ENABLE OR DISABLE EVENT RULES SELECTIVELY

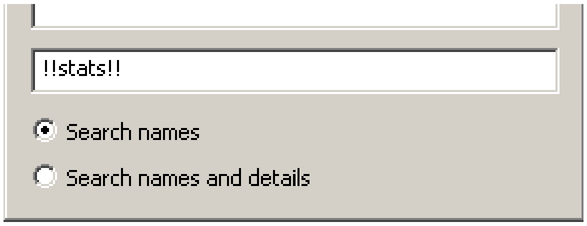
Use the migration tool to Enable Event Rules?

Abstract

If you have numerous Event Rules, like most customers, enabling them one at a time is rather difficult. This document will show you how to enable them by groups based on the name of the Event Rule.

Find a count of your Automation Rules

1. Login to your EFT system and press CTRL+F. In the search box, type !!STATS!!

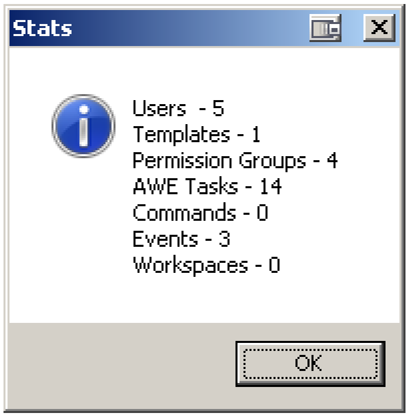


!!stats!!

● Search names

○ Search names and details

EFT will display how many Event Rules you have, in addition to other statistics.



Users - 5
Templates - 1
Permission Groups - 4
AWE Tasks - 14
Commands - 0
Events - 3
Workspaces - 0

This gives you the total number of Users, Templates, Permission Groups, AWE Tasks, Commands, Events and Workspaces (Workspaces is available on 7.1 or higher).

**Note: The option must be run on each individual Site that is created on the EFT server.

Working Smarter with the Migration tool

If you have several hundred—or several thousand—Event Rules, an EFT admin knows how hard it is to disable or enable a group or a mass number of Event Rules. In this document, you will learn how to enable or disable Event Rules without have to actually login through the EFT client.

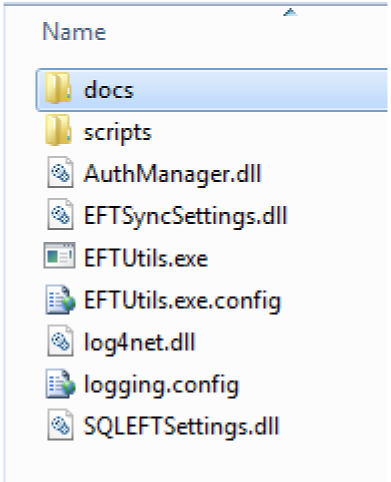
This does not require RDP access, however this will require:

1. Migration tool (that matches the EFT version)
2. EFT Admin Interface (the same version installed on the server to which you want to connect) on either a workstation or a server.

It is also recommend that some experience or training has been done with the Migration tool, however it is not required as this is a simple process. The Tool Set was creating to make EFT administration simple and easy for the team.

Configuring the Migration Tool

1. Unzip the correct build for the Migration Tool. The extracted files should be similar to the following:

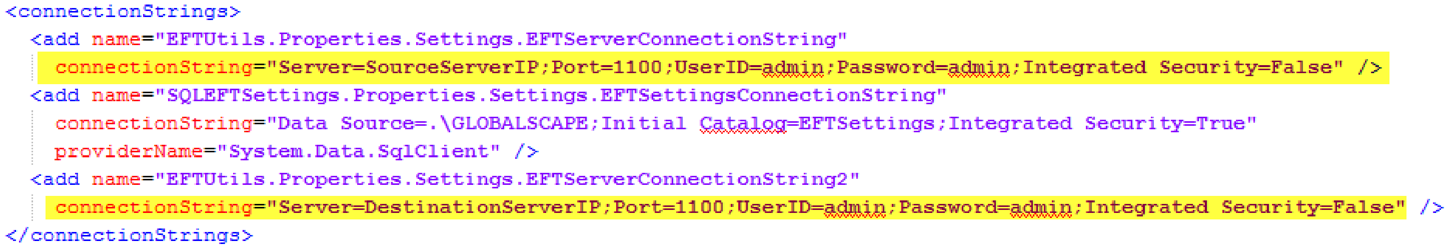


```
Name
docs
scripts
AuthManager.dll
EFTSyncSettings.dll
EFTUtils.exe
EFTUtils.exe.config
log4net.dll
logging.config
SQLEFTSettings.dll
```

2. Editing the configuration file for the Migration Tool involves the *EFTutils.config* using NotePad or a preferred editor.

3. Edit lines 15 and 20

    a. These are connection strings from a source (line 15) to a destination (line 20)



```
<connectionStrings>
  <add name="EFTUtils.Properties.Settings.EFTServerConnectionString"
    connectionString="Server=SourceServerIP;Port=1100;UserID=admin;Password=admin;Integrated Security=False" />
  <add name="SQLEFTSettings.Properties.Settings.EFTSettingsConnectionString"
    connectionString="Data Source=.\GLOBALSCAPE;Initial Catalog=EFTSettings;Integrated Security=True"
    providerName="System.Data.SqlClient" />
  <add name="EFTUtils.Properties.Settings.EFTServerConnectionString2"
    connectionString="Server=DestinationServerIP;Port=1100;UserID=admin;Password=admin;Integrated Security=False" />
</connectionStrings>
```

Please Note: You are doing an initial sync from a working environment into the new EFT HA configuration system. Effectively, this Node1 of this EFT HA will be identically like that of Production! Event Rules may need to be disabled as this could trigger if the Event Rules were accessing the same shares.

4. Additional information editing the configuration:

   a) Edit Lines 46

   b) This controls how the system will export the information from EFT:

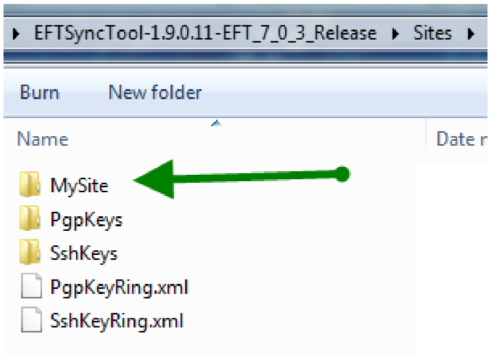
   Below is the original setting. This exports everything to smaller files in the root of the Migration tool tool directory. (Useful if the customer has only 1 Site.) This is the default setting.

```
<setting name="XMLOutput" serializeAs="String">
  <value>Exported_EFT_Settings_{0}.xml</value>
</setting>
```

If you have more than one Site, it is recommended that you use a "path" in the configuration. This allows you to export to a \Sites\MySite\

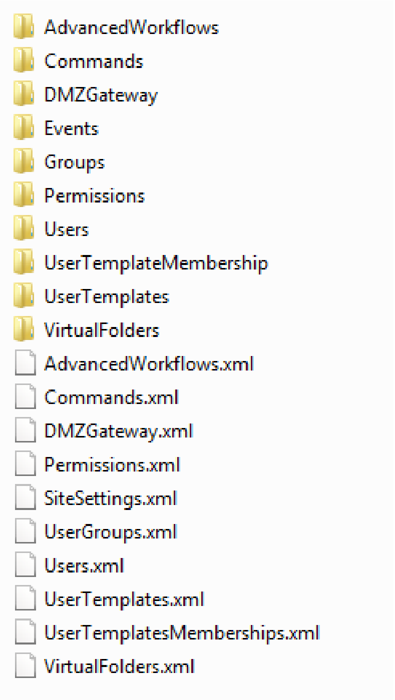
```
<setting name="XMLOutput" serializeAs="String">
  <value>D:\Download\EFTSyncTool-1.9.0.11-EFT_7_0_3_Release\Sites\</value>
</setting>
```

Here is an example of what the directory creates:



MySite
PgpKeys
SshKeys
PgpKeyRing.xml
SshKeyRing.xml

Inside of this directory is the newly export configuration



AdvancedWorkflows
Commands
DMZGateway
Events
Groups
Permissions
Users
UserTemplateMembership
UserTemplates
VirtualFolders
AdvancedWorkflows.xml
Commands.xml
DMZGateway.xml
Permissions.xml
SiteSettings.xml
UserGroups.xml
Users.xml
UserTemplates.xml
UserTemplatesMemberships.xml
VirtualFolders.xml

So it is possible to export each Site into its Site directory so that each can be reconfigured.

*****WARNING** – if you do not do the export to a directory as this suggests, you will have to copy the XML from the root of the Migration tool directory BEFORE you export a different Site as the names of the files are reused and you could potentially over write the existing export from the other Site.*

Creating Event Rule List using Directory Listing

You can create an Event Rule list by using CMD.exe with the following command:

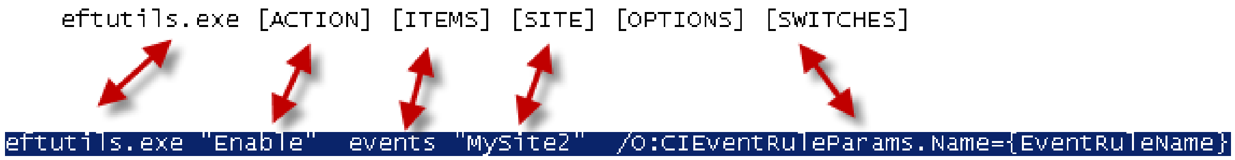
```
dir /b >print.txt
```

For Power shell users:

```
Get-ChildItem d:\ -name >DirectoryList.log
```

The Enabling or Disabling script

The script to enable or disable Event Rules via COM API using EFT Sync is easy. Let us review the common usage of the command line perimeters.



```
eftutils.exe [ACTION] [ITEMS] [SITE] [OPTIONS] [SWITCHES]
```

```
eftutils.exe "Enable"  events "MySite2"  /O:CIEventRuleParams.Name={EventRuleName}
```

Some typical commands that may be used:

1. Disabling 1 event rule at a time:

```
eftutils.exe "Disable"  events "MySite2"  /O:CIEventRuleParams.Name={EventRuleName}
```

2. Enable 1 event rule at a time:

```
eftutils.exe "Enable"  events "MySite2"  /O:CIEventRuleParams.Name={EventRuleName}
```

3. Enable all Event Rules in 1 sweep:

```
eftutils.exe Enable events "MySite2" /all
```

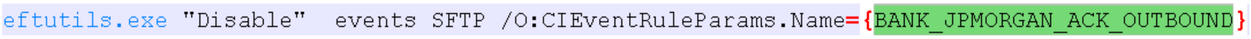
4. Enable all Event Rules in 1 sweep:

```
eftutils.exe Disable events "MySite2" /all
```

The script should now look like:

```
REM ** Go Live 5/16 Event Rules
REM
eftutils.exe "Enable"  events SFTP /O:CIEventRuleParams.Name={BANK_JPMORGAN_ACK_OUTBOUND}
eftutils.exe "Enable"  events SFTP /O:CIEventRuleParams.Name={BANK_JPMORGAN_ACH_INBOUND }
eftutils.exe "Enable"  events SFTP /O:CIEventRuleParams.Name={BANK_GFF_TREASURY }
eftutils.exe "Enable"  events SFTP /O:CIEventRuleParams.Name={BANK_JPMORGAN_OUTBOUND}
```

The most important part of this is the actual single line that enables or disables:



```
eftutils.exe "Disable"  events SFTP /O:CIEventRuleParams.Name={BANK_JPMORGAN_ACK_OUTBOUND}
```

Simply changing the EVENT RULE name is all that is required to reuse this line.

This script helps allow scripts to be imported using EFT Sync (see other documentation on how to promote code from QA to Production) and enabled in a block process via COM API.

Enabling Event Rules makes it easier to verify the names of the Event Rules, which are displayed in reports, logs, and so on.