

## Learn Powershell | Achieve More

What is this Powershell of which you speak?

## Introducing PoshEventUI: A UI Way to Create Permanent WMI Events

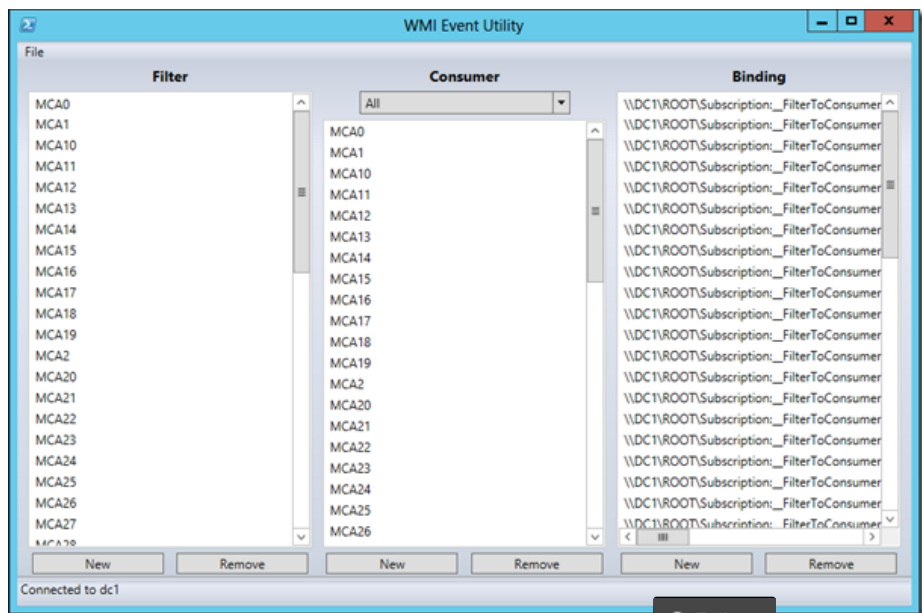
Posted on [August 16, 2013](#)

Something that I have been working on the past couple of months (in between other things) was a UI approach to creating permanent WMI events vs. a command line approach.

I really had only a few requirements that I wanted to achieve with this:

- Have a main window showing the current WMI events
- Have Add/Remove buttons for each instance (Filter, Consumer and Binding)
- Use separate windows for each instance
  - The Consumer window will have one window but will change based on the type of Consumer being created

So without further ado, here is my latest project: **PoshEventUI**



The main UI window is based on <http://powershell.codeplex.com/> and the `WmiEventHelper.exe` available from <http://powershell.codeplex.com/>

The download for this is at <https://www.powershellgallery.com/packages/PoshEventUI/0.9.0>

Once you download it, unblock the file by running `Unblock-File .\PoshEventUI_0.9.0.zip` in a PowerShell prompt. The `Unblock-File` works by removing the 'Zone.Identifier' file from the file.

```
PS C:\Users\Administrator\Desktop> Unblock-File .\PoshEventUI_0.9.0.zip
VERBOSE: Performing operation "Unblock-File" on Target "PoshEventUI_0.9.0.zip".
PS C:\Users\Administrator\Desktop>
```

Follow "Learn Powershell | Achieve More"

Get every new post delivered to your Inbox.

Join 168 other followers

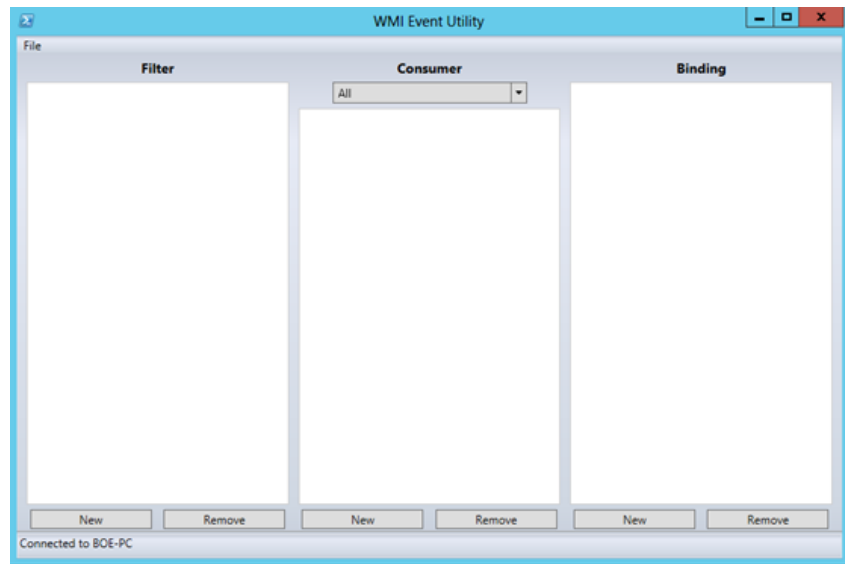
Sign me up

Powered by WordPress.com

Navigate through the unzipped folder and run `.\wmieventutility.ps1`

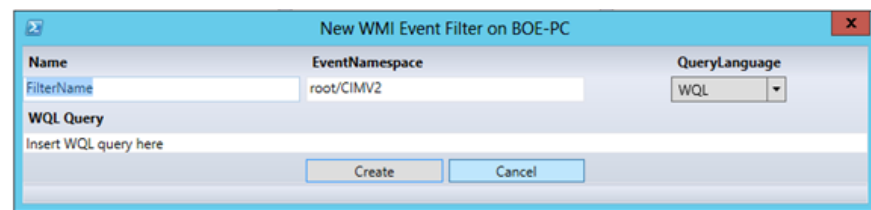
```
PS C:\Users\Administrator\Desktop\PoshEventUI_0_9> .\WMIEventUtility.ps1
```

Once the window has been opened, you can choose to create a **New** instance or to **Remove** an instance.

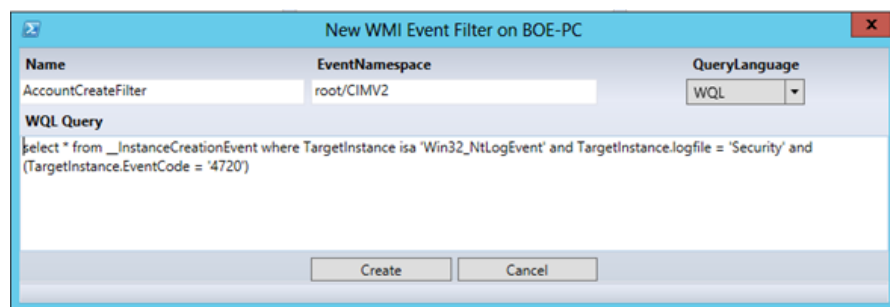


Let's work through each of these just to get an idea on what you can do.

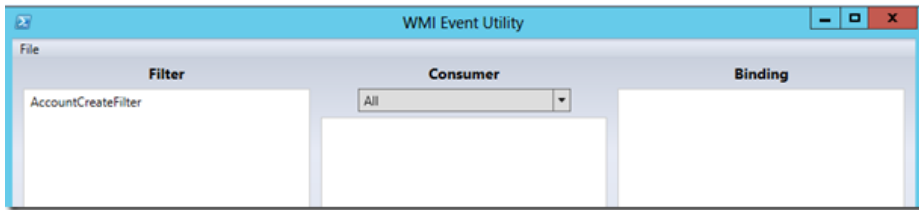
First off is the **Filter**.



Here you can specify a **Name** and a **WQL Query** that will be used to monitor for a specific event in WMI. You can look at my articles on [Temporary Events](#) and [Permanent Events](#) for ideas or look at [some searches on your favorite search engine](#). Also available is some great information in the PowerEvents documentation that shows more on working with WQL queries and also provides some great examples.

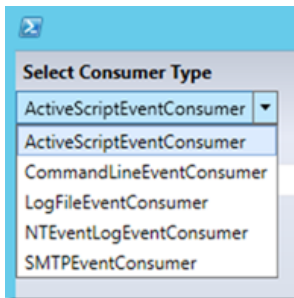


Once completed, click **Create** and it will now be added to the WMI repository.

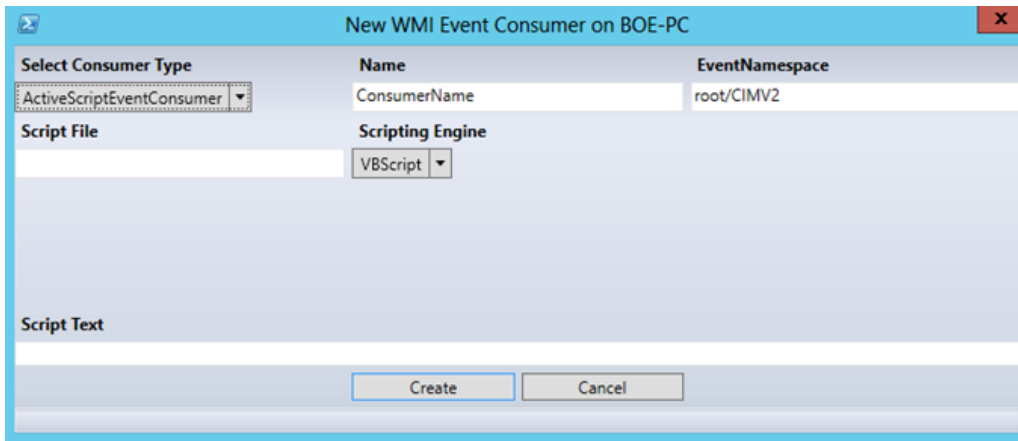


Next up is the **Consumer** creation. There are 5 possible consumers to choose from and you can have multiple consumers setup with a filter via the Binding, so use whatever you wish to accomplish your requirement.

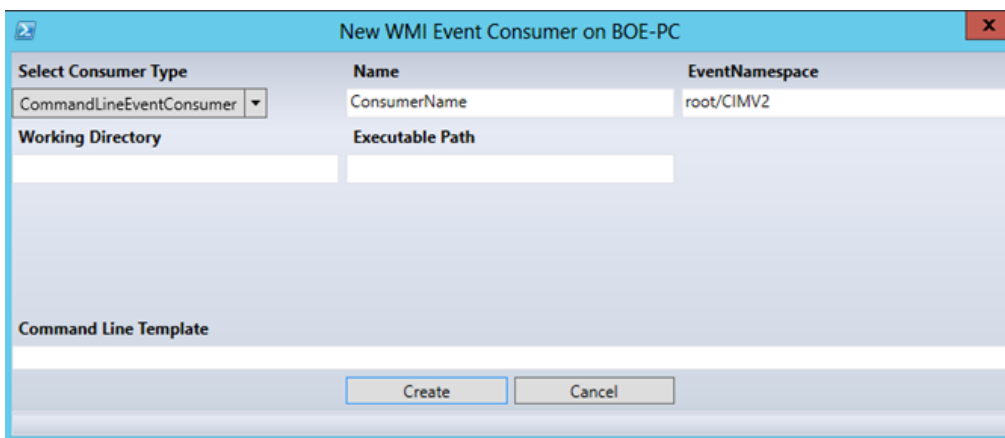
Lets look at all of the possible Consumer choices. You can pick whichever consumer you prefer from the drop down menu in the upper left hand corner labeled **Select Consumer Type**.



### ActiveScriptEventConsumer



### CommandLineEventConsumer



## LogFileEventConsumer

The screenshot shows a Windows-style dialog box titled "New WMI Event Consumer on BOE-PC". It has a light blue header bar with a close button (X) in the top right corner. The dialog is divided into several sections. At the top, there are three columns: "Select Consumer Type" with a dropdown menu showing "LogFileEventConsumer", "Name" with a text box containing "ConsumerName", and "EventNamespace" with a text box containing "root/CIMV2". Below these, there are three more columns: "File Name" with an empty text box, "Maximum File Size (0 - 65535)" with an empty text box, and "Encoding" with a checkbox labeled "IsUnicode". At the bottom left, there is a section labeled "File Text" with a large empty text area. At the bottom right, there are two buttons: "Create" and "Cancel".

## NTEventLogEventConsumer

The screenshot shows a Windows-style dialog box titled "New WMI Event Consumer on BOE-PC". It has a light blue header bar with a close button (X) in the top right corner. The dialog is divided into several sections. At the top, there are three columns: "Select Consumer Type" with a dropdown menu showing "NTEventLogEventConsumer", "Name" with a text box containing "ConsumerName", and "EventNamespace" with a text box containing "root/CIMV2". Below these, there are three more columns: "Source" with an empty text box, "Event ID" with an empty text box, and "Category" with an empty text box. Below these, there are three more columns: "UNC Server Name" with an empty text box, "Event Type" with a dropdown menu showing "Success", and "Category" with an empty text box. At the bottom left, there is a section labeled "Insertion String Templates" with a large empty text area. At the bottom right, there are two buttons: "Create" and "Cancel".

## SMTPEventConsumer

The screenshot shows a Windows-style dialog box titled "New WMI Event Consumer on BOE-PC". It has a light blue header bar with a close button (X) in the top right corner. The dialog is divided into several sections. At the top, there are three columns: "Select Consumer Type" with a dropdown menu showing "SMTPEventConsumer", "Name" with a text box containing "ConsumerName", and "EventNamespace" with a text box containing "root/CIMV2". Below these, there are three more columns: "To" with an empty text box, "From" with an empty text box, and "Subject" with an empty text box. Below these, there are three more columns: "Cc" with an empty text box, "Bcc" with an empty text box, and "Reply To Line" with an empty text box. Below these, there are two columns: "SMTPServer" with an empty text box and "HeaderFields (separate by ',' or ';') with an empty text box. At the bottom left, there is a section labeled "Message" with a large empty text area. At the bottom right, there are two buttons: "Create" and "Cancel".

In this case I am going with an SMTP consumer.

The dialog box is titled "New WMI Event Consumer on BOE-PC". It contains the following fields:

Select Consumer Type	Name	EventNamespace
SMTPEventConsumer	AccountCreateSMTPConsumer	root/CIMV2

To	From	Subject
SystemAdministrator@domain.com		New Account Created

Cc	Bcc	Reply To Line

SMTPServer: smtpserver.domain.com

HeaderFields (separate by ',' or ';'):

Message: A new account was created! Please review the following information below:  
%TargetInstance.%

Buttons: Create, Cancel

Note that with the **From** field blank, it will default to [WMI@<computername>.com](mailto:WMI@<computername>.com) for the address.

Once you have the picked out your consumer and entered the necessary information, click **Create** and you will be taken back to the main window with the new consumer listed.

The main window is titled "WMI Event Utility". It has three sections:

- Filter:** AccountCreateFilter
- Consumer:** All (dropdown menu), AccountCreateSMTPConsumer (list)
- Binding:** (empty)

You can event filter the Consumers based on the type using the drop-down menu.

The dropdown menu is titled "Consumer" and shows the following options:

- All
- ActiveScriptEventConsumer
- CommandLineEventConsumer
- LogFileEventConsumer
- NTEventLogEventConsumer
- SMTPEventConsumer

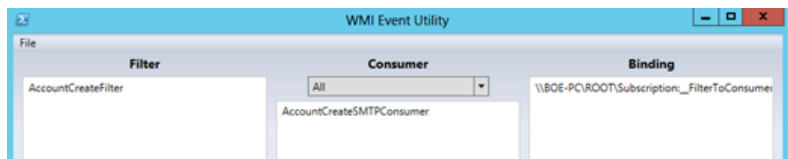
Last on the list is to bind these together using the **Binding**.

The dialog box is titled "New WMI Event Consumer Binding on BOE-PC". It contains the following fields:

Filter	Consumer
AccountCreateFilter	AccountCreateSMTPConsumer

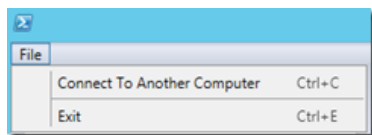
Buttons: Create, Cancel

Not really a lot to it. You pick the Filter and Consumer and click **Create**. This will create the binding and enable the WMI event subscription.

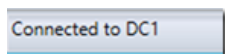
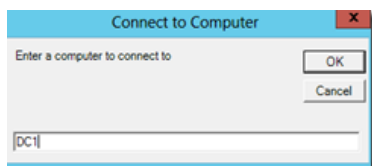


That is really all there is to it! The trick is really knowing the WQL query for the Filter and then determining what kind of consumer fits this best.

Almost forgot... You can even connect to remote systems to add and remove event subscriptions! Just click on the File menu and select **Connect to Another Computer**.



Enter a computername and click **OK** and away you go.



Please keep this mind that it is in **Beta**, so there will most likely be bugs crawling around. Just stop by the [Issues page](#) and let me know what they are and I will work to get rid of them. I do have plans for a Template feature which will have pre-determined Filters as well as the option to save custom filters as templates for use later. This may also move over to the Consumers as well at a later date.

Hope everyone enjoys this!

[About these ads](#)

#### Share this:



Be the first to like this.

#### Related

[PowerShell and Events: Permanent WMI Event Subscriptions](#)  
In "powershell"

[PowerShell and Events: WMI Temporary Event Subscriptions](#)  
In "powershell"

[PowerShell Profile Removal GUI](#)  
In "powershell"

**About Boe Prox**

Microsoft PowerShell MVP working as a Senior Systems Administrator

[View all posts by Boe Prox →](#)

This entry was posted in [GUI](#), [powershell](#), [WPF](#) and tagged [eventing](#), [permanent events](#), [PoshEventUI](#), [Powershell](#), [wmi](#). Bookmark the [permalink](#).

### 3 Responses to *Introducing PoshEventUI: A UI Way to Create Permanent WMI Events*

**Rodrigo says:**

September 17, 2013 at 9:14 am

Yeah, i think this idea very interesting for a new version. I will see this article for try create a consumer for multiples systems.  
tk

[Reply](#)**Rodrigo says:**

September 16, 2013 at 5:13 pm

Hi Boe Prox this project really helped me, but now i need create a permanent event to notify sql services to 70 servers, the issue is, i need create one by one or there a way for create to all servers together?

Tks,  
Rodrigo Figueiredo

[Reply](#)**Boe Prox says:**

September 16, 2013 at 9:31 pm

Glad you enjoy the utility! Currently I do not have a way to do a bulk creation against multiple systems. But this sounds like a nice feature request for a future update. I would recommend using PowerEvents  
<http://powerevents.codeplex.com> to script against for creation of a WMI event consumer.

[Reply](#)

---

**Learn Powershell | Achieve More**

The Twenty Ten Theme.  Create a free website or blog at WordPress.com.