

# Command Syntax Part 1

## Intro

Now we're gonna dive into Command Syntax. If you have never seen any of this before this could be one of the more challenging sections. What I mean is you may need to review this section or lectures more than once.

Let's go ahead and type **help get-eventlog -showwindow**, press return. Go ahead and click settings, now make sure all these check boxes are checked and click ok.

Go ahead scroll down to the SYNTAX section. You gonna use the syntax section of show-window. What I've done is copied the Syntax section into my scripting pane.

## Command Structure

**Every Cmdlet in PowerShell follows this basic structure**

**Verb-Noun -param1 <argument1> -param2 <arg2, arg3> separated by a comma.**

What are all these **brackets**, hyphens, angle brackets, braces **all about**? I've already **shown** you **what parameters are**. If you recall parameters always start with a **hyphen**. **Parameters** are **options** that **describe** what the cmdlet **will do**.

To make this a little easier to understand, its **lunchtime** here in America so I want you to think of any cmdlet, or in this example the **get-eventlog** cmdlet as a **pizza**. I know that sounds a little **crazy**, but bear with me. Now we all know that when you go to any pizza shop you can order **just cheese pizza** or you can order a bunch of **toppings**, like this.

It may be easier for you to understand it this way. Get-Eventlog is the plain pizza and the parameters are the toppings. Just remember that parameters always start with a hyphen, and you can add parameters to build functionality into your cmdlet.

Ok, now that we have a **good idea** how parameters are used. Let's **move on** to **parameter sets**.

## Parameter Sets:

If you see a command name **more than once**, that means that there'll be at least **one unique parameter** in each set.

Notice in the **first set** there are several **unique parameters** such as **-logname**, **-instanceId**, **-After**, **-Before**, **-Newest** and **several others**.

In the **second set** you have **-AsString** and **-List**.

Notice also the **-computername** is parameter listed in **both sets**. That means you can use the **-computername** parameter when **using either set**.

In our example **type get-eventlog -logname application**, we're using the **first parameter set**.

Now try and **use a parameter** from the **second set**. Click space, type dash.

**Try using -list-** You'll see -list is **not there**. If you **type -list** and press return. You'll get an **error**.

So, what I am showing you is that if you start using the parameters from **one set** you **can't jump over** and use parameters from the **other set**. Those parameters **won't work**.

### Arguments < >

The **angle brackets** indicate an **argument**. What's **inside** the angle brackets is called a **value type**.

In our **example** we **type get-eventlog**, space dash **logname**.

The logname parameter has a **value type** called **<string>** which can be an alpha-numeric value.

Press the **space bar** In this case it's a **text string** such as a single word like security or **application**, **press enter**.

### Multiple Arguments [ ]

Notice the parameter **-InstanceId** and the **argument** **<Int64 [ ]>** . int stands for integer. See the **two square brackets**?

Note the **square brackets** are **inside** the **angle brackets**.

This means that it can take **multiple arguments** separated by a **comma**.

Let's go ahead and add our new parameter.

**Space, hyphen**, now select **-instanceID** now **type 0,1**.

Now we'll explain it a little more. Our command is **get-eventlog**, our first parameter is **-logname**, the **angle brackets** indicate an **argument**. Inside the angle brackets is a **value type** and the **value type is string** which in this case is a text string. We chose the **application log**. The next parameter is **- InstanceID** which takes an **argument < >** the value type is **<Int64>** which refers to an **integer** or numeric. Again, notice that within the **angled brackets are two square brackets**. This means that **-instanceID** can take multiple arguments. In this case I'll type **0,1** separated by a **comma**. And now we can go ahead and **press return**. **We can see that the command did run**.

Note: **Not all** parameters **can take multiple arguments**, you will always want to check this.

For example, **type get-eventlog -logname security -newest 3,2** press return, and you get an error.

Checkout the syntax for the parameter **-newest**. It can take an **argument** but **not multiple arguments**. Notice there are **not two square brackets** within the **angle brackets**. This shows that -newest can only take a **single argument**.