

Managing EFT™ Email Notifications

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Enterprise 6.0 and later

DISCUSSION

EFT provides the ability to take a number of actions as part of its Event Rule automated process capabilities. One of the most common actions to take in reaction to many stimuli is to send an email to a person or a group to alert them of the occurrence. Sometimes this may be to notify an interested employee of a file uploaded by a client, or maybe it will indicate that a step in a process has failed. In new implementations, it's often seen as desirable to send an email when an automated process completes successfully. In this article we will take a look at managing your address book, sending failure emails, sending success emails, and sending emails back to connected clients.

ADDRESS BOOK

EFT has a built-in address book capability. By default the address book is empty, but clicking the To, CC, or BCC buttons in any email notification will bring up the addresses associated with the users on that site, along with a search field, allowing you to quickly pinpoint the desired recipients. However, it's very common that email notifications will primarily be sent to a person or several persons or even a distribution group email address, for the purpose of notifying the appropriate EFT administrative personnel of a success or failure. As such, EFT will automatically fill in any new email notification action recipients with whatever addresses you define in the Address Book.

With your Server selected in administration interface, selecting the **SMTP** tab on the right will present you with the ability to add contacts to your Address Book. The first one you add will be automatically populated as the "To" recipient in any new email notifications. Any additional contacts in the Address Book will be automatically populated as "CC" recipients in any new email notifications. Existing email notifications will remain as they were already configured, so that any changes you make to the Address Book will only be reflected in email notification actions added after the change is made.

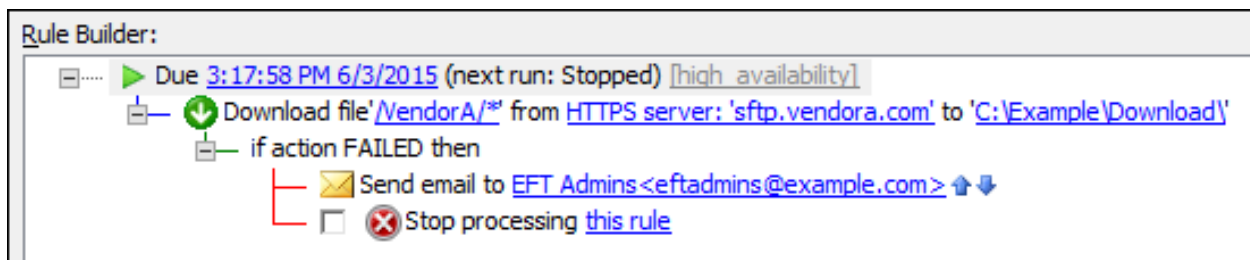
As a simple test, add two or three different contacts to the Address Book, apply your changes, and then add a new "Send notification email" action to an Event Rule. You will see that the email will be sent to the first contact in the Address Book, while additional contacts will be CC'ed.

Managing EFT™ Email Notifications

NOTIFYING ON FAILURE

When configuring an Event Rule to perform actions, it is often desirable to send a notification email to alert the appropriate parties if some action in that Event Rule fails to execute successfully. Generally the appropriate parties will be the EFT administrators, who may then investigate further.

For example, let's say that we need to download some files from VendorA who hosts a remote SFTP server, in which case we simply add and configure the Download action. However, if that download fails for some reason, we want to notify a distribution group, "EFT Admins," that the failure occurred. To do so, simply expand the "if action FAILED then" child of the Download action, add a new "Send notification email" action, and configure the email recipients and contents as desired. When completed, the only time that notification email will be sent is when that Download action fails.



NOTIFYING ON SUCCESS

While notifying on failure is straightforward, notifying on success requires more attention to be paid to the logic of your Event Rule. Technically speaking, there is no such thing as a "Send success email notification" action, only sending an email. The circumstances under which an email notification is sent depends entirely on how you configure your Event Rule.

Take the above example of sending a notification email when the Download action fails. If you then simply add another email notification as the next action in the Event Rule and consider it a "success message" you will find that if the Download action fails, you will actually get both emails, the failure notification as well as the success message. **That's because you did not tell EFT to stop processing the rule if the Download action failed.** Only by selecting the check box to stop processing the rule when that action failed can you rely on subsequent actions being taken only when the prior action succeeded.

Managing EFT™ Email Notifications

Therefore, only if you enable the option to stop processing the rule when an action fails can you then consider a subsequent email notification to be a success message. Below is an example of a properly configured success message, with the "Stop processing this rule" check box selected.



In this event rule, at 3:17:58 PM on 6/3/2015, you want to download a file via HTTPS from sftp.vendora.com to EFT's hard drive at C:\Example\Download\.

- If the action FAILS, then you want EFT to send an email to the EFT admins and stop processing that rule.
- If the action does not fail, you want to send an email to EFT Admins.

You will need to edit the bodies of the emails to reflect success/failure of the action. The default content for the email is similar to the following, which simply tells you that the event was triggered:

This message was sent to you automatically by Globalscape EFT Server on the following event: Scheduler (Timer) Event.

Server Local Time: 06 Nov 15 13:31:21

SENDING EMAILS TO CONNECTED CLIENTS

Whether sending failure notifications or success messages, if an Event Rule is reacting to actions taken by a client, it may be appropriate to include the client as a recipient in a notification email or otherwise create a new and separate notification email to be sent to the client. You can use the %USER.EMAIL% context variable in the "To" field of an email notification, as long as it is an Event type that involves a connected client triggering it, such as a file being uploaded or a login attempt failing. This does not apply to Scheduler (Timer)

Managing EFT™ Email Notifications

Event and Folder Monitor events. The account being used by the connected client must have an email address populated in the account's properties.

For example, let's say that an automated process at VendorA will occasionally upload an encrypted file that we must decrypt before sending along to a downstream application server. We can easily create an "On File Uploaded" Rule with the proper conditions to react to that specific scenario by decrypting the file and sending along the resulting decrypted file to the application server. However, what happens if the decryption fails? We certainly don't want to send bad data along to the application server, and we want to notify the EFT administrators that the failure has occurred. We may also want to notify our contact at VendorA that the decryption failed. This is especially relevant because nearly every time any decryption fails, it's because the file was encrypted with the wrong public key, and EFT can't fix that. Instead, the sender must go back and encrypt the file with the correct public key, then upload the new, correctly encrypted file.

To address this scenario, in our "On File Uploaded" Rule, we will ensure that the "Stop processing this rule" check box is selected under the Decrypt action, and add an email notification to the EFT admins team about the failure. We will also add a "Send notification email" Action to the email address associated with the account that performed the upload of the file that failed to decrypt by adding the %USER.EMAIL% variable to the "To" field of the email.

E-mail Notification Message

To...: %USER.EMAIL%;

Cc...:

Bcc...:

Subject: File failed to decrypt: %FS.FILE_NAME%

Message: This is an automated emssage from your friends at Example, Inc.

A file %FS.FILE_NAME% was uploaded to us at sftp.example.com with the account %USER.LOGIN%, but we were not able to decrypt the file. This is most often due to the file being encrypted with a different public PGP key than the one originally provided by Example, Inc.

Please double check and either run the procedure again to encrypt the file with the correct key and upload the results or contact us if you believe you have received this message in error.

EFT Admins at Example, Inc.
John Doe, Senior Partner Support Admin

Variables:

Logon Name	%USER.LOGIN%
Logon Password	%USER.PASSWORD%
Account Enabled	%USER.ENABLED%
Settings Template	%USER.SETTINGS_LEVEL%
Full Name	%USER.FULL_NAME%
Description	%USER.DESRIPTION%

☐ Send copy to user associated with this event (if applicable) ☒ Override 'From:' field: John Doe <john.doe@example.com>

OK Cancel

Managing EFT™ Email Notifications

Note that in this example, the "From" field has been modified from the global default provided in the **SMTP** tab to instead reflect the email address of a particular employee responsible for supporting the relationship with the vendor when technical issues arise. This is not required but is a helpful and professional touch that makes replying to the email easy.

Additionally, note that you do have the option to simply send a copy of the email to the user that triggered this event. This is possible for any Event type where a connected client is involved in triggering the Event Rule and where the account used has its email address field populated. However, it may not be desirable to copy an external party or internal business user on a failure notification email sent to technical internal staff. Those emails will tend to be utilitarian and to the point, they may contain physical pathing and other information not appropriate or relevant to share outside the internal technical staff, and they rarely will contain clear and professionally worded instructions on how to react to the notification or address the issue. Generally, such messages are simply not intended or formulated for external or business user consumption. And since sending failure notifications to external parties or internal business users tends to be an exception case, it's often better to simply add and configure a separate email notification when called for.

GlobalSCAPE Knowledge Base

<https://kb.globalscape.com/Knowledgebase/11244/Managing-EFT™-Email-Notifica...>