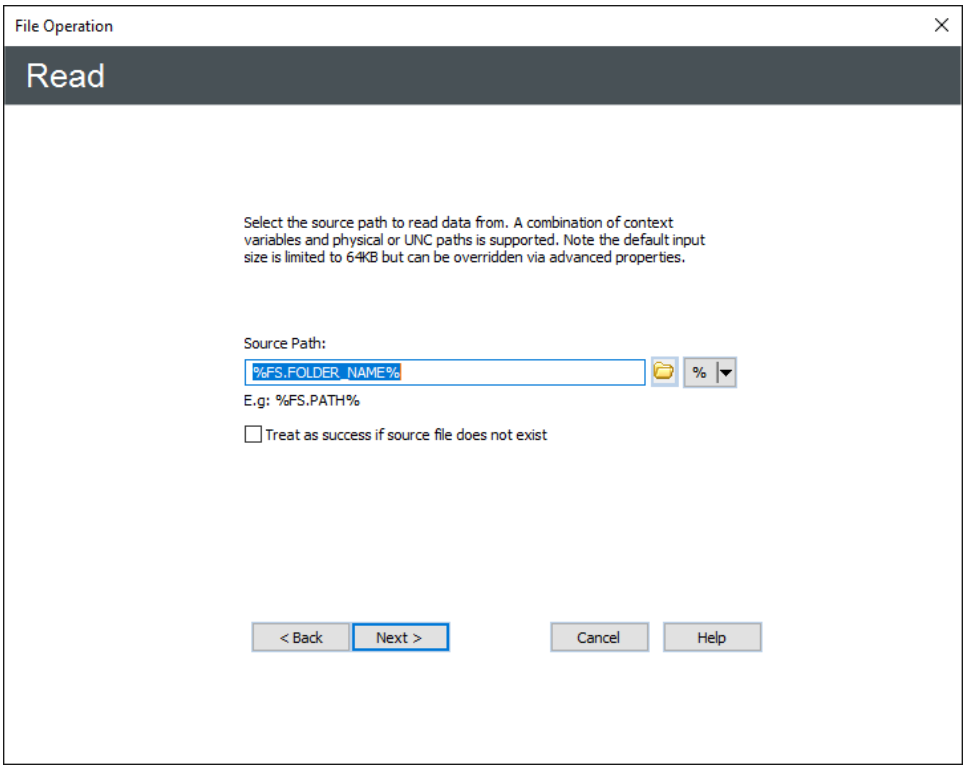
2. Select the linked text (blue or red) to specify parameters for the Action.
3. In the **Operation** list, click an operation:
    - **Read** - Read data from a file into a variable for processing (see note below)
    - **Write** - Write data to a file, creating the file if necessary, or appending to an existing file (see note below)
    - **Rename** - Rename and keep original (Copy) or remove the original (Move)
    - **Delete** - Delete one or more files
    - **Concatenate** - Concatenate the contents of two or more files and outputs the result onto a destination file
    - **Checksum** - Obtain the hash for a file, which is useful for integrity checking

    By default, the File Action can only read or write 64KB of data. If you want to read and write more than 64KB, you will need to add the advanced properties MaxFileActionReadSize and MaxFileActionWriteSize and set the limits to how much you want to read/write. Refer to Advanced Properties for details.

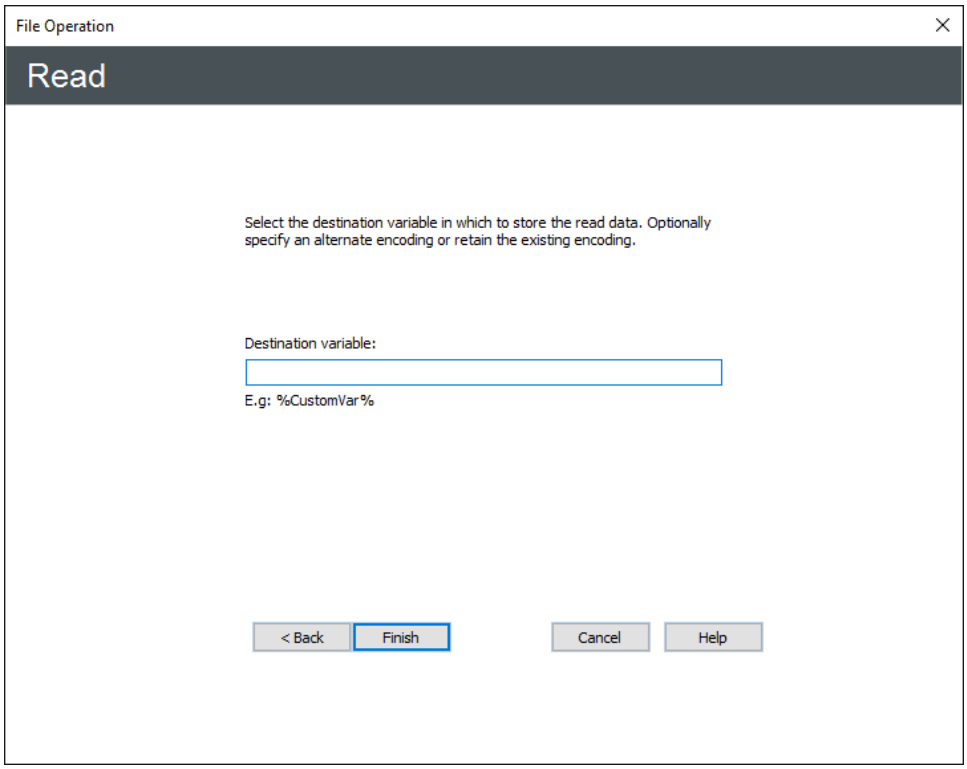


4. (Optional) Select the **Use alternate credentials to access the file system** check box, then provide the **Username** and **Password** needed to log in. Otherwise, it will use the EFT server service account.
5. Click **Next**. The next page that appears depends on the operation selected, as shown below.
6. After defining the Action, click **Apply** to save the Action.

Read

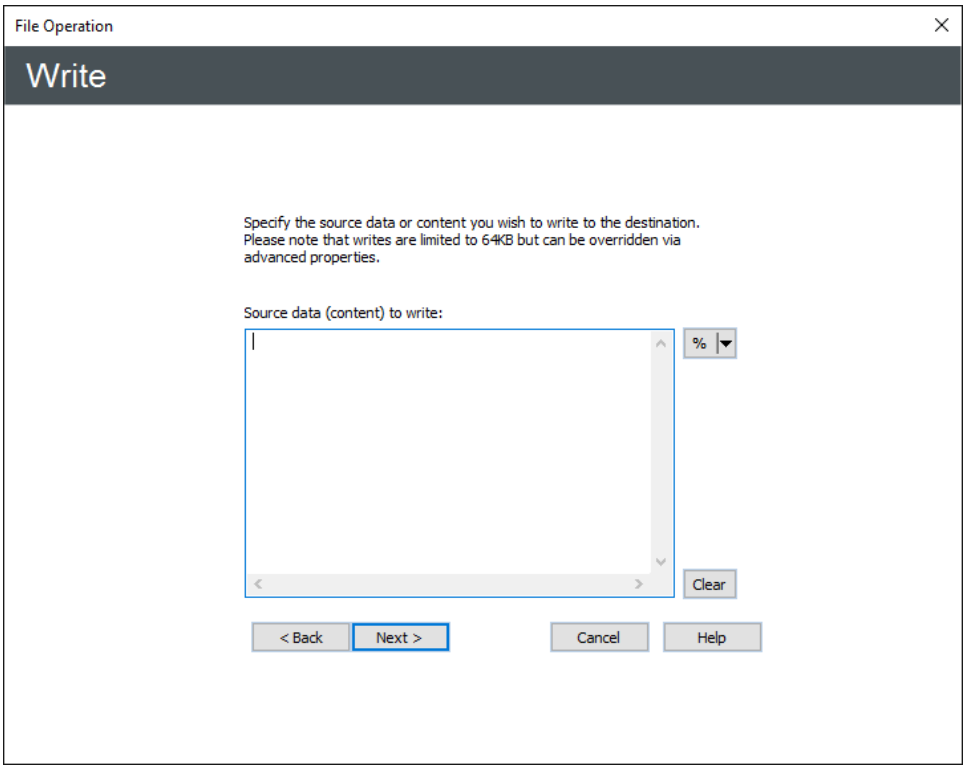


a. Specify the **Source path** with variables or by selecting the folder icon and browsing.
b. Select the **Treat as success if the source file does not exist** if you don't want this action to counted as a failure in that case.
c. Click **Next**.

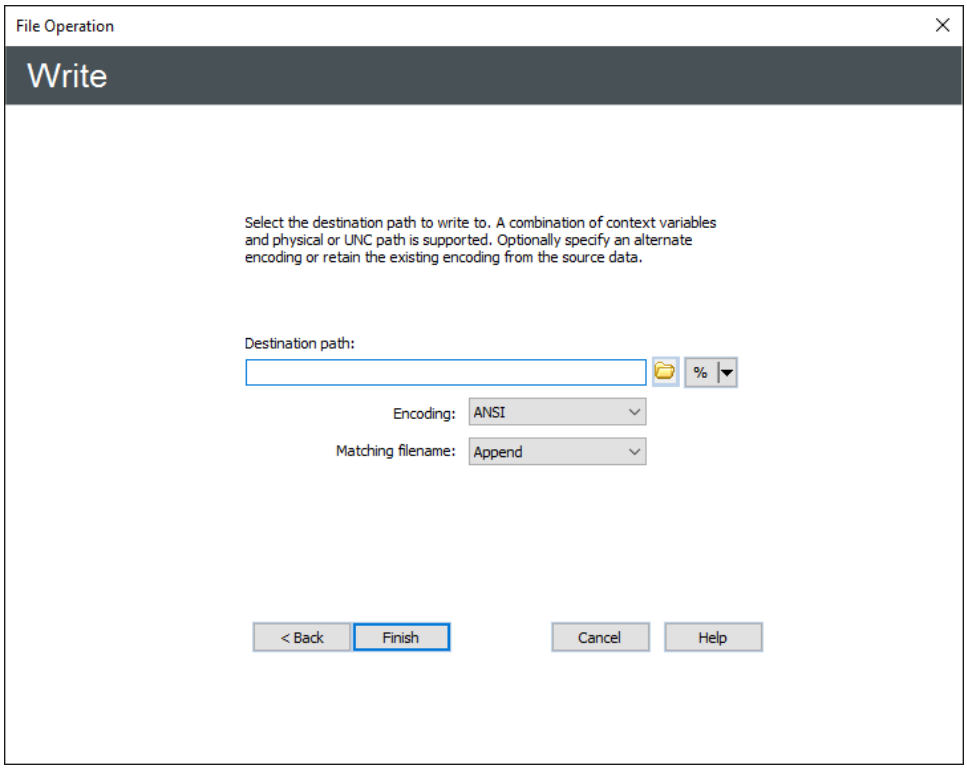


d. Specify the **Destination variable** into which to store the read data, then click **Finish**. Refer to Flow: Variable Action for details of creating variables.

Write



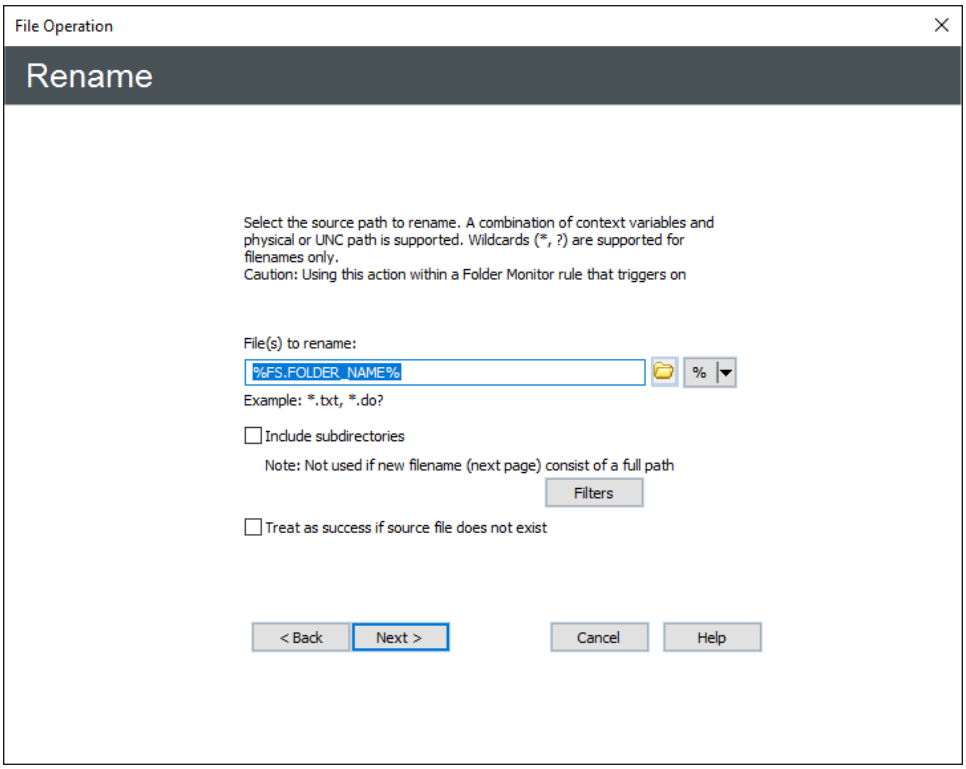
a. In the **Source data** box, specify the source data or content that you want to write to the destination. Writes are limited to 64KB, but that can be overridden via advanced properties. Use the variable (%) drop-down list to add EFT variables, such as %FS.FILE_NAME%. Click **Next**.



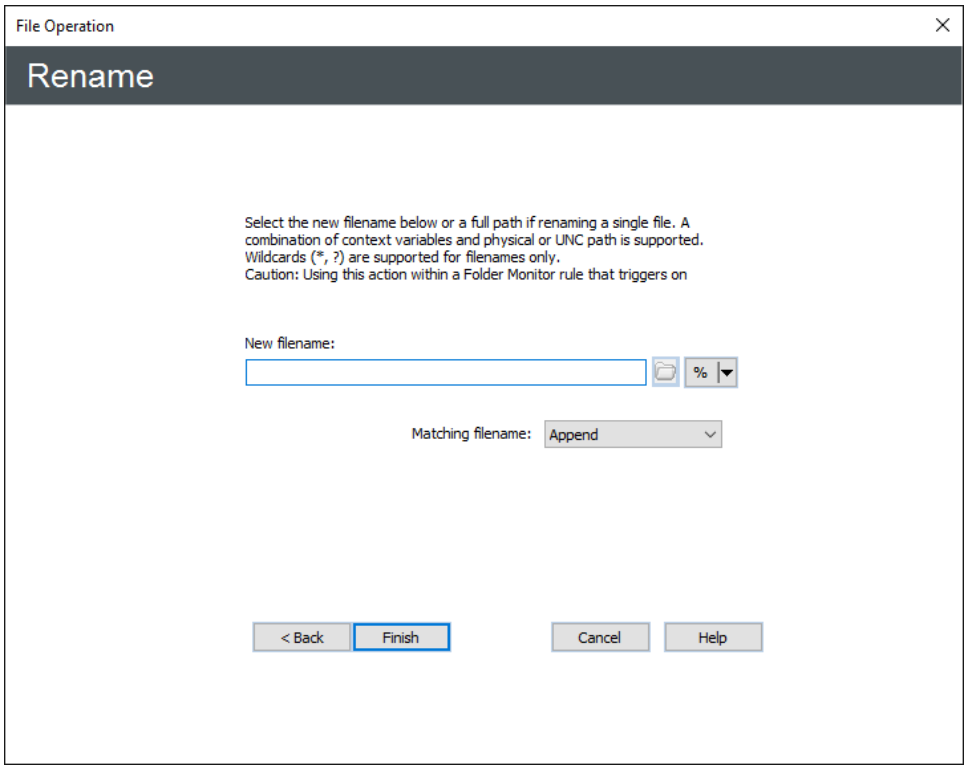
b. Specify the **Destination path** with variables or by selecting the folder icon and browsing.

c. Specify the **Encoding** (**ANSI**, **UTF8**, **Unicode**, **UnicodeBigEndian**), and what to do about a **Matching filename** (**Append**, **Skip**, **Numerate**, **Overwrite**, **Fail**), then click **Finish**.

Rename



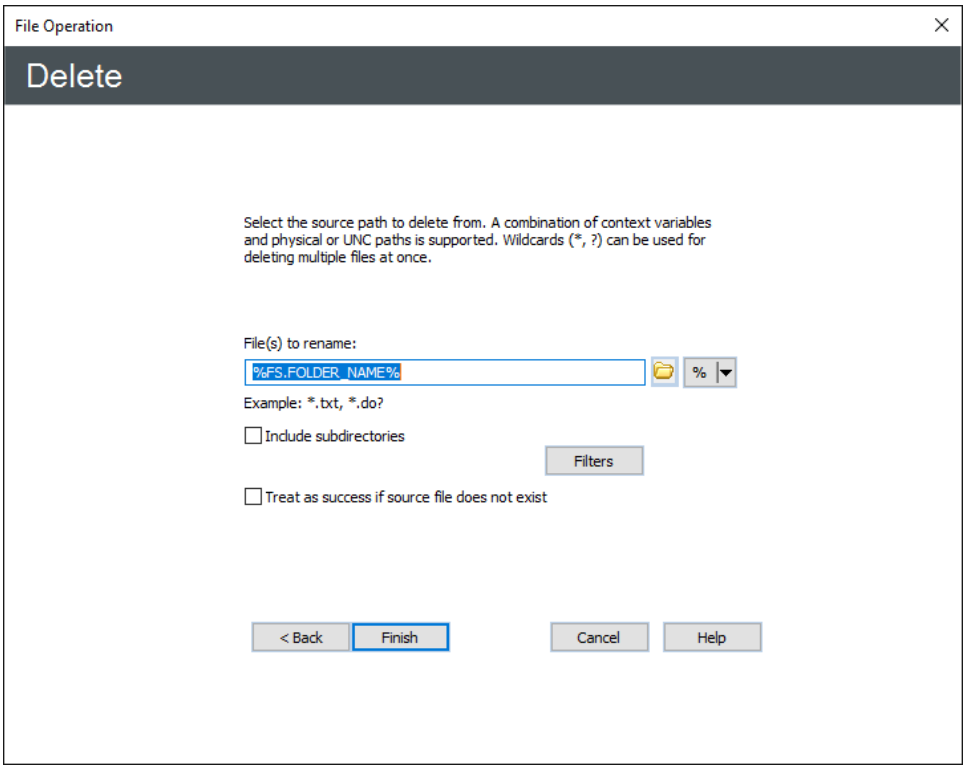
a. Specify the **File(s) to rename** with variables or by selecting the folder icon and browsing.
b. Select the **Include subdirectories** check box to rename subdirectories also. Do not select the check box if the new filename consists of a full path.
c. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
d. Click **Next**.



e. Specify the **New filename** with variables or by selecting the folder icon and browsing.

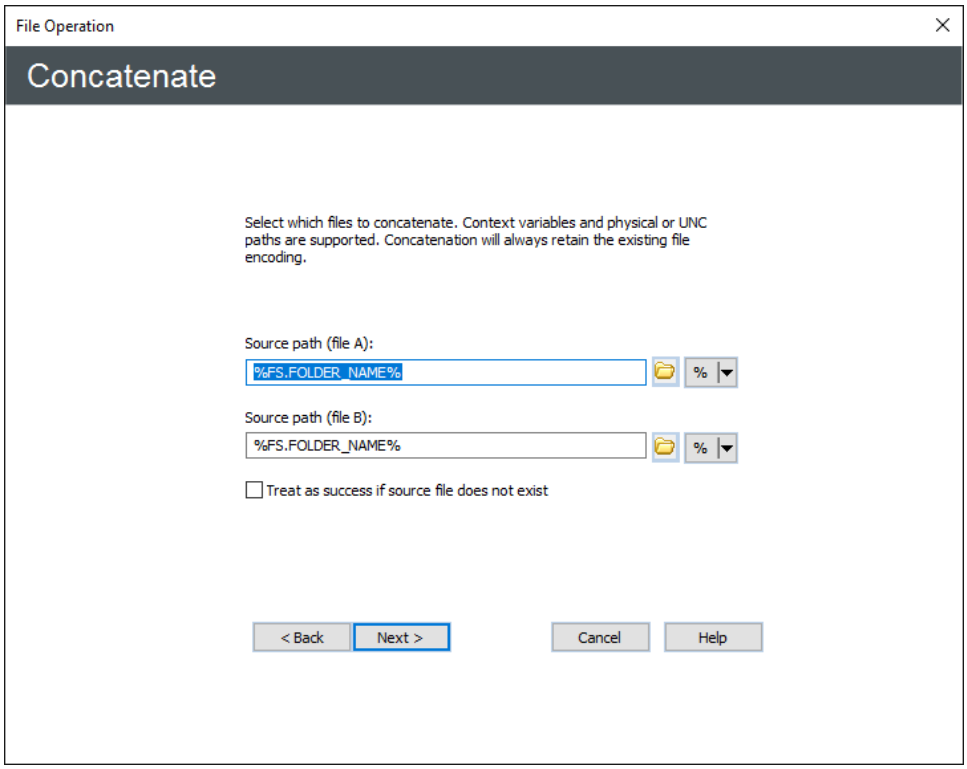
f. Specify what to do about a **Matching filename** (**Append**, **Skip**, **Numerate**, **Overwrite**, **Fail**), then click **Finish**.

Delete

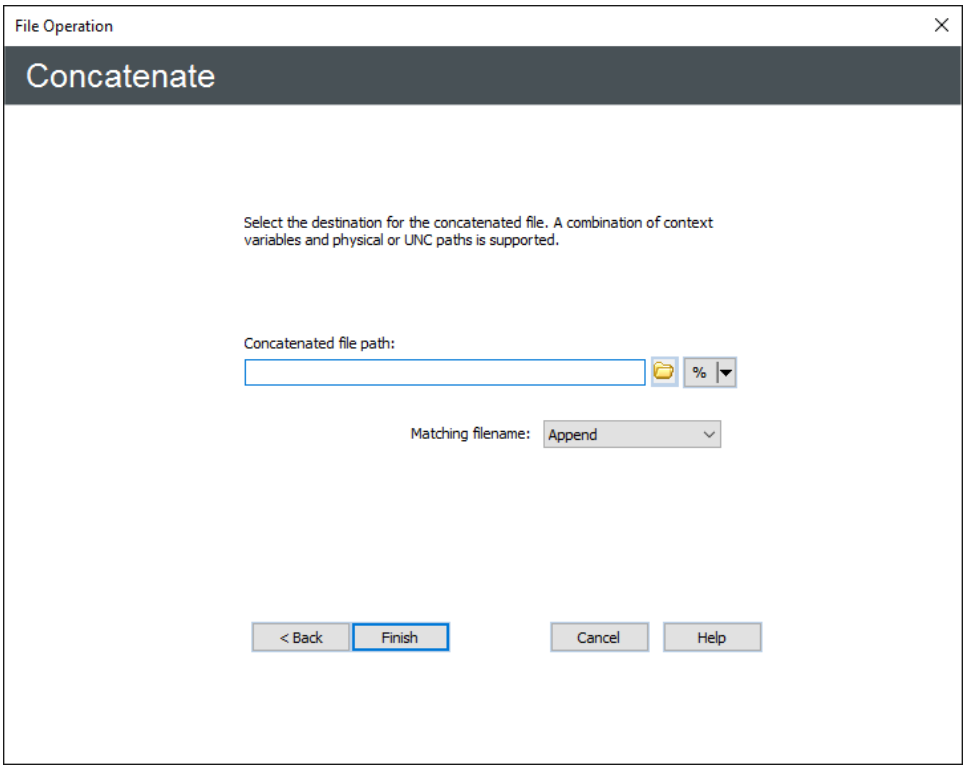


a. Specify the **File(s) to delete** with variables or by selecting the folder icon and browsing.
b. Select the **Include subdirectories** check box to rename subdirectories also. Click **Filters** to exclude one or more files. Specify multiple files and wildcards with commas. For example *.txt,*.pd?.
c. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
d. Click **Finish**.

Concatenate



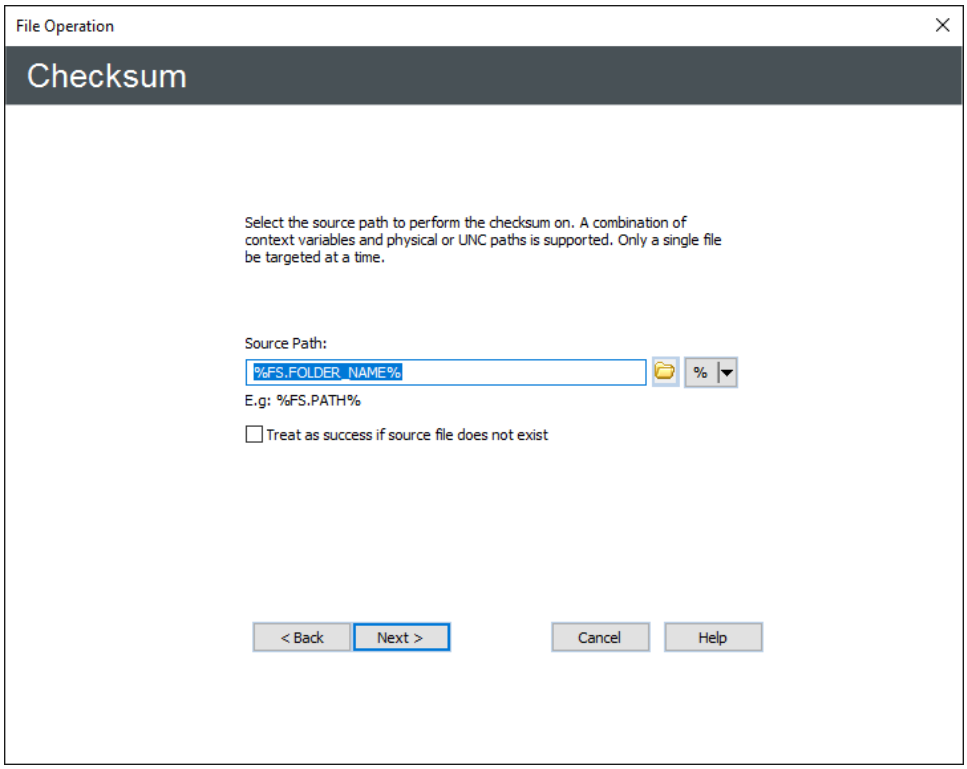
a. Specify the **Source path** for file A and file B with variables or by selecting the folder icon and browsing.
b. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.
c. Click **Next**.



d. Specify the **Concatenated file path** with variables or by selecting the folder icon and browsing.

e. Specify what to do about a **Matching filename** (**Append**, **Skip**, **Numerate**, **Overwrite**, **Fail**), then click **Finish**.

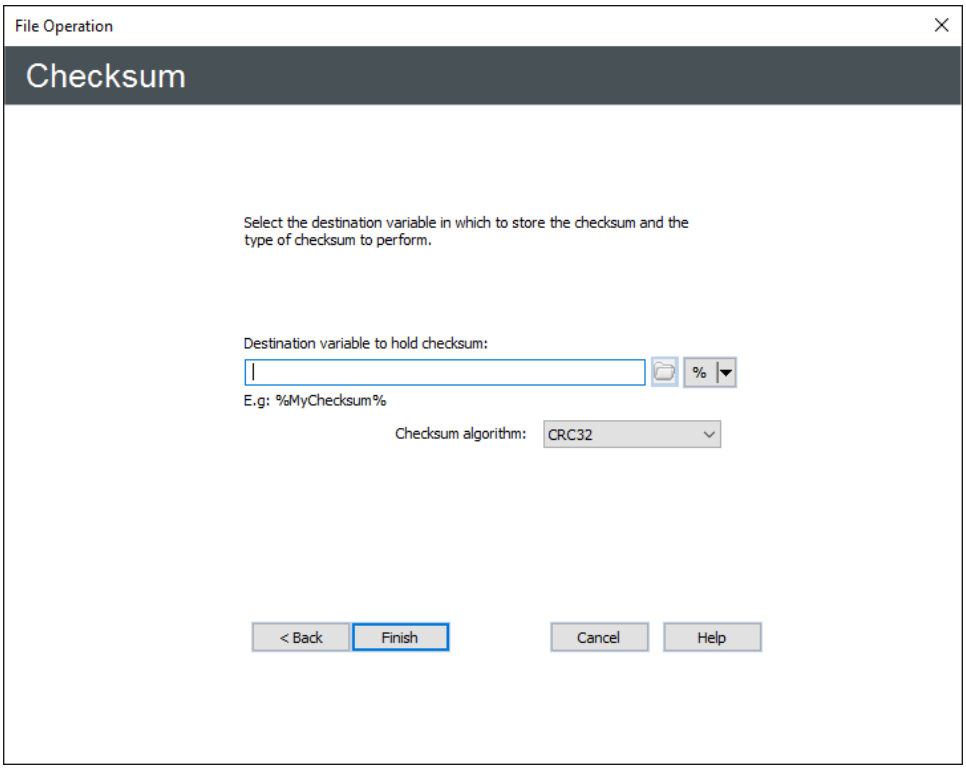
Checksum



a. Specify the **Source path** with variables or by selecting the folder icon and browsing.

a. Select the **Treat as success if the source file does not exist** check box if you don't want this action to counted as a failure in that case.

b. Click **Next**.



a. Specify the **Destination path** with variables or by selecting the folder icon and browsing.
b. Specify the **Checkusm algorithm** (**CRC32**, **MD5**, **SHA1**, **SHA256**, **SHA384**, **SHA512**) and then click **Finish**.

File: Scan Action

The **File: Scan** Action is used to send a file to an antivirus or data loss prevention scanner for processing.

- How does File: Scan work in Event Rules?
- File Scan Action Example
- File: Scan Action
- Scanning Metadata

Content Integrity Control

EFT's ICAP functionality is invoked through Event Rules, sending files to antivirus or data leak prevention (DLP) servers that detect file pass/fail based upon user-defined rules. Users can configure rules on a DLP server to send a reply to EFT with access denied if the file contains social security numbers (SSNs) or credit card numbers (CCNs), for example. Antivirus servers scan the files for viruses and return a response to EFT whether a virus was found or not. (Refer to File: Scan Action for the procedure for adding the action to an Event Rule.)

The Internet Content Adaptation Protocol (ICAP) is an HTTP-like protocol that is used for virus scanning and content filtering. According to RFC 3507:

ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages. It allows ICAP clients to pass HTTP messages to ICAP servers for some sort of transformation or other processing ("adaptation"). The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. Typically, the adapted messages are either HTTP requests or HTTP responses.

On a DLP server, you can define rules to search files for SSNs or CCNs. For example, if you send a file containing a valid CCN, the DLP server will flag it and return a denied message to EFT. (To test this rule, you can put the universal test credit card number 4111 1111 1111 1111 in a text file and send it through the DLP via an EFT Event Rule.)

On an antivirus server, you can specify violation text in ICAP response headers: “X-Virus-ID:INFECTED” or ”X-Response-Info:blocked” or both (semicolon-separated).

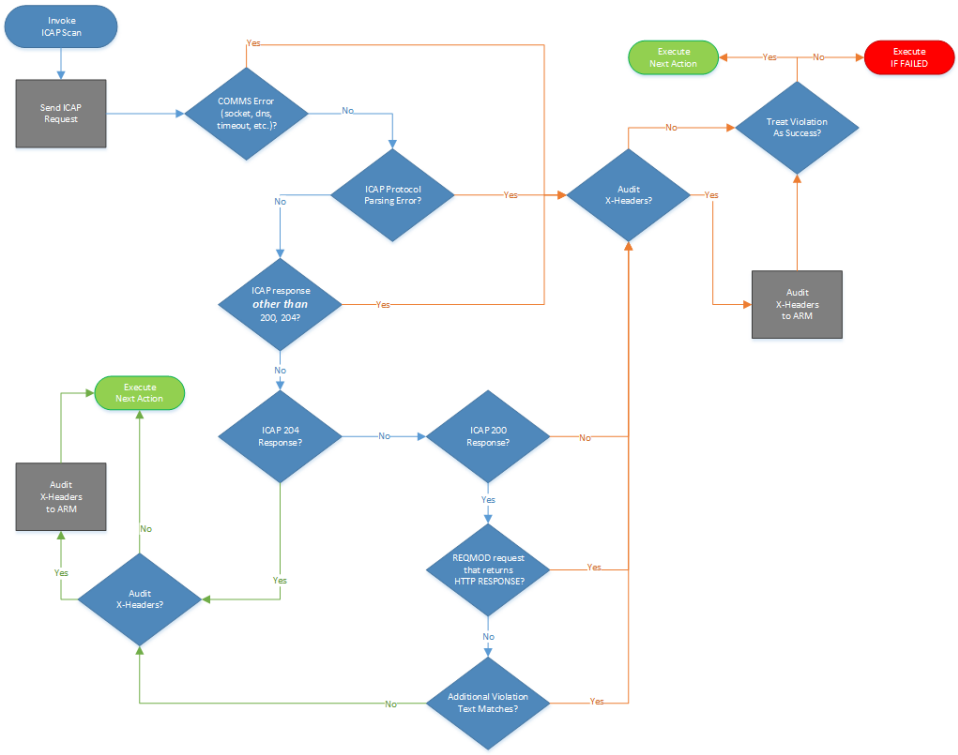
EFT does not return an error or any type of indicator from the Content Integrity Control Action if a file isn't completely processed/analyzed by an antivirus or DLP server due to the size of the file being larger than what is supported by that particular server. For example, MyDLP will process a maximum of 10 MB of data; if a flag is embedded in a file that is after the 10 MB limit, MyDLP will not detect the policy violation.

Suppose EFT sends an 11 MB file to myDLP, which has a max processing capacity of 10 MB. The myDLP server has a policy to return a failure for any files containing credit card numbers. The 11 MB file has a credit card number embedded at the end of file. As a result, the myDLP server would return to EFT that the Action was a success, because the myDLP server did not process the credit card number.

Refer to Content Integrity Control Tab for details of creating a CIC profile.

Content Integrity Control Actions are also captured in the EFT log, after you enable `#log4cplus.logger.Events.ContentIntegrityControl=TRACE` in the logging.cfg file. (Remove the # in front of that line.)

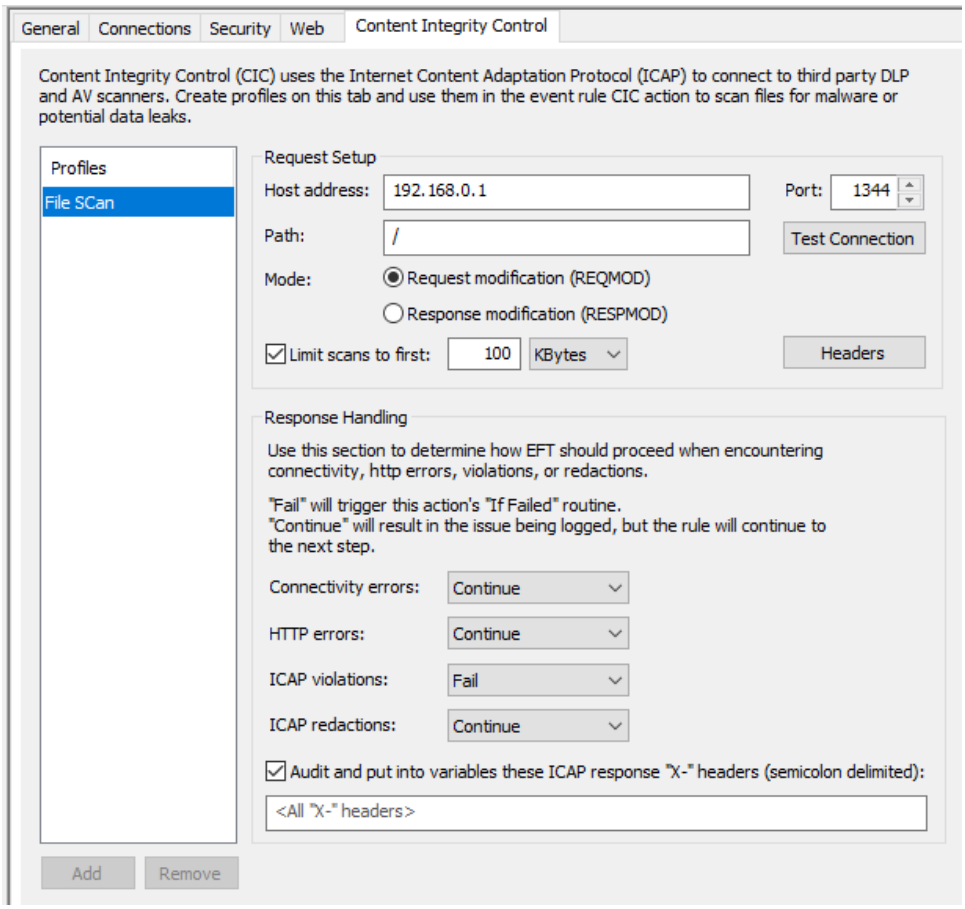
Below is a diagram demonstrating EFT decision points for Content Integrity Control (ICAP) success or failure.



Content Integrity Control Tab

Content Integrity Control is used to send a file to an antivirus scanner or data loss prevention solution for processing. When a **File Scan** Action is added, a file that triggers the Event Rule is sent to an ICAP server for processing. When the file passes, other Actions can occur, such as moving the file to another location. If the file fails, processing can stop, or other Actions can occur, such as sending an email notification.

Refer to Global Antivirus Scanning for details of configuring Global antivirus on this tab.



To remove a profile

- To remove a profile, select its name in the list, and then click **Remove**.

How does File: Scan Work in Event Rules?

The **File: Scan** Action is used to send a file to an antivirus or data loss prevention scanner for processing. When this Action is added, a file that triggers the Event Rule is sent to an ICAP server for scanning. When the file passes the scan, other Actions can occur, such as moving the file to another location. If the file fails the scan, processing can stop, or other Actions can occur, such as sending an email notification. EFT fully

supports RFC3507 section-3.1 and section-4.8. EFT can adapt the outgoing response if the ICAP server indicates that adaptation is necessary.

How does File: Scan work in Event Rules?

The **File: Scan** Action allows ICAP clients to pass HTTP messages to ICAP servers to scan the file(s) in the Event Rule that is passing through EFT.

You can create reusable profiles on the Content Integrity Control Tab and you can create a custom Content Integrity Control (CIC) profile as you need it, as described below.

Important info about how EFT uses the File Scan Action

IMPORTANT:

- Using the File Scan Action with encrypted files will not return an accurate result. Copy/move the files to a folder that is not encrypted to process with the ICAP server.
- ICAP servers don't all offer the same features. The action was tested with:
  - Clearswift version 5
  - Symantec DLP version 14.5.0.24028
  - Kaspersky version 5.5
- When using the action, EFT needs to use POST in HTTP requests. Refer to knowledgebase article https://kb.globalscape.com/KnowledgebaseArticle11375.aspx for information about enabling an advanced property.
- **File Uploaded** and **Workspace Created** events are triggered after a file is uploaded and after a Workspace is created. Only after the event triggers will the action begin communication with the ICAP server, and then redacts the file, if needed. Therefore, there may be delays between when a Workspace is created and a file is redacted. Use the **File Uploaded** event to trigger the action, then use the **File: Scan** action and "Fail" to prevent the message from being sent. Use the **Before Download** event trigger to scan the file before it's downloaded.

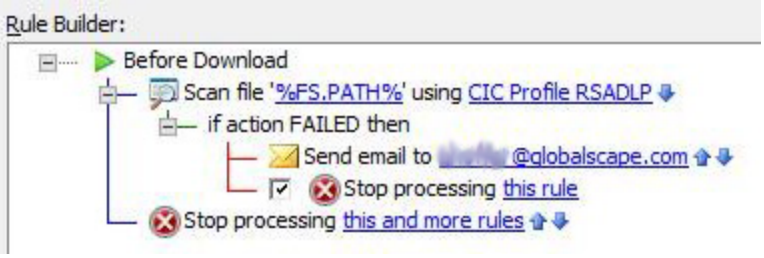
.

Scan a File Using the File: Scan Action

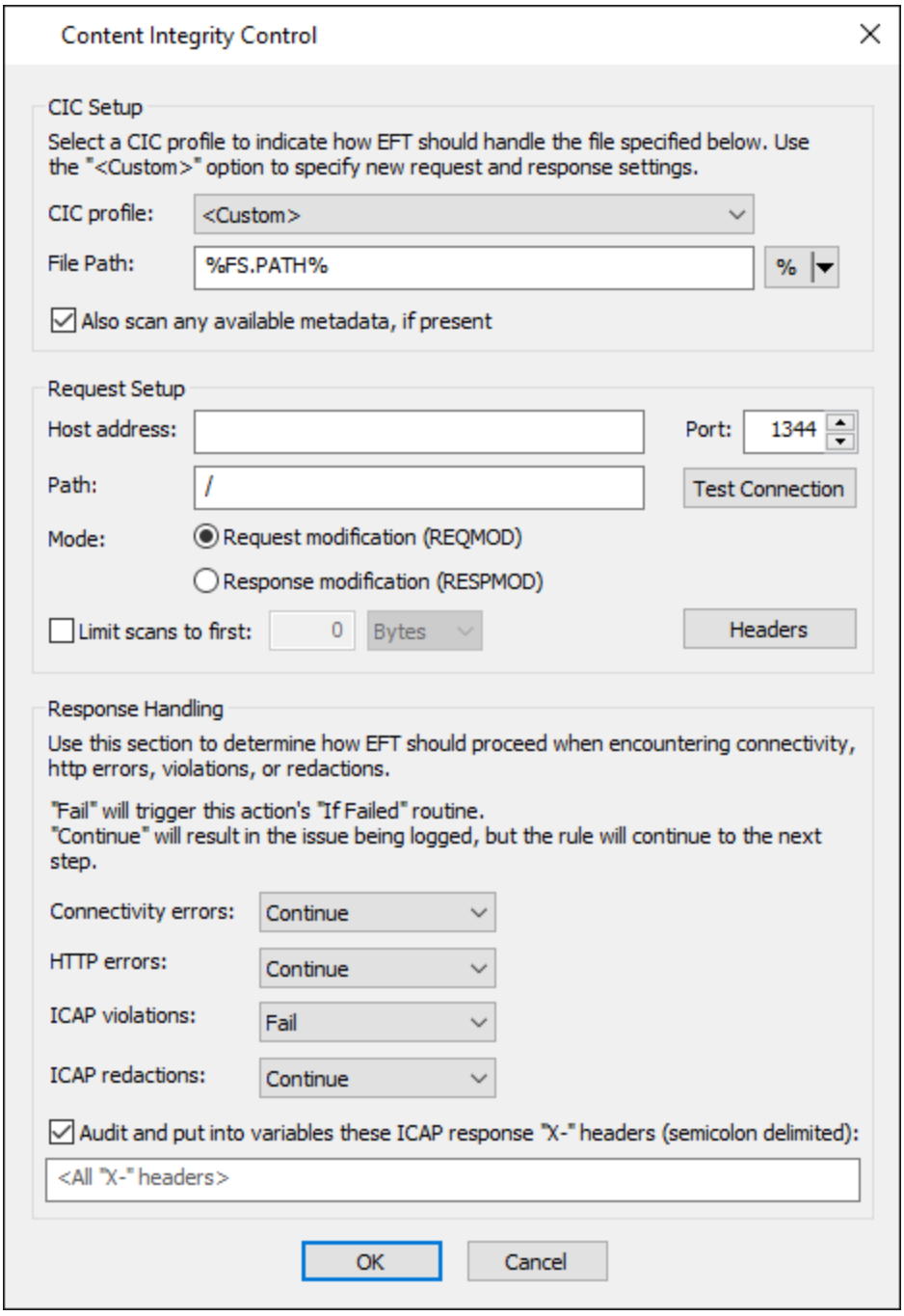
The **File: Scan** Action is used to send a file to an antivirus or data loss prevention scanner for processing.

To scan a file using the File: Scan Action

1. Create a new Event Rule, such as a Folder Monitor Event.
2. Add relevant Conditions.
3. Add the **Content Integrity Control** Action. For example:

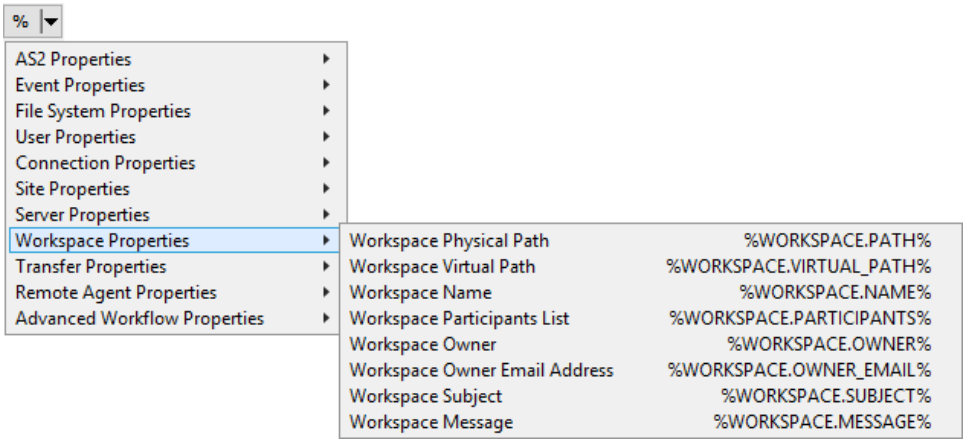


4. In the Action, click either of the underlined/linked items. The **Content Integrity Control** dialog box appears.



5. Click the **CIC Profile** drop-down list to select a predefined profile, or select **<Custom>**.
6. **File Path** - Physical location of the file to send to the ICAP server; %FS.PATH% is the default. You can specify another variable or drive and UNC paths. Wildcards are unsupported.

- **%** - Click the drop-down list if you want to specify other context variables:

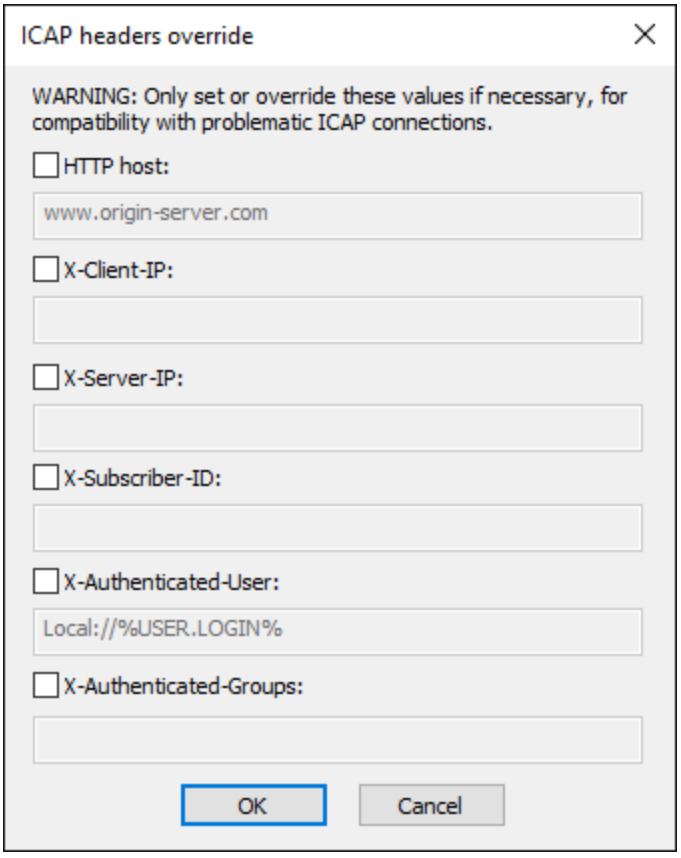


7. **Also scan any available metadata, if present** - Metadata includes the field name of Workspaces send operations. Consult your ICAP server for detailed information. The check box is selected by default.
    - The context variables Workspace Subject (%WORKSPACE.SUBJECT%) and Workspace Message (%WORKSPACE.MESSAGE%) (see above) relate to this feature.
8. If you specified a <Custom> profile, complete the rest of the fields in the dialog box:
    a. **Host address**, **Path, Port** - These settings depend on settings in the antivirus or DLP (ICAP) server.
        - The **Host address** field should be the URL of the ICAP server (the field cannot be blank).
        - By default, the port is set to 1344.
    b. **Test Connection** - After you specify the connection to the ICAP server, test the connection. If connection fails, verify these settings match the settings defined in the antivirus or DLP solution. (In earlier versions, **Test Connection** doesn't work with %variable% in the connection field.)
    c. **Mode** - Specify one of the following:
        - **Request modification (REQMOD)** - - Request modification mode: Embeds file contents in an HTTP PUT request body, which is then sent in the body of an ICAP request to the server. The ICAP server may respond with a modified version of the embedded request, or a new HTTP response. The ICAP response will depend on your ICAP server's implementation.

- **Response modification (RESPMOD)** - Response modification mode: Embeds file contents in an HTTP 200 OK response body, which is then sent in the body of an ICAP request to the server. The ICAP server may respond with a modified version of the embedded response. The ICAP response will depend on your ICAP server's implementation.

d. **Limit scans to first *n* bytes** - (Optional) Specify the number of bytes to scan. Some antivirus solutions only require a subset of a file's contents to test against their database of malware signatures. To keep from transferring large files in their entirety when we only need the first *n* bytes, you can specify how many bytes are sent to the ICAP server. When this check box is cleared, the entire file is transferred to the ICAP server. If the file is smaller than the Max scan size, the entire file will be transferred for scanning.

9. **Headers** - (Optional) In v8.0.5 and later, only set these values if needed for problematic ICAP connections. Headers can be used to override the REQMOD/RESPMOD X-headers sent by EFT, to fine-tune the connection to the ICAP server. These headers are displayed in the ICAP server logs.



- **HTTP host** - The EFT site's local host address (do not use "localhost"); The default is to show the EFT HTTP Host if supplied (not localhost), otherwise "www.origin-server.com"; If you override the Host value, then that value is used instead. The order is: user override value -> EFT HTTP Host if supplied (not localhost) -> or www.origin-server.com as last resort.
- **X-Client-IP** - Blank by default
- **X-Server-IP** - Blank by default
- **X-Subscriber-ID** - Blank by default
- **X-Authentication User** - Provide a string with variables.
  - **LDAP** - Example: "LDAP://pdc/samaccountName=%LOGIN.LOGIN%,DC=s5development,DC=local"
  - **AD** - Examples: WinNT://{NetBIOSDomainName/sAMAccountName}, WinNT://pdc/s5dev\arybin
  - **Other** - Examples: Local://%USER.LOGIN%, Local://%SERVER.NODE_NAME%
- **X-Authenticated Groups** - Blank by default
- User can override and use context variables if desired as field elements. EFT will base-64 encode.

Note the difference between "ICAP Header" and "HTTP Header." The ICAP Header is a header with service information EFT sends to the ICAP server. The HTTP header is a part of information EFT sends to ICAP for analysis. That is, the HTTP header will be analyzed, not the ICAP header. The HTTP header is shown in ICAP log files.

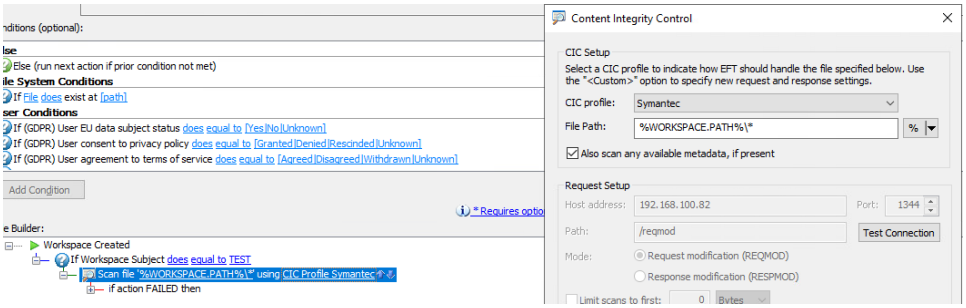
10. Under **Response Handling**:
    - Specify whether transfer should **Continue** or **Fail** when the following occur: **Connection errors**, **HTTP errors**, **ICAP redactions**.
11. **Audit and put into variables these ICAP response "X-" headers** - (Optional) Specify “X-“ headers for auditing using ARM. If this option is enabled and no “X-“ headers are specified, all “X-“ headers will be audited. Use semicolons between multiple items. Note this check box only affects whether the specified headers are audited by ARM, regardless of success or failure.
12. Click **OK** to save the changes in the Event Rule. The name of the profile appears in the Event Rule Action.

Scanning Metadata

In general, "metadata" is "data that provides information about other data." Metadata does not provide the content of the data, such as the text of a message or an image itself. In Workpaces, for example, metadata can be subject, message, and attached file of a Workspaces message. The File: Scan action scans metadata to look for ICAP violations in the content, such as a full credit card number.

To test the metadata feature

1. Create an Event Rule using the **Workspace Created** event.
2. Add the **If Workspace Subject** Condition with the subject **does equal to** TEST.
3. Add the **File: Scan** Action.
4. Specify your ICAP server or use your CIC profile to scan the files.
5. In the **File Path** box, select the variable **%WORKSPACE.PATH%**, then add a backslash and an asterisk: *****. This will ensure the attached file is scanned.
6. Select the **Also scan any available metadata, if present** check box. This will ensure the metadata are scanned.



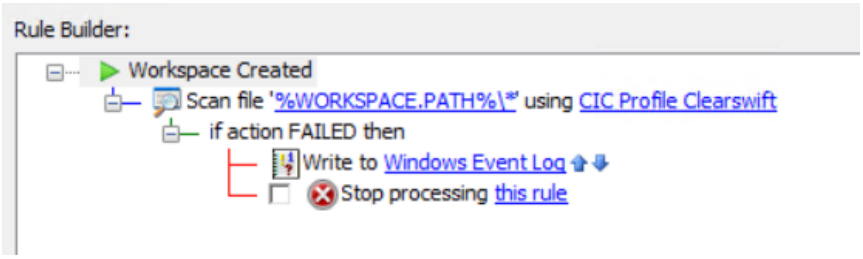
7. Save and run the Event Rule. The subject, message, and attached file will be scanned when using the Web Transfer Client to send a file. The message will be flagged if there are any violations in the message due to ICAP policy.

   Since you cannot predict what information will be in the Subject or Message, you can add an "if action FAILED" action, such as an email notification or Write to Windows Event Log, instead of a Condition.

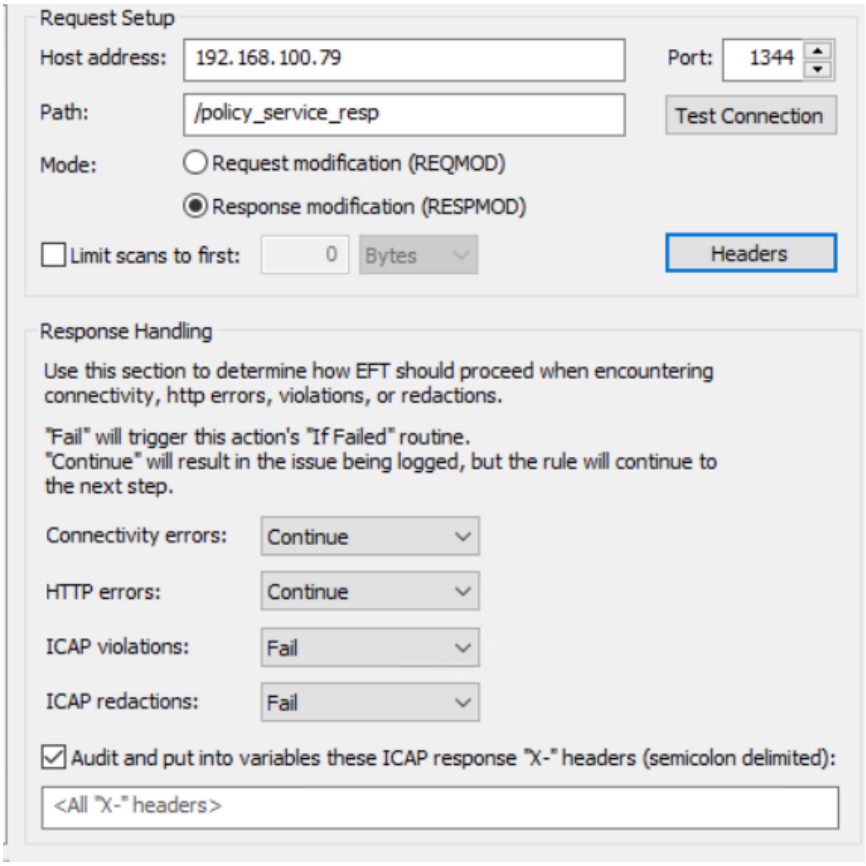
File Scan Action Example

Below is an example of a **Workspace Created** Event Rule with a **File Scan** Action and an **if action failed** action to **Write to Event Log.**

In this example, when a Workspace is created, the File Scan action uses the Clearswift profile to scan any files in that Workspace when it was created. If the scan finds any ICAP violation or redactions, it writes the information to the Windows Event Log. A file in the Workspace named BadCreditCard.txt contains a credit card number, which will fail the File Scan.

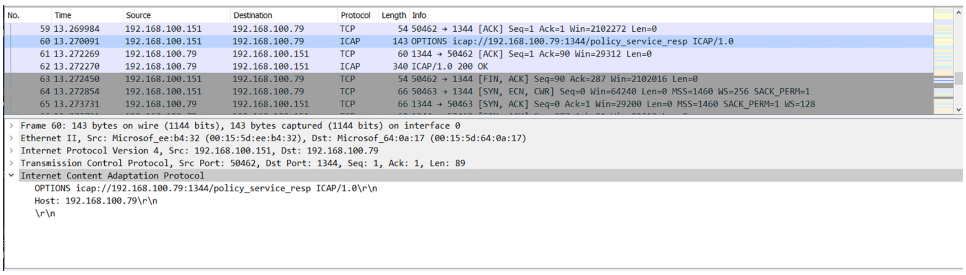


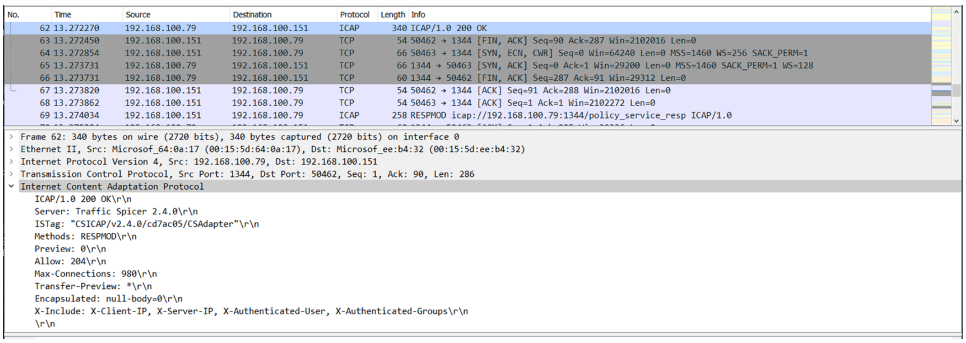
The profile was configured to work with a Clearswift ICAP server.



Details of the RESPMOD messages using Wireshark:

An example of EFT sending the Option method to a Clearswift ICAP server and the ICAP response:





Subject of a message sent with a file:

```
RESPMOD icap://192.168.100.79:1344/policy_service_resp ICAP/1.0
Host: 192.168.100.79
Allow: 204
X-Authenticated-User: TG9jYWw6Ly9keWVsYWNpYw==
Encapsulated: req-hdr=0, res-hdr=58, res-body=162

GET /BadCreditCard.txt HTTP/1.1
Host: 192.168.100.151

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 14
Cache-Control: no-cache

e
Subject Matter
0

ICAP/1.0 204 No Content
Server: Traffic Spicer 2.4.0
ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"
```

Message sent with the file:

In the Wireshark readout, you can see the contents of the message:

```
411 1111 1111 1111
  Now is the time...
```

and then at the bottom of the file, you can see the credit card number was redacted:

```
**** **** **** ****
Now is the time
...
RESPMOD icap://192.168.100.79:1344/policy_service_resp ICAP/1.0
        Host: 192.168.100.79
        Allow: 204
        X-Authenticated-User: TG9jYWw6Ly9keWVsYWNpYw==
        Encapsulated: req-hdr=0, res-hdr=58, res-body=162

        GET /BadCreditCard.txt HTTP/1.1
        Host: 192.168.100.151

        HTTP/1.1 200 OK
        Content-Type: application/octet-stream
        Content-Length: 39
        Cache-Control: no-cache

        27
        4111 1111 1111 1111
        Now is the time ...
        0

        ICAP/1.0 200 OK
        Server: Traffic Spicer 2.4.0
        ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"
        X-Virus-ID: Credit Card Numbers
        X-Infection-Found: Type=1; Resolution=1; Threat=Credit
Card Numbers;
        X-Violations-Found: 1
        BadCreditCard.txt
        Credit Card Numbers
        0
        1
        Encapsulated: res-hdr=0, res-body=104

        HTTP/1.1 200 OK
```

```
        Content-Type: application/octet-stream
        Content-Length: 39
        Cache-Control: no-cache

        27
        **** **** **** ****
        Now is the time ...
        0
  File contents scanned and redacted:
        RESPMOD icap://192.168.100.79:1344/policy_service_resp
ICAP/1.0
        Host: 192.168.100.79
        Allow: 204
        X-Authenticated-User: TG9jYWw6Ly9keWVsYWNpYw==
        Encapsulated: req-hdr=0, res-hdr=58, res-body=163

        GET /BadCreditCard.txt HTTP/1.1
        Host: 192.168.100.151

        HTTP/1.1 200 OK
        Content-Type: application/octet-stream
        Content-Length: 341
        Cache-Control: no-cache

        155
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        4111 1111 1111 1111
        fubar
        0

        ICAP/1.0 200 OK
        Server: Traffic Spicer 2.4.0
        ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter"
        X-Virus-ID: Credit Card Numbers
```

```
        X-Infection-Found: Type=1; Resolution=1; Threat=Credit
Card Numbers;
        X-Violations-Found: 1
        BadCreditCard.txt
        Credit Card Numbers
        0
        1
        Encapsulated: res-hdr=0, res-body=105

        HTTP/1.1 200 OK
        Content-Type: application/octet-stream
        Content-Length: 341
        Cache-Control: no-cache

        155
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        **** **** **** ****
        fubar
        0
```

EFT Log has the following information for this example:

```
02-05-21 13:18:23,255 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Processing
 Content Integrity Control request for profile [2576e336-6a20-
4d35-af8d-81094e4fa91c],
 file
[C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage
\Subject
 Matter\\*], scan metadata: 1
        02-05-21 13:18:23,255 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
```

```
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Checking
 file:
C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage\S
ubject
 Matter\\BadCreditCard.txt
        02-05-21 13:18:23,271 [1216] ERROR
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - ICAP
redaction
 found during CIC action, file
[C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage\
Subject
 Matter\\BadCreditCard.txt], profile[Clearswift] action failed.
        02-05-21 13:18:23,271 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Content
 of file:
'C:\InetPub\EFTRoot\MySite\Usr\<username>\WorkspacesSendMessage\
Subject
 Matter\\BadCreditCard.txt' was redacted.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Infection-Found: Type=1; Resolution=1; Threat=Credit Card
Numbers;]
 in response.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Infection-Found%: " Type=1;
Resolution=1;
 Threat=Credit Card Numbers;"
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Violations-Found: 1] in response.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Violations-Found%: " 1"
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
```

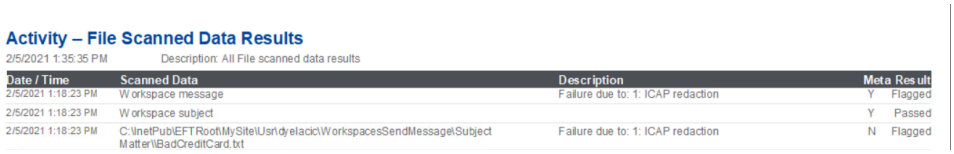
```
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Virus-ID: Credit Card Numbers] in response.
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
EVENT_ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Virus-ID%: " Credit Card
Numbers"
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Auditing
 these X headers [X-Infection-Found: Type=1; Resolution=1;
Threat=Credit
 Card Numbers;;X-Violations-Found: 1;X-Virus-ID: Credit Card
Numbers]
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Scanning
 workspace subject
        02-05-21 13:18:23,271 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Checking
 metadata: Workspace subject
        02-05-21 13:18:23,287 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Scanning
 workspace message
        02-05-21 13:18:23,287 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Checking
 metadata: Workspace message
        02-05-21 13:18:23,302 [1216] ERROR
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - ICAP
redaction
 found during CIC action, metadata[Workspace message], profile
[Clearswift]
 action failed.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Overriding
```

```
 existing event context property %WORKSPACE.MESSAGE%
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Define
 event context variable %WORKSPACE.MESSAGE%: "**** **** ****
****
        Now is the time ..."
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Infection-Found: Type=1; Resolution=1; Threat=Credit Card
Numbers;]
 in response.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Overriding existing event context property %X-Infection-Found%
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Infection-Found%: " Type=1;
Resolution=1;
 Threat=Credit Card Numbers;"
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Violations-Found: 1] in response.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Overriding existing event context property %X-Violations-Found%
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - EVENT_
ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Violations-Found%: " 1"
        02-05-21 13:18:23,302 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> - Found
header
 [X-Virus-ID: Credit Card Numbers] in response.
        02-05-21 13:18:23,302 [1216] WARN
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
```

```
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
EVENT_ACTION_CONTENT_INTEGRITY_CONTROL:
 Overriding existing event context property %X-Virus-ID%
        02-05-21 13:18:23,318 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
EVENT_ACTION_CONTENT_INTEGRITY_CONTROL:
 Define event context variable %X-Virus-ID%: " Credit Card
Numbers"
        02-05-21 13:18:23,318 [1216] TRACE
Events.ContentIntegrityControl.MySite.On_Workspace_Created_Rule
 <HTTP.ProcessRequest; Rule: On Workspace Created Rule> -
Auditing
 these X headers [X-Infection-Found: Type=1; Resolution=1;
Threat=Credit
 Card Numbers;;X-Violations-Found: 1;X-Virus-ID: Credit Card
Numbers]
        02-05-21 13:18:23,318 [4124] INFO SMTP <> - The
 number of messages are pending for send: 1
```

The ARM Report:

The report displays the failure of the message, and that the file was redacted.



Activity – File Scanned Data Results

2/5/2021 1:35:35 PM Description: All File scanned data results

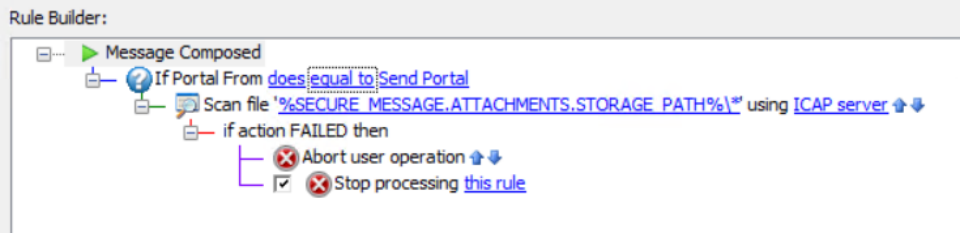
Date / Time	Scanned Data	Description	Meta	Result
2/5/2021 1:18:23 PM	Workspace message	Failure due to: 1: ICAP redaction	Y	Flagged
2/5/2021 1:18:23 PM	Workspace subject		Y	Passed
2/5/2021 1:18:23 PM	C:\InetPub\EFTRoot\MySite\Usr\dyelacic\WorkspacesSendMessage\Subject Matter\\BadCreditCard.txt	Failure due to: 1: ICAP redaction	N	Flagged

Flow: Abort User Operation

The **Flow: Abort User Operation** action is used to allow administrators to abort a user's requested operation. The action is only available with the **Message composed** event trigger.

For example, using the Event Rule as defined below, when a user defines a message in the Send portal and attempts to send a file that contains a credit card number, the file is sent to the ICAP server to be scanned and then the file is blocked or redacted because of the credit card number and moved to a quarantine location.

In this case, the **Abort user operation** action blocks the message from being sent, the user receives a failure message, and the Workspace is not created.



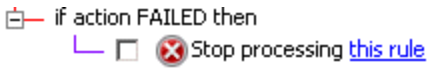
- This action cannot be configured to run asynchronously.
- The ICAP server
- The response code is always 403; the Advanced Property, AbortUserOperationHTTPCode can be used to set a different value.
- The response message is derived from EFT message templates for HTTP response codes.
- The headers sent back are the standard ones used for a normal failure situation.

Flow: Stop Processing Action

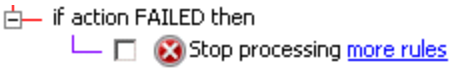
The *Stop Processing* Action is added automatically with each of the Actions except for the Send notification email Action, or you can add it after an Event or Condition.

When importing event rules from version 8.0 or later, the multi-line "Create or set variable" event action will import with the multiple lines. When upgrading, this path removes the multiple lines. The event rule will end up with a single "create or set variable" event rule action.

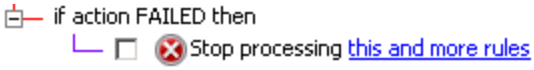
The Stop Processing Action ends processing of Event Rules, depending on your selection:



- **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.



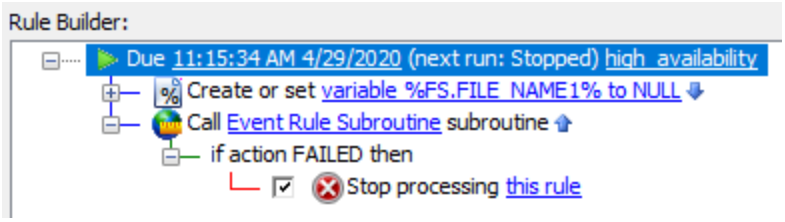
- **more rules**—The current Rule continues executing, the next Rules in order are not started. That is, it allows the current Rule to complete its processing, but no further matching Rules will continue to process.



- **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.

Action lines are collapsed by default, if no "if failed" values are set.

- The line is collapsed by default if no if-failed action is specified
- The line is expanded by default if an if-failed action is specified

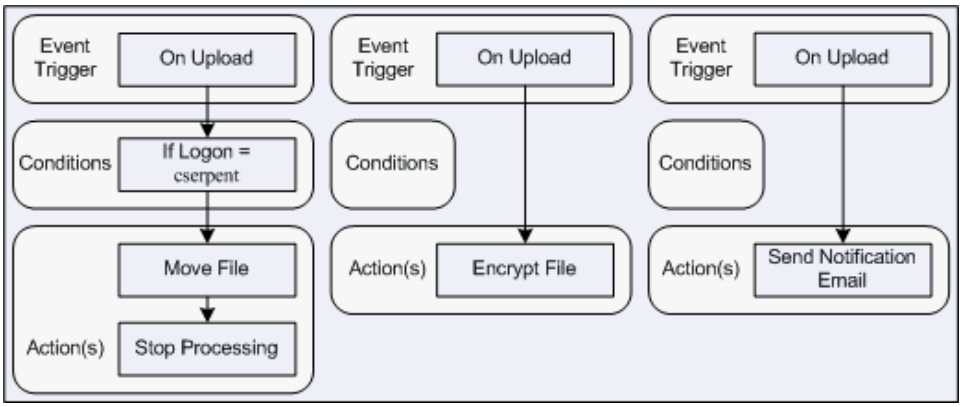


- The Create or set variable action does not have an "if action failed" option

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 (that is, when the next "File Uploaded" Event happens), EFT 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 email notification when a file is uploaded.

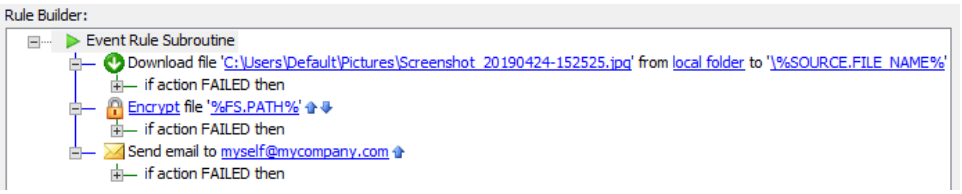
A recurring Timer does not stop recurring if the Rule Actions fail; it will recur as scheduled until you disable or delete the Rule. In the case of Timer Rules, "Stop processing this rule" means "do not execute any further Actions with this Rule" (such as sending an email), but it does NOT mean that 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).

Flow: Subroutine Action

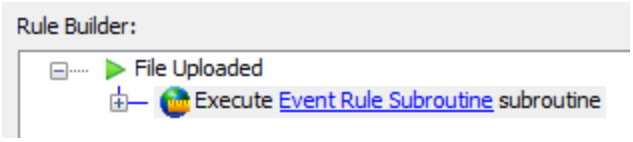
(Requires EAM) The **Flow: Subroutine** Action allows you to call an Event Rule Subroutine event trigger from within another event rule. The primary purpose of the Flow: Subroutine action is to help you break up larger rules into smaller, reusable ones. Obviously, you would have already created other rules to call. These sub tasks would be rules that you commonly use, such as sending email notifications, moving files, encrypt/decrypt, and so on.

To create an event with the Subroutine action

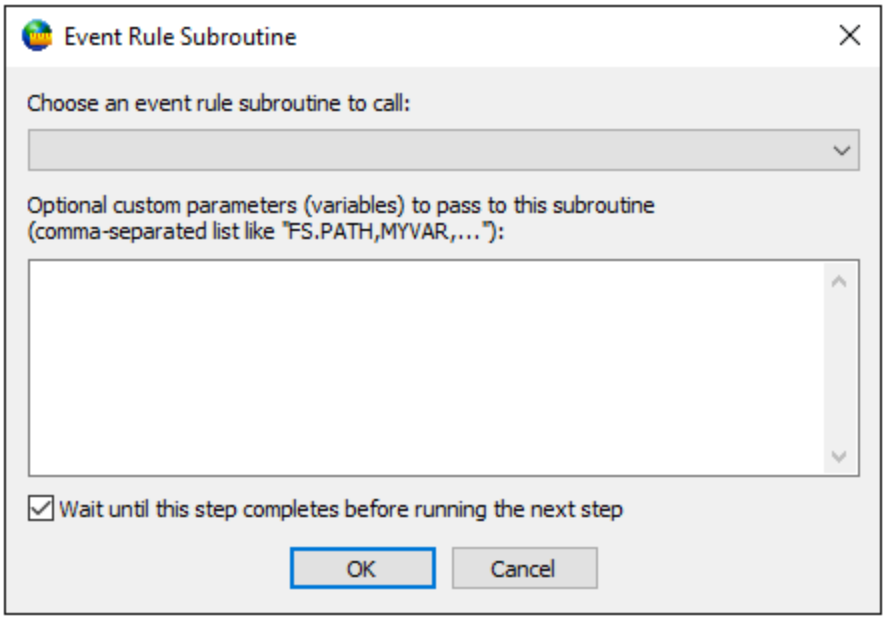
1. First use the Event Rule Subroutine event trigger to create a subroutine that contains frequently used actions.



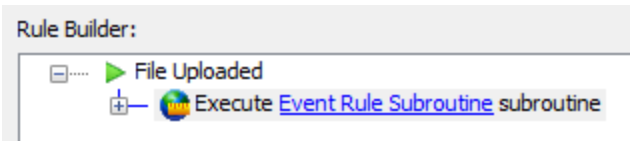
2. Then Create a new event rule and add the **Flow: Subroutine** action to the Event Rule.



3. Click the link in the action to open the **Event Rule Subroutine** dialog box.



4. Click the **Choose a rule to trigger** drop-down list to specify which event rule to trigger, and then specify parameters (variables) to pass to the rule (optional).
5. (Optional) The **Wait until this step completes before running the next step** check box is selected by default. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)



6. Click **OK** to close the **Event Rule** dialog box and accept the changes.

Notes:

- If there is no FAILED action set, then the call to the subroutine is asynchronous, and the subroutine is placed into a queue.
- The number of threads serving the queue, which applies to all Sites on a server, (that is, executing async subroutines) is defined by the **RunningAsyncSubroutinesLimit** advanced property. The default is 10; 0 equals no limit
- The per-Site limit on queue size is defined by the **QueuedAsyncSubroutinesLimit** advanced property. The default is 0, which equals no limit.
- The Events logger should be used for troubleshooting.

Related COM API objects:

- **EventRuleSubroutine** value is added to **EventType** enum
- **RunEventRuleAction** value is added to **EventActionType** enum
- **ICIRunEventRuleActionParams** interface is added to allow new action handling with two read/write properties:
  - [string] RuleName - the name of the subroutine to invoke [array of strings]
  - Variables - the variables to pass to the subroutine
- **ICIRunEventRuleActionParams** class is added implementing **ICIRunEventRuleActionParams** interface
- Create and configure action set action:

```
Params = CreateObject
("SFTPCOMInterface.CIRunEventRuleActionParams")
 actionParams.RuleName = "Event Rule Subroutine"
actionParams.Variables
 = Array("VAR1", "VAR2", "VAR3") rule.AddActionStatement
 0, actionParams
```

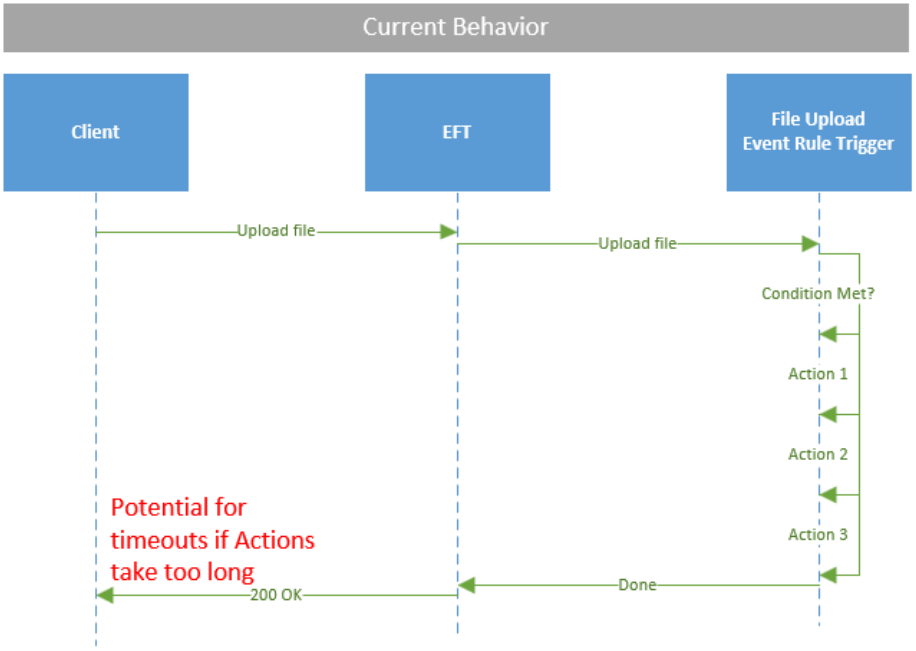
- Read action:

```
set params = action.GetParams()
 MsgBox "Rule name: " & params.RuleName for each var in
params.Variables
 MsgBox "Variables: " & var next
```

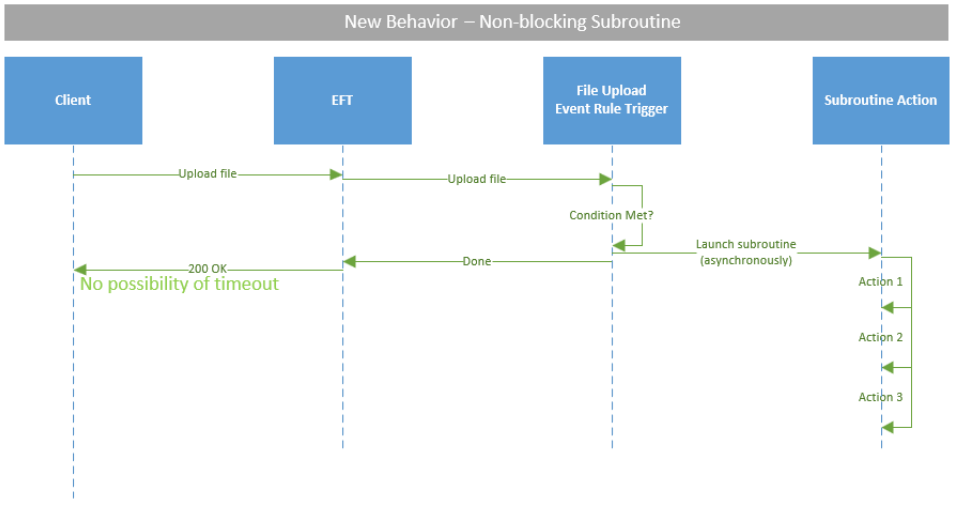
EFT Subroutine Action Behavior

While the primary purpose of the Subroutine action is to help you break up larger rules into smaller, reusable ones, there is an additional benefit. Without the Subroutine action,

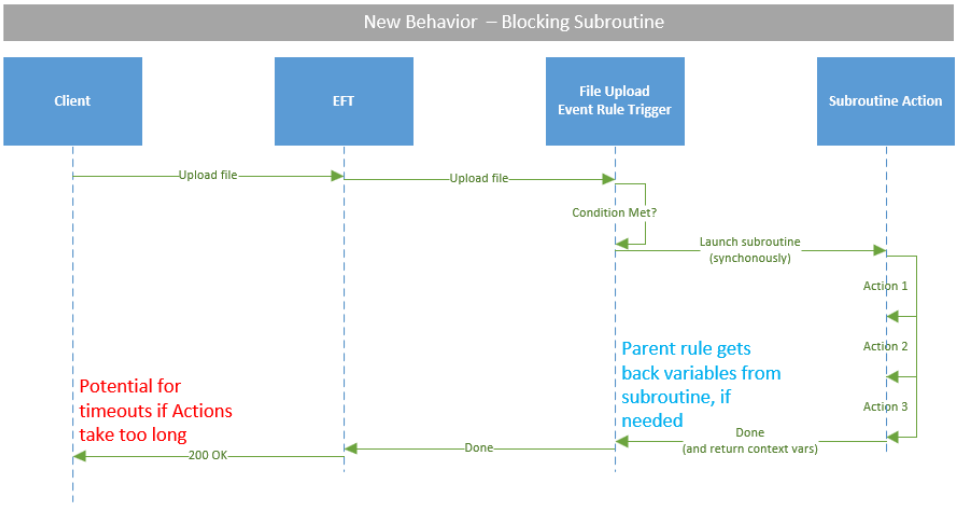
rules triggered by file uploads do not return a positive completion reply to the remote client until after all actions in the rule have completed, which results in an increased risk of a client time out:



By adding a subroutine action, you can instruct the rule triggered by the upload to call a subroutine in a non-blocking (asynchronous) manner, which allows the upload rule to return the positive completion reply much sooner, mitigating the risk of timeouts:



If desired, subroutines can be called in a blocking (synchronous) fashion which, while increasing the chance of client timeouts, is useful when the parent action needs a result from the subroutine to properly complete its task:



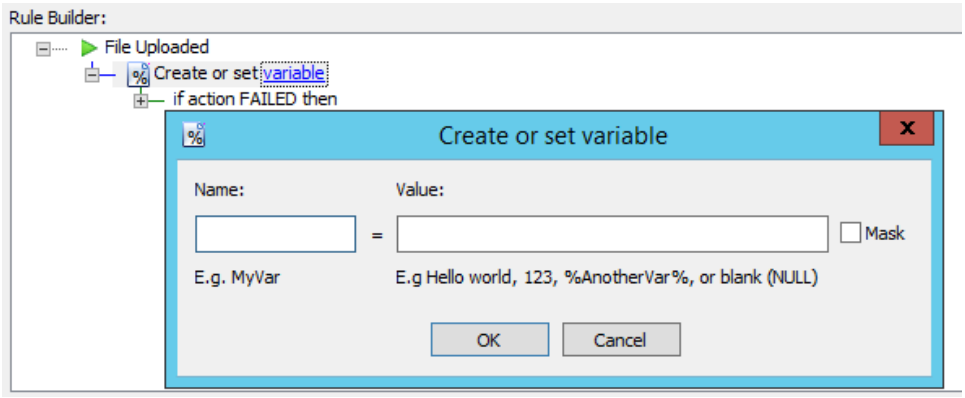
Flow: Variable Action

The **Flow: Variable** Action is used to create or modify a variable to be used in Event Rules. This Action can be used in any events in EFT.

If you attempt to create a new variable with the same name as an existing variable, the existing variable is overwritten and a new variable is not created.

To create a variable in a rule

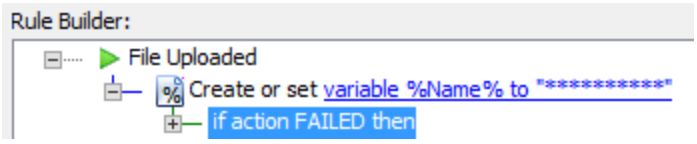
1. In the administration interface, connect to EFT and click the **Server** tab.
2. Create a new Event Rule.
3. Add the **Create or set variable** Action to the rule.
4. In the Rule Builder, click the **variable** link. The **Create or set variable** dialog box appears.



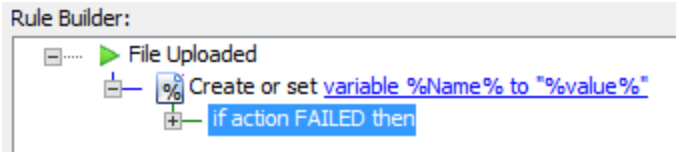
5. Provide a **Name** for the variable:

- You can specify any character besides the percent sign (%); however, it is recommended to use uppercase and lowercase letters and numbers
- EFT automatically handles the % whether or not % symbol is provided for variable name
- Reserved names (other context variables) are allowed. This will overwrite their existing values.
- Variable names are case sensitive

6. Provide a **Value** for the variable:
   - The value can be blank (NULL), a value, or another variable. You can specify multiple variables, and existing EFT variables. The existing variable's value will be overwritten when this action is triggered.
   - A blank value equals to NULL (NULL not "NULL")
   - EFT will perform casting (converting the variable to its value), as it does today
   - Another variable can be used (passed by reference, not as a pointer)
7. If you want the value to be hidden, select the **Mask** check box. Masked values are replaced with asterisks (**********) in interfaces. On export, values are exported in hex.

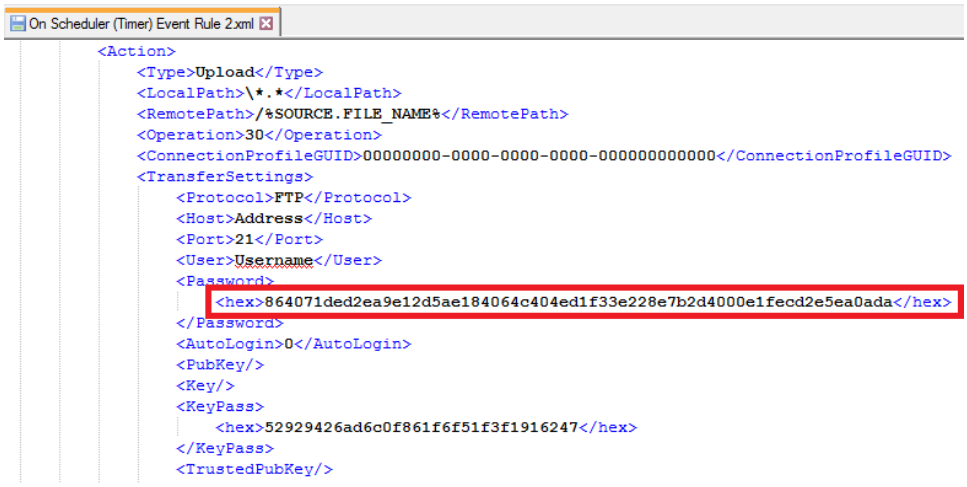


8. Click **OK** to save the **Create or set variable** Action in the rule. The rule in the Rule Builder updates to show your variable definition:



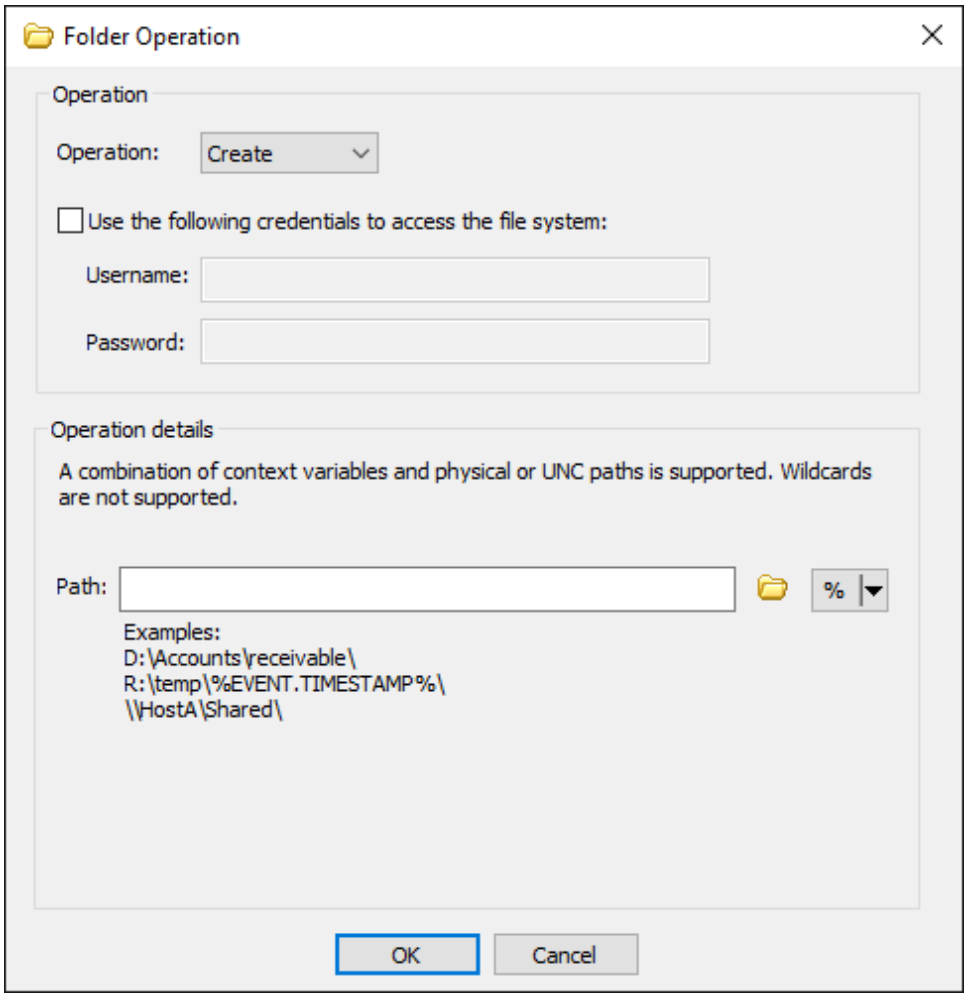
9. Add other conditions or actions as needed, then click **Apply** to save the rule.

Variables are masked in interfaces and in export files:



Folder: Operation Action

(Require EAM) The **Folder: Operation** Action is used to create, rename, or delete a folder.



To create, rename, or delete a folder

1. Add the **Folder: Operation** Action to the rule, then click the link in the rule to open the **Folder Action** dialog box.
2. In the **Operation** list, click **Create**, **Rename**, or **Delete**.
3. Select the **Use the following credentials to access the file system** check box, then provide the username and password needed to log in to create, rename, or delete the folder.
4. In the **Path** box, provide the path where the folder is that you want to delete, or the location of the folder that you want to create or rename. You can use physical or UNC paths, but not wildcards. You an also click the folder icon to

browse to a path, and click the **%** drop-down to add a variable.

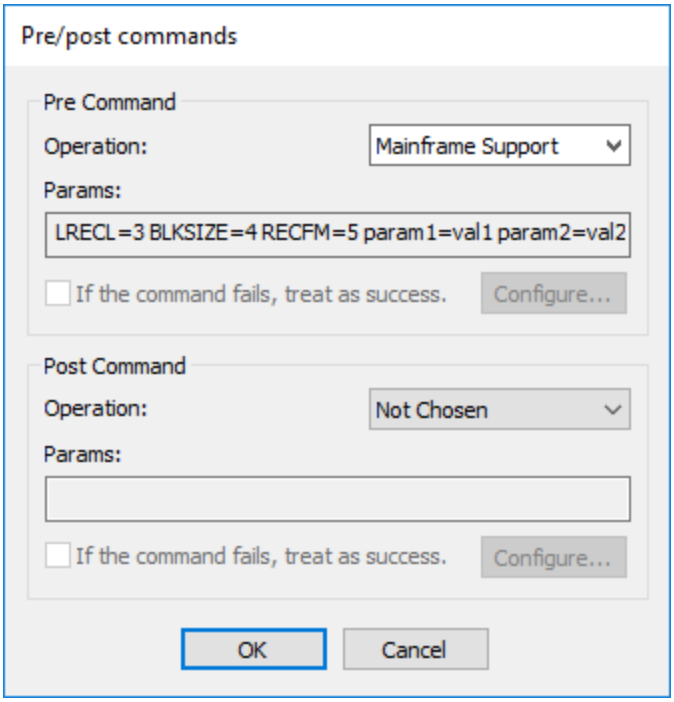
5. Click **OK** to save the Action.

Pre and Post Commands

(Requires FTC module) When connecting to a mainframe for file transfers, you might need to provide specific parameters in the Protocol: Upload Action and Protocol: Download Action.

To define commands to occur before and after the upload or download action

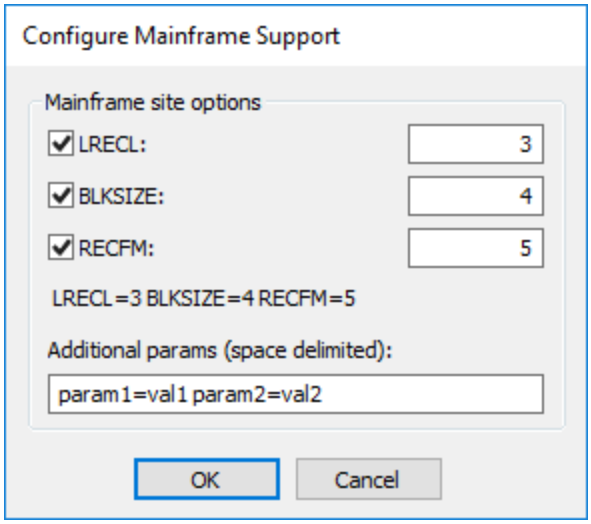
1. When defining the **File Offload Configuration** or **File Download Configuration** to connect to a mainframe computer, click **Pre/Post**.



2. In the **Pre/post commands** dialog box, click the **Operations** drop-down list to specify one of the following operations to occur before and after the Upload Action.
    - Not Chosen
    - Create Folder
    - Remove Folder
    - Rename Folder
    - Delete File

- Mainframe Support - Used to specify information that may be required when sending a file/dataset to a mainframe computer.

3. For the Upload action, in the **Params** box, you can specify any other necessary parameters that need to be passed.
4. Select the **If the command fails, treat as success** check box if you want the event rule to continue.
5. When you choose the **Mainframe Support** operation, then click **Configure**, the **Configure Mainframe Support** dialog box appears.



6. Select the applicable check boxes and provide the parameters:
   - **LRECL** = Logical Record Length; By default, Windows creates files with a logical record length of 256, at which point the line wraps. You can specify a different length in this box.
   - **BLKSIZE** = Block Size of the data set; Normally a multiple of LRCEL.
   - **RECFM** = Record Format; Specifies the characteristics of the records in the data set as:
     - F - Fixed record length
     - V - Variable record length
     - U - Undefined record length
     - B - Blocked records
     - S - Spanned records
     - A - Records contain ISO/ANSI control characters
     - M - Records contain machine code control characters

For the Upload action, the **Additional params** box can be used to provide other parameters as needed. Separate multiple parameters with a space (not a comma).

7. Click **OK** to save the Pre/post commands configuration.

Datasets in Event Rules

You can create and interact with a dataset using Event Rules dataset Actions.

The data in a dataset is laid out like a database table, which has a unique name and consists of columns and rows. The columns consist of pre-defined units of data. The rows contain the actual data for the columns. An example of a simple dataset containing customer data is illustrated below. The name of the dataset is Customers. The first row (in bold) contains the unique names of the dataset columns, which in this case, describes the data type. All other rows include the actual data as described by each column.

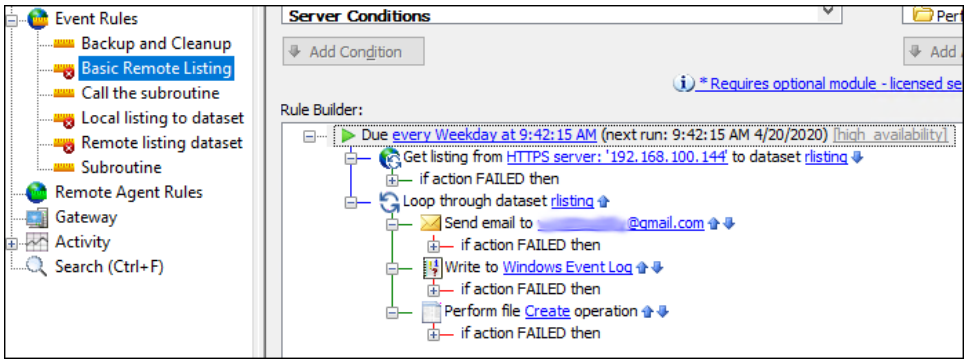
Datasets are accessed in the same way that you access information in a database, by specifying the column and row where the data resides. Every dataset created and used must have a unique name. The unique name of the dataset must be referenced followed by the column name enclosed in percentage signs. For example:
`%DatasetName.ColumnName%`

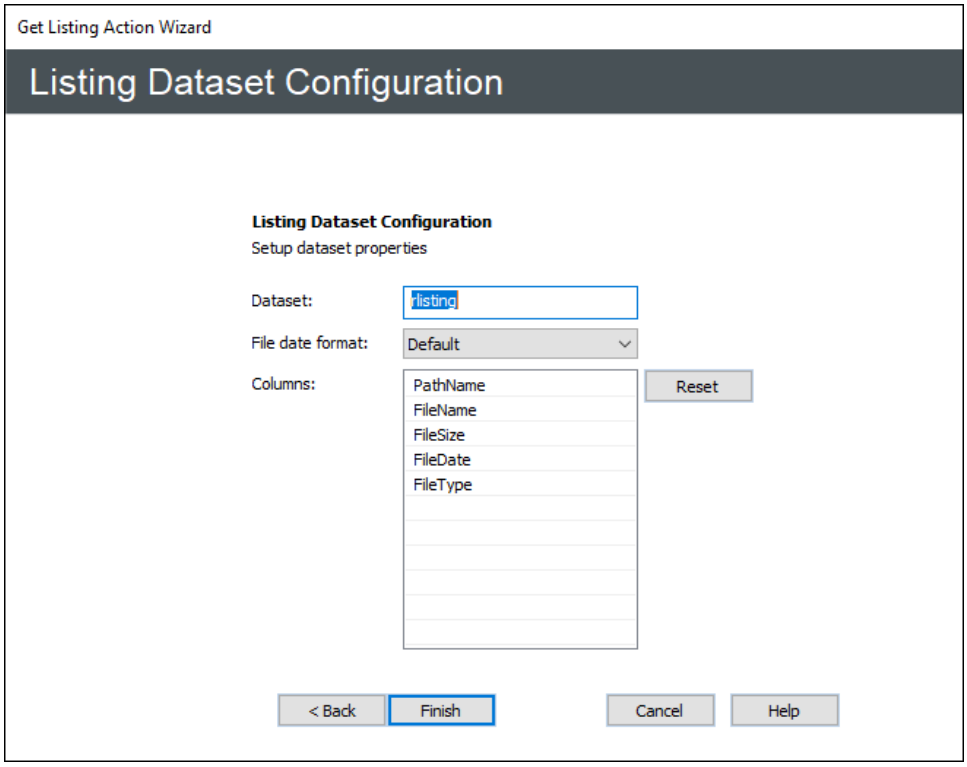
When a dataset is created, the current row is automatically set to 1 (assuming that the dataset has any data, since it is possible for a dataset to have 0 rows, such as when a SQL Query returns no data). A dataset is of minimal use, however, unless one can access the other rows. Typically, this is accomplished by using the Loop through Dataset action, which takes a dataset name as a parameter and automatically increments the current row with each iteration. The loop continues until all the rows have been accessed. In this way, you could make a task that performs operations on each row of the dataset while using the same expression. For example: `%Customers.Email%.`

Using a Loop through Dataset Action is not the only way to access dataset rows. It is possible to directly access a particular row of a dataset by supplying the row number within the expression. For example, if the dataset contains five rows and you need to get the data in row 2, simply enter the row number enclosed in parenthesis directly after the dataset name. For example: `%DatasetName(2).ColumnName%.`

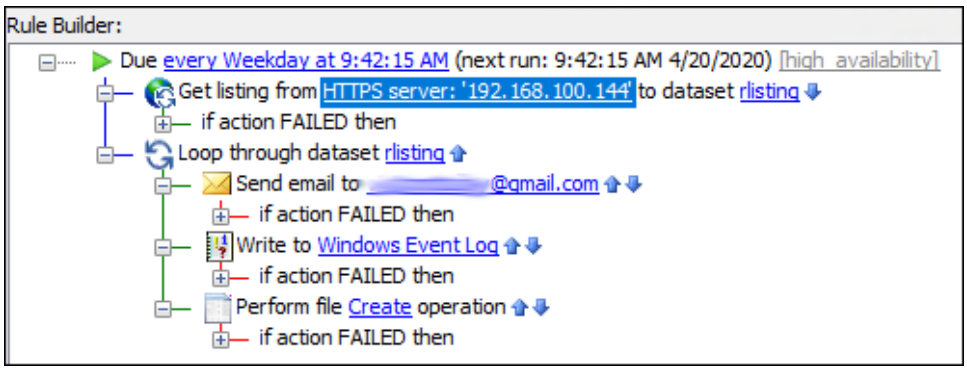
Example of creating and using a dataset in Event Rules

Create an Event Rule to connect to a remote EFT, login as that remote user, grab the contents of the user's home directory, and pipe it out to a dataset. You can list to the dataset over any protocol, HTTPS, SFTP, FTPS





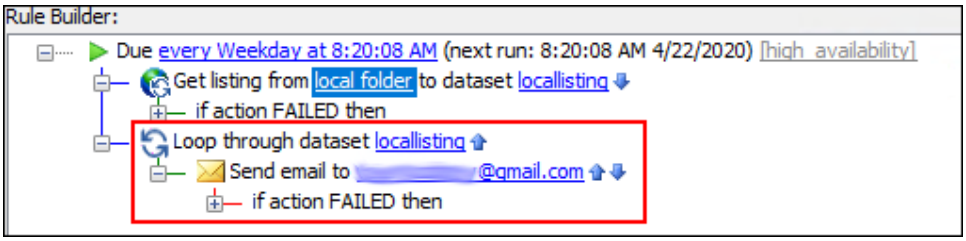
You can take the contents of that dataset and output the contents via Email, Windows Event Log, or write to a file.



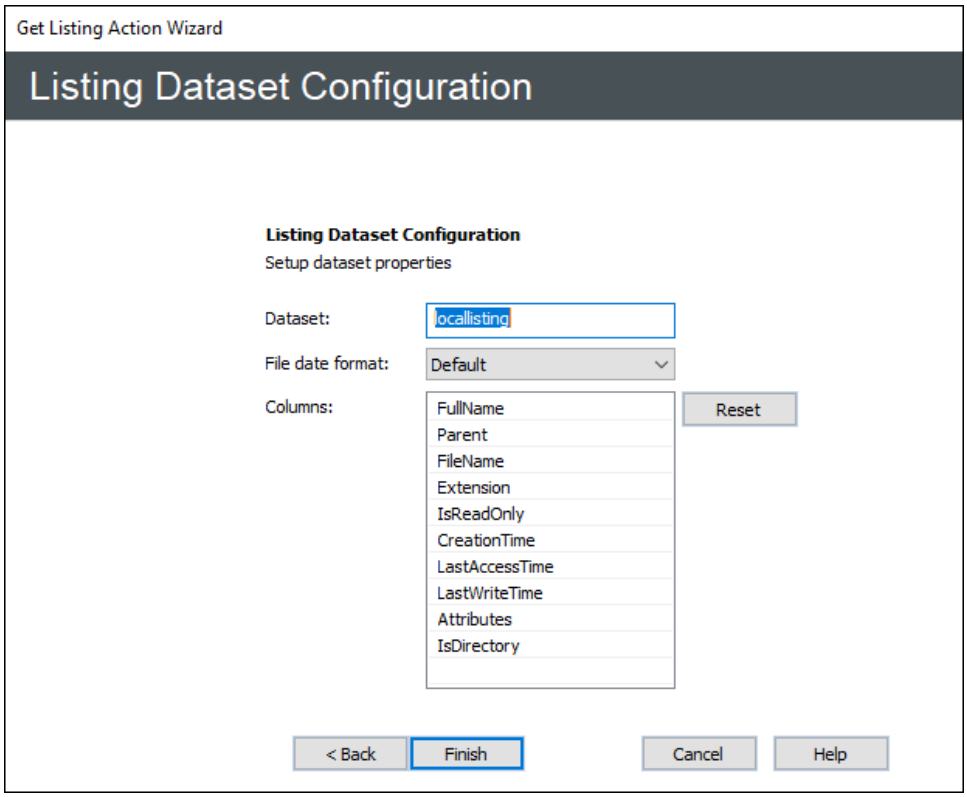
Below is an example of what contents you need to put in the Email, WEL, or file write to grab the contents:

```
Total Rows    =  %rlisting.TotalRows%
Total Columns = %rlisting.TotalColumns%
Current Row = %rlisting.CurrentRow%
Column Names = %rlisting.ColumnNames%
%rlisting.CurrentRow.FileName%
%rlisting.CurrentRow.FileSize%
%rlisting.CurrentRow.FileDate%
%rlisting.CurrentRow.FileType%
```

Local listing to dataset



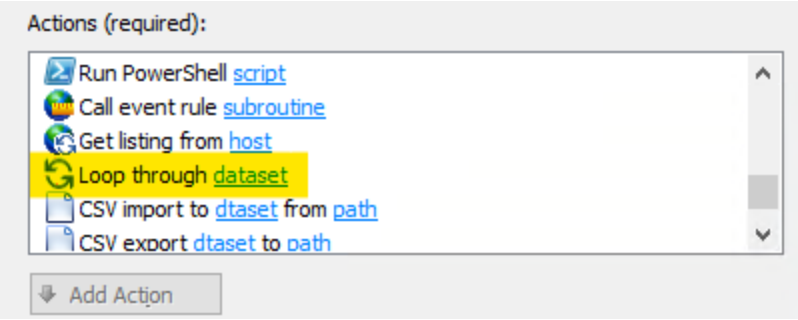
Get Listing from Host Action



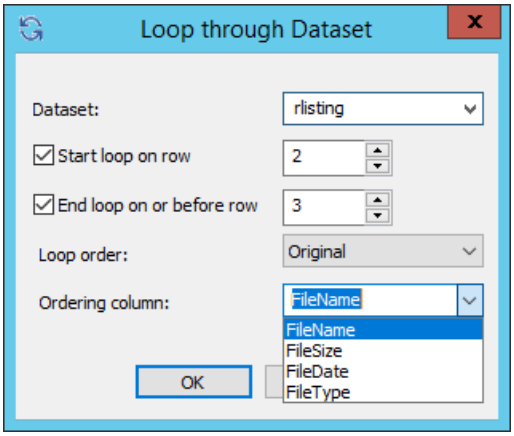
Below is an example of what contents you need to put in the Email, WEL, or file write to grab the contents of the local listing:

```
Total Rows   =  %locallisting.TotalRows%
Total Columns = %locallisting.TotalColumns%
Current Row = %locallisting.CurrentRow%
Column Names = %locallisting.ColumnNames%
Full Name = %locallisting.CurrentRow.FullName%
Parent = %locallisting.CurrentRow.Parent%
File Name = %locallisting.CurrentRow.FileName%
Extension = %locallisting.CurrentRow.Extension%
Is Read Only = %locallisting.CurrentRow.IsReadOnly%
Creation Time = %locallisting.CurrentRow.CreationTime%
Last Access Time = %locallisting.CurrentRow.LastAccessTime%
Last Write Time = %locallisting.CurrentRow.LastWriteTime%
Attributes = %locallisting.CurrentRow.Attributes%
Is Directory = %locallisting.CurrentRow.IsDirectory%
```

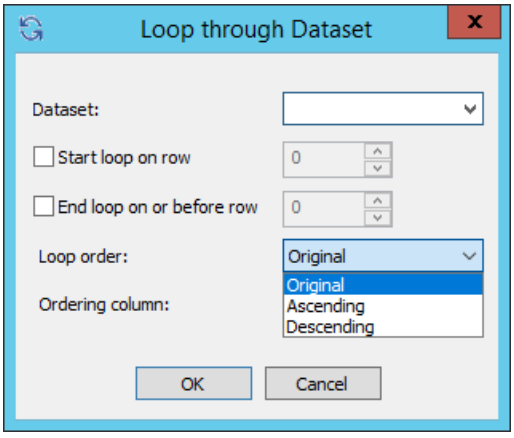
Loop Through Dataset Action



You can specify to loop through the whole dataset, or start and end on a specific row, and specify the column for ordering.

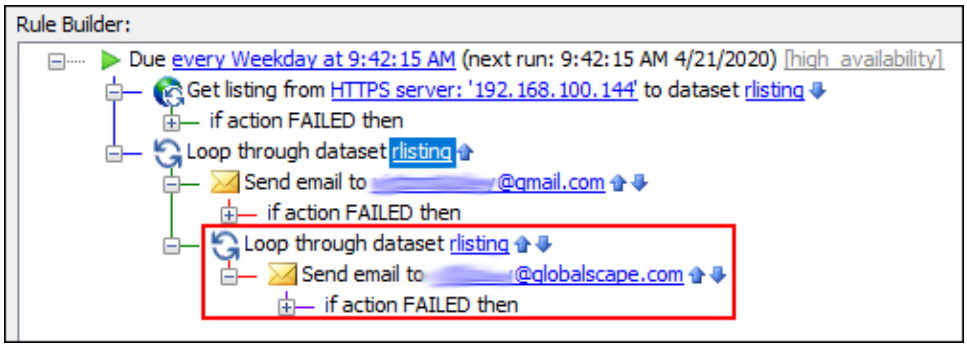


You can specify the order of the loop to start from its Original order, or specify an Ascending or Descending order.



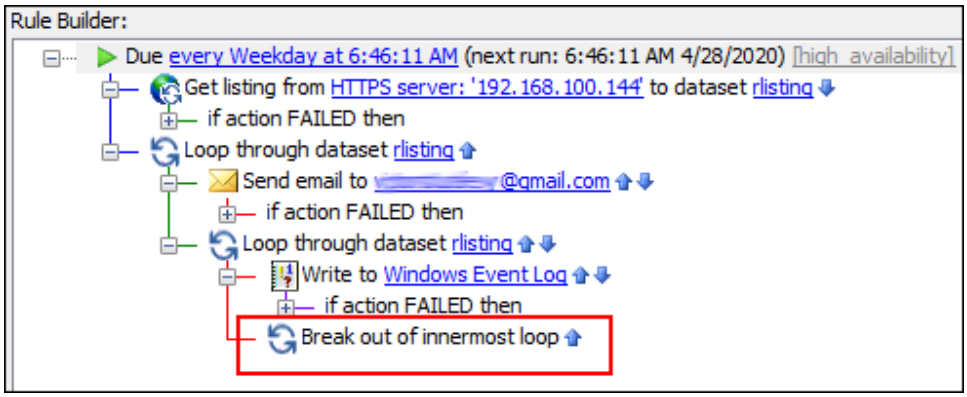
Loops can also be added into other loops

In this event rule, for each cycle of the external loop it will perform an internal loop:



Break from loop

When conditions in the loop are met, there is no need to continue parsing the dataset. In this event rule, the second loop will break after it runs through the dataset one time. The first loop will continue until complete.



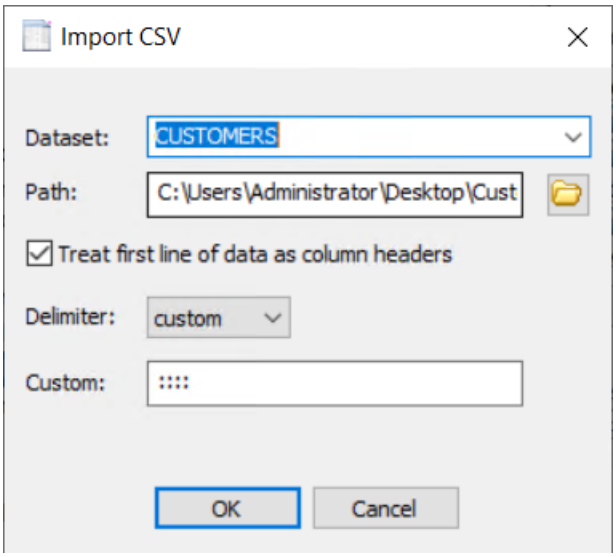
CSV Export/Import to Dataset to/from Path

You can import data from a CSV file into a dataset, so that you can later import that work with this dataset in EFT's rules (loop through dataset for example)

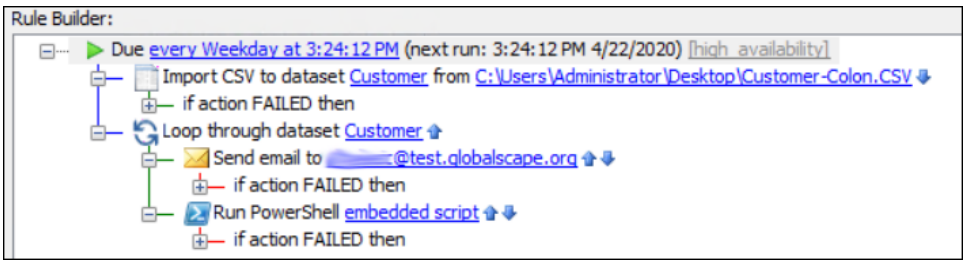
In the **CSV import to dataset** dialog box is used to specify the source CSV file (Click the file icon and click the file that you want to import). In this way, you can create and populate a dataset. Advanced options allow you to treat the first line of data as column headers and specify the delimiter format (comma, semicolon, tab, space, or custom). Comma is the default.

If the option "Treat first line of data as column headers" is not selected, the dot notation for referencing the fields in a records will be: Column0, Column1, Column2, and so on.

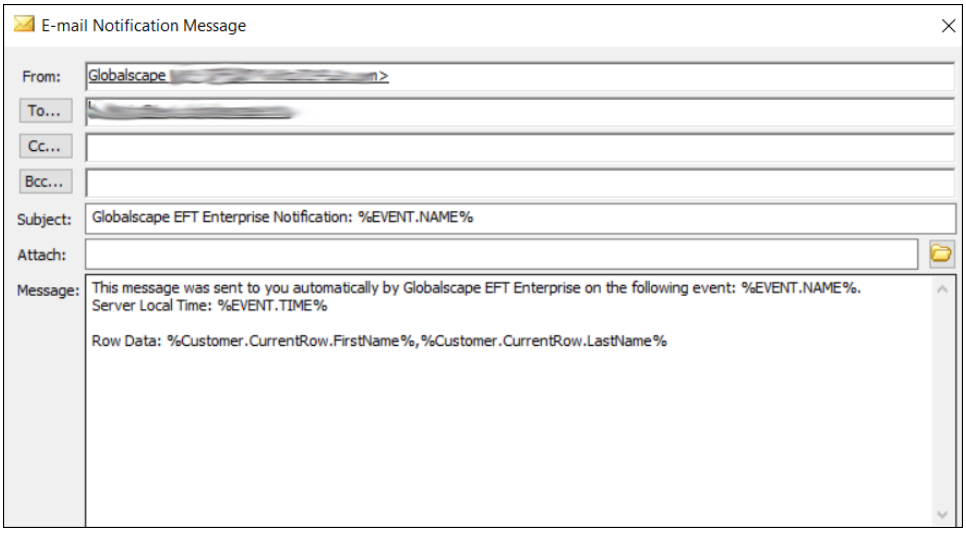
For the record below it would be `%Customer.CurrentRow.Column0%`.



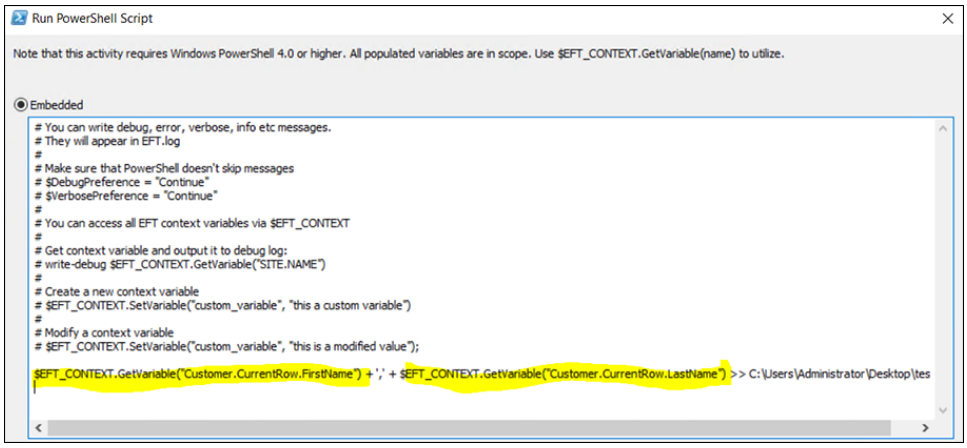
You can create an Event Rule that reads in a CSV-formatted file and then uses the records in the dataset in the steps of the Event Rule:



Referencing the dataset in dot notation will look like this in the **Send notification email** Action:

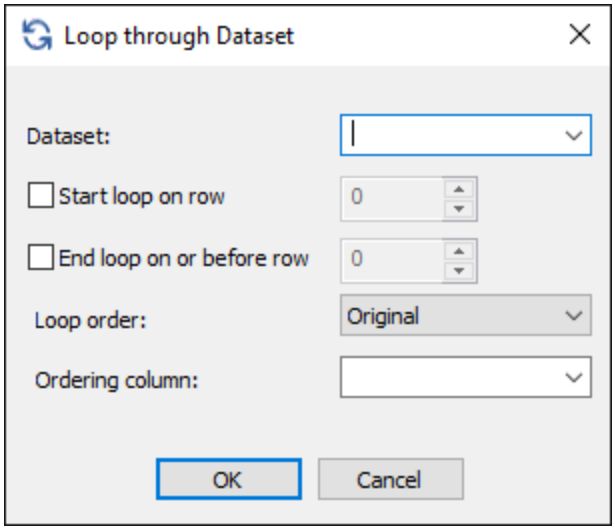


PowerShell does not handle the % sign. The example below shows how to reference custom variables:



Loop: Dataset and Loop Break Action

(Require EAM) A **Loop: Dataset** Action reads through ("parses") a dataset until the end of the dataset is reached or a Loop Break is used to stop the loop.



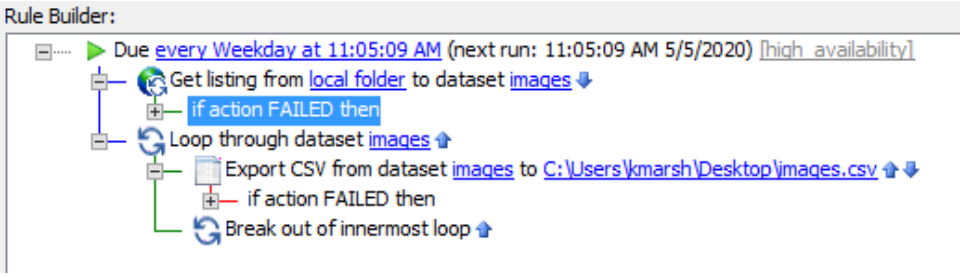
- You can specify to loop through the whole dataset, or start and end on a specific row.
- You can specify the order of the loop to start from its original order, or specify an Ascending or Descending order.
- You can specify the **Ordering column** for the loop. The default is the first column.
- Loops can also be added into other loops (see example provided below).

- Loop break action is not available outside of a loop statement and is not visible when selecting event rule. Also, you can't move a Loop Break out of the most outer loop in the Rule Builder using drag & drop.

Loop Break

The Loop Break Action is only displayed when it is usable. You can break from a loop when conditions are met earlier in the loop and there is no need to continue parsing the dataset.

In this Rule, the second loop will break after it runs through the dataset 1 time. The first loop will continue until complete.



Dataset size is limited to 10,000 rows to avoid out-of-memory crashes.

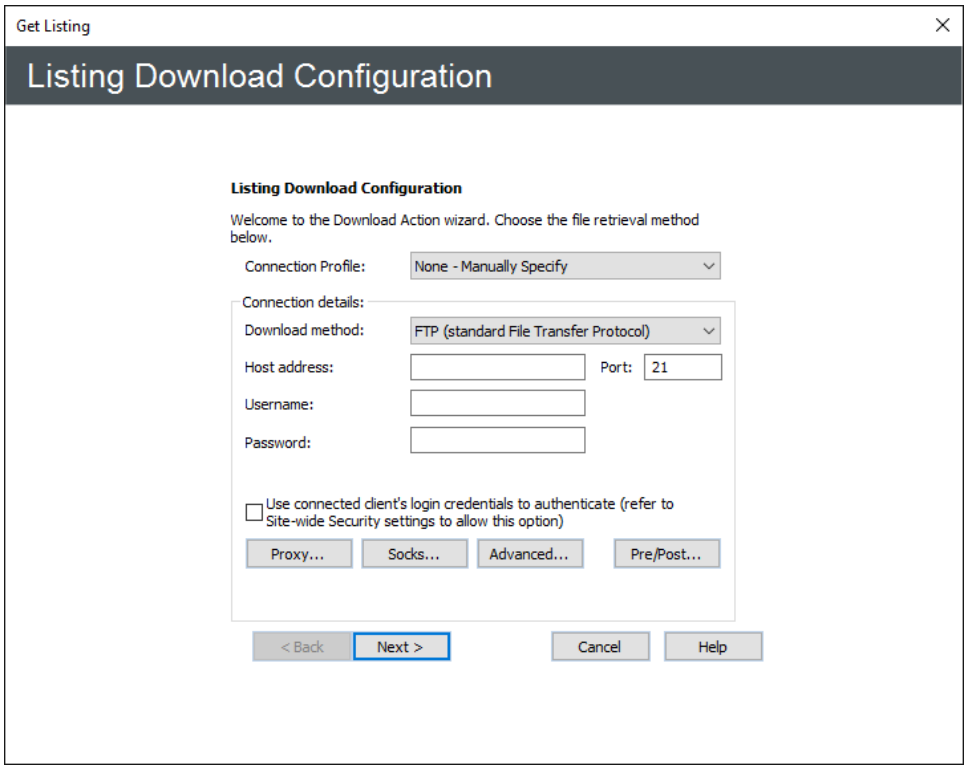
Protocol: Listing to Dataset Action

(Require EAM) The **Protocol: Listing to Dataset** Action is used to read from a remote directory listing to create a dataset or read from a CSV file to create a dataset.

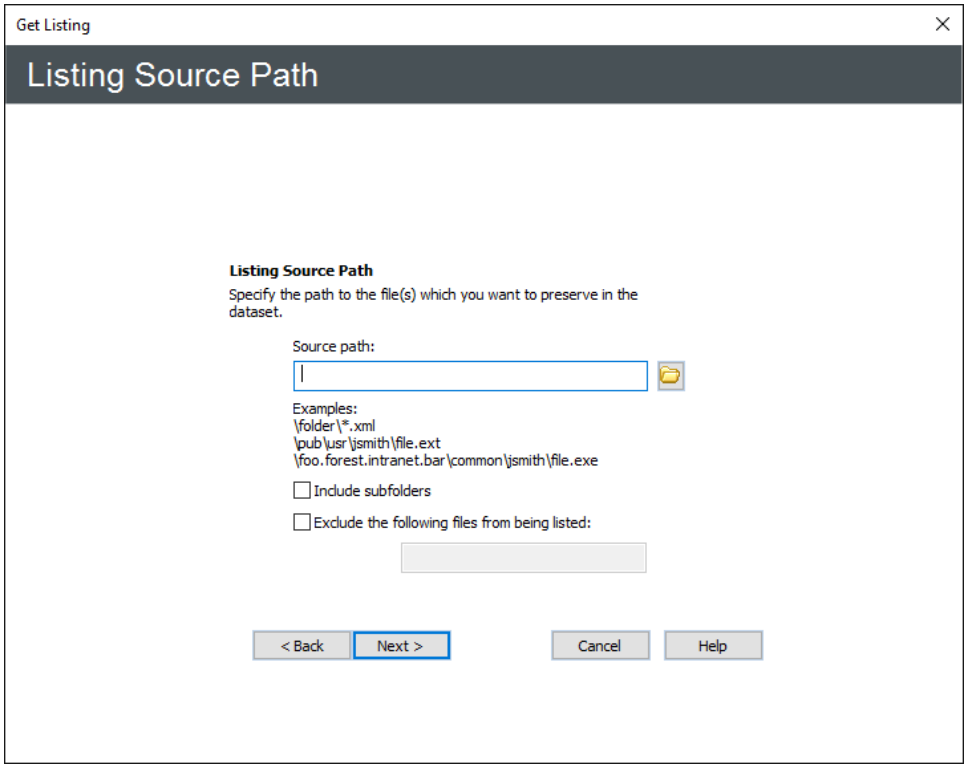
> **NOTE:** Dataset size is limited to 10,000 rows to avoid out-of-memory crashes.

To create the dataset

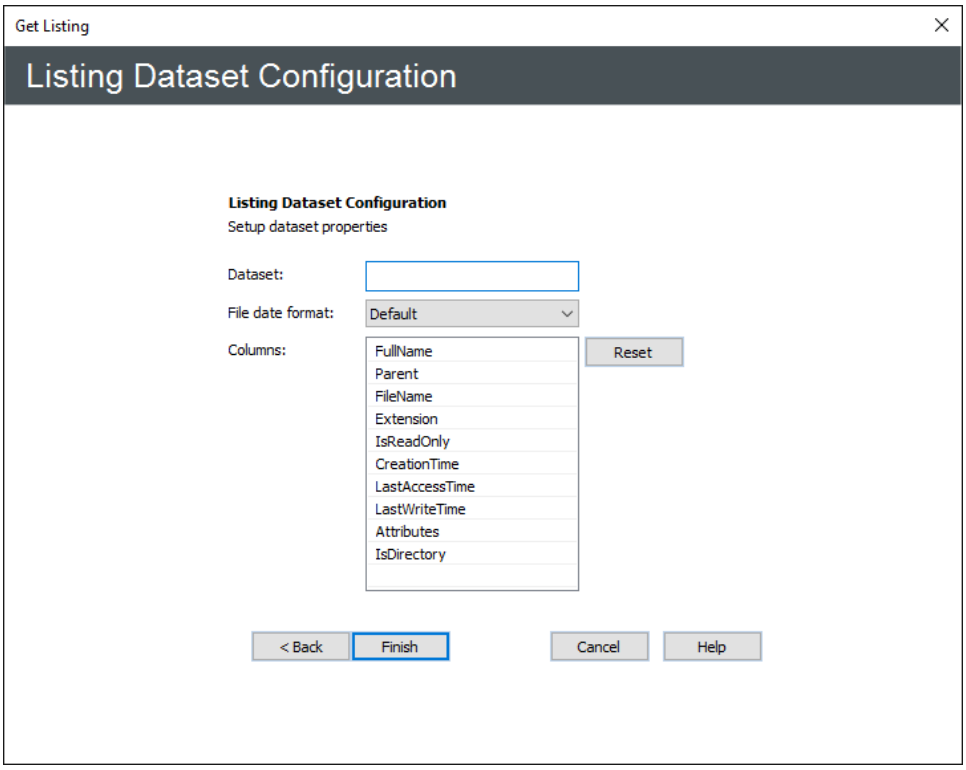
1. Create an Event Rule using the Scheduler (Timer) Event.
2. Add the **Get listing from host** Action to the Rule.
3. Click the server link to open the **Get Listing Action** wizard.
4. Specify the **Connection** details. (See Download Action for details, if needed.)



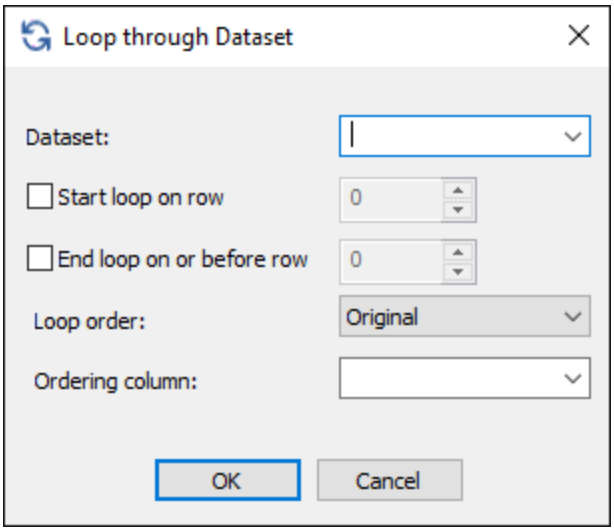
5. Specify the **Source path** (See Download Action for details, if needed).



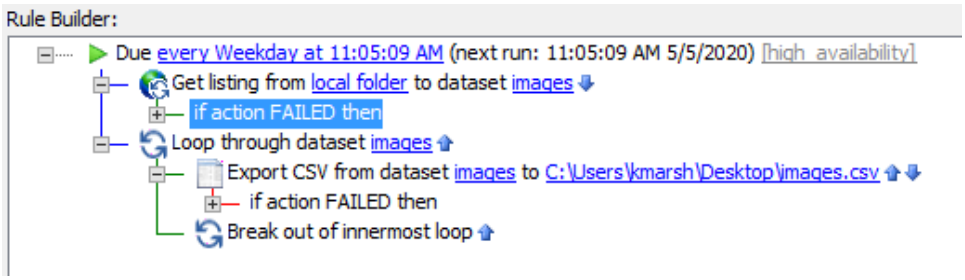
6. Specify the **Dataset properties.**



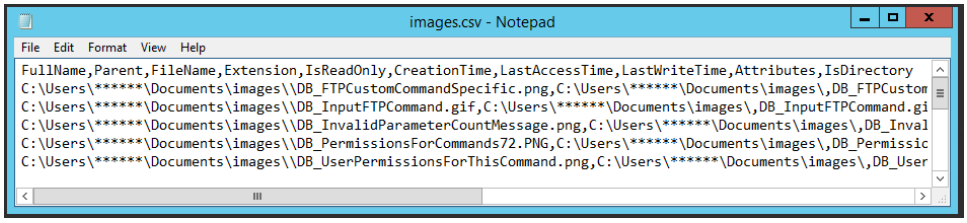
7. The **Dataset** can name can be whatever you want.
8. The **File date format** can be **Default**, **Epoch**, or **ISO-8601**.
9. The **Columns** are based on the directory you're pointing to.
10. Click **Finish** to close the wizard.
11. Add the **Loop through dataset** Action, and specify the Loop properties. (Refer to Loop Through Dataset Action for more information, if needed.)



12. The **Dataset** name that you specified in the **Get Listing Action** wizard appears as a selection in the **Dataset** drop-down list..
13. The column names from the **Get Listing Action** wizard appear in the **Ordering column** drop-down list.
14. Click **OK**.
15. Add an Action for what to do with the data, such as the CSV export dataset to path Action.



16. Using the **CSV export dataset to path** Action, the output looks similar to this:



17. Which you can then open as a spreadsheet:

	A	B	C	D	E	F	G	H	I	J
1	FullName	Parent	FileName	Extension	IsReadOnl	CreationTime	LastAccessTime	LastWriteTime	Attributes	IsDirectory
2	C:\Users\	C:\Users\	DB_FTPCustomCommandSpecific.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:59	A	FALSE
3	C:\Users\	C:\Users\	DB_InputFTPCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	2/10/2010 9:22	A	FALSE
4	C:\Users\	C:\Users\	DB_InvalidParameterCountMessage.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:59	A	FALSE
5	C:\Users\	C:\Users\	DB_PermissionsForCommands72.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	9/30/2015 15:42	A	FALSE
6	C:\Users\	C:\Users\	DB_UserPermissionsForThisCommand.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:58	A	FALSE
7	C:\Users\	C:\Users\	ER_DB_ExecuteCommand_Doscript.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:04	A	FALSE
8	C:\Users\	C:\Users\	ICON_NewCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	12/6/2007 9:59	A	FALSE
9	C:\Users\	C:\Users\	ILLUST_CommandTree.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	6/8/2009 13:34	A	FALSE
10	C:\Users\	C:\Users\	ILLUST_DisabledCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	7/17/2009 16:26	A	FALSE
11	C:\Users\	C:\Users\	ILLUST_RuleBuilder_ExecuteCommand.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	11/4/2008 10:14	A	FALSE
12	C:\Users\	C:\Users\	TAB_CommandList61.gif	.gif	FALSE	5/4/2020 11:26	5/4/2020 11:26	6/8/2009 13:36	A	FALSE
13	C:\Users\	C:\Users\	TAB_CommandSettings.png	.png	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 16:59	A	FALSE
14	C:\Users\	C:\Users\	WIZ_CustomCommandWizard1.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:02	A	FALSE
15	C:\Users\	C:\Users\	WIZ_CustomCommandWizard2.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:01	A	FALSE
16	C:\Users\	C:\Users\	WIZ_CustomCommandWizard3.PNG	.PNG	FALSE	5/4/2020 11:26	5/4/2020 11:26	5/22/2019 17:00	A	FALSE

Protocol: AS2 Action - Sending Files to an AS2 Partner via Event Rules

(Requires AS2 module) 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 can be used for Folder Monitor, Timer, and all file-based Events.

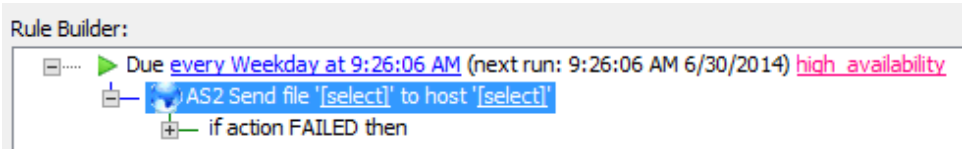
UTF-8 filenames/non-ASCII characters are not supported over the AS2 protocol. It is the responsibility of the trading partners to determine the file-naming limits imposed by their trading environments. Refer to RFC 2183, section 2.3 for details of filename parameters.

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:

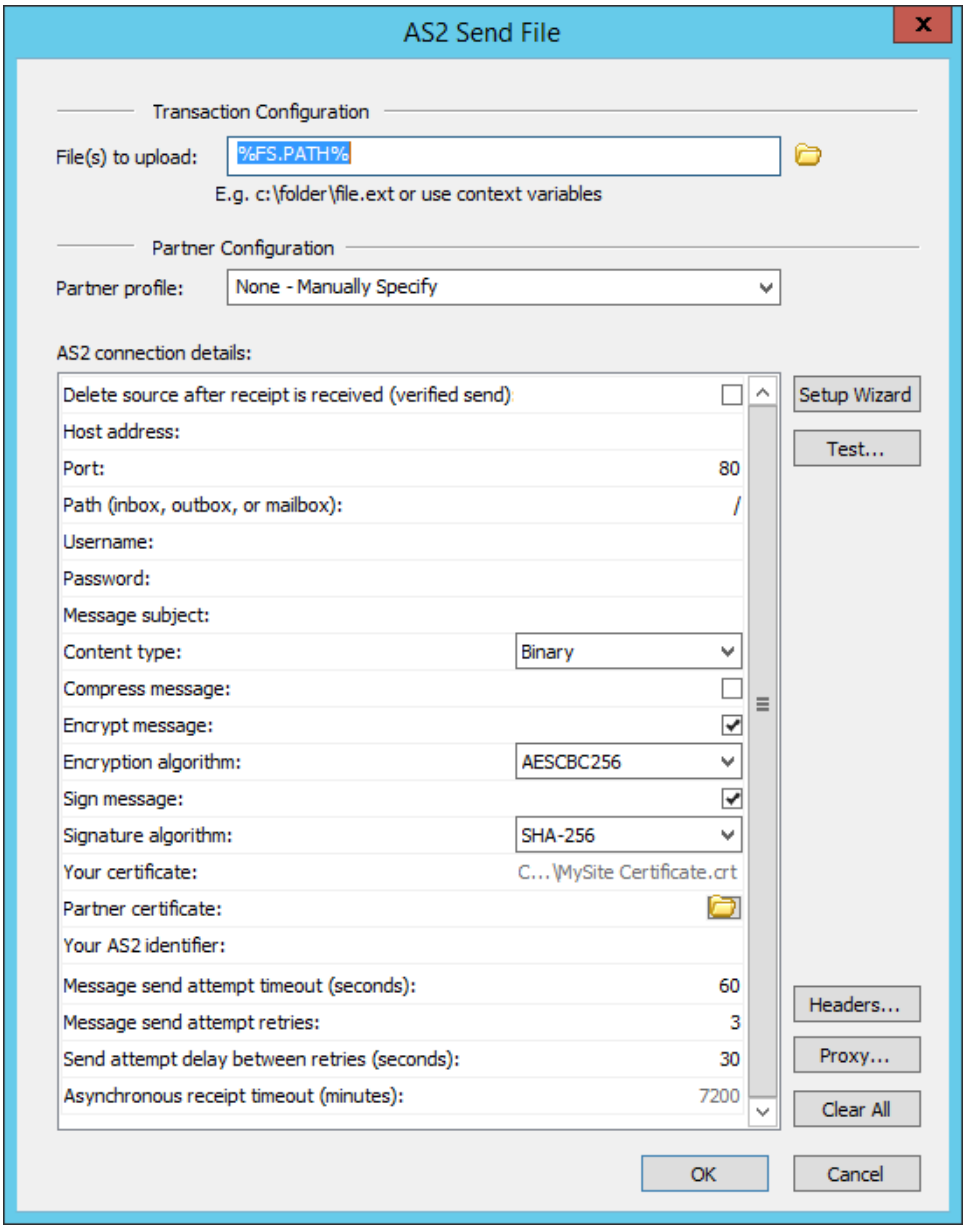
- No receipt was provided
- The receipt was not signed
- The MIC value returned did not match the original file/message MIC
- EFT was unable to:
    - verify the receipt signature
    - establish a connection to the remote host
    - upload the file to the remote host
    - send an the receipt asynchronously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



3. Click one of the underlined text links. The **AS2 Send File** dialog box appears.



4. 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

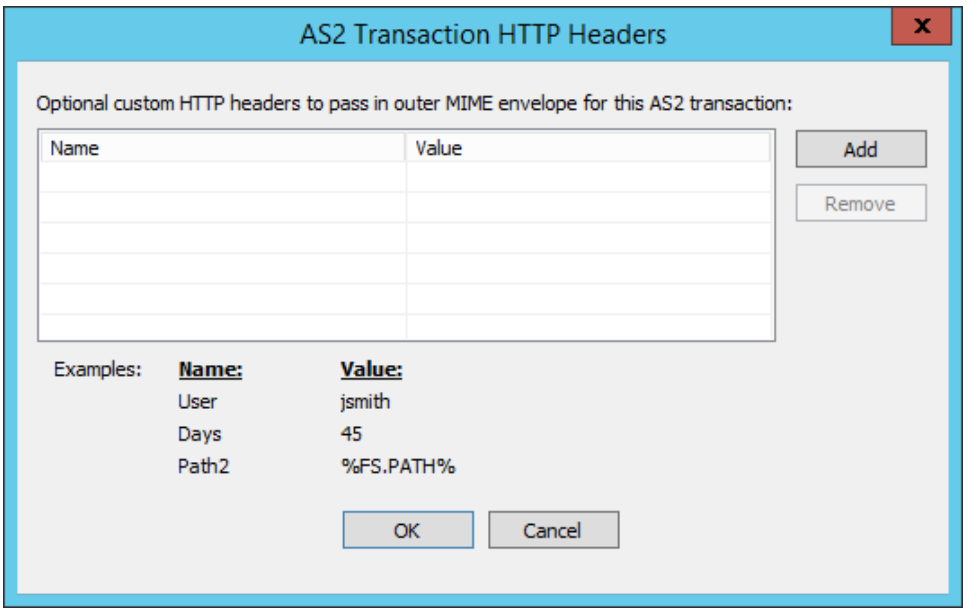
not be sent all at once; each file will have a unique message ID.)

5. 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.

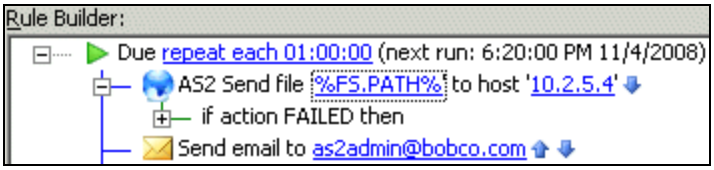
     When you use AD, LDAP, or ODBC authenticated accounts as AS2 partners, if the account in the external database is changed, deleted, or disabled, any Event Rule or Command that references the account will fail. For example, if an AD user SSmith is renamed SJones, you will have to update any Event Rule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

6. To test the configuration, click **Test.**
7. (Optional) Click **Headers** to add a custom header. The purpose of custom HTTP headers is to pass additional or required information to the recipient's server. The **Name** and **Value** fields can each contain up to 255 characters. The **Value** field can use context variables.



- To add the header, click **Add**, then provide the name and value in the table, as shown in the examples in the dialog box.

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



12. Click **Apply** to save the Event Rule on EFT.

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. Can be variables or paths. e.g. **c:\temp\robert.txt** or (if relative path) **\rob.txt** 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 (for example, 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
Path (inbox, outbox, or mailbox)	Optional	Relative path (similar to User Home Folder); forward slash (/) by default
Username	Optional	User login name
Password	Optional	Password

Field	Required/Optional	Description
Message subject	Optional	AS2 message subject
Content type	Required	AS2 content type. Options include: • **X12** - Format used by many healthcare, insurance, government, transportation, and finance organizations. • **EDIFACT** - Format adopted by the International Organization for Standardization (ISO) as the ISO standard ISO 9735. • **XML** - File format used for structured documents. • **EDI Consent** - Provides a standard mechanism for "wrapping" the EDI objects but does not specify any details about those objects. • **Binary** (default) - e.g., executables, word processing files, database, spreadsheet, and multimedia files • **Plaintext** - e.g., text and HTML files
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: • Request a signed receipt (default) • Don’t request a receipt • Request an unsigned receipt

Field	Required/Optional	Description
Receipt delivery	Required	Specifies receipt delivery method: Synchronous (default) or Asynchronous Asynchronous receipts will be returned to the domain name specified on the Site's **Connection** tab using the standard or secure listener port specified on that same page (depending on whether you specified HTTP or HTTPS for the remote host value).

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 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. 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).

AS2 Information in the Database

The Auditing and Reporting module (ARM) must be installed to use the AS2 module. If the ARM database is not configured properly, AS2 functionality is not available.

The following information is audited to the ARM database and provided in ***AS2 Transaction Reports* on page 295** and the ***Transfers - AS2 Status Viewer* on page 296**:

- Date/Time
- Raw HTTP Headers
- File name
- MDN
- MIC*
- Content Type
- Message-ID
- Remote/Local File path (mailbox)
- Remote/Local Host (hidden by default)
- Status: Success (S), Failure (F), or In Progress (IP)
- Direction: Inbound or Outbound
- EFT AS2 ID
- Partner AS2 ID
- Error (only if Failure) occurred, the verbose error. Otherwise "None".
- Action:
  - Inbound Connection (S, F, IP)
  - Outbound Connection (S, F, IP)
  - Receive File (S, F, IP)
  - Send File (S, F, IP)
  - Send Receipt Asynchronous (S,F,IP)
  - Send Receipt Synchronous (S,F,IP)
  - Receive Receipt (S,F, IP)
  - Receipt Verification (S,F)

*EFT calculates the AS2 MIC using SHA-1. (Refer to RFC 3335 for details.) You can ignore the words "MD5" that appear in the MIC column of the AS2-related reports (**tbl_ AS2Transactions** column).

AS2 Transaction Reports

The Auditing and Reporting module (ARM) gathers AS2 data and provides the data in the Transfers - AS2 node and in predefined AS2 reports. You can also define your own custom reports.

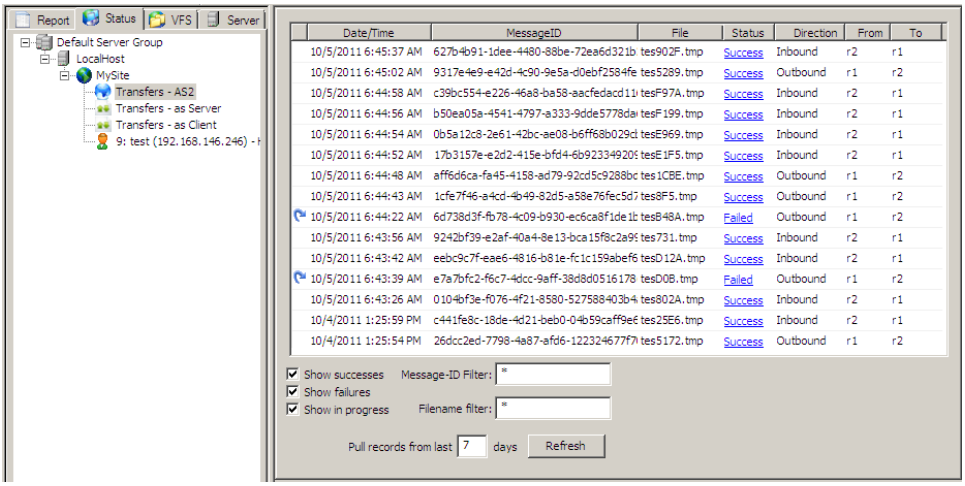
- *AS2 Transactions (Summary)* report - A transaction report that displays more detailed information than what is shown on the **Transfers – AS2** node. The report queries all AS2 transactions for the dates specified, grouped by Site, sorted by date, and listed in reverse chronological order. You can add Report Filters for the following data:
  - StartTime
  - MessageID
  - FileName
  - TransactionID
  - FromAS2ID
  - ToAS2ID
  - TransactionStatus (rolled up transaction status)

- **Success** - File was received/sent MDN successfully received/sent
- **Failure** - Transaction failed to receive/send after all retries or MDN not received/sent after all retries
- **In Progress** - Transaction started or is in progress (transferring or waiting for next retry or waiting for MDN, etc.)

- *AS2 Transactions (Detailed)* report - A verbose AS2 file transfer report that provides the information necessary for troubleshooting problem transactions. You can add Report Filters for the following data:
  - StartTime
  - MessageID
  - FileName
  - TransactionID
  - FromAS2ID
  - ToAS2ID
  - TransactionStatus
  - Sitename
  - Error (Displays **None** if there are no errors)

Transfers - AS2 Status Viewer

EFT provides a sub-node on the **Status** tab that displays a history of AS2 transactions (retrieved from the ARM database).



The **Transfers - AS2** node displays the history of AS2 inbound and outbound transfers, including the result from the MDN. For example, if a file transaction attempt fails 10 times in a row, but succeeds on the 11th attempt and the MDN is sent, the **Transfers - AS2** node reports the transaction as a success. If all of the transaction's file transfer

retries fail, then the **Transfers - AS2** node reports the transaction as a failure. If retries are still occurring at the time the **Transfers - AS2** node is invoked, the transaction will be marked as **In Progress**. You can view details of each transaction by clicking its **Status** column. EFT will query and then display (in the default text editor) the details surrounding that transaction as obtained from the ARM database.

When the **Transfers - AS2** node is selected, the last 7 days of transaction summaries are displayed in reverse chronological order. You can change the default of 7 days to display from 1 to 999,999 days of data. Click **Refresh** to display all transactions that may have occurred since the last opening or refresh of the **Transfers - AS2** node.

The node displays the following information:

- **Date and Time** - Last recorded status for the transaction
- **Message ID** - From AS2 header
- **File** - Name of file transferred
- **File Path** - Local inbox or outbox; this column is hidden by default
- **Remote Host Address** - Host address of the sender (Inbound)/receiver (Outbound). This column is hidden by default.
- **Status** - Contains a hyperlink that, when clicked, pulls the *AS2 Detailed* report for that transaction. The report displays transaction details, which is most helpful for in-progress or failed transactions.
  - **Success** - Transaction completed and MDN successfully received/sent
  - **Failure** - Transaction failed to send after all retries or MDN not received/sent
  - **In Progress** - Transaction started or in progress (transferring or waiting for next retry or waiting for MDN, etc.)
- **Direction** - **Inbound** or **Outbound**
- **From** - Server's AS2 ID or the Partner ID (depends on direction)
- **To** - Server's AS2 ID or the Partner ID (depends on direction)

The **Resubmit** icon , to the left of failed transactions, allows you to resubmit the file(s) and/or MDN(s). You can also resubmit a file, or group of files by multi-selecting failed transaction rows, then right-clicking and clicking **Resubmit**. If you resubmit a file that is a part of multi-file transaction, all of the files will be resubmitted. You can only resubmit failed transactions. You cannot resubmit in-progress or successful transactions.

Customizing the Display

You can customize the **Transfers - AS2** status viewer to suit your needs:

- Choose the columns to display or hide by right-clicking on a column header, then selecting/clearing the column name in the submenu.
- Sort by a specific column in ascending or descending order by clicking the column header.
- Define filters to display or hide rows based on **Status**, **Message-ID**, or **File Name**.
    - To filter the display based on status, select or clear the **Show successes**, **Show failures**, and **Show in progress** check boxes, and then click **Refresh**
    - To filter the display based on the message-ID, in the **Message-ID** box, type the message ID, and then click **Refresh**.
    - To filter the display based on the filename, type a name in the **Filename** box, and then click **Refresh**.
    - To change the number of days of history to display, in the **Pull records from last**<*n*>**days** box, type the number of days, from 1 to 9999.
- Refresh or clear the display by right-clicking an empty row, and then clicking **Refresh**, or in the filter area, click **Refresh**.

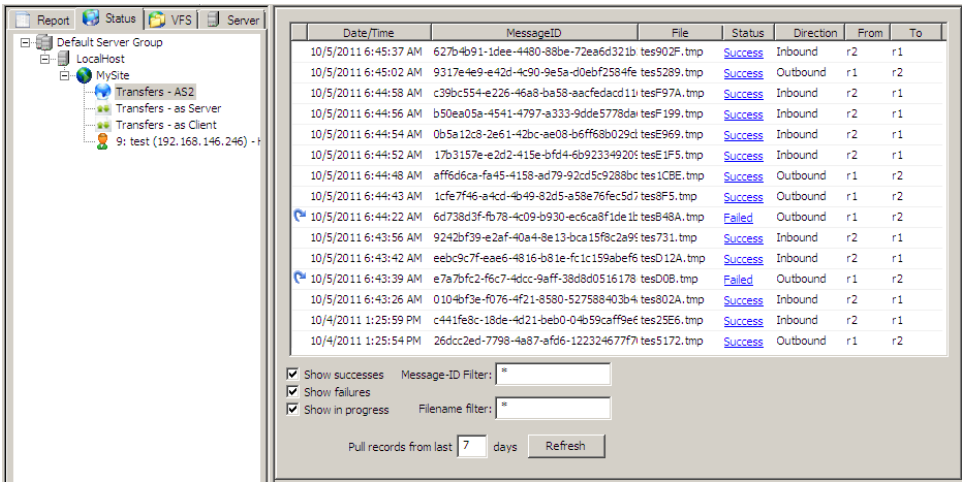
Resubmitting AS2 Transmissions

In the **Transfers - AS2** node, the **Resubmit** icon to the left of failed transactions allows you to resubmit the file(s) and/or MDN(s). You can only resubmit failed transmissions. You cannot resubmit in-progress or successful transmissions.

- **Outbound**. If a failure was an outbound transaction (failed after all retries and the MDN was never received), you can attempt to send the same file again.
- **Inbound**. When an inbound transaction fails, resubmit is allowed only when the failure was due to a failure in sending the receipt (MDN). (EFT cannot resubmit the file, because it did not send it to begin with.) The resubmit action attempts to resend the MDN receipt.

To resubmit a transmission

1. In the administration interface, connect to EFT, and click the **Status** tab.
2. Expand the Server and Site nodes, and then click the **AS2 Transactions** node. The Site's AS2 transactions appear in the right pane.



3. Click in the row of the failed transaction to select it, and then click the **Resubmit** icon . A confirmation prompt appears.
4. Click **Yes**. The transaction is resubmitted and appears in a new row. The resubmitted transaction populates a new row in the **Transfers – AS2** node with the new transaction and new message ID.

   There can be multiple rows (other transmissions) between the failed transmission and the resubmitted transmission.

AS2 Transaction Success and Failure Notification

EFT can execute a command or send an email to notify you of the success or failure of AS2 transactions. The email or Command is triggered when all message send attempts have been attempted or the asynchronous MDN wait time has expired (if applicable).

The email notification and custom command are configured by clicking the applicable link in the **AS2 Inbound** and **AS2 Outbound** tabs or in the AS2 Partner Access wizard.

- Clicking the Transaction FAILED/SUCCESS notification email link, **[Add]**, opens the Edit Mail Template dialog box.
- Clicking the Transaction FAILED/SUCCESS send command link, **[Add]**, opens the Custom Command dialog box. (You will have to define the custom command before using it in the notification.)
- Each of the fields are optional

Field	Description
Transaction FAILED notification email	Opens the **Edit Mail** dialog box in which you can specify an email notification for failed transaction.
Transaction SUCCESS notification email	Opens the **Edit Mail** dialog box in which you can specify an email notification for successful transaction.
Transaction FAILED run command	Opens the **Custom Command** dialog box in which you can specify a **Command** to run upon failed transaction.
Transaction SUCCESS run command	Opens the **Custom Command** dialog box in which you can specify a **Command** to run upon successful transaction.

- Refer to email Notification Action for details of defining an email notification.
- Refer to Creating a Command to create a command and refer to Script: Custom Command Action for details of using a Command.

Protocol: Download Action

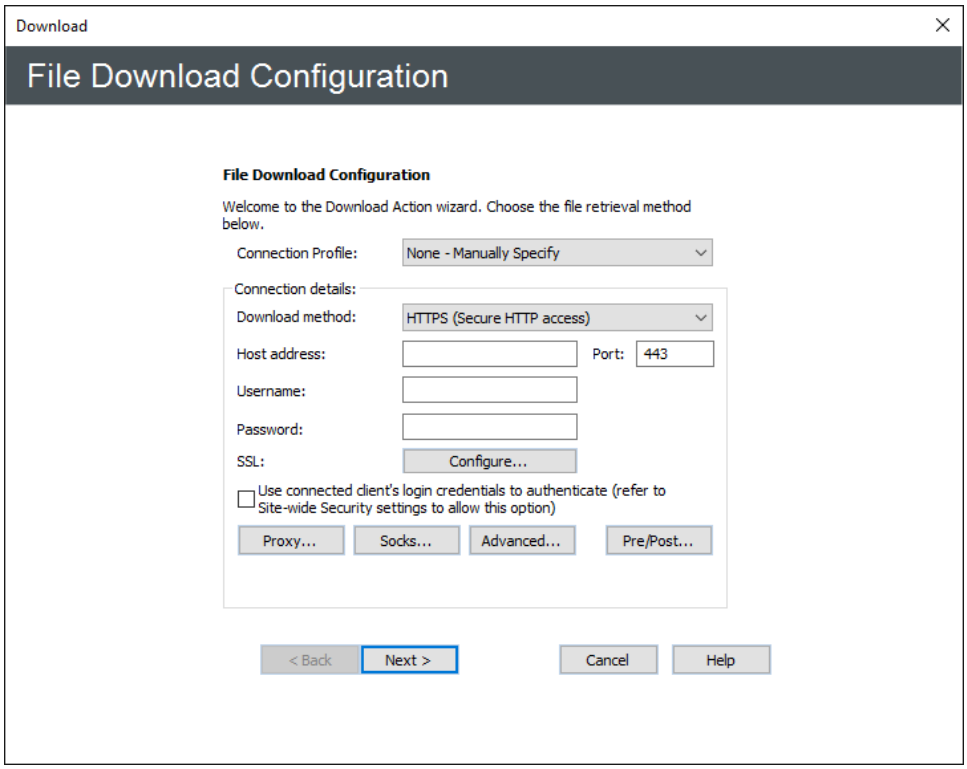
(Requires FTC module) You can configure an Event Rule to copy or download from a specific location to a specified local folder using a particular protocol when an Event occurs. You must provide EFT with connection information (protocol and login details) and file information (source path and destination 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 does the transfer, including all retries, before moving on to the next Action, such as an email 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.
- When setting up the File Download Action using variables, the remote connection test fails because variables appear undefined.

Refer to Connection Profiles for details of setting up a Connection Profile before defining the Action.

To set up EFT 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 **Protocol: Download**. The Rule parameters are added to the Rule in the **Rule Builder**.
3. Click one of the undefined parameters where the parameters are listed in the **Rule Builder**. The **File Download Configuration** wizard appears.



4. In the **Connection Profile** box, specify a connection profile for this Event. If none is specified, you will need to configure the **Connection details** as described below.
5. 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)**.
6. (Optional) If you selected **Local (Local Files or LAN)**, provide the **Windows account** username and **Password** for connecting to remote shares (not local folders).

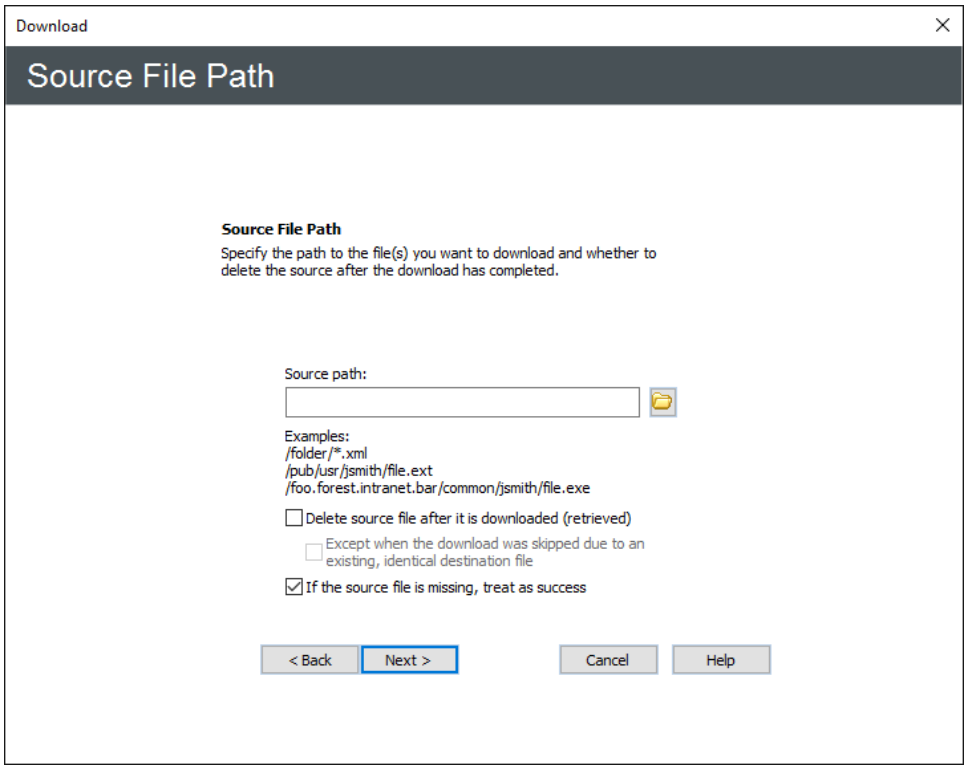
   These credentials are used only if/when a resource cannot be accessed using the credentials under which the EFT service is running. The **Optional credentials override** feature allows you to specify an alternate set of logon credentials for accessing remote network shares to which the EFT service account may not have access (due to security constraints).

   If alternate credentials are specified, EFT will use its current security token (associated with the "Log on as" account specified in the EFT service settings) for local folder access and then new security token (associated with the alternate logon credentials) for the remote source folder accessed over network connections (e.g. network shares).

- Think of Local Transfer as an operation (offload or download) with a remote server.
- Think of "Optional credentials override") as "credentials to access remote server."
- For download action, it is "credentials for source folder."
- For copy/move (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):
  - Offload: local (EFT) => remote ("override credentials")
  - Download: local (EFT) <= remote ("override credentials")
  - TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
  - TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

7. 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 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.
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 and remote server's SSL certificate information.
11. If you are connecting to a remote host through a SOCKS server, click **SOCKS** and provide the SOCKS connection information.
12. If you are connecting to a remote host through a proxy, click **Proxy**. Provide the proxy connection information.

13. To specify transfer options and time stamps, click **Advanced**. Specify the advanced transfer options, such as connection retry attempts and delay between retries.
14. To specify pre or post commands for connections to a mainframe computer, refer to Pre and Post Commands
15. Click **Next**. The **Source File Path** page appears.



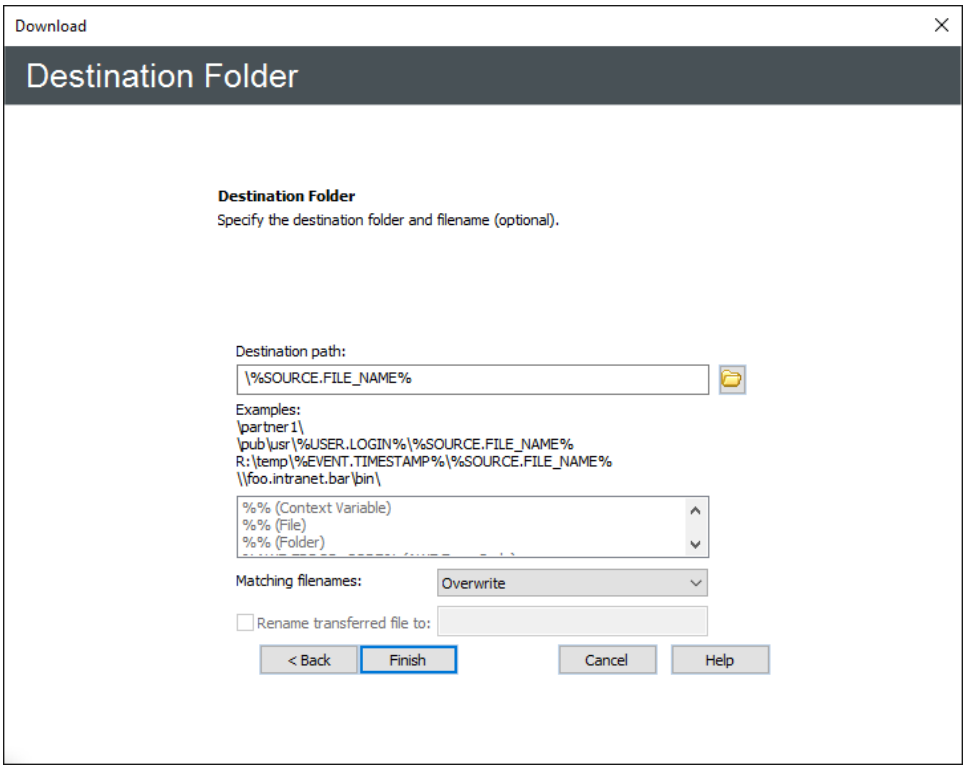
16. In the **Source path** box, provide the path to the file(s) that you want to download. For example, type:

    ```
    /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.

17. 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.)
    - Select the **Except when** ... check box if you do not want to delete the source file after it is downloaded if the download was skipped.
18. Select the **If source file is missing, treat as success check box** to treat remote file downloads as success, even if file is missing. (The client DLL in EFT doesn't have a mechanism for detecting if the file exists on the remote server or not.)

19. ***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.
20. Click **Next**. The **Destination File Folder** page appears.



21. The optional folder synchronization feature can also synch the destination folder with the source folder (2-way synchronization).
22. 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.
    - In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, or **Numerate** files that exist with the same name. If **Overwrite** is selected, EFT performs a CRC match for the files.
23. If desired, select the **Rename transferred file to** check box, then specify a new name.
24. Click **Finish**, then click **Apply** to save the changes on EFT and/or add other Actions and Conditions to the Rule.

Protocol: Email Action

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

The EFT log will display an error message when a file larger than 30 MB is attached to a **Send notification email** Action in an Event Rule.

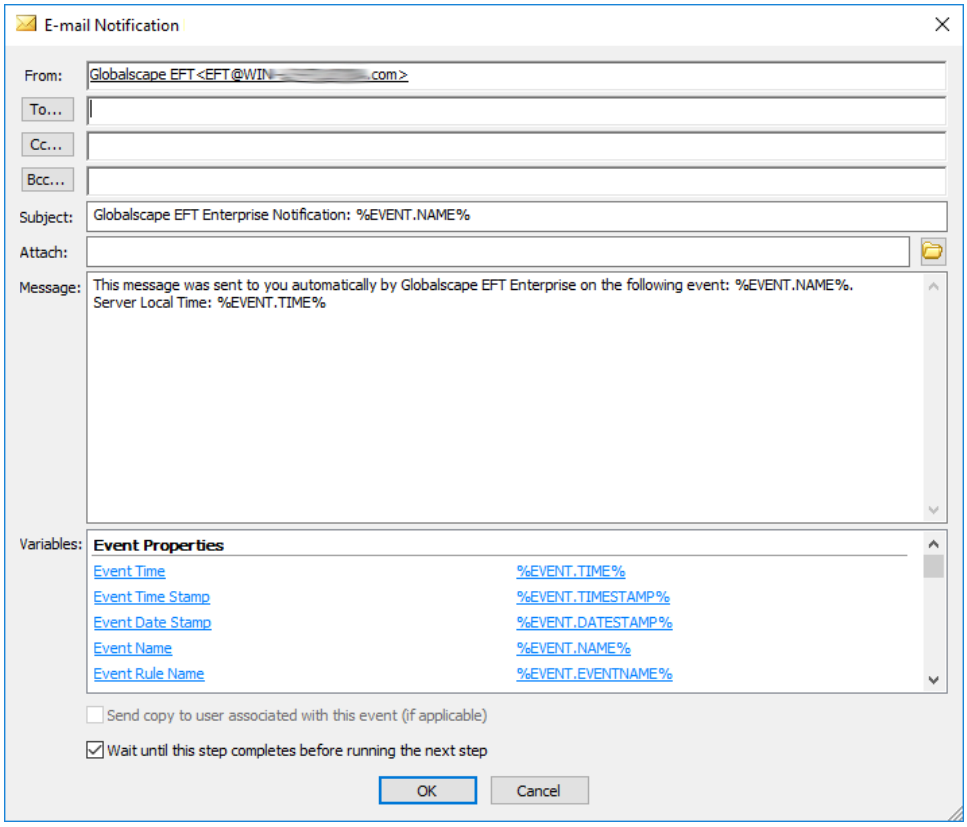
On Sites using AD Authentication, the EFT must have "Log On as a domain user" permission for email notifications to work.

To customize an Event Rule email 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 **email Notification Message** dialog box appears.



4. The **To** box displays the first email address defined in EFT 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, then specify the address.
5. Type the email 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 email addresses defined on EFT 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 email address of the logged-in user who is uploading a file, for example, if defined in the **User Account Details** dialog box).

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

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

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

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

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

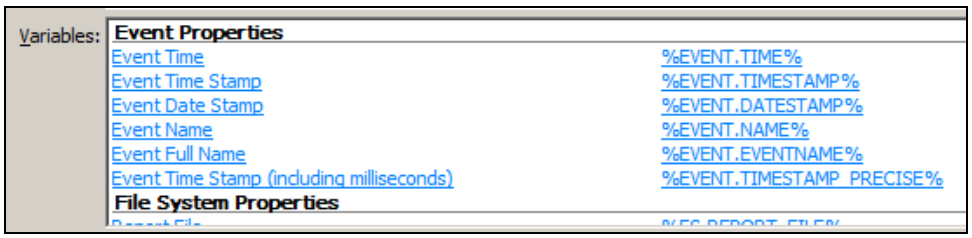
   %EVENT.NAME% is the Server-defined name for the Event (for example, File Renamed);
   %EVENT.EVENTNAME% is the user-defined name for the Event (for example, My File Renamed Event Rule).
   Also, be aware that your recipient might get hundreds of emails every day; therefore, "Here's the info you wanted"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

7. In the **Attach** box, click the folder icon to browse for a file to attach to the email. You can use a specific file path or a context variable, that contains data.

%FS.REPORT_FILE% - The full path of the report generated by the Generate Report Action, including the file name. This variable can be used in copy/move, OpenPGP, and custom commands that have a failure Event defined, but should not be used for custom command actions that do not have a failure Event defined. 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 stops processing the Event Rule, do not use this variable in email notifications; use %FS.REPORT_CONTENT% instead.

%FS.REPORT_CONTENT% - Contents of the report generated by the Generate Report Action. This variable is typically used after creation of an HTML report, in an email notification action, where it is desirable to embed the HTML contents of the report as the email body.

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



- If you want only the information contained to the variable in your email 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 email.)

10. 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.
11. (Optional) The **Wait until this step completes before running the next step** check box is selected by default. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails. **To allow the next step to run before this action completes**, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)
12. Click **OK**.
13. Click **Apply**. When the Event is triggered, the email notification is sent. The **Send notification email** Action in Event Rules puts the message into a send queue unless "Stop processing this rule" is enabled for a failed Action.

Creating an Email Notification Template

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

To create an email notification template

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

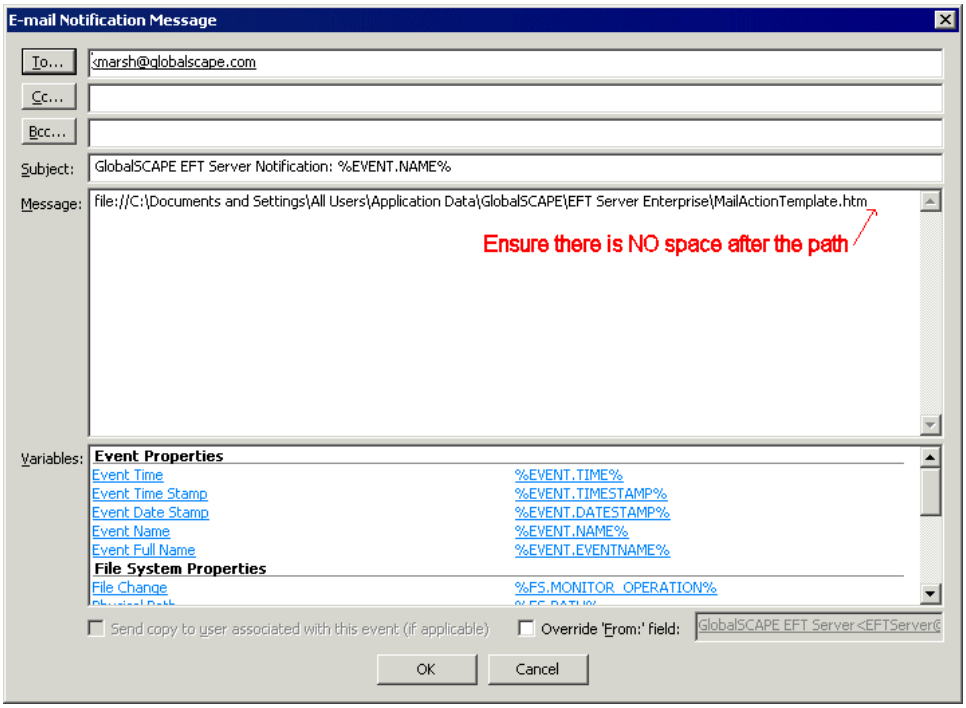
```
<HTML>
   <BODY>
        <P>This message was sent to you automatically by
Globalscape
        EFT on the following event: %EVENT.NAME%.</p>
        <HR>
        <P><B>Server Local Time:</B> %EVENT.TIME%</P>
        <P><B>Logon Name:</B> %USER.LOGIN%</P>
        <P><B>Email Address:</B> %USER.EMAIL%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

2. Define the email adding each of the variables that you want. You can add your custom EFT 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. (If you are logging into EFT 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 email notification.
6. In the **Message** box of the **email Notification Message** dialog box, type `file://` and the path to the email template, and then click **OK**. For example, type:

   ```
    file://C:\Documents and Settings\All Users\Application
   Data\Globalscape\EFT Server\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 email that is triggered by EFT. It is highly recommended that you do a test to be sure you get the results you want.

Send an Email Notification When a Certain User Uploads a File

Refer to the Globalscape Knowledgebase topic #11151 for information about sending an email notification when a certain user uploads a file.

Protocol: Synchronize Action

(Requires FTC module) The **Protocol: Synchronize Action** allows you to make a local folder list match a remote folder, or a remote folder match a local folder. The Synchronize Action is available for any Event Rule for which copy, move, or download actions are used. The wizard allows you to synchronize or mirror the folders:

With respect to EFT rules:

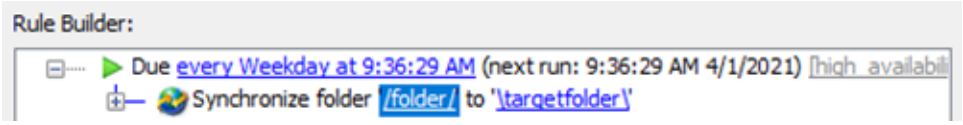
- "Mirror local – duplicate EFT's contents to the remote server"
- "Mirror remote – duplicate the remote server's contents to EFT"

With respect to RAM Agent rules

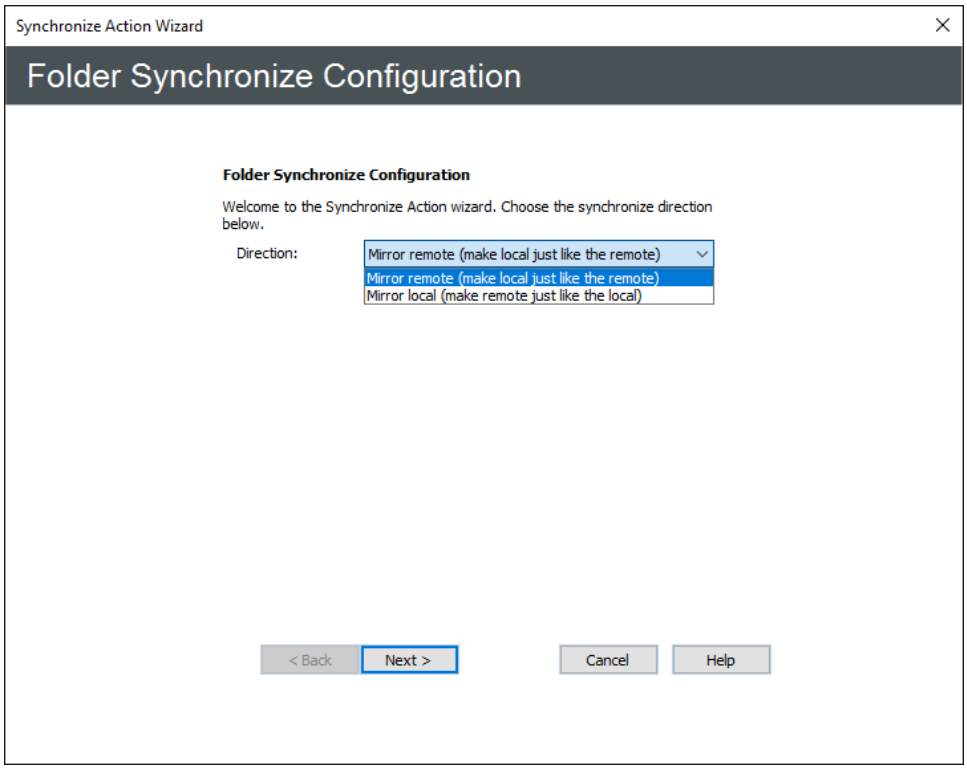
- "Mirror local – duplicate Agent's contents to the remote server"
- "Mirror remote – duplicate the remote server's contents to the Agent"

To define the Synchronize Action

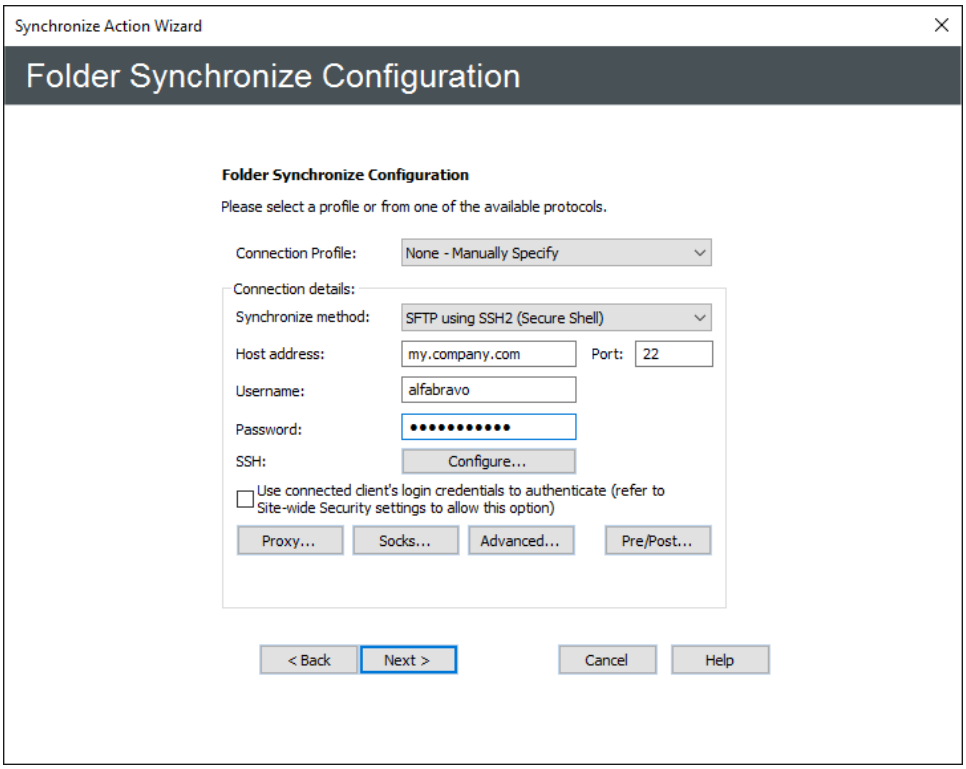
1. Follow the procedure in Creating Event Rules or select the Rule to which you want to add the Action.
2. In the **Actions** list, click **Protocol: Synchronize**. The Rule parameters are added to the Rule in the **Rule Builder**.



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

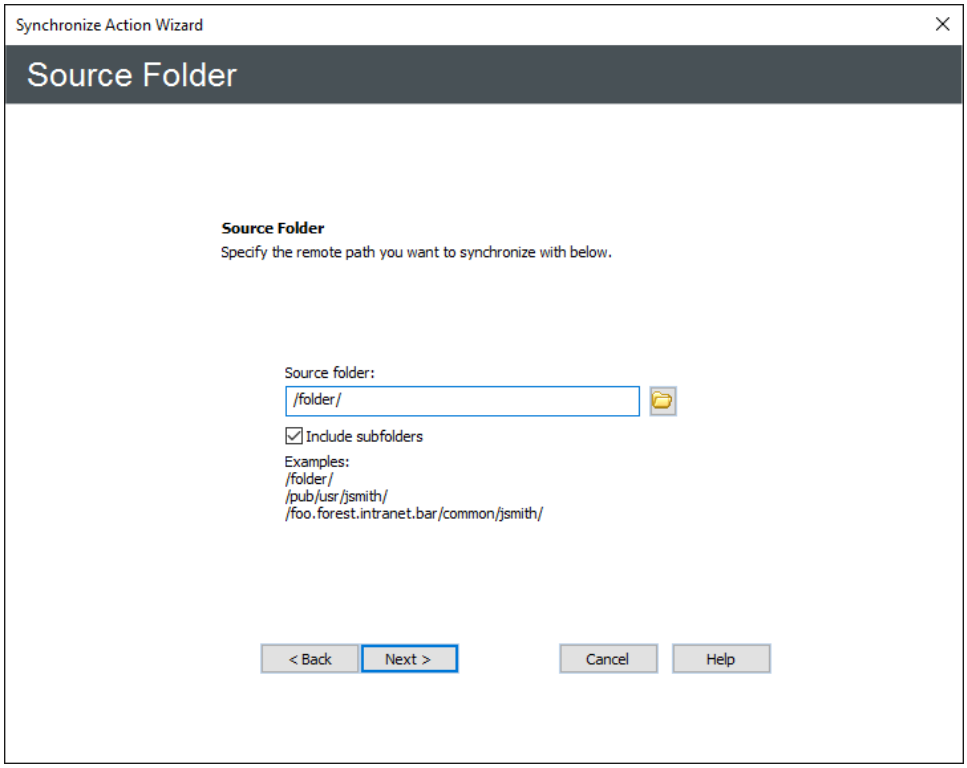


4. In the **Direction** list, specify whether to **Mirror remote** or **Mirror local,** then click **Next**. The **Configuration** page appears.



5. In the **Connection Profile** box, specify a connection profile for this Event. If none is specified, you will need to configure the **Connection details** as described below.
6. Click the **Synchronize method** list to specify a **method** for the connection: **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)**.
7. In the **Host address** box, type the IP or host address of the EFT to which you want to connect.
8. The **Port** number for the selected protocol changes automatically based on the offload method. Provide a different port number, if necessary.
9. In the **Username** and **Password** boxes, type the username and password used to authenticate.
10. 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.
11. If you chose **SFTP**, provide the client SFTP certificate information.
12. If you chose a protocol that uses SSL (FTPS or HTTPS), provide the client and remote server's SSL certificate information.

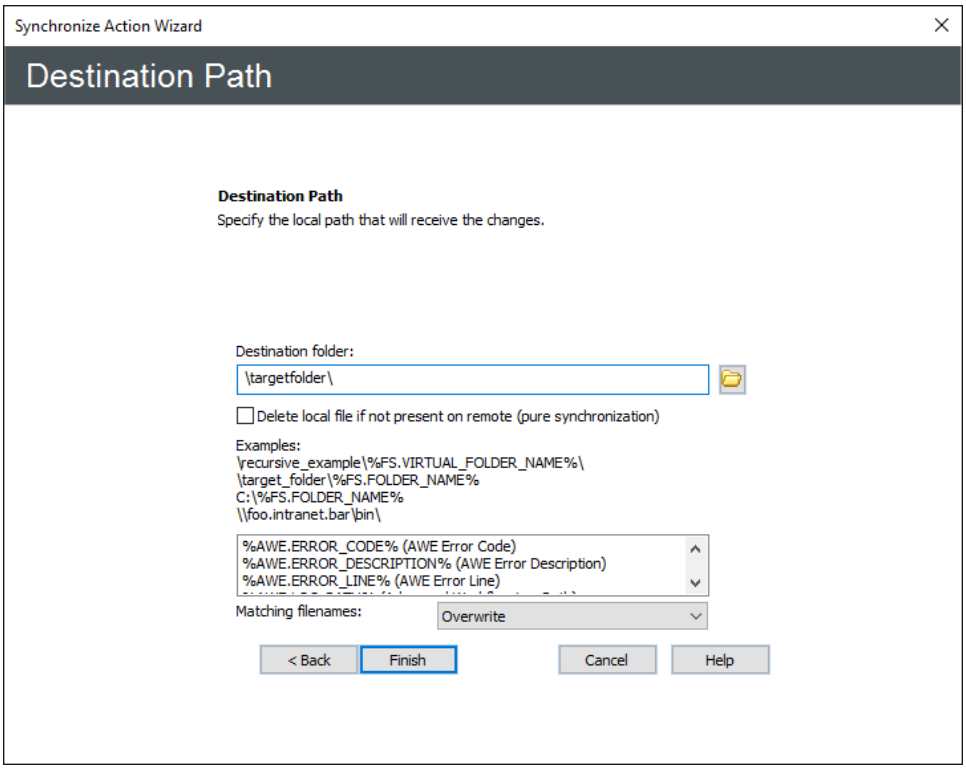
13. If you are connecting to a remote host through a SOCKS server, click **SOCKS** and provide the SOCKS connection information.
14. If you are connecting to a remote host through a proxy, click **Proxy**. Provide the proxy connection information.
15. To specify transfer options and time stamps, in the Offload wizard, click **Advanced**. Specify the advanced transfer options, such as connection retry attempts and delay between retries.
16. Click **Next**. The **Source Folder** page appears.



17. In the **Source path** box, provide the path to the file(s) that you want to synchronize. For example, type:

    ```
    /pub/usr/jsmith/file.txt or
    \\mydomain\common\jsmith\file.txt
    ```

18. Select the **Include subfolders** check box if you also want to synchronize the subfolders of the source folder.
19. Click **Next**. The **Destination Path** page appears.



20. 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.
21. To make local folder match the remote folder, select the **Delete local file if not present on remote**.
22. In the **Matching filenames** box, specify whether to **Overwrite**, **Skip**, **Skip if size is the same**, **Skip if size and time are the same**, **Smart Overwrite**, or **Numerate** files that exist with the same name. (Refer to Smart Overwrite for more information about Smart Overwrite.) This setting only applies to the initial transfer, not when the transfer is interrupted and then resumed. When resuming, EFT will follow the Smart Overwrite settings (that is, performs a CRC match for the files; if the files are identical, the destination file is not overwritten).
    - **Overwrite**—Overwrite any existing file with the same name.
    - **Skip**—Skip the transfer if a file with the same name exists in the destination directory.
    - **Skip if size is the same**—Skip the transfer if a file with the same name and size exists in the destination directory.

- **Skip if size and time are the same**—Skip the transfer if a file with the same name, size and timestamp exists in the destination directory. *When using this overwrite method, the preserve remote/local time stamps option must be enabled or the files may always be overwritten. These settings can be found under the Advanced Options of the connection profile.
- **Smart Overwrite**—EFT 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. (Supported only on FTP transfers.)
- **Numerate**—If a file in the destination folder has the same name as the file you are transferring, EFT renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT renames the transferred file to "Copy (2) of file.txt" and so on.

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

> **NOTE:** If **Skip if size and time are the same** is selected, EFT will skip overwriting when the filename, size and time stamp of the files are identical. When using this overwrite method, the preserve remote/local time stamps option must be enabled or the files can always be overwritten. These can be found in the **Advanced** options under the **Connection Details** area on the configuration page of the wizard.
>
> Synchronization action fails to delete file with **Numerate** set.

Protocol: Upload Action

(Requires FTC module) You can configure EFT to upload (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 with connection information (protocol and login details) and file information (source path and destination path).

The Upload Action can be applied to all File Server Events; the User Events "User Quota Exceeded," "User Logged In," and "User Logged Out"; and the Server Events "Timer" and "Log Rotated."

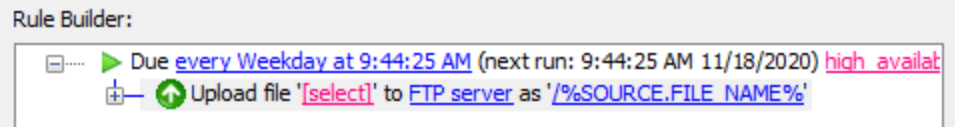
- If you create an Upload Rule that sends a file transfer activity report, the file transfer that triggered the Rule is not included in the report.
- When you add a Upload file to host action to a rule, the Client FTP offload engine performs retries upon failures (network failures is the typical example) based upon the settings in the Advanced Options dialog box. Be aware that the **Protocol Upload** Action does the transfer, including all retries, before moving on to the next Action, such as an email 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.

- 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.
- When EFT opens a file for copy, it uses FILE_SHARE_READ sharing mode. This mode ensures that a file cannot be changed by another process while EFT copies it, preventing corruption of the file.
- Configure the retry logic in the Copy Action for **Local (Local Files or LAN)** offload events. If an Event Rule triggers and you had large amounts of small files that were copied over a LAN share, some of the files could copy over at 0 KB. This retry logic will try the copy again if the file is locked or in use so the destination file will not have a 0 kb size.

Refer to Connection Profiles for details of setting up a Connection Profile before defining the Action.

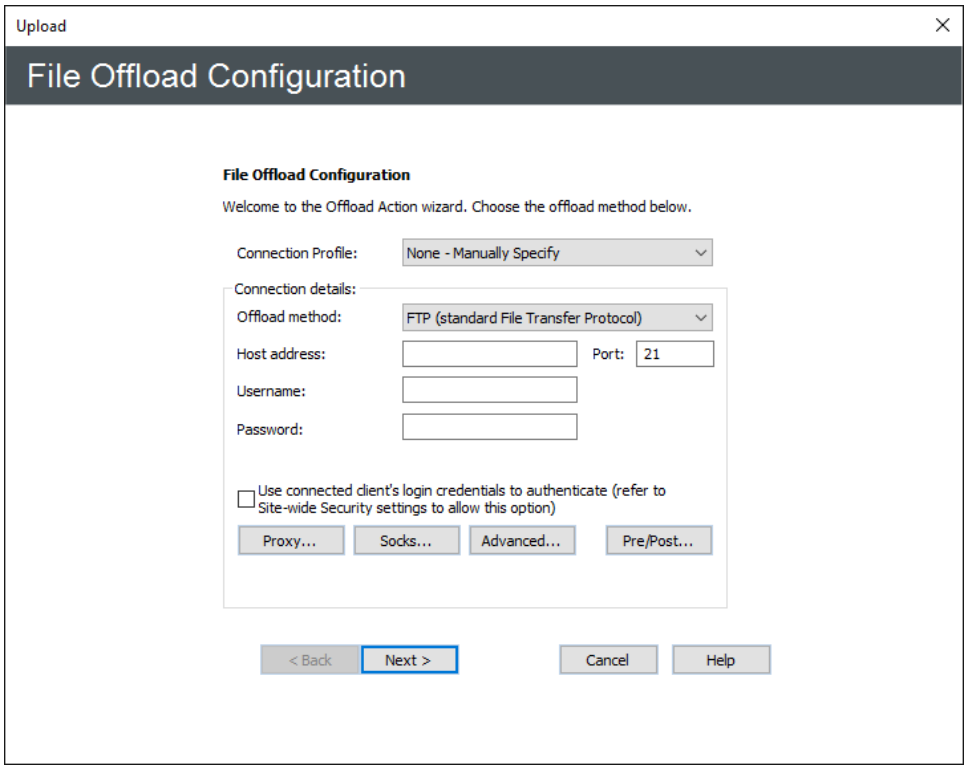
To configure EFT to upload files

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 **Protocol: Upload Action**.



3. In the **Rule Builder**, click one of the undefined parameters (for example, '[select]' or '/%SOURCE.FILE_NAME%').

   The **Upload/File Offload Configuration** wizard appears.



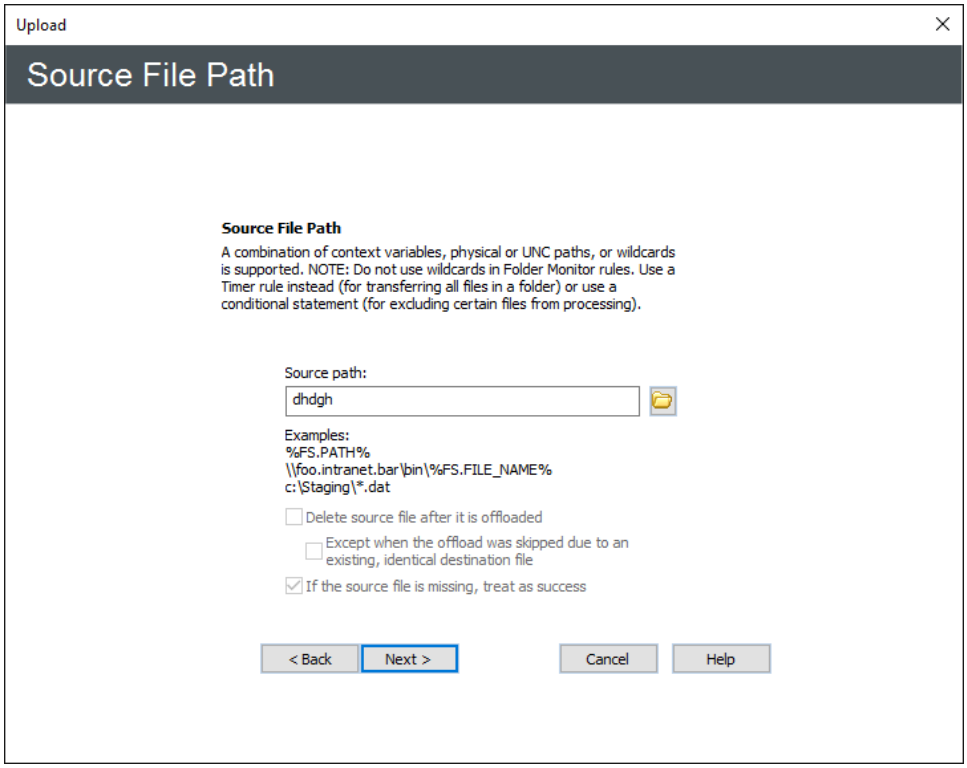
4. In the **Connection Profile** box, specify a connection profile for this Event. If none is specified, you will need to configure the **Connection details** as described below.
5. On the **Offload method** box, specify a protocol type for the connection: **Local (Local File or LAN)**, **FTP (standard 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)**.
6. (Optional) If you selected **Local (Local Files or LAN)**, under **Optional credentials override**, provide the **Windows account** username and **Password** for connecting to remote shares (not local folders).
    - These credentials are used for the remote ***destination*** folder ONLY for upload actions. The source (Local) folder will still use EFT server service account at all times. (When using download (PULL) actions over LAN, the same concept applies, but credentials will be used for the source directory and EFT server service account for the destination.)
    - Only if/when a resource cannot be accessed using the credentials under which the EFT service is running do you need to include the **optional credentials.** The **Optional credentials override** feature allows you to specify an alternate set of logon credentials for accessing the ***destination*** network shares to which the EFT service account may not have access

(due to security constraints).

- If alternate credentials are specified, EFT will use its current security token (associated with the "Log on as" account specified in the EFT server service settings) for LOCAL folder access and then a new security token (associated with the alternate logon credentials) for the remote ***destination*** folder accessed over network connections (e.g. network shares).
- Think of Local Transfer as an operation (offload or download) with a remote server.
- Think of "Optional credentials override" as "credentials to access remote server."
- For download action, it is "credentials for source folder."
- For upload (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):
  - Offload: local (EFT) => remote ("override credentials")
  - Download: local (EFT) <= remote ("override credentials")
  - TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
  - TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

7. If you chose **Local**, click **Advanced** to configure retry attempts, then skip to the Source File Path page step.
8. If you chose anything but **Local** do the following;
   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. (Optional) Provide the **Username** and **Password** needed to establish the connection.
   d. To configure advanced options, click **Advanced**. Refer to Advanced Transfer Options for details.
9. 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 on the Site's **Security** tab by the Persist username and password credentials for use in Event Rule context variables check box.

10. If you chose **SFTP**, provide the client SFTP certificate information.
11. If you chose a protocol that uses SSL (FTPS or HTTPS), provide the client and remote server's SSL certificate information.
12. If you are connecting to a remote host through a SOCKS server, click **SOCKS** and provide the SOCKS connection information.
13. If you are connecting to a remote host through a proxy, click **Proxy**. Provide the proxy connection information.
14. To specify transfer options and time stamps, in the Offload wizard, click **Advanced**. Specify the advanced transfer options.
15. (optional) To define commands to occur before and after this operation, click **Pre/Post**. Refer to Pre and Post Commands for details.
16. Click **Next**. The **Source File Path** page appears.

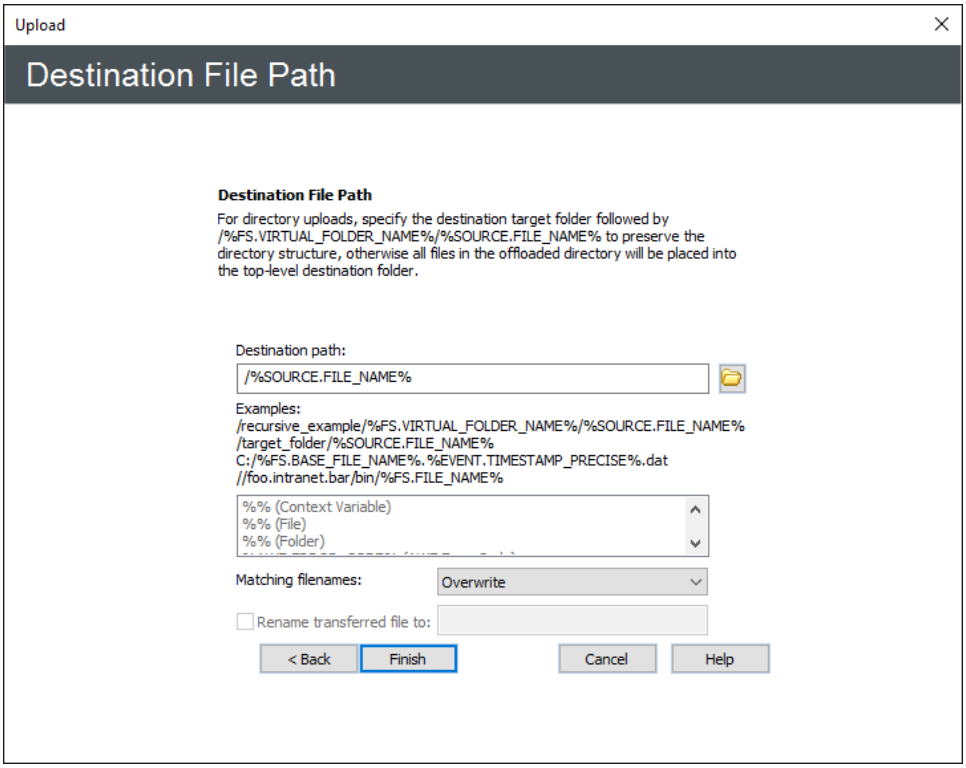


17. In the **Source path** box, provide the path to the file(s) that you want to offload. (No validation is performed.) For example, type:

    `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 file name.

18. 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.)
    - Select the **Except when** check box if you do not want to delete the source file after it is offloaded if the offload was skipped.
19. 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.
20. Click **Next**. The **Destination File Path** page appears.



21. 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.) This setting only applies to the initial transfer, not when the transfer is interrupted and then resumed. When resuming, EFT will follow the Smart Overwrite settings (that is, performs a CRC match for the files; if the files are identical, the destination file is not overwritten).
    - **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 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. (Supported only on FTP transfers.)
    - **Numerate**—If a file in the destination folder has the same name as the file you are transferring, EFT renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT 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.
    - Only FTP and FTPS are currently supported.
    - EFT executes a RNFR + RNTO sequence for FTP transfers on the remote server. If the remote server supports cross-folder rename (as EFT 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.

22. Click **Finish** then click **Apply** to save the changes on EFT 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 (for example, `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.FI
    LE_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.

Script: Advanced Workflow Action

(Requires AWM module; formerly AWE) You can use Advanced Workflow actions to design scripts, batch files, macros, or any other code-intensive process using an easy drag-and-drop interface. Then you can insert the workflow in event rules.

For details of creating Advanced Workflows, refer to the Advanced Workflows help documentation.

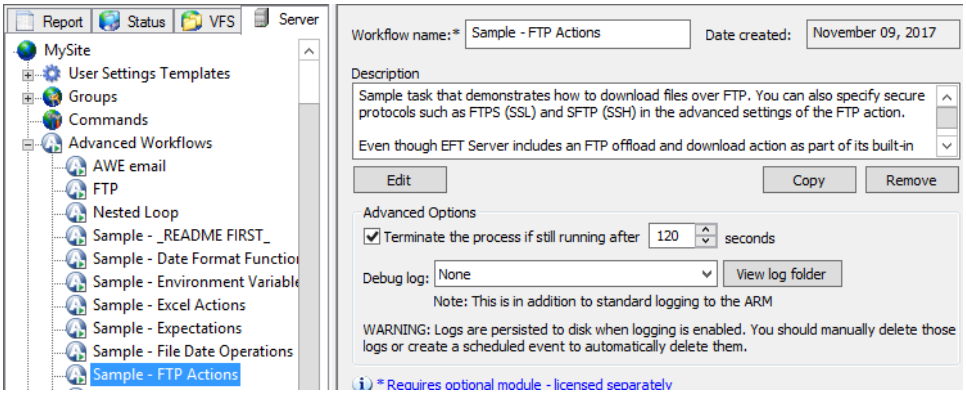
Sample Workflows

The Advanced Workflows module includes several samples to demonstrate how to create a workflow. The comments in the workflow provide instructions. The sample files are stored in **C:\ProgramData\Globalscape\EFT Server** in a database file named SiteConfig.<GUID> file (one for each Site).

> **NOTE:** In the Advanced Workflows module, variables cannot contain periods; therefore, in each variable that contains a period, the period is replaced with an underscore. For example, change `%CONNECTION.LOCAL_IP%` to `%CONNECTION_LOCAL_IP%`

To view the sample workflows

1. In the EFT administration interface, connect to EFT and click the Server tab.
2. In the left pane, expand the Site node for the Site that you want to configure, then click the Advanced Workflows node. The node expands to show the Sample Workflows.



3. In the left pane, click a sample workflow. The right pane displays the properties of the selected workflow.
4. Do one of the following to open the workflow in the Task Builder:

- In the right pane, click **Edit**.
- In the left pane, double-click the workflow.

5. View the comments in the Steps pane for instructions on how to configure the workflow. Use this guidance to create similar workflows.
6. If you want to save the sample workflow with your changes, click **Save and Close**. The workflow is saved in **C:\ProgramData\Globalscape\EFT Server** in a database file named SiteConfig.<GUID> file.

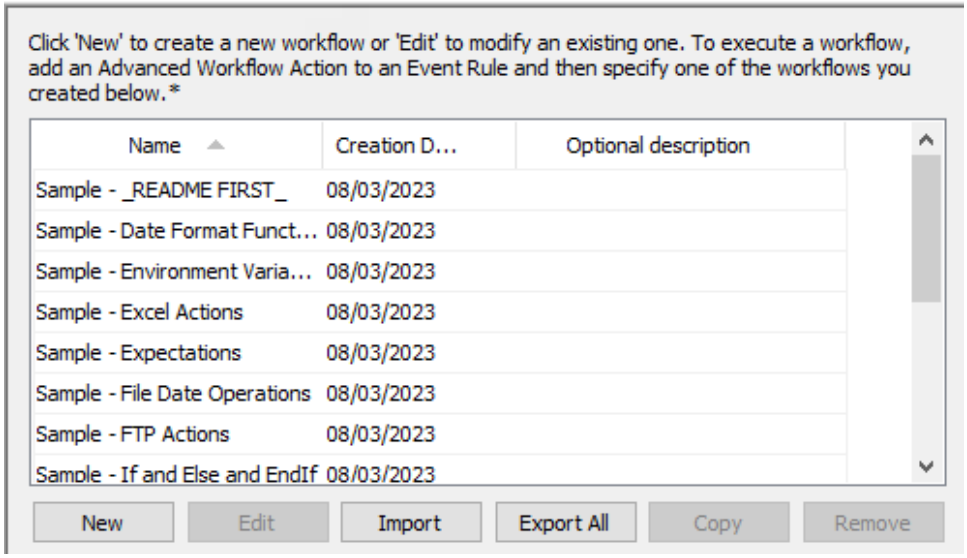
If you have accidentally overwritten a sample workflow and you want to revert to the original version of the sample file, you can copy the original from the default location (**C:\ProgramData\Globalscape\EFT Server\AWE**). You could also make a backup copy so you don't lose the original.

The Workflow Task Builder Overview

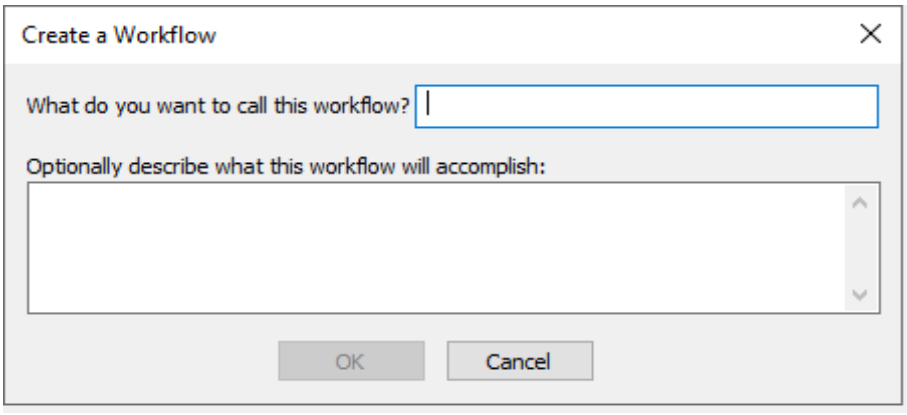
The Task Builder is used to create the workflow (Task) that you want to use as an event rule Action.

To open the Task Builder

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

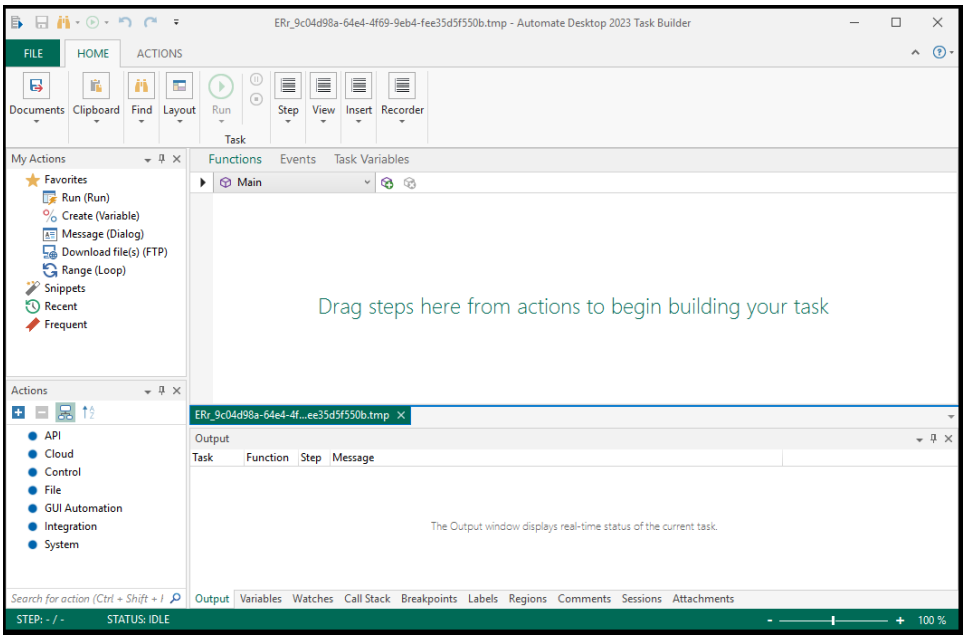


4. In the right pane, click **New**. The **Create a Workflow** dialog box appears.



5. In the **What do you want to call this workflow** box, specify a name for the Workflow, then click **OK**.

   The Workflow **Task Builder** appears.



For details of how to create or edit workflows, refer to Creating Workflows for Use in an Event Rule.

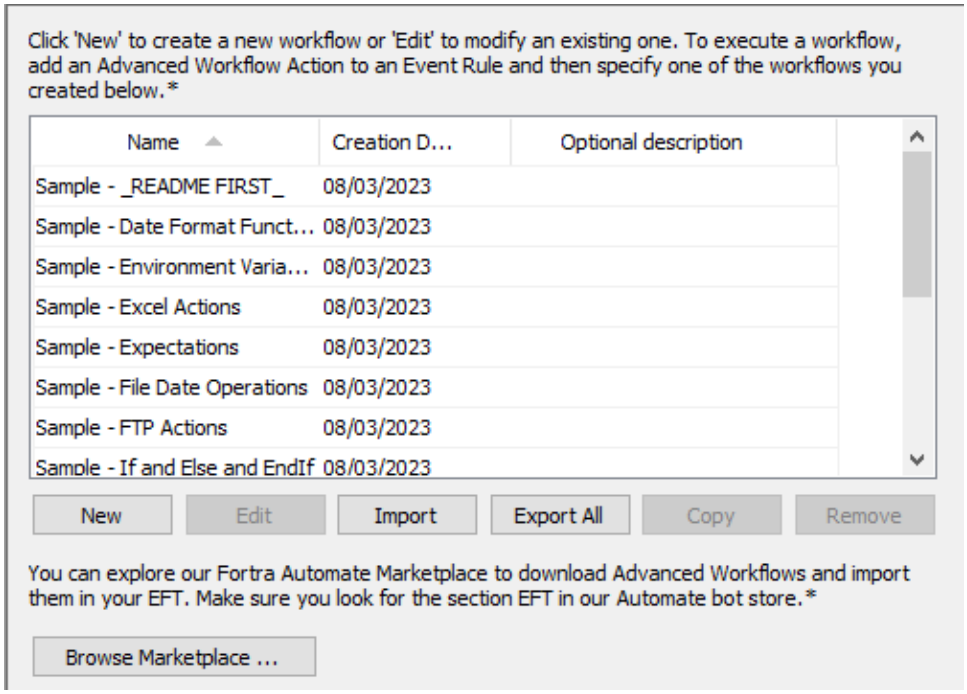
Creating Workflows for Use in an Event Rule

(Requires Advanced Workflow Module) Similar to Commands, Workflows are used in Event Rules as Actions or triggers. When you create a Workflow, it is saved in the SQLite database file in **C:\ProgramData\Globalscape\EFT Server**.

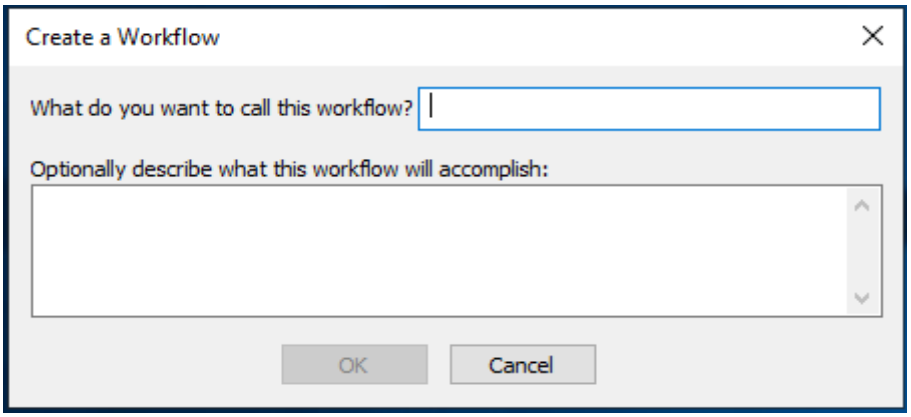
During the Advanced Workflow trial, when a new Workflow is created, a message appears (prior to the **Create a Workflow** dialog box) informing you that the Advanced Workflow module is an optional module and that the trial begins when the first Workflow is created.

To create a Workflow

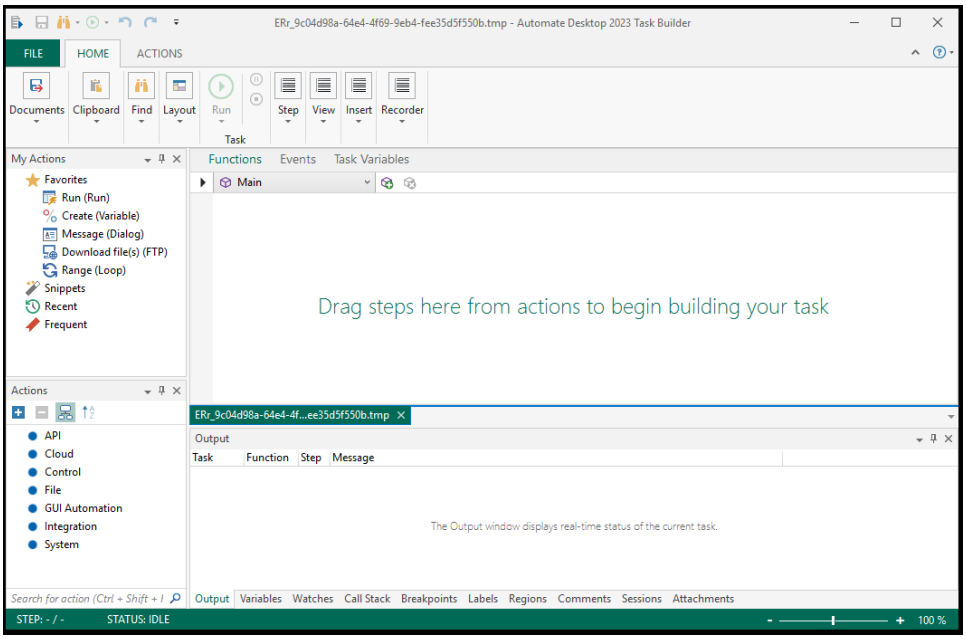
1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the **Advanced Workflows** node.
3. In the right pane, the **Advanced Workflows** tab appears.



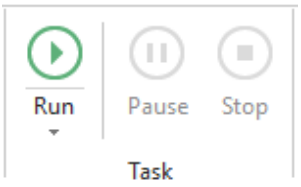
4. In the right pane, click **New**. The **Create a Workflow** dialog box appears.



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.



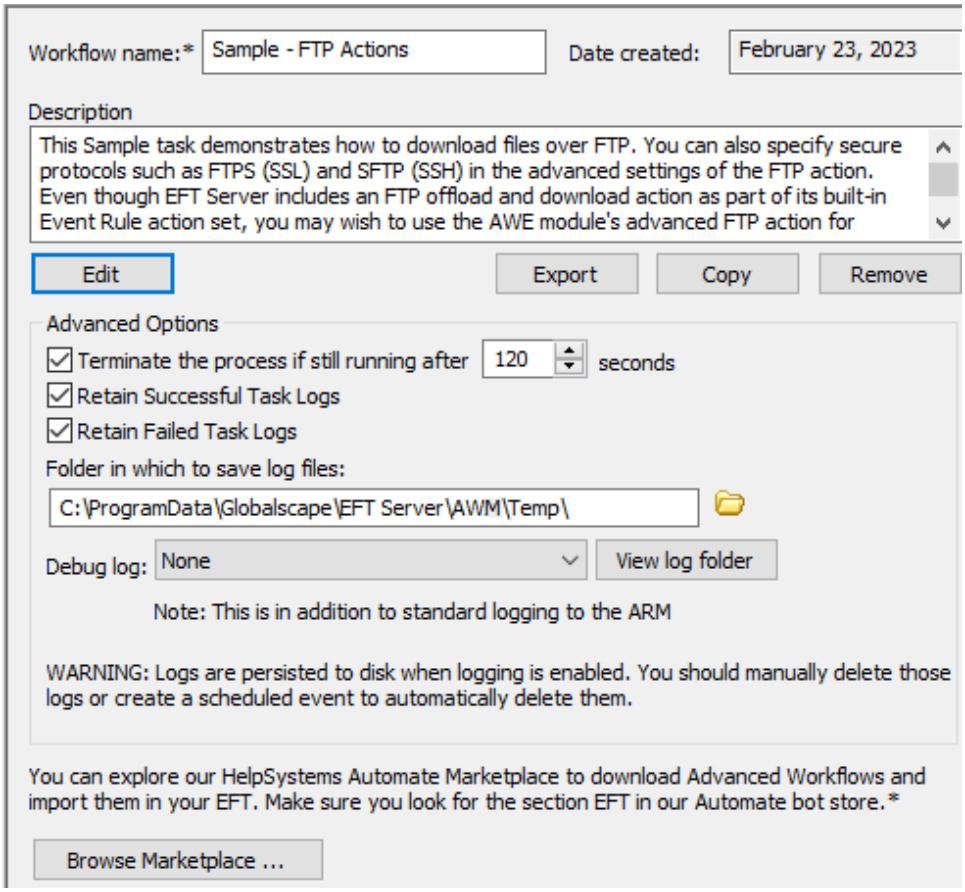
7. The tree in the left pane lists the steps that you can add to the Workflow. The right pane displays the steps in the Workflow.
8. Drag items from the **Actions** list to the **Steps** pane to create your Workflow.
9. Use the **Run** icon on the Debug toolbar to test the steps. You can run the whole Workflow all at once, run only a selected step, or run 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** pane of the Site 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.
- Select the **Retain Successful Task Logs** check box if you want to keep all successful attempts for this Workflow
- Select the **Retain Failed Task Logs** check box if you want to keep all failed attempts for this workflow
- Specify the location in which to save logs, if different than the default of C:\ProgramData\Globalscape\EFT Server\AWE\Temp\ (for example, in a shared location)
- Specify the level of debug logging in the **Debug log level** box, **None**, **Minimal**, **Normal**, or **Verbose** (None is the default).
- Click **View log folder** to view the CSV logs created by this workflow, saved in <installation_folder>\AWE\Temp. If you enable the logging, you should manually delete the files after you're done with them or create a Scheduled event in EFT to delete them automatically.

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

Adding a Workflow Action to an Event Rule

(Requires the Advanced Workflow module.) With Advanced Workflow Actions, EFT 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.

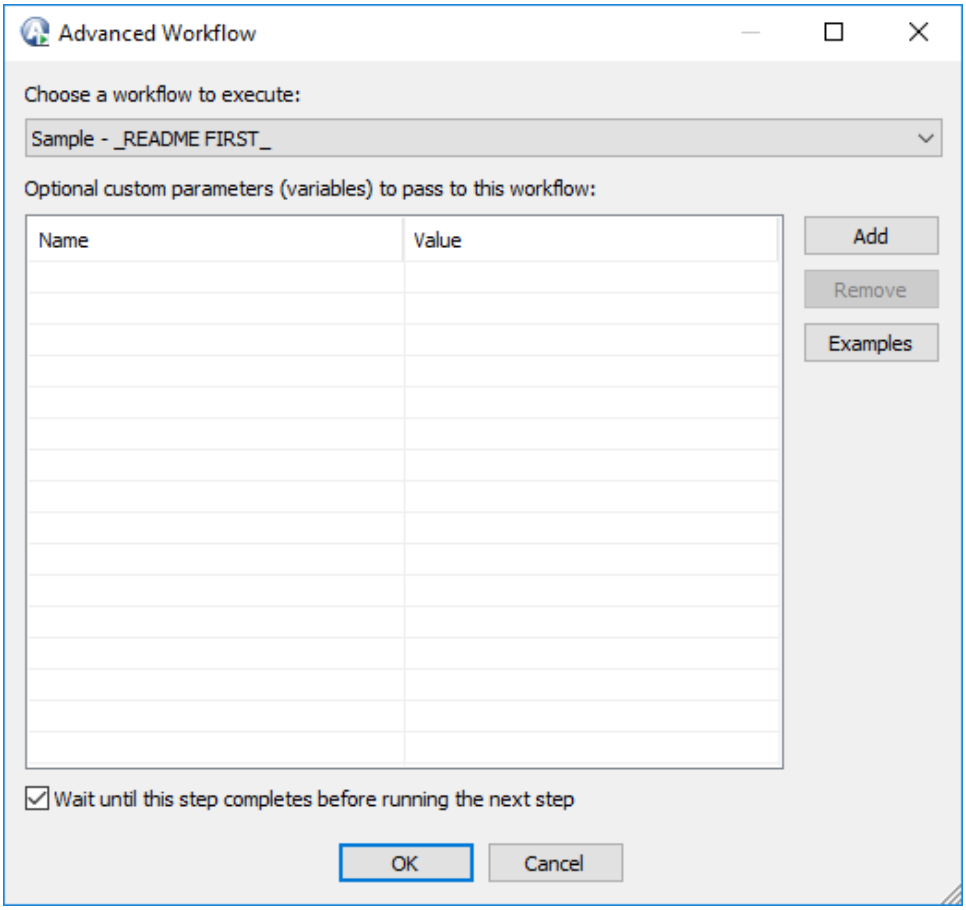
The workflows created for use in Event Rules are executed using the EFT server administrator credentials, unless you specify otherwise. If a resource cannot be accessed using the credentials under which the EFT service is running, you need to include the **optional credentials for the destination server.**

- Think of "Local Transfer" as an operation (offload or download) with a remote server.
- Think of "Optional credentials override" as "credentials to access remote server."
  - For download action, it is "credentials for source folder."
  - For copy/move (offload), it is "credentials for destination folder."
- "Credentials to access local folder" ("source" for offload and "dest" for download) is Event Rule execution context (EFT account, or Folder Monitor account for FM rules, or Connected Client account for client-originated rules on an AD site):

- Offload: local (EFT) => remote ("override credentials")
- Download: local (EFT) <= remote ("override credentials")
- TEST1: Offloads file from "local" Share A (access as EFT account, i.e., X) to "remote" folder B (access as Y) => Fails, as X has no permissions on A.
- TEST2: Downloads file from "remote" Share A (access as Y) to "local" folder B (access as EFT account, i.e., X) => Succeeds, as Y has permissions on A and X has permissions on B.

To add a Workflow to an Event Rule

1. Create a Workflow.
2. Create an Event Rule.
3. In the **Actions** list, double-click **Script: 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.



5. 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.
6. (Optional) Specify custom parameters to pass to the Workflow in the **Name** and **Value** columns, and then click **Add**.
7. (Optional) The **Wait until this step completes before running the next step** check box is selected by default.

a. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails.
b. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)

8. Click **OK**. The **Advanced Workflow** link in the **Rule Builder** updates with the name of the Workflow.
9. Add other Actions as needed, and then click **Apply** to save the changes on EFT.

Script: Custom Command Action

(Requires EAM) The topics below provide the procedures for configuring and using Commands in EFT.

Custom Commands

EFT's *Custom 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's Event Rules.

When the Event Rule is triggered, EFT executes the specified custom Command and attributes. To configure EFT to execute Commands, you first create the command, 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 on the **Server** tab, 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.)

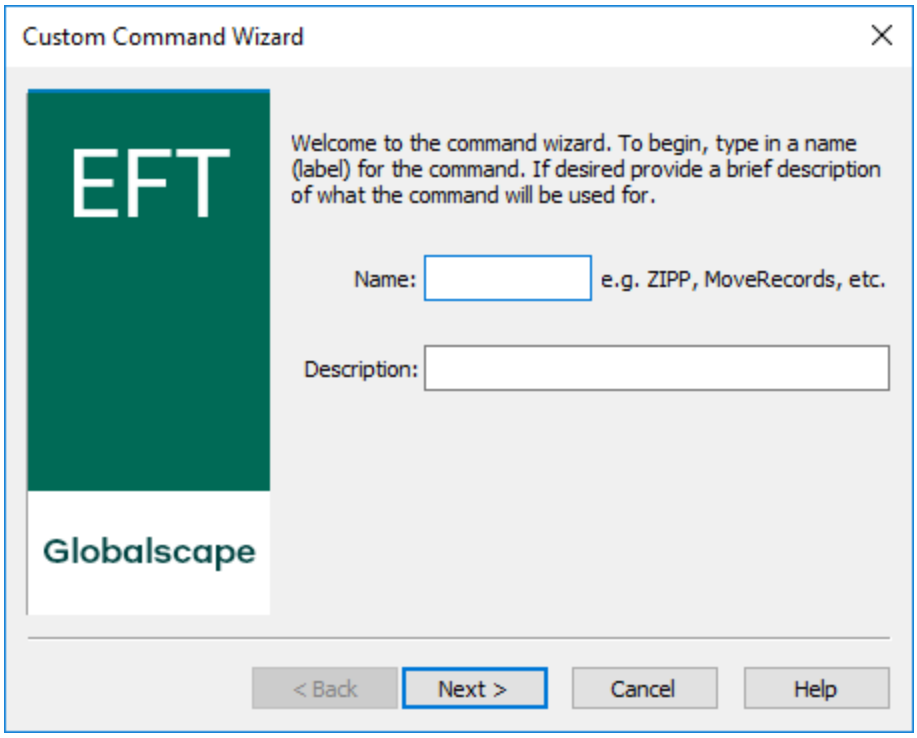
Creating a Command with the Custom Command Wizard

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

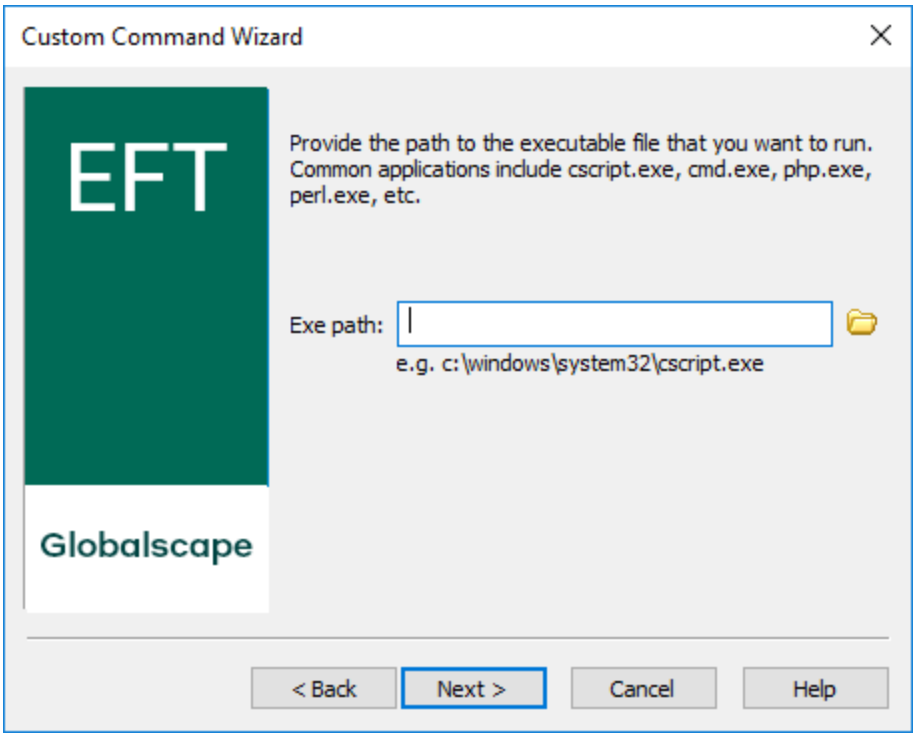
To create a command with the Custom Command wizard

1. In the left pane, right-click the **Commands** node, and then click **New Command**.
2. Click the **Commands** node in the left pane, then, in the right pane, click **New**.
3. Press CTRL+M.

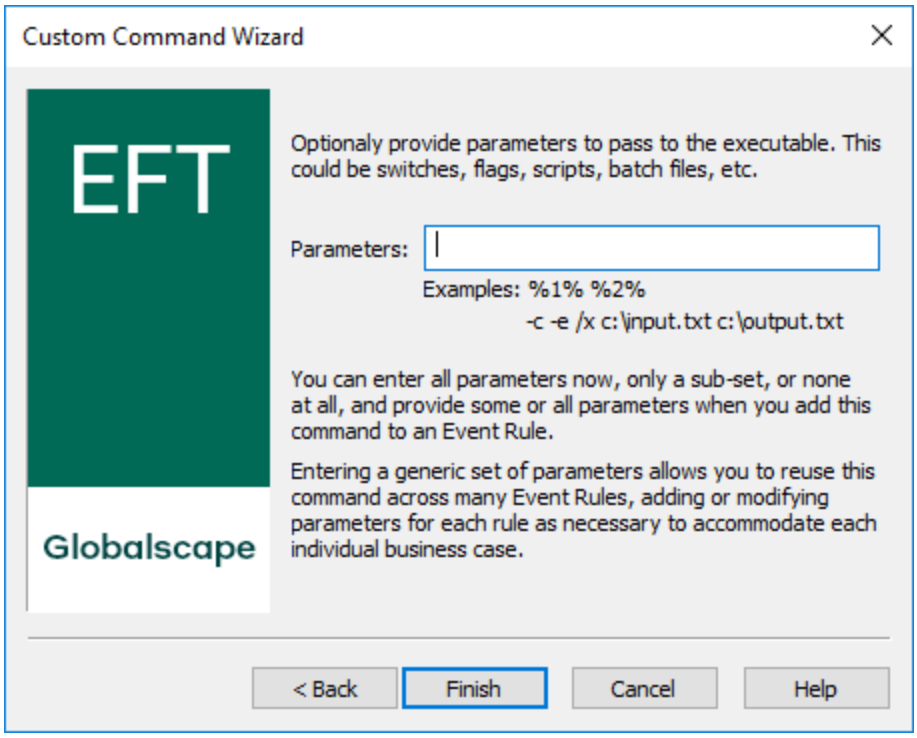
   The **Custom Command Wizard** appears.



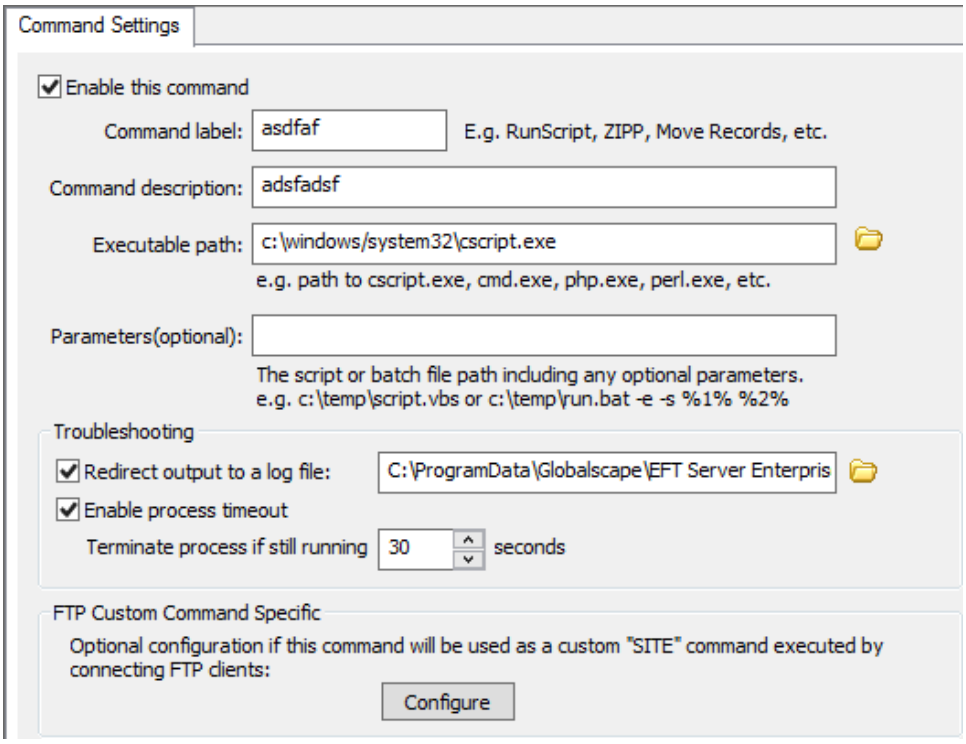
4. In the **Name** box, type a descriptive name for the command. You will reference the Command name in Event Rules, so you should give the Command an intuitive name. For example, instead of `Command 1`, you might call it `Run CScript`.
5. Provide a **Description** that will help you identify the command.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



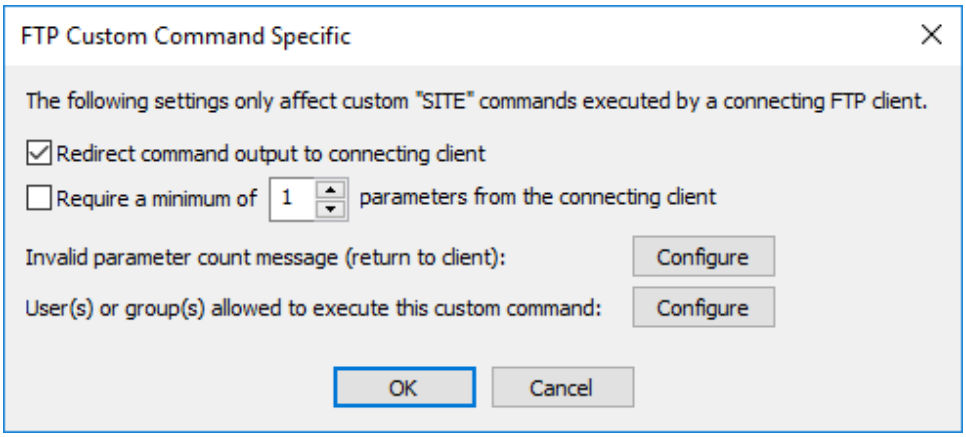
7. In the **Path to executable** box, browse to or type the path to the executable. For example, you can specify a program, a batch file, or a Windows scripting executable, such as cscript.exe or wscript.exe. If you are connected to EFT remotely, you can type the path to the file, but be sure the path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



8. (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, then modify them or add additional parameters when you add the Command to an Event Rule.
9. Click **Finish**. The Command is added to the **Commands** node for the Site and appears in the **Command Settings** tab in the right pane.



10. 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.

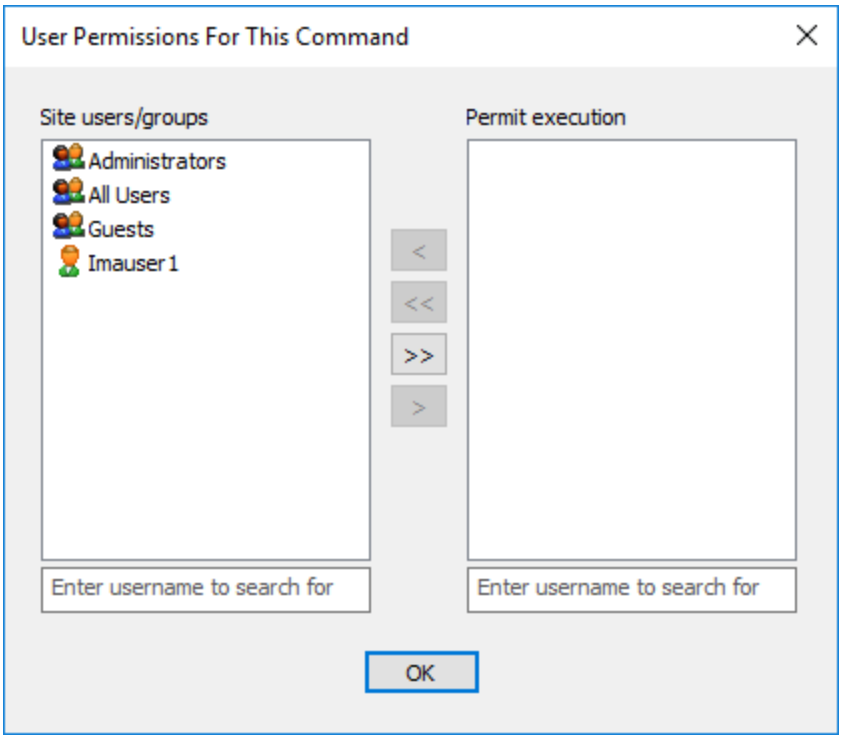


11. Select the **Redirect command output to connecting client** check box to redirect the output from the executed command to the client in a 220 response message. If the check box is not selected, then the output of the command is not returned to the client, even though the command is still executed 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).

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. To search for specific users, type the username in the search box.



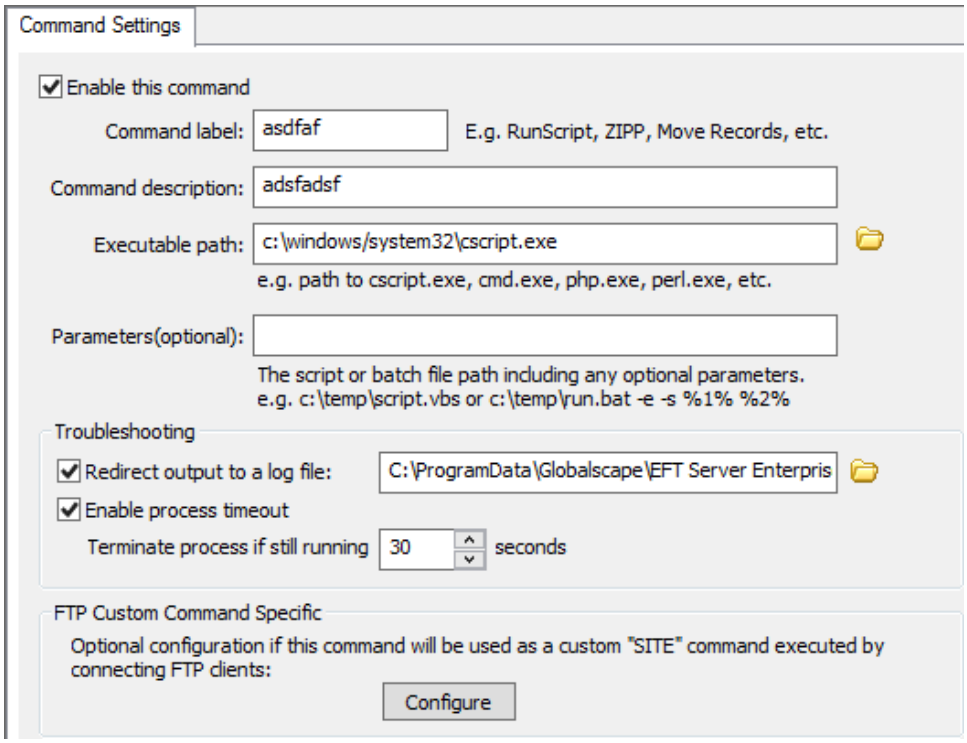
13. Click **OK**, then click **Apply** to save the changes on EFT.

Editing a Command

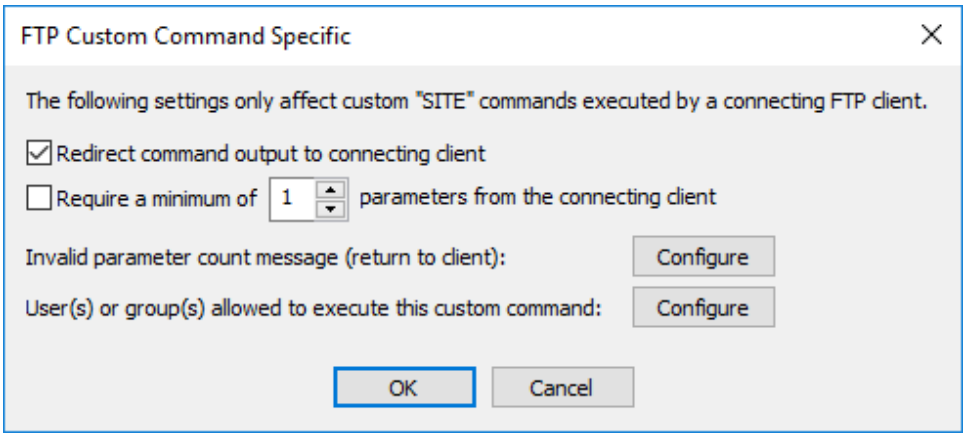
The procedure below describes how to edit a command that you can execute with an Event Rule. For a general introduction to Commands, refer to Introduction to Commands. To create a command, refer to Creating a Command with the Custom Command Wizard.

To edit a command

1. In the administration interface, connect to EFT, then click the **Server** tab.
2. On the **Server** tab, 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.

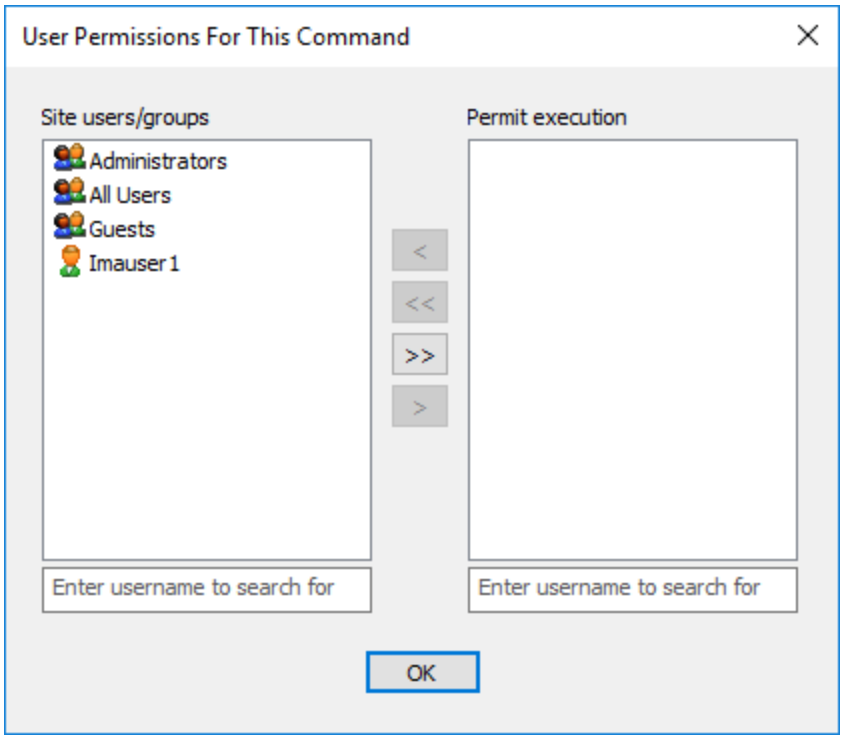


4. The **Command label** box displays the name you gave the Command. You will reference the Command label in the Event Rule and **Custom Command** dialog box (in the **Select Command** drop-down menu), so you should give the Command an intuitive name. For example, instead of `Command 1`, you might call 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, 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 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.
13. To provide a message that users will receive when the parameter number is not met, next to **Invalid parameter count message**, click **Configure**.

14. Provide the message, and then click **OK**.
15. 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**.



16. 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**.
17. Click **Apply** to save the changes on EFT.

Custom Command Example

The following example Command shows the configuration of a custom Command from the perspective of both EFT and a client. To follow the example exactly, you will need to download and install CuteFTP, which is available as a free trial and can be downloaded from the website. However, any client that supports custom commands or raw FTP commands will work. The command example described below copies EFT log files from the **Logs** folder to **C:\Temp** using the Windows xcopy command and CuteFTP's command-line functions.

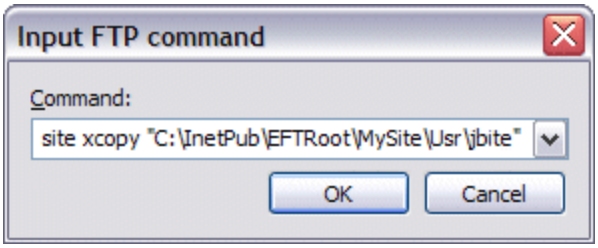
To create a custom Command

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, 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 Creating a Command with the Custom Command Wizard to define a Command that uses **xcopy**.

You can run this command example "on the fly" in the FTP client (in this example, CuteFTP), or insert the Command in an Event Rule. Each of these methods is described below.

Using the Command "on the fly" in CuteFTP

1. Start CuteFTP, and create a connection to EFT. (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**, 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 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 (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. (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.

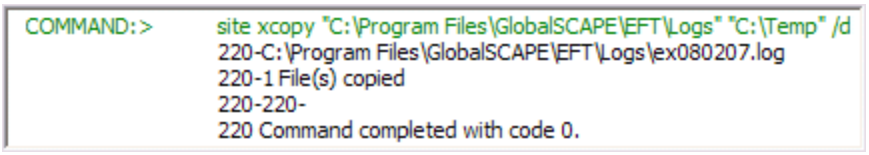
   You must be connected to an FTP server in order for the Commands option to be available.

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
   ```

   > **NOTE:** Commands must start with *site* and then the command name you used in EFT, 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.
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 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 **Script: Custom Command** Action. Using this method, you would have to define the parameters in the **Execute Command** dialog box from within the Event Rule. See also Script: Custom Command Action.

Possible Error Situations

- If you repeat the hard coded parameters in both the client and EFT, 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, 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 side.
- You must give the FTP client user permission to run the Command on the **Permissions** tab on EFT; 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 logged in to from a Local System account.
- EFT can return an error if the client provides the wrong number of parameters or invalid parameters.
- To limit security vulnerabilities to EFT, the EFT 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).

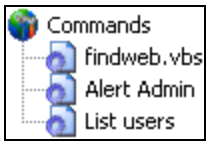
Viewing and Deleting Commands

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, edit, delete, and add new Commands.

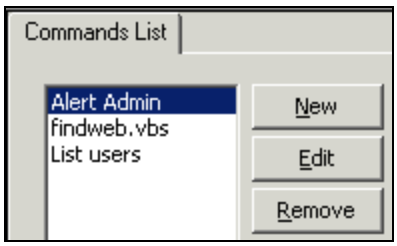
To view the Commands defined on a Site

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, 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, 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. When you create a new Command, the **Enable this command** check box is selected on the **Command Settings** tab.

To enable or disable a Command

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, 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.
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.

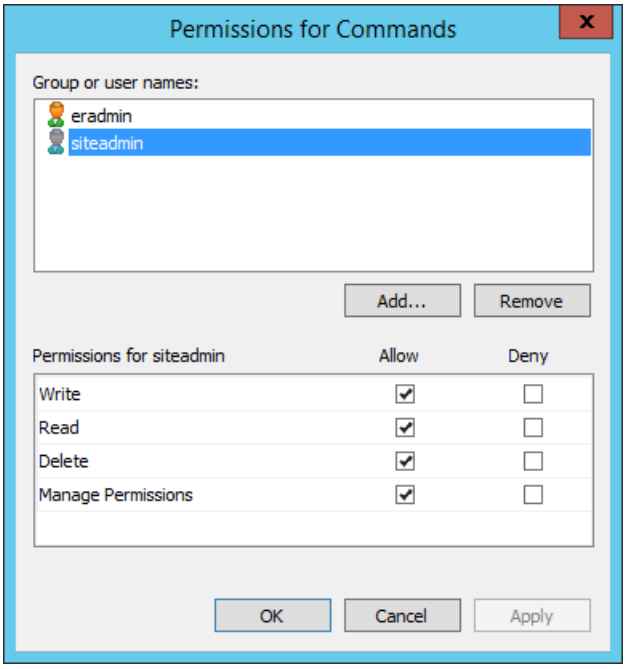
4. To enable the Command, select the **Enable this command** check box, and then click **Apply**. When the Command is enabled, the x within a red circle does not appear over the Command's icon.

Command Permissions

Certain delegated administrators have all permission (Write, Read, Delete, and Manage Permissions) to manage the Custom Commands. Granular permissions allow the EFT administrator to control which administrators have control over certain objects. For example, you might want to give the Site administrator permission to Manage Permissions, but give the Event Rules administrator only Read permission.

To edit permissions

1. Right-click the **Commands** node or a specific command, then click **Permissions**.



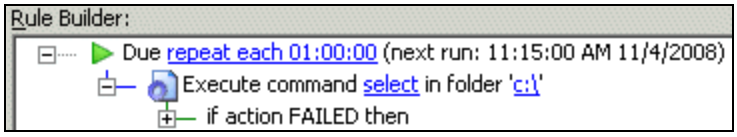
2. Clear the check boxes for the permission you do not want to assign; select the check boxes for the permissions that you want to explicitly **Allow** or **Deny**.
3. When you assign permissions at the Commands node, the permissions are inherited by the Commands. You can change the permissions for each of the Commands and for each administrator, if necessary.
4. Click **OK**.

Using the "Script: Custom Command" Action

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

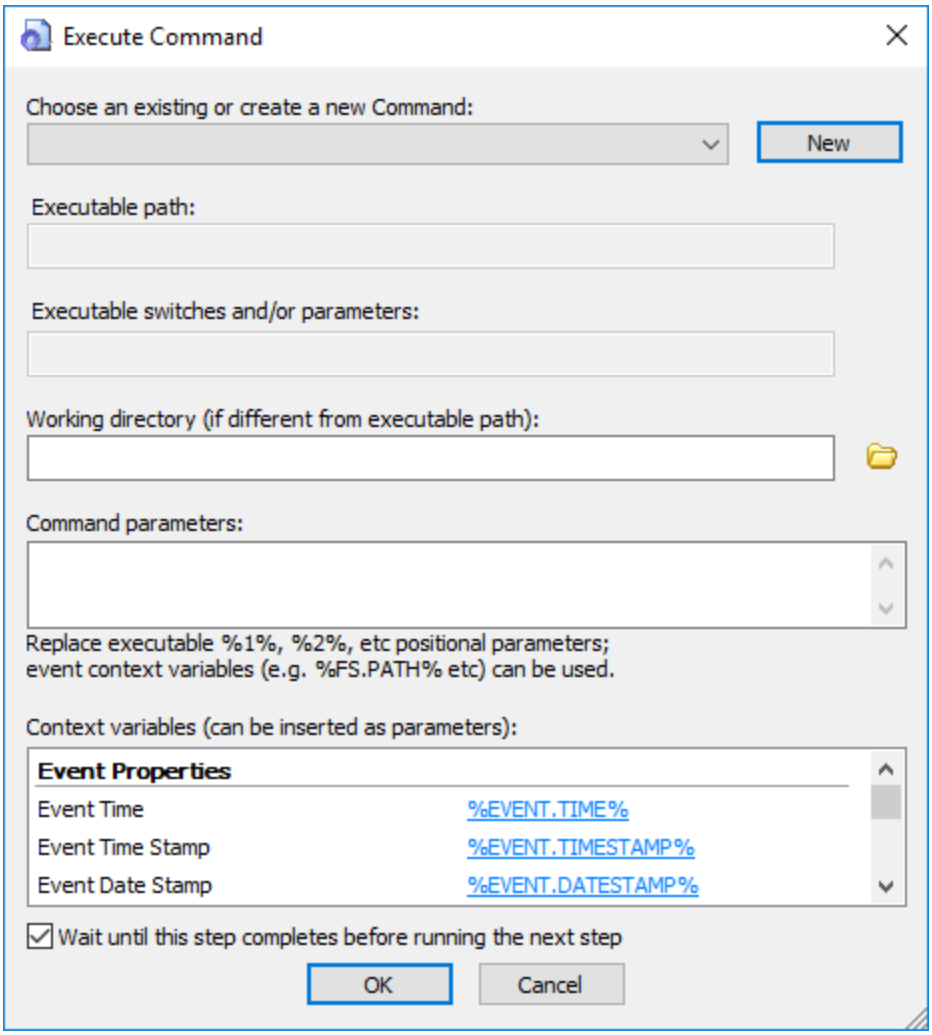
To execute a Command from EFT's Event Rule system

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, 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 computer, not the remote interface).
9. (Optional) In the **Command parameters** box, include any parameters for the command.

You can select 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 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. (Optional) The **Wait until this step completes before running the next step** check box is selected by default. When the check box is selected, you can select the "If failed" action, and populate it with actions to run in case the rule fails. To allow the next step to run before this action completes, clear the check box. If check box is not selected, a prompt appears to confirm: "This step will be executed asynchronously (non-blocking), which means EFT won't wait for this step to be completed before running the next step. This could yield undesirable results if the next step depends on the output or outcome of this one. Are you sure you want to make this action asynchronous?" (All actions in the IF FAILED section are lost if the parent action is switched from async to sync mode.)
11. Click **OK** to save the Command.
12. Add other Actions as needed, and then click **Apply** to save the Event Rule.

Example: Using a Command in an Event Rule to Copy Files

If you want to copy EFT's files to another location based on the date (for example, 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 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, then execute the Command to `xcopy` the newer files to the destination location.

To define an Event Rule to copy log files

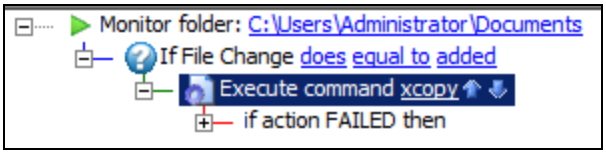
1. Create a custom command to execute the Windows Xcopy command. The executable is (by default) in **c:\windows\system32\xcopy.exe**.
2. In the **Working directory** box, type the path or click the folder icon to specify the folder in which the script or custom command executable resides (**C:\windows\system32**).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

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

You could also add an email 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).

Script: PowerShell Action

(Requires EAM) The **Run PowerShell script** Action is used in Event Rules to execute a PowerShell script. (Requires Windows PowerShell 4.0 or later.)

EFT will always use Windows PowerShell ISE (if available on the target machine) to edit the embedded script, regardless of your default setting.

A PowerShell log is enabled and saved in the **\ProgramData** folder as **\Logs\powershell.log**.

100s of PowerShell functions and cmdlets are available. Refer to https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-date?view=powershell-7 for cmdlets examples and information about using PowerShell.

VariantWrapper for variables to be passed as VARIANT will fail in PowerShell. (This is a bug in PowerShell.)

EFT context variables (where populated) need to be passed into the script. The script will access variables with `$EFT_CONTEXT` global variable via the `GetVariable` method. Create or modify context variables by using `SetVariable` method of `$EFT_CONTEXT` global variable.

The script action is able to modify or create any variables except the systems environment (`%ENV.`) pseudo variables. When `%ENV.[value]%` is used in event rules, EFT will look up the [value] from the systems environment variables.

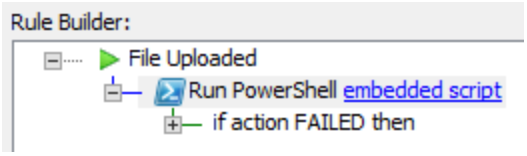
When referencing a dataset in PowerShell, PowerShell does not handle the % symbol, so this is how it would be accessed: ("Customer.CurrentRow.FirstName")

```
$EFT_CONTEXT.GetVariable("Customer.CurrentRow.FirstName") + ','
+
$EFT_CONTEXT.GetVariable("Customer.CurrentRow.LastName")
>>C:|Users\Administrator\Desktop\test
```

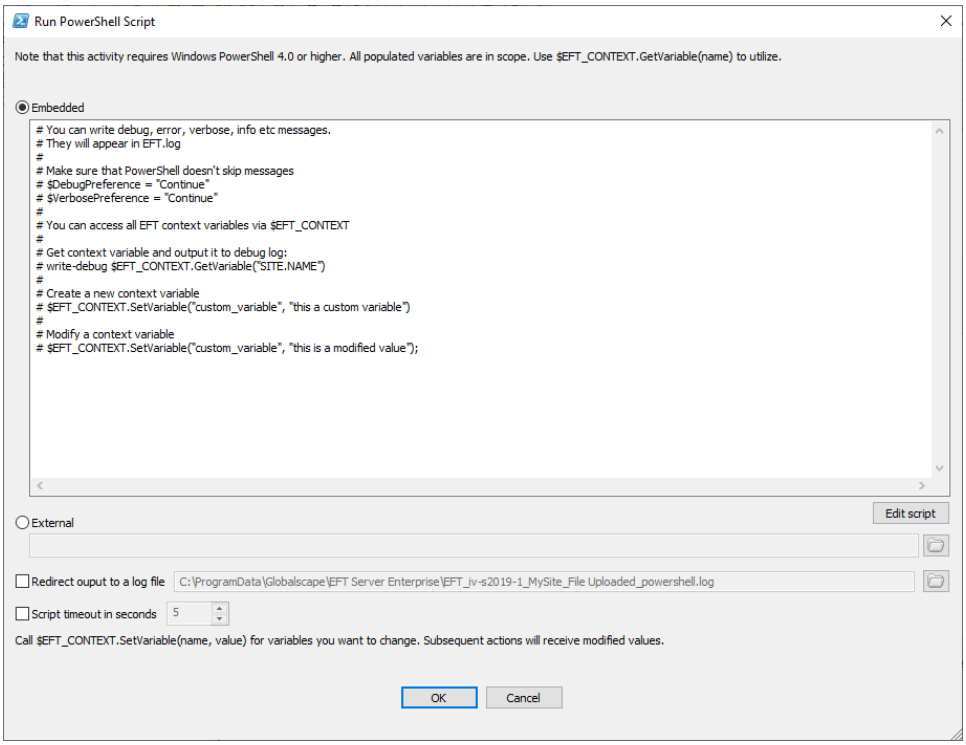
To user a PowerShell script in an event rule

1. In the administration interface, connect to EFT and click the **Server** tab.
2. Create a new Event Rule.

3. Add the **Run PowerShell script** Action to the rule.



4. In the Rule Builder, click the **embedded script** link. The **Run PowerShell Script** dialog box appears with a sample script that is commented out.



5. Click **Embedded** if you want to paste a script into the dialog box or click **External** of you want to point to a PowerShell script in a folder that EFT can access.
6. To create a PowerShell log file, select the **Redirect output to a log file** check box, then specify where to save the log. By default, it is saved to **C:\ProgramData\Globalscape\EFT Server\<computer_name>_<site_name>_<event_rule_name>_powershell.log**.
7. If you want to analyze PowerShell output in context with the event trigger and all associated actions with that event, you would need to clear the **Redirect** check box, apply changes, then open logging.cfg, un-comment the Event.PowerShell logger (remove the #), then save the logging.cfg file. (If you leave the **Redirect** check box selected, the PowerShell logs will not appear in logging.cfg for this action.)
8. Click **Edit Script** to view/edit the script in a text editor. (Windows PowerShell ISE is the default editor.)

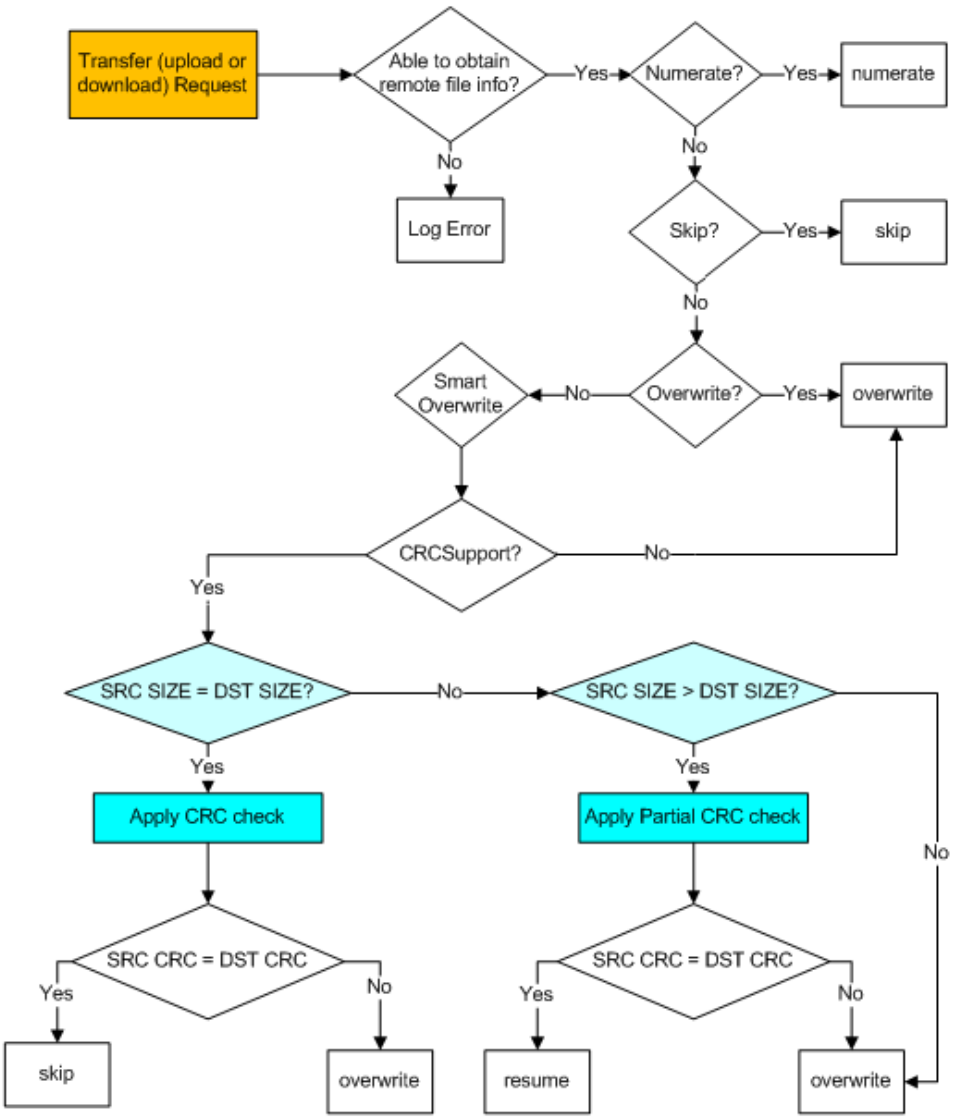
9. Select the **Script timeout** check box and specify the number of seconds before terminating the script.
10. Click **OK** to save the action.
11. Add other conditions or actions as needed, then click **Apply** to save the rule.

Smart Overwrite

On the **Destination File Path** page of the Protocol Upload Action wizard, you can specify what EFT 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.

Smart file transfer is complex multi-step process in which intermediate steps are allowed to fail. Occasionally these intermediate steps that fail will cause ERRORs in the transfer log, yet the file transfer does succeed.

- **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 renames the transferred file to "Copy of file.txt." If the same transfer occurs again, EFT renames the transferred file to "Copy (2) of file.txt" and so on.
- **Smart Overwrite =** EFT performs a CRC match of the files. (Supported only on FTP transfers.)
    - 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 will perform CRC on the portion of the source file that matches the length of the destination file. If the contents match, then EFT 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 overwrites the file without performing CRC first.



System: Backup Action

A Backup Server Configuration Event Rule is defined and enabled by default to back up EFT 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.

IMPORTANT: If the Timer Event Module is not licensed, the default Backup Server Configuration rule will not function after the trial has expired.

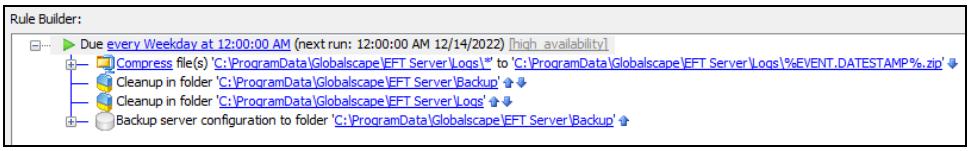
When you create your first Site, a new **Backup and Cleanup** rule is created that runs the System: Backup and System: Cleanup Actions once a day at midnight, using all defaults for naming and backup location. The default Rule includes a Cleanup Action to delete backup files (*.bak) older than 30 days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

> **NOTE:** You should specify a backup location that is not on the EFT server hard drive. If EFT's hard drive fails, you will need to use the backup to restore configuration. Ensure that EFT has permission to write to the folder that you specify for backup, especially if EFT is installed in a cloud location.

The default folder for backups, **C:\ProgramData\Globalscape\EFT Server\Backup**, is a hidden folder. In Windows File Explorer, click the **View** tab, then select the **hidden items** check box.

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

1. Create a Rule using the Timer, Service Stopped, Server Started, Event Rule Subroutine, GDPR Exercised, or IP Added to Ban List Events. If you are using the Timer Event, click the "Due <link>" hyperlink to define the backup schedule in the **Timer Event** dialog box. Refer to Scheduler (Timer) Event for details, if necessary.
2. Double-click the **System: Backup** Action or click it, and then click **Add**. The Action is added to the Rule.
3. 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's Application Data folder (for example, **C:\ProgramData\Globalscape\EFT Server\Backup**). You should change this location to a hard drive other than the one on which EFT is installed.
4. Click the folder icon to select the folder in which to save the backup file, and then click **OK**.
5. (Optional) Add the **System: Cleanup** Action to removed old backups. Refer to Clean-Up 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.
6. Add other Actions as needed, such as email notifications.
7. Click **Apply** to save the changes on EFT.
8. Click **Run Now** to test the Rule and verify that a file named "Server Configuration Backup <MM-DD-YYYY_HH-MM-SS>.bak" is saved in the assigned location.



The default **Backup and Cleanup** Event Rule includes a Compress files action and a Cleanup Action. Additionally, a Cleanup action is added to clean up the Logs folder. If you do not want to save logs created by LAN transfers, you can disable the logs using an advanced property. Refer to Event Rules Client Log for more information.

System: Cleanup Action

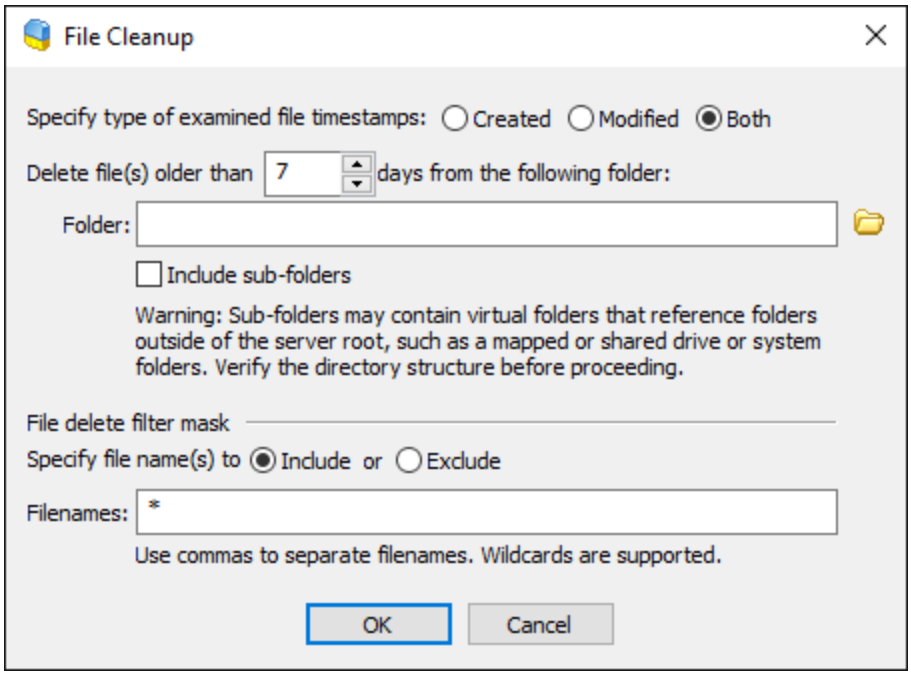
When you create your first Site, a Timer Rule is created that runs the System: Backup Action once each day at midnight, using all defaults for naming and backup location (\backup\Server Configuration Backup [Month] [Day] [Year].bak). The Rule includes a **Cleanup** Action to delete backup files (*.bak) 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. **After the trial expires, you should license the Timer Event module to continue backup/cleanup on a schedule.**

The **Cleanup** Action is available with the Scheduler (Timer), Event Rule Subroutine, Folder Monitor, GDPR Exercised, IP Added to Ban List, and REST Invocation, Events.

At the interval that you specify, EFT 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 configure EFT to cleanup files automatically

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 Action Parameters** dialog box appears.



4. Specify which type of file timestamps you want to delete: **Created** time, **Modified** time, or **Both** created and modified times.
5. 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.
6. In the **Folder** box, click the folder icon to specify the folder that you want to clean up.
7. To clean up subfolders in the specified folder, select the **Include sub-folders** check box.
8. 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 is configured to delete all *.bak files in **C:\ProgramData\Globalscape\EFT Server\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***.
9. Click **OK** to close the dialog box.
10. Click **Apply** to save the changes on EFT.

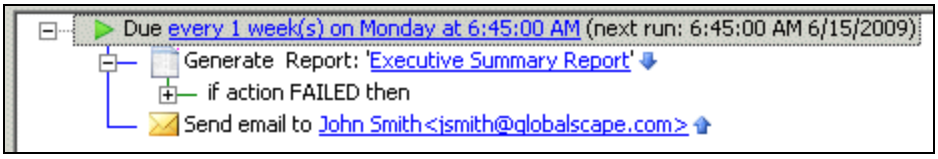
System: Report Action

(Requires ARM) When the Auditing and Reporting module is activated, you can configure an Event Rule to generate a report, then email it or save it to a file. If you add the Generate Report Action to a Rule, you must also tell EFT what to do with the report (save it or email 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 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 automatically generates a report of PCI/High Security-related configuration and functions. The report is converted to HTML and then emailed or saved to a file specified by the EFT administrator.

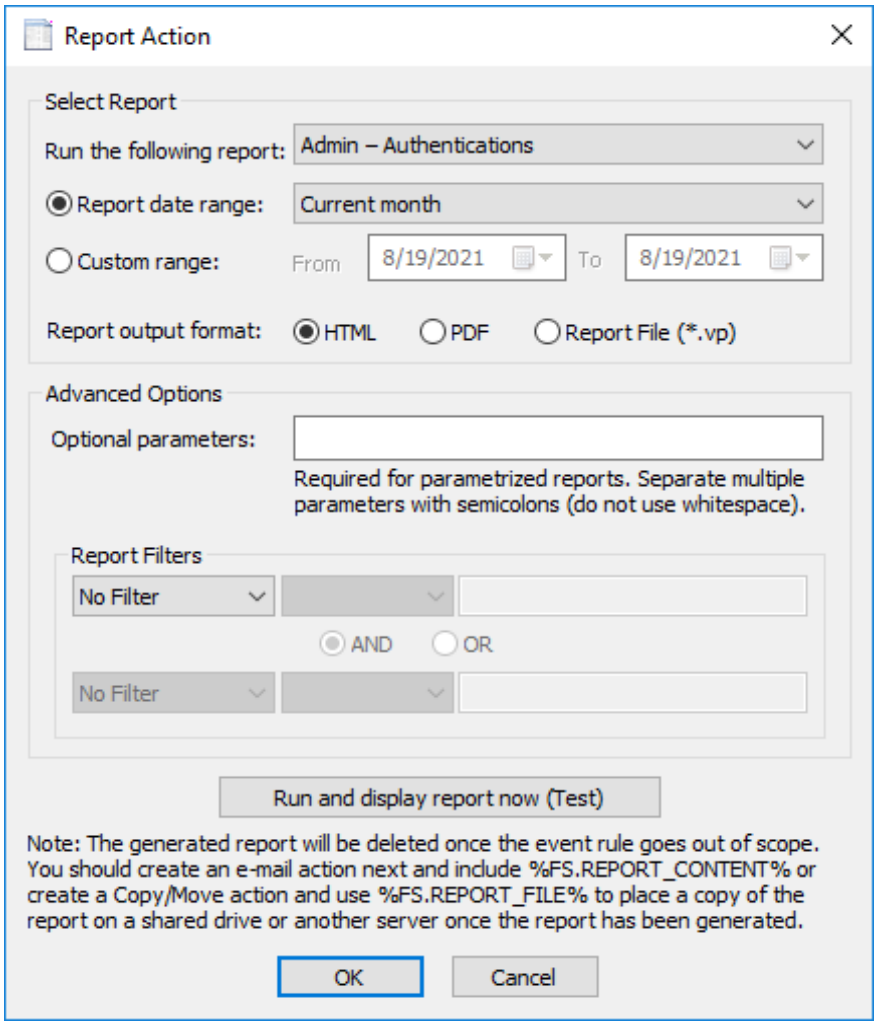
The automatic **Generate Report** Action never prompts for parameters because it will be run from the service on a timer, and thus does not allow interaction by a user. Reports that require parameters but do not have sufficient administrator-defined parameters will not run.

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 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 (for example, 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), 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 email 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 email notifications. When %FS.REPORT_CONTENT% is added to the body of email notifications, the content is displayed inline in the email in HTML format. (You must specify the HTML format in the **Report output format** area,)

The variable %FS.REPORT_FILE% can be used in copy/move, OpenPGP, and Custom Command Actions that have a failure Event defined, but should not be used for Actions that do not have a failure Event defined. Instead, use %FS.REPORT_CONTENT% for email notifications, 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 a complete list of EFT variables, see Variables. Do not use %FS.REPORT_FILE% in email notifications.

User Action

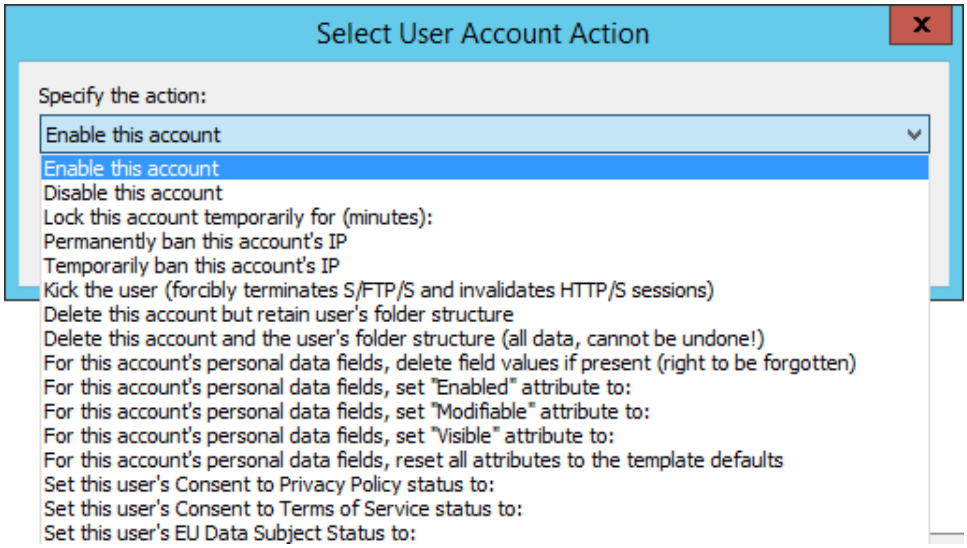
The **User** Action can be added to applicable Event Rules to perform actions such as disabling/locking the account, banning the account, and so on. The Action is ***not*** available for triggers associated with operating system events: Timer, Folder Monitor, Cloud object monitor, Server, and Site events.

(Available Actions contains a table of which Actions are available with which Event Triggers.)

The **User** Action is useful for things like compliance requests in which users might ask that an organization remove all traces of their account (for example, HIPAA, GDPR) .

To specify User Actions

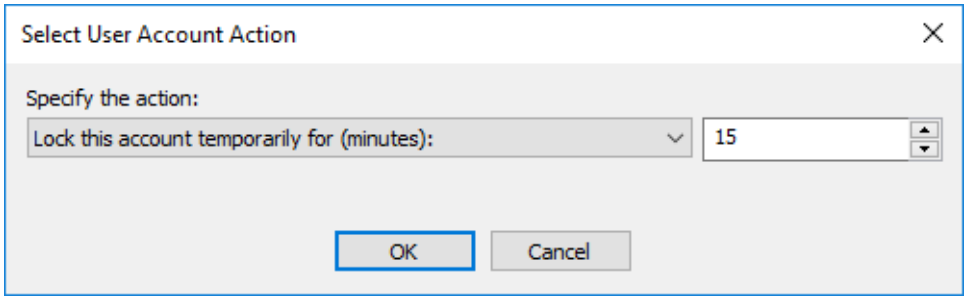
1. After you create an Event Rule, add any applicable Conditions and then add the User Account Action.
2. In the Event Rule, click the link in the Action to specify an Action. The **Select User Account Action** dialog box appears.



Actions (named for their specific function) include:

- Enable this account
- Disable this account
- Lock this account temporarily for (minutes)

  When you choose **Lock this account temporarily for (minutes)**, a field appears in which you can specify up to 15 minutes.



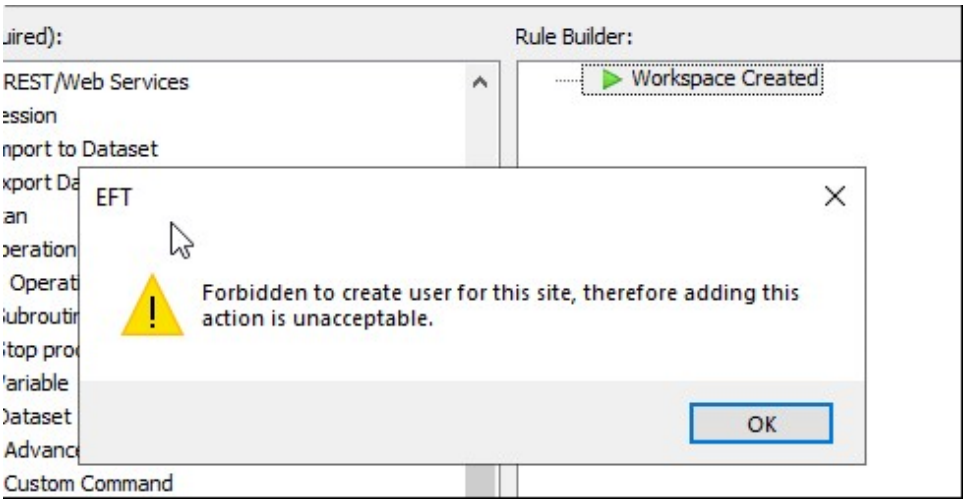
- Permanently ban this account's IP
- Temporarily ban this account's IP
- Kick the user (forcibly terminates SFTP, FTP, and FTPS, and invalidates HTTP and HTTPS sessions)
- Delete this account but retain user's folder structure
- Delete this account and the user's folder structure(removes all data and cannot be undone)
- For this account's personal data fields, delete field values is present (right to be forgotten)
- For this account's personal data fields, set "Enabled" attribute to: True, False
- For this account's personal data fields, set "Modifiable" attribute to: True, False
- For this account's personal data fields, set "Visible" attribute to: True, False
- For this account's personal data fields, reset all attributes to the template defaults.
- Set this user's Consent to Privacy Policy status to: Unknown, Granted (implicit), Granted (explicit), Denied, Rescinded
- Set this user's Consent to Terms of Service status to: Unknown, Agreed (implicit), Agreed (explicit), Disagreed, Withdrawn
- Set this user's EU Data Subject Status to: Unknown, Yes, No

3. Click **OK** to save the Action.
4. Add any other Actions, as needed, then click **Apply** to save the Event Rule.

User Create Action

On Globalscape-authenticated and ODBC-authenticated sites, you can add the **User: Create** action to an event rule when you want a certain event to trigger the creation of a new user. This action is available to any event trigger.

NOTE: If you try to add the **User: Create** action to an event rule on an LDAP-authenticated or AD-authenticated site, EFT will present the error message "Forbidden to create user for this site":



Event Rule Administrators are not able to create or edit event rules with the User: Create action. This behavior is by design; Event Rule administrators are not able to create users. An error message will be presented in the interface when attempting to perform this action.

When you click the **select** link, the **New User Creation** wizard appears in which you can add variables to populate the user definition. Context variables are available in the following fields: **Login**, **Password**, **Email**, all fields in the **User Account Details** dialog box, and the **Home folder** path (on the second page of the wizard).

NOTE: If the user name already exists, the "create" action will fail and the error is logged in the EFT log file. No error is displayed in the interface.

You can also onboard new users via a form that feeds into a tool such as "Service Now." Service Now then invokes REST API and passes in numerous parameters, such as username, password, and so on. (Service Now is not a Globalscape product. For Service now help, please contact Service Now customer support.) Refer to RESTAPIExamples (ZIP file) for an example of creating a user with the REST API. Refer to Creating a User Account for more details of account creation.

Using Wildcards with Event Rule Actions

The **OpenPGP** Action, the **Copy/Move** Action, and the **File Name** Condition 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. For 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 respects Windows path syntax:

For example:

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

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

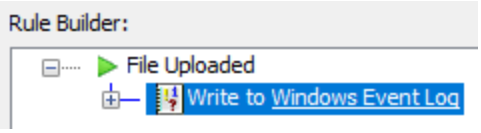
Test an Event Rule using a wildcard before you deploy it to ensure it works as expected and does not cause any unwanted behavior. For example, if you do not define the source path appropriately when a wildcard is used, it is possible to set up an Action that moves all the files out of a user's c:\windows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

Example: Using Wildcards in Event Rules to Download from WinSSHD

Refer to the Globalscape Knowledgebase topic #10569 for information about sending an email notification when a certain user uploads a file.

Windows Event Log (WEL) Action

The **Windows Event Log** Action is available for all Event Triggers to write to the Event Viewer. When you add the **Windows Event Log** Action to the **Rule Builder** and then click the hyperlink in the Action, the **Windows Event Log** dialog box appears. Use this dialog box to specify the WEL message parameters.

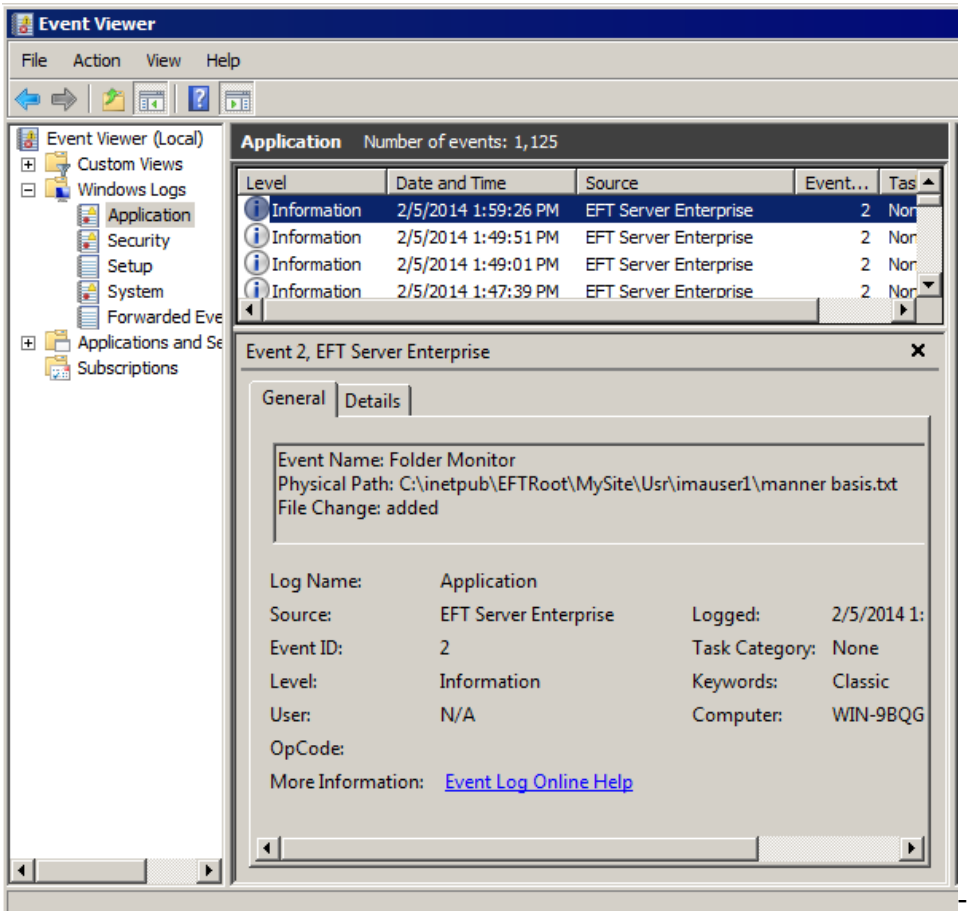


To configure the WEL message

1. In the **Type** box, click the down arrow and specify whether the message is an **Information**, **Warning**, or **Error** message. The default is Error.
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. By default, the message is whatever you have specified in the **Variable list**.
4. (Optional) In the **Variable list** box, click an EFT 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`, then press ENTER. The **Event Viewer** appears.
3. Click **Windows Logs > Application**. Double-click an EFT (Source) event. The **General** description and **Details** of the Event appear.



4. Notice that the description area displays the values of the variables that you provided in the **Windows Event Log Message** dialog box. In this example, we used the Event Name, Physical Path, and File Change variables. (Date and time are provided in the Event Viewer.)

Conditions

The topics below provide information regarding defining and using Event Rule Conditions.

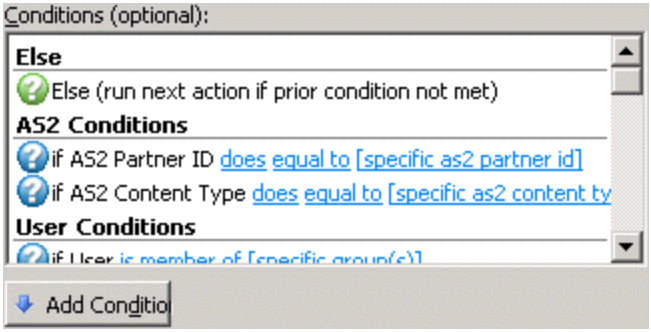
Using Conditions

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, 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.

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.

Conditions are organized by type:

- Advanced Workflow Conditions—Event is triggered based on Advanced Workflow criteria such an error.
- 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 Java-enabled Web Transfer Client
- Context Variable Condition—Event is triggered when a context variable equals or doesn't equal a specified string.
- Event Properties—Event is triggered based on a specific Event reason.
- 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 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.
- Workspaces-related Conditions—Event is triggered based on Workspace variables, such as folder owner.

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

Condition Placement

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

- When the Event Rule *trigger* (the very first item in the **Rule Builder**) 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 does not support.

```
ON FILE UPLOAD
{
 if ( %FS.FILE_NAME%  = "*.pgp" )
{
  PGPDecrypt %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

When you have multiple Conditions, you can change the order by clicking them using the up/down arrows next to the Condition, at the bottom of the Rule Builder, 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

To move C1 down, 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 and dragging the Condition icon at the far left of the Condition, or select the line and then 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 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

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 Builder**. 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
```

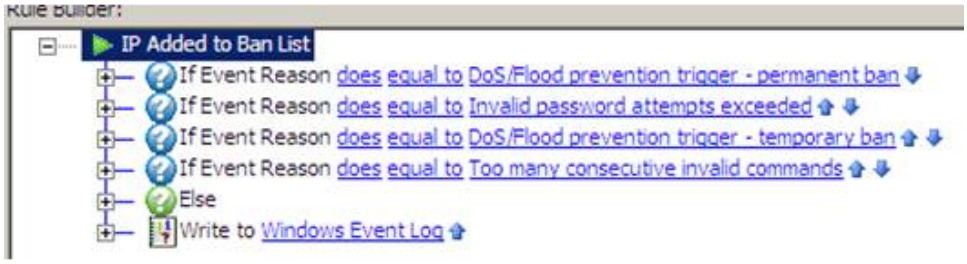
```
{ Run B }

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 administrators
```

Now click one of the AND hyperlinks to change it to OR. The Conditions change to:

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

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. The Conditions change to:

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

With the AND in this 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 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
administrators (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 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, 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 to change it.

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

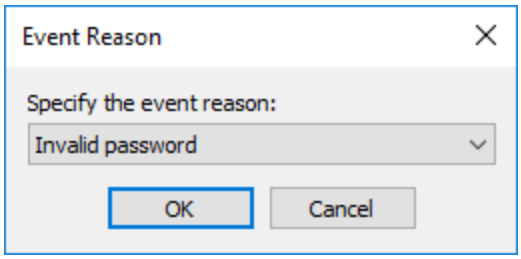
If you need to use more complex criteria using AND and OR, you can use wildcard logic to create any logic that wildcards support. For example, if you add the **File Name** Condition to the **Rule Builder**, you can then define the path mask using complex logic with wildcards.

Event Properties

Event Properties are used in several Failed events, as described below. The Event Properties allow you to get a more specific reason why an event failed.

- **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).

	Connection Event	User Events		File Server Events			
Event Reason	**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				

	Connection Event	User Events		File Server Events			
Event Reason	**User Connect Failed**	**User Login Failed**	**User Logged Out**	**Download Failed**	**Upload Failed**	**Verified Upload Failed**	**Verified Download Failed**
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				

Advanced Workflow Conditions

You can apply Advanced Workflow Conditions to any events except the Cloud-Based events.

To use one or more Advanced Workflow Conditions

1. Create the Event Rule.
2. Double-click the Condition, or click the Condition, then click **Add Condition**.
3. In the **Rule Builder**, click the hyperlinks in the Condition to specify if the Condition **does** or **does not** and **less than**, **equal to**, or **greater than** the [code], [test], or [number].
4. Then add one or more Actions and click **Apply**.

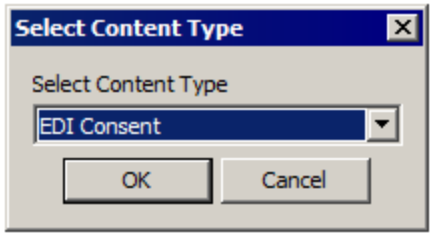
> **NOTE:** The Advanced Workflow Conditions below are available for any events except cloud-based events. They are named for their function. For example, the "If Advanced Workflow Error Description" condition will trigger the event if the Error Description in the Advanced Workflow has or doesn't have the text specified.

- If Advanced Workflow Error Code does, does not, less than, equal to, or greater than [code]
- If Advanced Workflow Error Description does, does not, equal to [text]
- If Advanced Workflow Error Line does, does not, less than, equal to, or greater than [number]
- If Advanced Workflow Result Code does, does not, less than, equal to, or greater than [code]
- If Advanced Workflow Result Description does, does not, equal to [text]
- If Advanced Workflow Execution Time does, does not, less than, equal to, or greater than [ms]

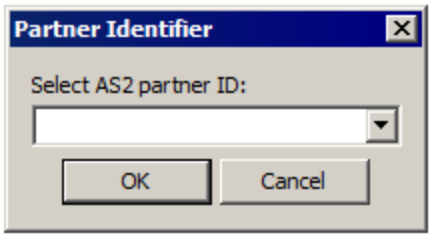
AS2 Conditions

You can apply AS2 Conditions to File Uploaded and AS2-related events.

- **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]**. Click **[specific AS2 content type]** to open the **Select Content Type** dialog box.



  3. Click the **Select Content Type** drop-down list to specify a (**X12**, **EDIFACT**, **XML**, **EDIConsent**, **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 no**t equal to **[specific AS2 Partner ID]**. Click **[specific AS2 Partner ID]** to open the **Partner Identifier** dialog box.



  3. Click the **Select AS2 partner ID** drop-down list to specify a partner.
  4. Click **OK**.

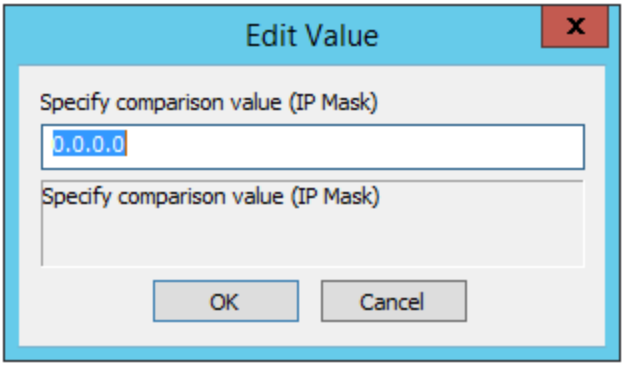
You can also specify the AS2 protocol with the **If Protocol Condition** described in Connection Conditions.

Connection Conditions

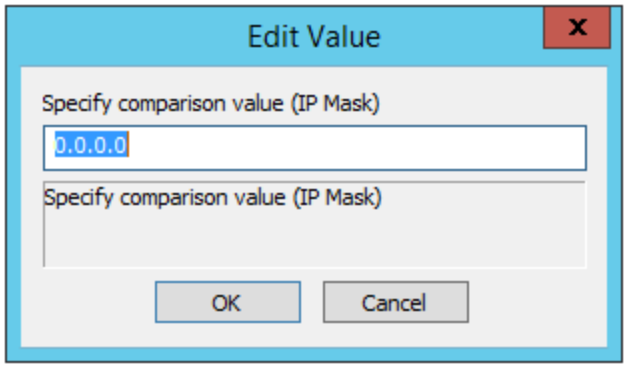
You can apply these Conditions to Connection Events, File system Events, and certain User Events.

By default, IP Access-related Event Rules are limited to 1000 rules.

- **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 to specify whether the remote IP address **does** or **does not** match **[ip mask]**.
  3. Click **[ip mask]** to open the **Edit Value** dialog box.

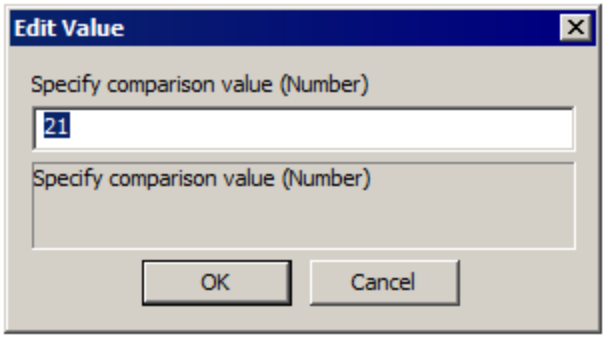


  4. Specify an IP address or and/or wildcards, and then click **OK** to add the Condition to the Event trigger.
- **If Local IP**—a connection is made to a local IP address that matches/does not match an IP address or IP mask.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the local IP address **does** or **does not** match **[ip mask]**.
  3. Click **[ip mask]** to open the **Edit Value** dialog box.

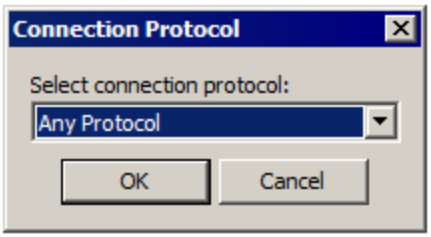


4. Specify an IP address or and/or wildcards, and then click **OK** to add the Condition to the Event trigger.

- **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 to specify whether the port number **does/does not equal to, greater than or equal to, less than, less than or equal to [value]**.
  3. Click [value] to open the **Edit Value** dialog box.



  4. Specify a port number, 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 the linked text to specify whether the protocol **does/does not equal to [ftp/ssl/tls/sftp/http/https/as2/adhoc]**.
  3. Click **[ftp/ssl/tls/sftp/http/https/as2/adhoc]** to open the **Connection Protocol** dialog box.



4. Click the **Select connection protocol** drop-down list to select the protocol (or specify **Any Protocol**).
5. Click **OK**.

- **If HTTP Query String**—does/does not contain/equal to <string>. Specify a string; enclosing quotes are not needed
- **If HTTP Headers List**—does/does not contain/equal to <string>. Specify a string; enclosing quotes are not needed

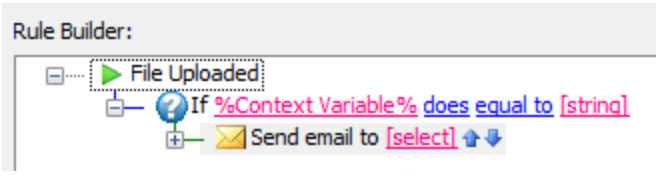
Context Variable Condition

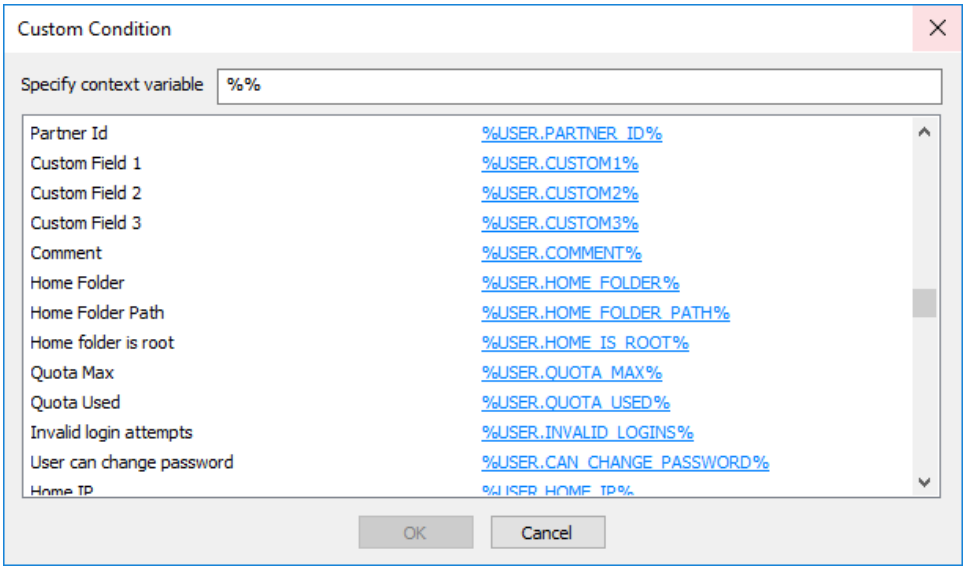
The Context Variable Condition is triggered when a context variable meets specific criteria: if %Context_Variable% is/is not, does/does not, equal/less than/greater than/, contain/start with a specified value. For example, %USER.HOME_FOLDER_PATH% to provide entire path to a user's home folder (for example, C:\InetPub\EFTRoot\MySite\Usr\asmith).

(This is an oversimplified example; putting this Rule on a production network could potentially create huge logs.)

To use the Context Variable Conditions

1. Create an Event Rule and add one or more actions.
2. Add the **Context Variable** Condition.


Rule Builder:
File Uploaded
If %Context Variable% does equal to [string]
Send email to [select]


Custom Condition
Specify context variable
%%
Partner Id
%USER.PARTNER_ID%
Custom Field 1
%USER.CUSTOM1%
Custom Field 2
%USER.CUSTOM2%
Custom Field 3
%USER.CUSTOM3%
Comment
%USER.COMMENT%
Home Folder
%USER.HOME_FOLDER%
Home Folder Path
%USER.HOME_FOLDER_PATH%
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%
OK
Cancel

File System Conditions

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

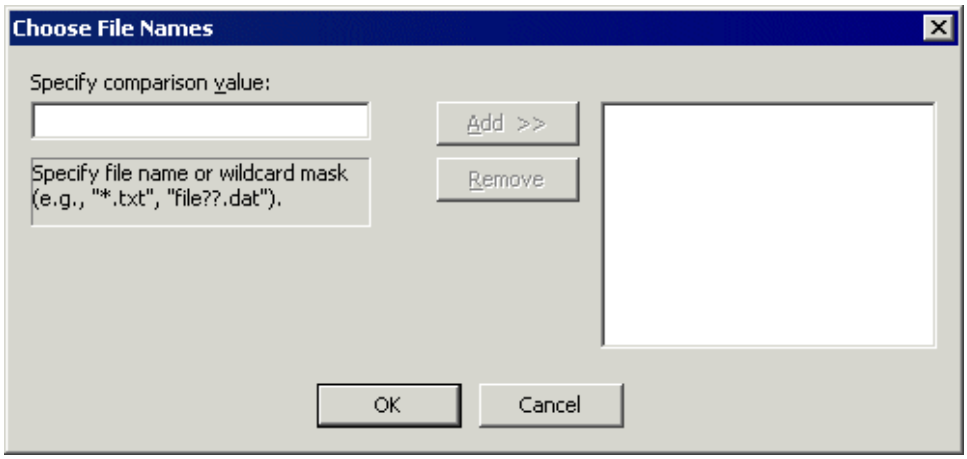
Using the File System Conditions

- **If File (or Folder) does exist at [path]**—a file or folder does or does not exist at specified path or variable.

- **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. Click **[path mask]** to open the **Choose Virtual Path** dialog box.
    4. Specify a path or wildcard, then click **Add** to move the path to the right text box.
    5. To remove a path, in the right text box, click the path or wildcard, and then click **Remove**.
    6. 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. Click **[path mask]** to open the **Choose Physical Paths** dialog box.
    4. Specify a path or wildcard, then click **Add** to move the path to the right text box. You can add multiple paths.
    5. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
    6. Click **OK** to add the Condition to the Event trigger.

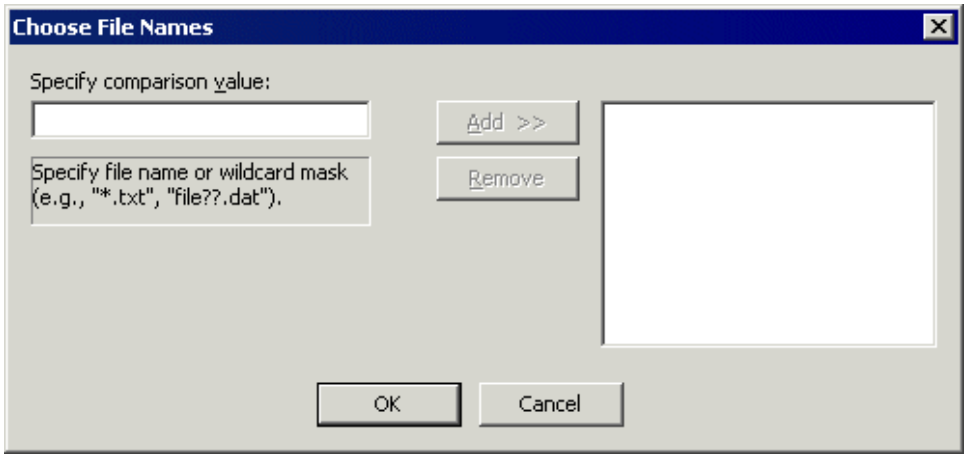
- **If Virtual Directory Name**—the virtual directory name does or does not match the path mask.
    1. Add the Condition to the Event Rule.
    2. In the Rule Builder, click the linked text to specify whether the virtual directory name **does/does not match [path mask]**.
    3. Click **[path mask]** to open the **Choose Virtual Directory Names** dialog box.
    4. 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.
    5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
    6. 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. Click **[path mask]** to open the **Choose Folder Names** dialog box.
    4. Specify a folder name or wildcard, then click **Add** to move the folder name or wildcard to the right text box. You can add multiple folders.
    5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
    6. 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. Click **[path mask]** to open the **Choose Virtual Folder Names** dialog box.
    4. 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.
    5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
    6. 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. Click **[path mask]** to open the **Choose File Names** dialog box.



4. Specify a file name or wildcard, then click **Add** to move the file name or wildcard to the right text box. You can add multiple file names.
5. To remove a path, in the right text box, click the file name or wildcard, and then click **Remove**.
6. Click **OK** to add the Condition to the Event trigger.

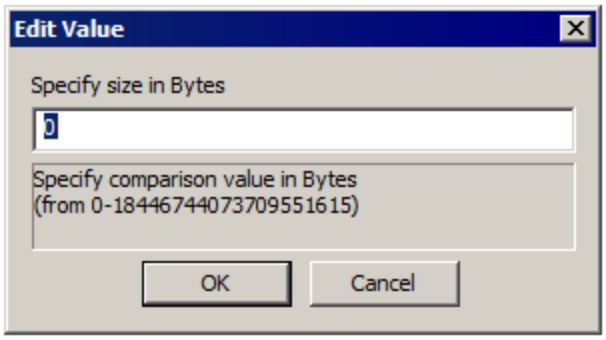
- **If Base File Name**—The portion of the filename to the left of the right most period; provided as a way to support rename. For example, if a file is downloaded as SomeFile.ext.tmp, the Base File Name is: SomeFile.ext.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not** match **[mask]**.
  3. Click **[mask]** to open the **Choose File Names** dialog box.



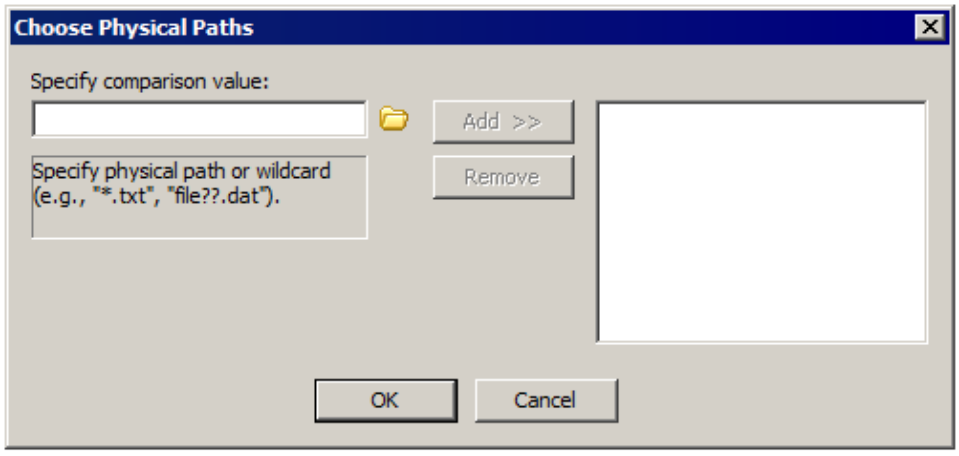
  4. Specify a file name or wildcard, then click **Add** to move the file name or wildcard to the right text box. You can add multiple file names.

5. To remove a file name or wildcard, in the right text box, click the file name or wildcard, and then click **Remove**.
6. 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)]**. Click **[size (B)]** to open the **Edit Value** dialog box.

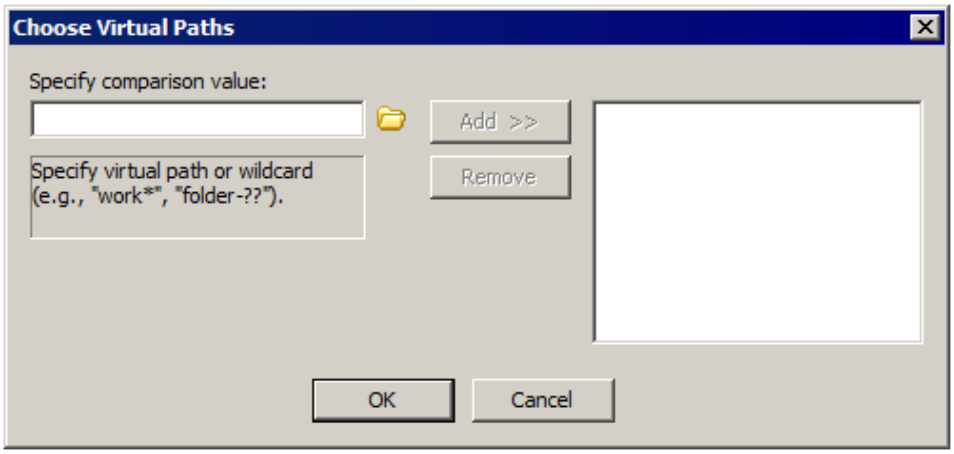


  3. Specify a file size in bytes, and then click **OK**.
- **If Physical Destination Path**—(for **File Moved** Event) the file or folder exists, does not exist at a physical location and/or wildcard.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the virtual path **does/does not match/start with [path mask]**.
  3. Click **[path mask]** to open the **Choose Physical Paths** dialog box.

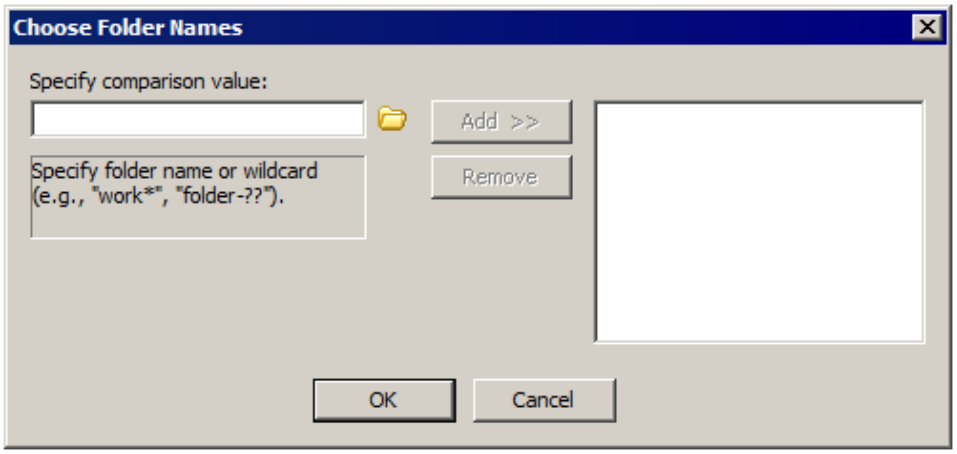


4. Specify a path or wildcard, then click **Add** to move the path or wildcard to the right text box. You can add multiple paths.
5. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
6. Click **OK** to add the Condition to the Event trigger.

- **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. Click **[path mask]** to open the **Choose Virtual Paths** dialog box.

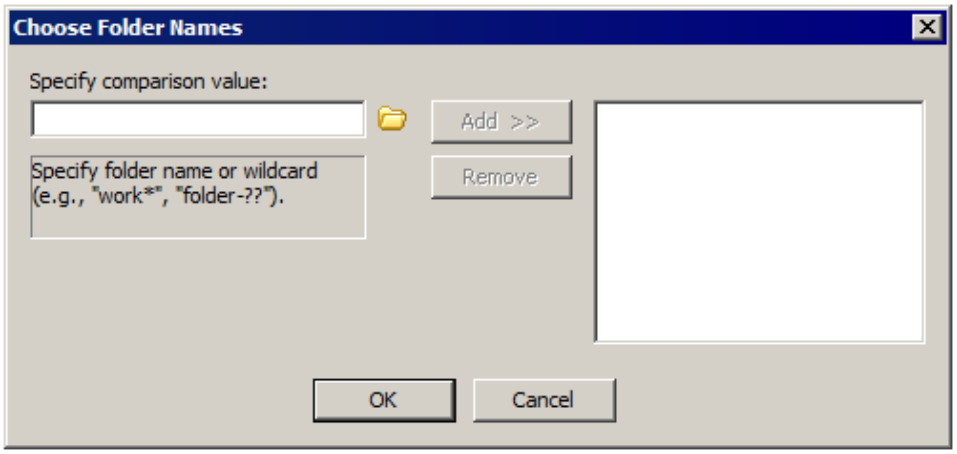


  4. Specify a path or wildcard, then click **Add** to move the path to the right text box. You can add multiple paths.
  5. To remove a path or wildcard, in the right text box, click the path or wildcard, and then click **Remove**.
  6. Click **OK** to add the Condition to the Event trigger.
- **If Physical 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 notmatch/start with[path mask]**.
  3. Click **[path mask]** to open the **Choose Folder Names** dialog box.



4. Specify a folder name or wildcard, then click **Add** to move the folder name or wildcard to the right text box. You can add multiple names.
5. To remove a folder name or wildcard, in the right text box, click the folder name or wildcard, and then click **Remove**.
6. 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. Click **[path mask]** to open the **Choose File Names** dialog box.



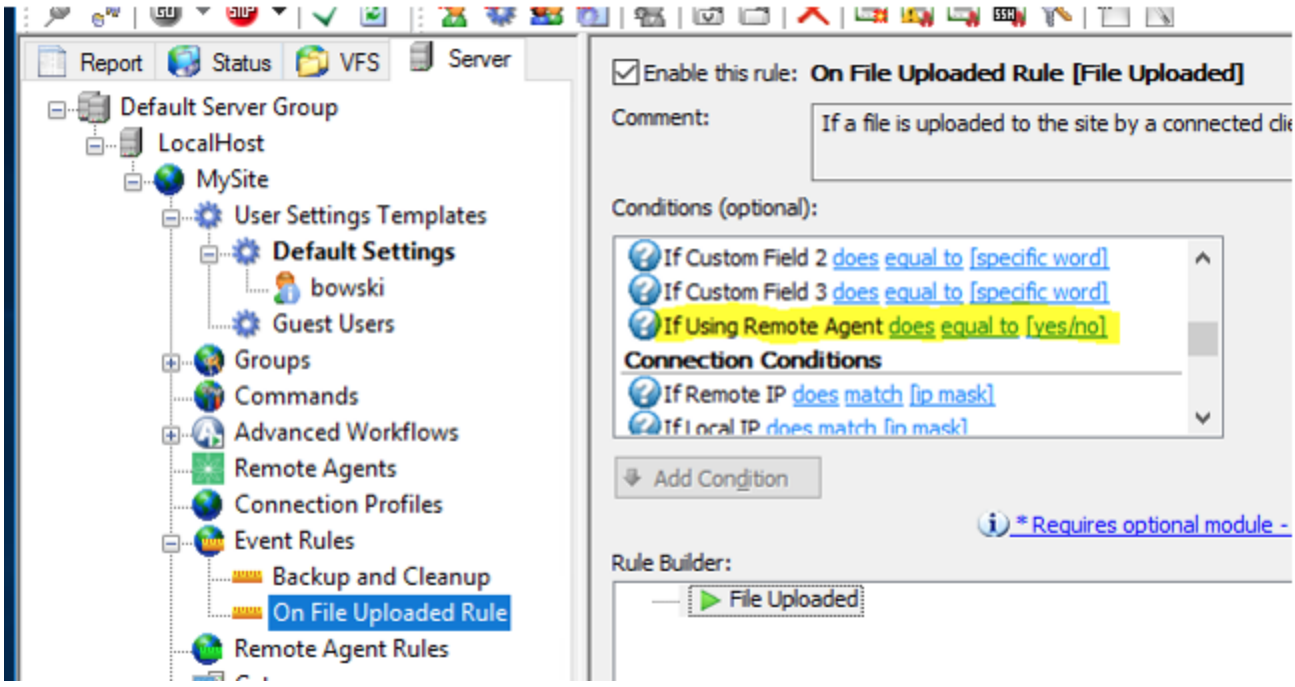
4. Specify a file name or wildcard, then click **Add** to move the file name or wildcard to the right text box. You can add multiple names.
5. To remove a file name or wildcard, in the right text box, click the file name or wildcard, and then click **Remove**.
6. Click **OK** to add the Condition to the Event trigger.

Remote Agent Event Rule Conditions

You can add a "If using Remote Agent does/does not equal to yes/no" to EFT Event Rules for the following events:

- File Uploaded
- File Downloaded
- File Upload Failed
- File Download Failed
- Before Download

This Condition works for HTTP and HTTPS interactions only.



Secure Message Conditions

Secure Message Conditions are available for Outlook Add-In, Send Portal, Reply, Drop Off, and Request File-related events.

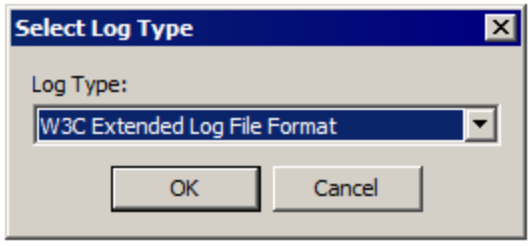
To use these conditions, add a Condition to the Rule, then click the linked text to specify the parameters. For each Condition, specify that the Condition does or does not equal the specified parameter.

- **If Portal From** does or does not equal to [specific portal type] - Specify a portal type: OAI, Send Portal, Reply, Drop Off, or Request File.
- **If Sender** does or does not equal to [text] - Specify a sender in the text box.
- **If Send Error** does or does not equal to [text] - Specify a send error in the text box.
- **If Subject** does or does not equal to [text] - Specify a subject in the text box.
- **If To Recipients** does or does not equal to [specified name(s)] - Specify a recipient in the string box.
- **If CC Recipients** does or does not equal to [specified name(s)] - Specify a recipient in the string box.
- **If BCC Recipients** does or does not equal to [specified name(s)] - Specify a recipient in the string box.
- **If Attachments** does or does not equal to [specified name(s)] - Specify a name in the string box.
- **If Attachments Storage Path** does or does not equal to [path mask] - Specify a value in the box.
- **If Body** does or does not equal to [text] - Specify a string for comparison.
- **If Body Is Secured** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Is Single Use** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Requires Account to Reply** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Requires Account to View** does or does not equal to [yes/no] - Click to specify yes or no.
- **If Message Expires On** does or does not equal to [specific timestamp] - Specify a string to match a timestamp.
- **If Notification Frequency** does or does not equal to [specific type] - Specify the notification frequency, IMMEDIATE, DAILY, NEVER.

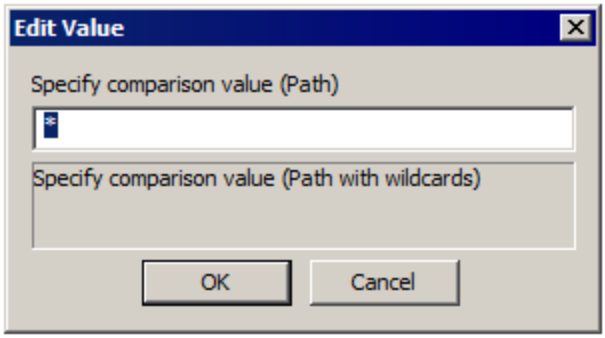
Server Conditions

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

- **If Server Running**—The EFT 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. Click **[specific type]** to open the **Select Log Type** dialog box.

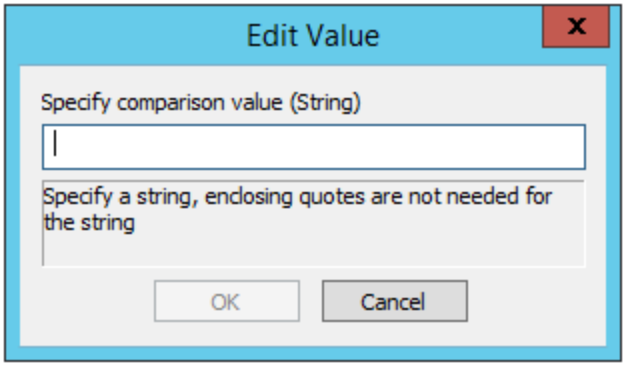


  4. Specify a **Log Type**, and then click **OK**.
- **If Log Location**—The log location matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the log location **does/does not** match **[path]**.
  3. Click **[path]** to open the **Edit Value** dialog box.

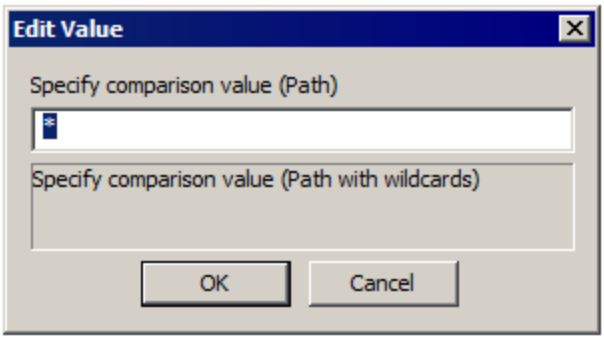


  4. Specify a path or wildcard, and then click **OK**.

- **If Node Name**—In HA cluster, EFT name matches/does not match a specific character string. Most often used when you want only one specific node to send email notifications or perform other actions. Not specifying a node can cause multiple nodes to perform the Action specified in the Event Rule.
  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. Click **[name]** to open the **Edit Value** dialog box.

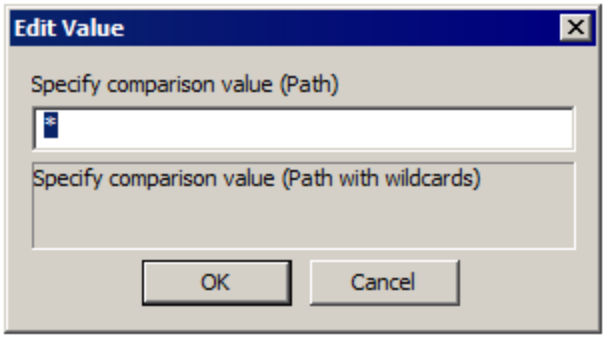


  4. Specify a name or wildcard, and then click **OK**.
- **If Old Log File Path**—(Used with the **Log Rotated** Event only) The old log file path matches a specific path.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the old log location **does/does not** match **[path]**.
  3. Click **[path]** to open the **Edit Value** dialog box.

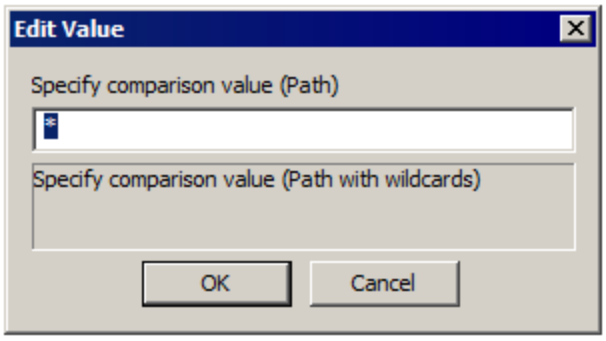


  4. Specify a path or wildcard, and then click **OK**.

- **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. Click **[path]** to open the **Edit Value** dialog box.

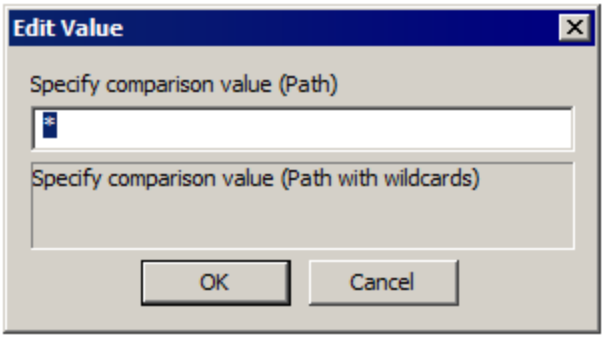


  4. Specify a path or wildcard, and then click **OK**.
- **If Old Log File Name**—(Used with the **Log Rotated** Event only) The old log file name matches a specific name.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the old log location **does/does not** match **[path]**.
  3. Click **[path]** to open the **Edit Value** dialog box.



  4. 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. Click **[path]** to open the **Edit Value** dialog box.



  4. Specify a path or wildcard, and then click **OK**.

Site Conditions

You can apply the Site Condition only to these User events: **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 not** equal to **yes/no**.

User Conditions

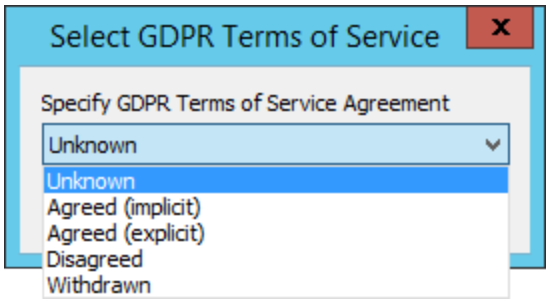
You can apply User Conditions to User Events and File system Events.

- In each of the GDPR-specific user conditions, click an option, then click **OK**.

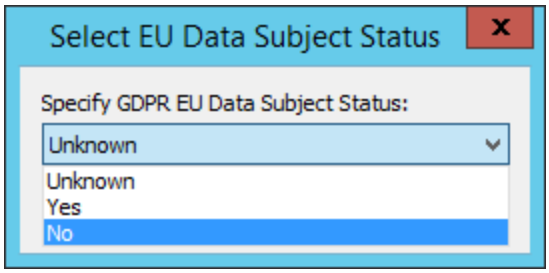
  For example, suppose you want to be notified any time an EU Data Subject joins a Workspace. You could configure an Event Rule to trigger on the **User Joins Workspace** event, with the **EU data Subject Status** condition set to **Yes**, and a **Send email notification** Action (with applicable content variables added), which could send that information to your email or the Data Protection Officer's email.

  - **If (GDPR) User consent to privacy policy** does or does not equal to:

  - **If (GDPR) User agreement to terms of service** does or does not equal to:

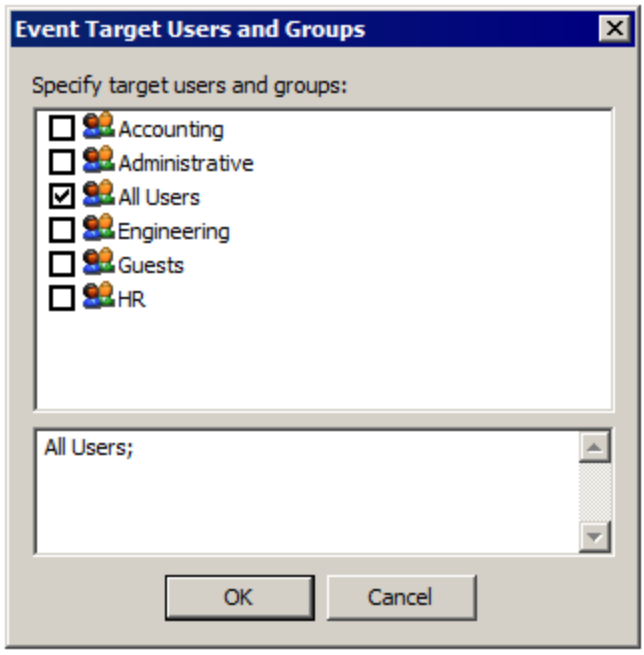


  - **If (GDPR) User EU data subject status** does or does not equal to:

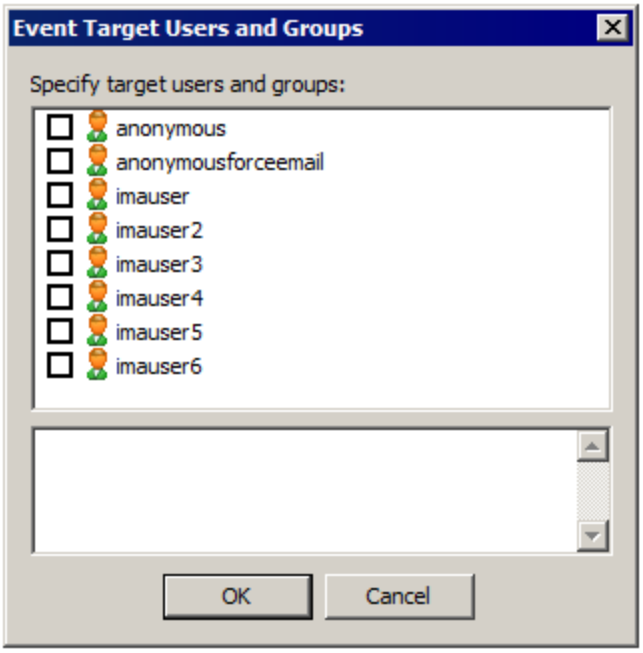


- **If DUNS number** does or does not equal to [specific word]. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If (GDPR) Right exercised article** ID does or does not equal [specific article ID]
- **If (GDPR) Reason given** does or does not equal to [specific word or phrase]. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **If User**—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. Click **[specific group(s)]** to open the **Event Target Users and Groups** dialog box.

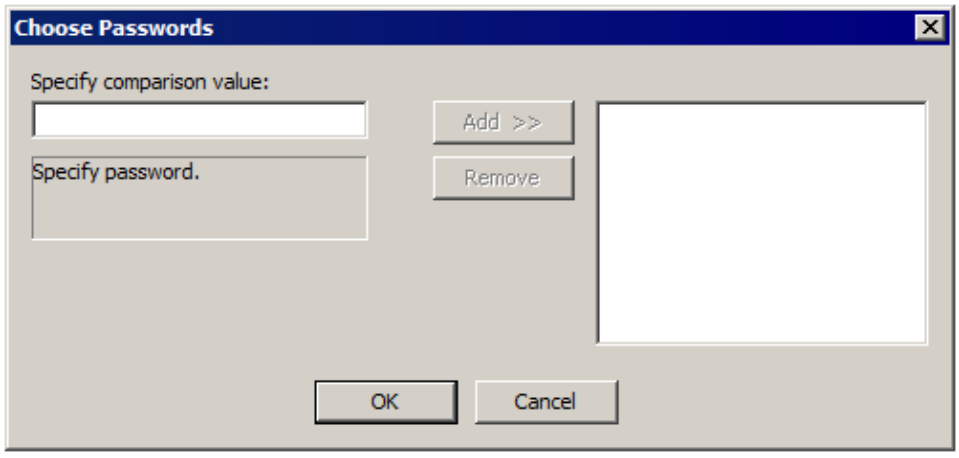


  4. Select the check box of the users/groups that will trigger the Event and clear the **All Users** check box if you don't want the Condition to apply to all users.
  5. Click **OK** to add the Condition to the Event trigger.
- **If Logon Name**—the user's username matches/does not match a specific username.
  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. Click **[specified name(s)]** to open the **Event Target Users and Groups** dialog box.



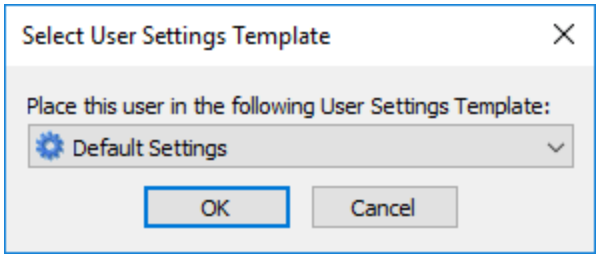
4. Select the check box of the users/groups that will trigger the Event and clear the **All Users** check box if you don't want the Condition to apply to all users.
5. Click **OK** to add the Condition to the Event trigger.

- **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. Click **[specified password(s)]** to open the **Choose Passwords** dialog box.

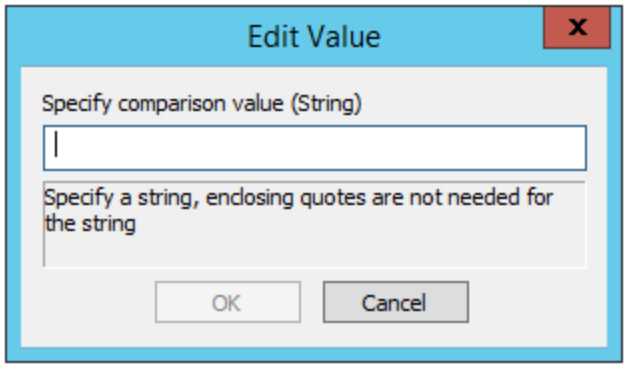


4. Specify a password, and then click **Add** to move the password to the right text box.
5. To remove a password, in the right text box, click the password, and then click **Remove**.
6. Click **OK** to add the Condition to the Event trigger.

- **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. Click **[Settings Template]** to open the **Select Settings Template** dialog box.

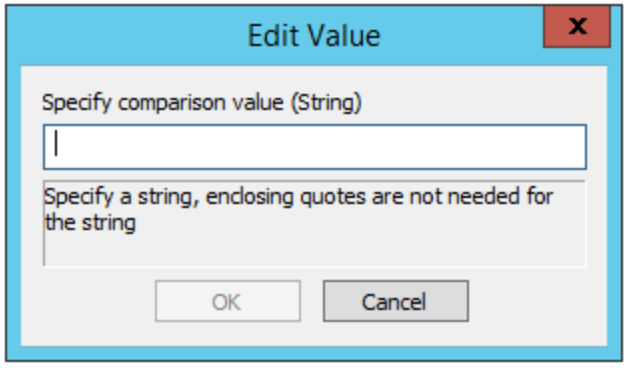


  4. Specify a Settings Template, then click **OK**. (Even if there is only one Settings Template, you still have to click **OK** in the **Select Settings Template** dialog box to complete the Condition.)
- **If Full Name**—a user's name matches/does not match, contains/equals a specific string.
  1. Add 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. Click **[name]** to open the **Edit Value** dialog box.

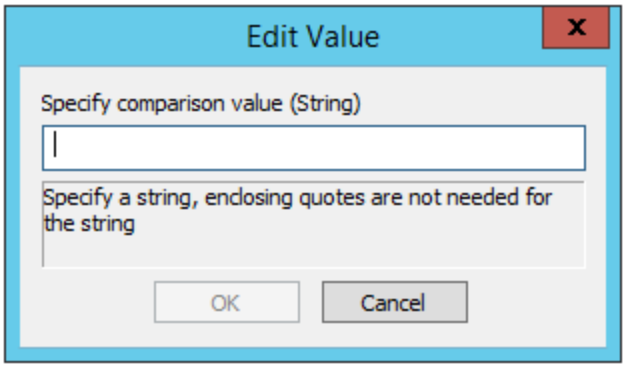


4. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **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. Click **[name]** to open the **Edit Value** dialog box.

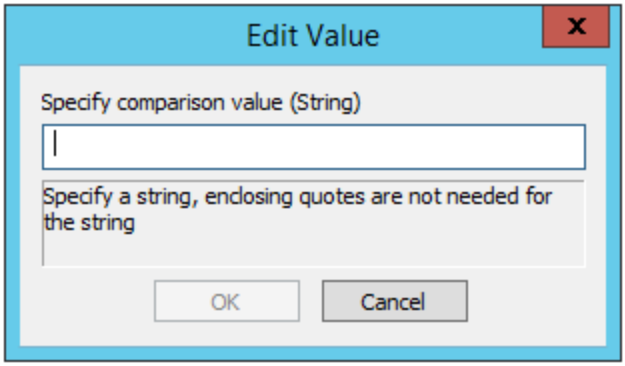


  4. In the **Edit Value** dialog box, specify a word, and then click **OK**.
- **If Comment**—the user's comment matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the comment **does/does not equal to/contain [specific word]**.
  3. Click **[name]** to open the **Edit Value** dialog box.

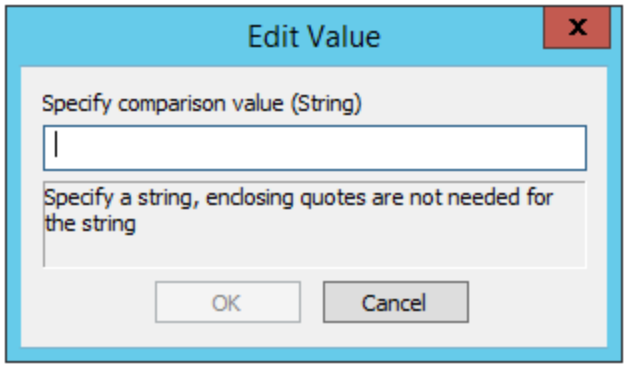


4. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **If EMail Address**—the user's email 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 notequal to/contain[specific word]**.
  3. Click **[name]** to open the **Edit Value** dialog box.

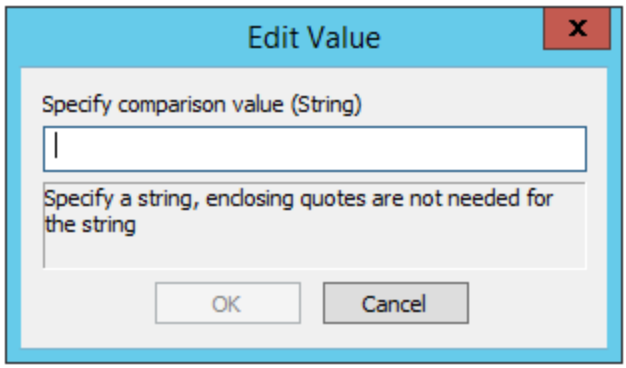


  4. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Phone Number**—the user's phone number matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the phone number **does/does not equal to/contain [specific word]**.
  3. Click **[name]** to open the **Edit Value** dialog box.

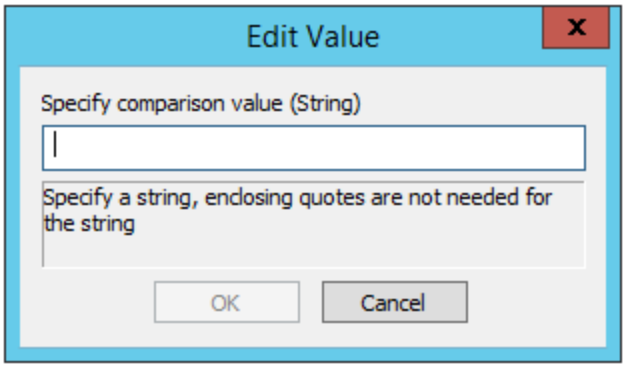


4. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **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. Click **[name]** to open the **Edit Value** dialog box.

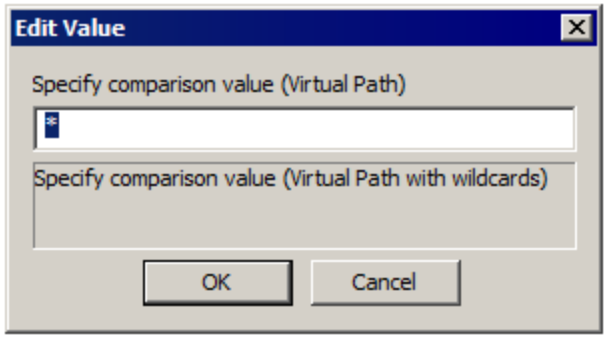


  4. In the **Edit Value** dialog box, specify a string, and then click **OK**.
- **If Fax Number**—the user's fax number matches/does not match, contains/equals a specific string.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the fax number **does/does not equal to/contain [specific word]**.
  3. Click **[name]** to open the **Edit Value** dialog box.

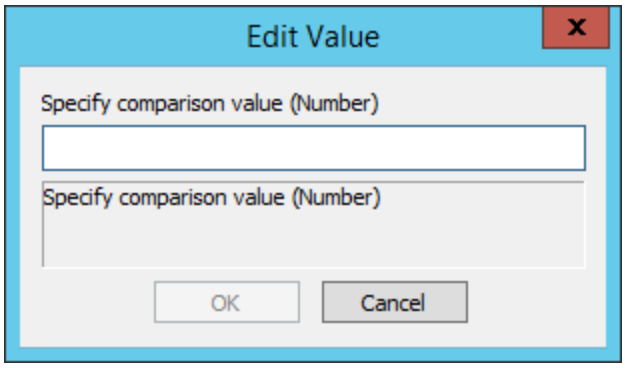


4. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **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. Click **[path]** to open the **Edit Value** dialog box.

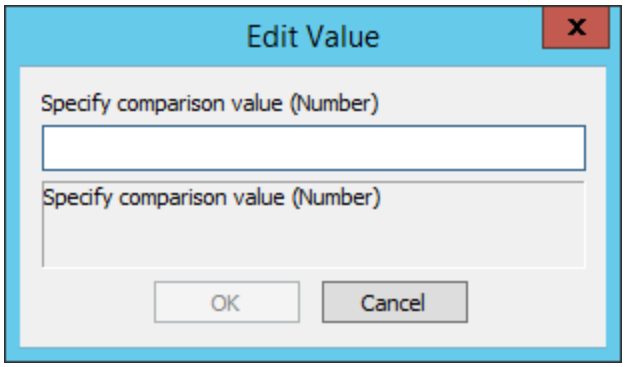


  4. Specify a virtual path, and then click **OK**.
- **If Home Folder is root**—the user's home folder is/is not their root directory.
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether home folder root **does/does not** equal to **[yes/no]**.
- **If Quota Max**—the user's account has a size limit **less than/equal to/not less than/not equal** to a size in megabytes.
  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. Click **[size (MB)]** to open the **Edit Value** dialog box.

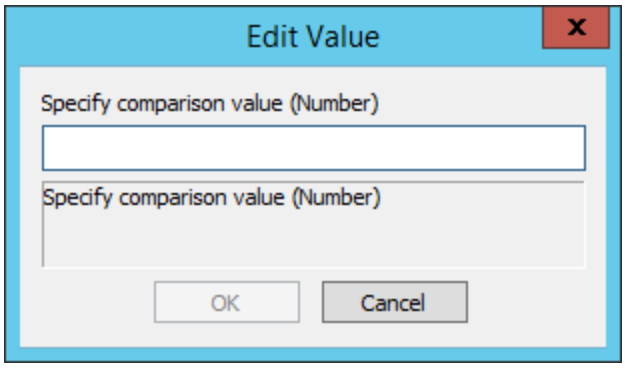


4. Specify the maximum quota, and then click **OK**.

- **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. Click **[size (MB)]** to open the **Edit Value** dialog box.



  4. In the **Edit Value** dialog box, specify a value, 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. Click **[number]** to open the **Edit Value** dialog box.

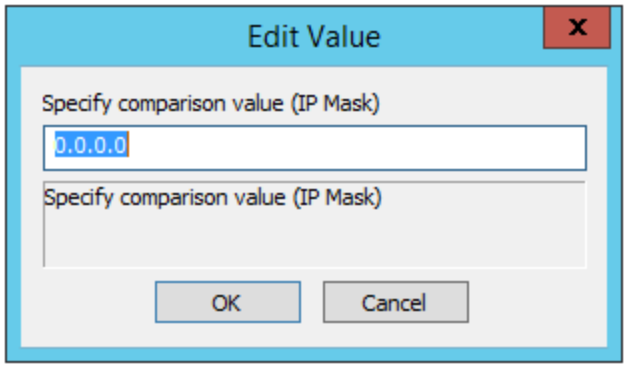


4. In the **Edit Value** dialog box, specify a string, and then click **OK**.

- **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.

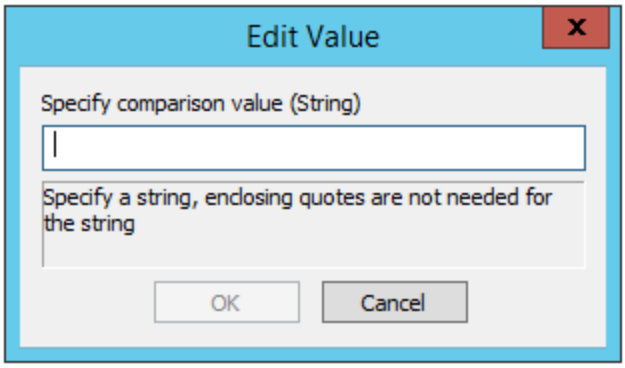
  By default, IP Access-related Event Rules are limited to 1000 rules.

  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. Click **[ip mask]** to open the **Edit Value** dialog box.



  4. 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]**.
- **If Account Locked Out**—the user is or is not locked out
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify **does/does not** equal to **[yes/no]**.
- **If Partner Id** - trigger the rule based on the user's Partner ID
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify that the Partner ID **does/does not/ is equal to/ less than/ less than or equal to/ greater than/ greater than or equal to [specific word]**.
- **If Custom Field [1/2/3]**—if user account has information in Custom Field 1, 2, or 3
  1. Add the Condition to the Event Rule.
  2. In the Rule Builder, click the linked text to specify whether the Custom Field **does/does not equal/contain [string]**.
  3. Click linked text to open the **Edit Value** dialog box.

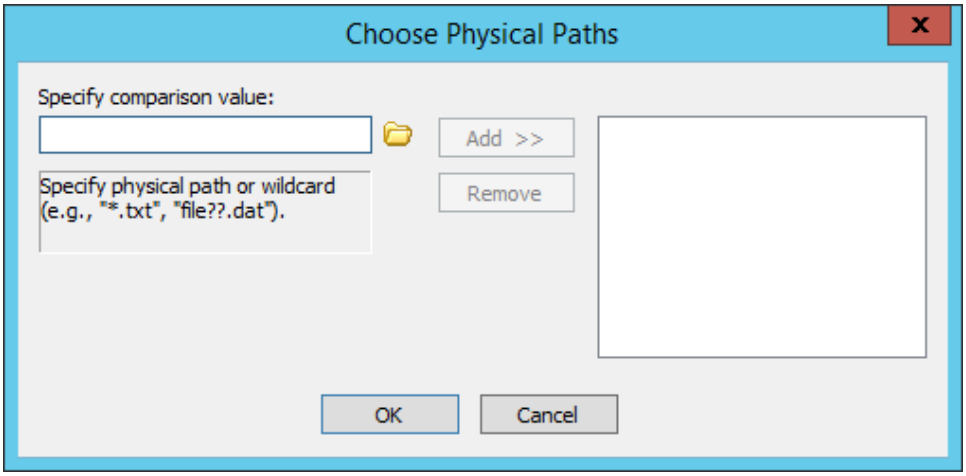


4. In the **Edit Value** dialog box, specify a string, and then click **OK**.

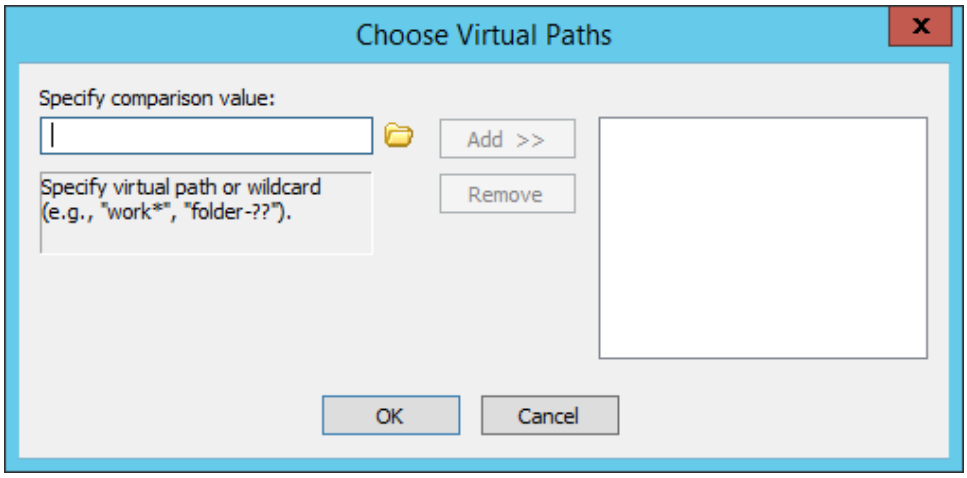
Workspaces Conditions

You can apply these Conditions to File Uploaded events.

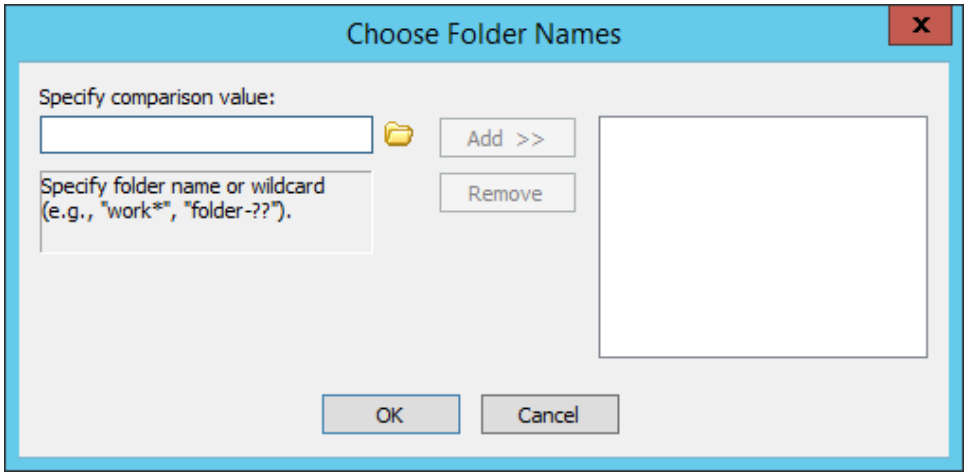
- **If Workspace Physical Path** - Tests whether the physical path does or does not match a path mask. Wildcards can be used.



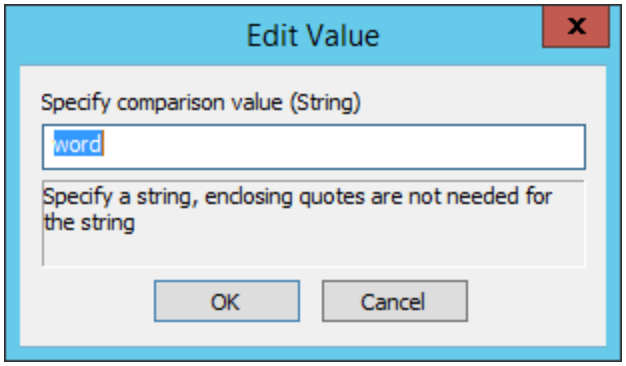
- **If Workspace Virtual Path** - Tests whether the virtual path does or does not match a path mask. Wildcards can be used.



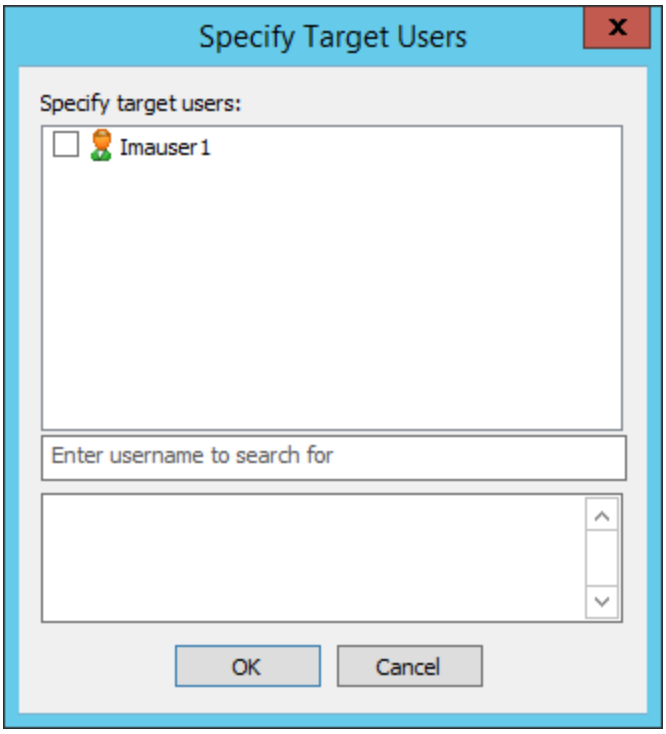
- **If Workspace Name** - Tests whether the folder name does or does not match a mask. Wildcards can be used.



- **If Workspace Participants List** - Tests whether the participant list does or does not contain a string specified.



- **If Workspace Owner** - Tests whether the Workspace Owner is or is not one of a list of specified users.



- **If Workspace Owner Email Address** - Tests whether the Workspaces Owner email address does or does not contain or is equal to a specified string.