* **BATCH ID: WiproNGA\_DWS\_B5\_25VID2550**
* **NAME:** Shrawani Shyam Balwadkar
* **RPS USER ID:** 34932
* **DATE**: 25-08-2025

**TOPIC:**

* **SCCM Powershell CMDLETS.**
* **Exploring CMTrace.**
* **SCCM Daily Maintenance Tasks.**
* **SCCM Report Creation.**
* **Create queries in configuration Manager.**
* **How to enable health attestation service communication on configuration manager client computers.**

**Brief Introduction to PowerShell**

**PowerShell is a cross-platform command-line shell and scripting language developed by Microsoft. It is built on the .NET framework and provides a powerful environment for automating administrative tasks, managing systems, and configuring various aspects of Windows, macOS, and Linux. Its core strength lies in its object-oriented nature, where commands (cmdlets) return objects rather than plain text, enabling more precise and flexible data manipulation.**

**Discovering Cmdlets**

**Cmdlets (pronounced "command-lets") are lightweight commands in PowerShell designed to perform specific functions. To discover cmdlets, the Get-Command cmdlet is used. This cmdlet can be used to find commands by name, type, or module. For example, to find all cmdlets related to services, one might use Get-Command \*Service\*.**

**Help File**

**The PowerShell Help system is accessed through the Get-Help cmdlet. This cmdlet provides detailed information about cmdlets, functions, scripts, and concepts. To get help for a specific cmdlet, use Get-Help &lt;CmdletName&gt;, such as Get-Help Get-Process. The help files explain the cmdlet's purpose, syntax, parameters, and provide examples of its usage. Get-Help can also be used to find conceptual help topics (e.g., Get-Help about\_Aliases). Help files can be updated using the Update-Help cmdlet.**

**Get-Member Cmdlet**

**The Get-Member cmdlet is crucial for understanding the properties and methods of objects returned by cmdlets. Since PowerShell returns objects, not just text, Get-Member allows users to inspect the structure of these objects. When a command's output is piped to Get-Member (e.g., Get-Process | Get-Member), it displays a list of all available properties (data associated with the object) and methods (actions that can be performed on the object) for that object type. This is invaluable for discovering how to interact with and manipulate the data returned by various PowerShell commands.**

Get started with Configuration Manager cmdlets

**Use Windows PowerShell to manage your Configuration Manager hierarchy. You can use PowerShell scripts to automate or extend Configuration Manager similar to other documented approaches using WMI and C#. For more information, see**[**Configuration Manager SDK**](https://learn.microsoft.com/en-us/mem/configmgr/develop/)**.**

**Run Configuration Manager cmdlets and scripts in PowerShell from the Configuration Manager console or from a Windows PowerShell session. When you run Configuration Manager cmdlets by using the Configuration Manager console, your session automatically runs in the context of the site.**

**Note**

**All currently supported versions of Configuration Manager current branch support Windows PowerShell version 5.1. If you've already installed PowerShell version 7, you can still use PowerShell version 5.1. For more information, see**[**Using PowerShell 7 side-by-side with Windows PowerShell 5.1**](https://learn.microsoft.com/en-us/powershell/scripting/install/migrating-from-windows-powershell-51-to-powershell-7#using-powershell-7-side-by-side-with-windows-powershell-51)**.**

**The Configuration Manager PowerShell cmdlet library supports PowerShell 7. For more information, see**[**Support for PowerShell version 7**](https://learn.microsoft.com/en-us/powershell/sccm/overview?view=sccm-ps&viewFallbackFrom=sccm-ps%27#support-for-powershell-version-7)**.**

**Starting in version 2103, the ConfigurationManager PowerShell module requires Microsoft .NET version 4.7.2 or later.**

**PowerShell from the Configuration Manager console**

**The easiest method to open PowerShell is directly from the Configuration Manager console.**

1. **Launch the Configuration Manager console. In the upper-left corner, there's a blue rectangle. Select the white arrow in the blue rectangle, and choose Connect via Windows PowerShell.**
2. **After Windows PowerShell loads, you'll see a prompt that contains your site code. For example, if the site code is "ABC", the prompt looks like: PS ABC:\>**
3. **To verify it works, use the Get-CMSite cmdlet. This cmdlet returns information about the Configuration Manager site you're currently connected to and any child sites. For example, the site server name, installation director, site name, and version.**

**Note**

**When you start PowerShell or the PowerShell ISE from the Configuration Manager console, it uses the AllSigned execution policy for the Process scope. If this default secure configuration is too much for your environment, there are two options to work around it:**

* **Change the execution policy with a command similar to the following example: Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope Process**
* [**Import the Configuration Manager PowerShell module**](https://learn.microsoft.com/en-us/powershell/sccm/overview?view=sccm-ps&viewFallbackFrom=sccm-ps%27#import-the-configuration-manager-powershell-module)**.**

**Import the Configuration Manager PowerShell module**

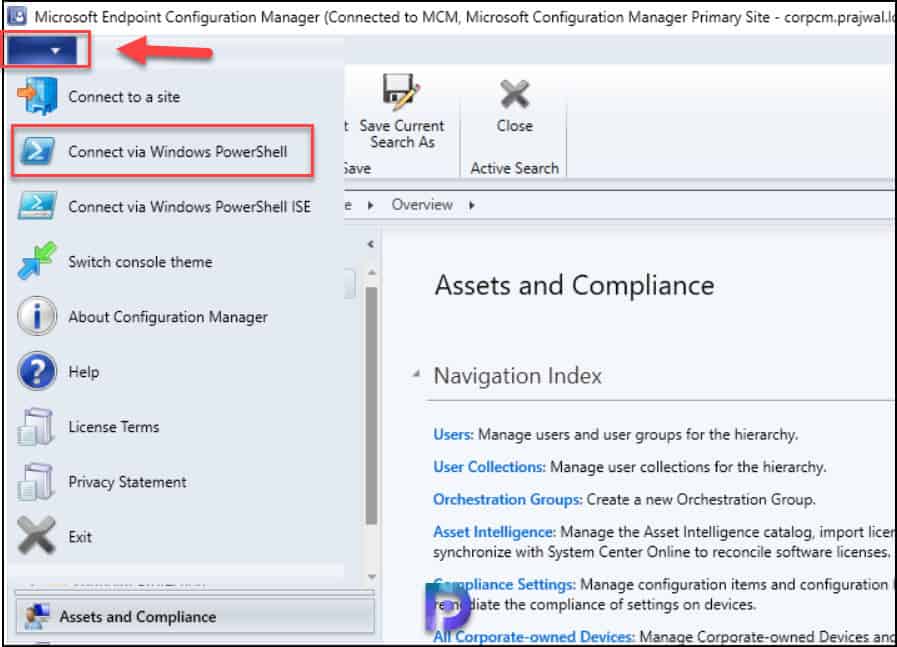
**Connect to Configuration Manager from an existing Windows PowerShell session by manually loading the Configuration Manager module.**

1. **Open a Windows PowerShell session from the Start menu.**
2. **Import the Configuration Manager module by using the Import-Module cmdlet. Specify the path to the Configuration Manager module, or change to the directory that contains the module. By default, the module is at the following path: C:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\bin\ConfigurationManager.psd1**

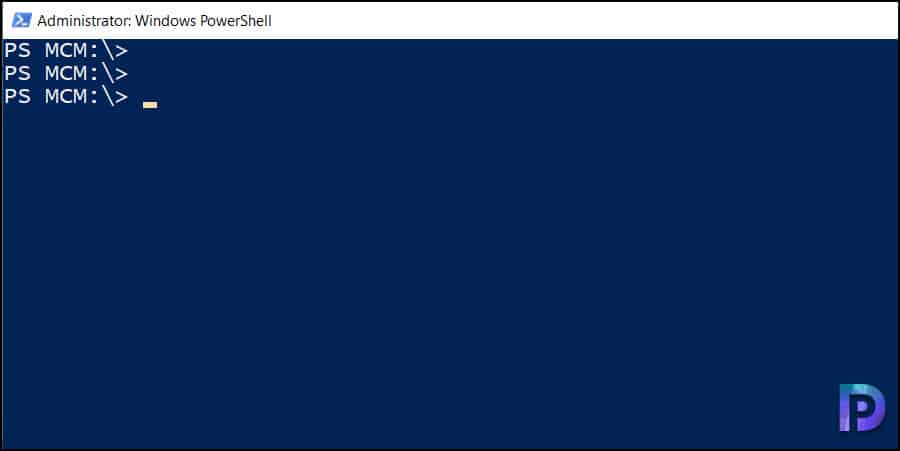
**How to Launch PowerShell from the ConfigMgr Console**

Perform the following steps to launch PowerShell from the SCCM console:

* Launch the Configuration Manager console.
* In the upper-left corner, there’s a blue rectangle. Select the white arrow in the blue rectangle, and choose **Connect via Windows PowerShell**.



After Windows PowerShell loads, you’ll see a prompt that contains your [site code](https://www.prajwaldesai.com/change-site-code-of-configuration-manager-client/). For example, if the site code is “**MCM**“, the prompt looks like: PS MCM:> This confirms that you have successfully launched the PowerShell from the SCCM console.



**Run Get-CMSite PowerShell Command**

To verify if you have successfully connected to PowerShell from the ConfigMgr console, run the Get-CMSite cmdlet. This cmdlet returns information about the Configuration Manager site you’re currently connected to and any child sites. For example, the site server name, SCCM build number, installation directory, site name, and version.

SmsProviderObjectPath       : SMS\_Site.SiteCode="MCM"

BuildNumber                 : 9096

ContentLibraryLocation      :

ContentLibraryMoveProgress  : 100

ContentLibraryStatus        : 3

Features                    : 0000000000000000000000000000000000000000000000000000000000000000

InstallDir                  : C:\Program Files\Microsoft Configuration Manager

Mode                        : 0

ReportingSiteCode           :

RequestedStatus             : 110

SecondarySiteCMUpdateStatus : 2

ServerName                  : corpcm.prajwal.local

SiteCode                    : MCM

SiteName                    : Microsoft Configuration Manager Primary Site

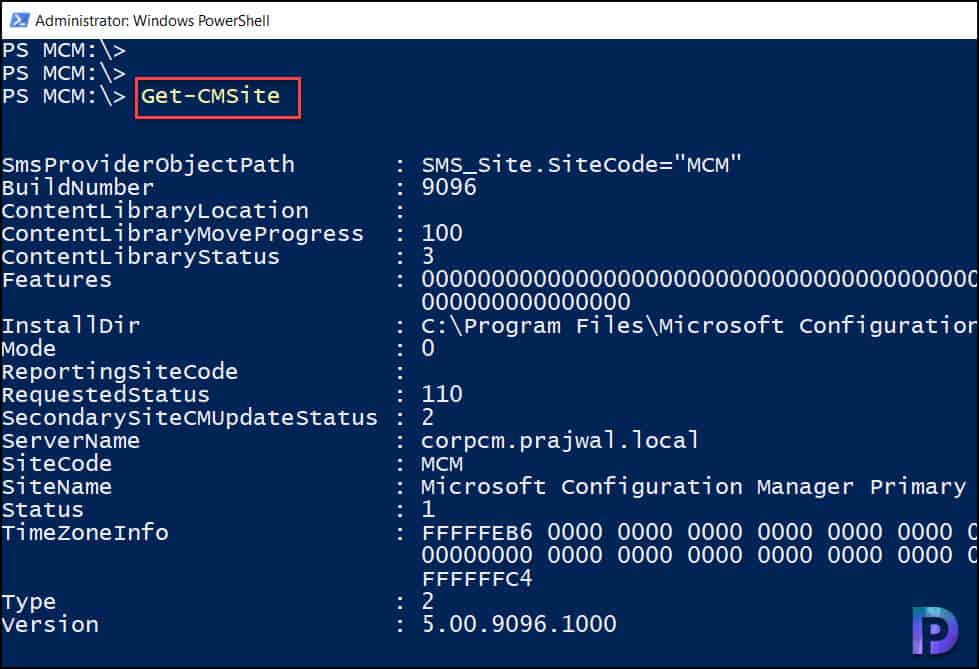
Status                      : 1

TimeZoneInfo                : FFFFFEB6 0000 0000 0000 0000 0000 0000 0000 0000 00000000 0000 0000 0000 0000 0000 0000

                              0000 0000 FFFFFFC4

Type                        : 2

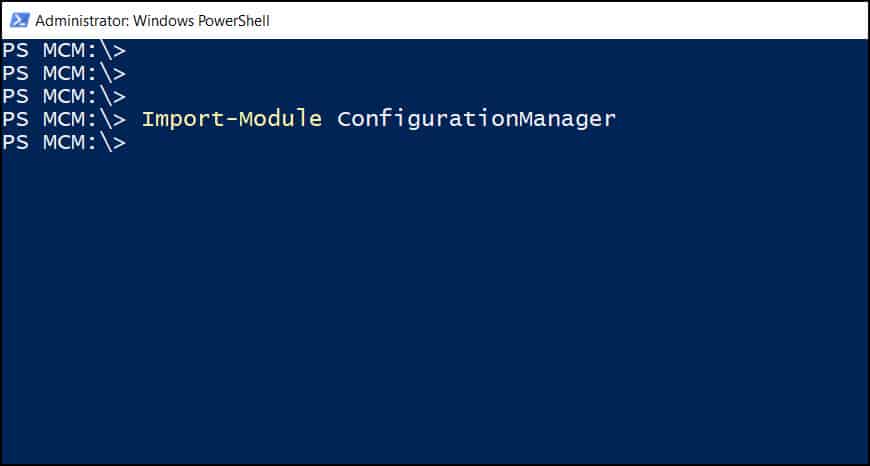
Version                     : 5.00.9096.1000



**Import the Configuration Manager PowerShell module**

You can connect to Configuration Manager from an existing Windows PowerShell session by manually loading the Configuration Manager module.

* Open a Windows PowerShell session from the Start menu.
* Import the Configuration Manager module by using the **Import-Module ConfigurationManager** cmdlet.



**Reviewing log files by using the Configuration Manager Trace tool**

* **Opening Log Files:**
  + Launch CMTrace.exe, typically found in %WinDir%\CCM on client machines or in the \SMSSetup\Tools folder of the Configuration Manager source media.
  + Use File &gt; Open to browse and select the desired .log or .lo\_ file.
  + Consider the "Ignore existing lines" option when opening for real-time troubleshooting, as it only displays new entries.
* **Real-time Monitoring:**
  + CMTrace automatically refreshes, displaying new log entries as they are written.
  + The "Pause" button can be used to temporarily stop automatic refreshing for detailed examination.
* **Filtering and Highlighting:**
  + Use the Filter option to narrow down log entries based on text, component, thread, or date and time, aiding in the identification of specific events or issues.
  + Highlighting functionality allows users to visually emphasize specific text within the log for easier tracking.
* **Error Lookup:**
  + The tool includes an error lookup feature that can help in understanding error codes encountered within the logs, providing context for troubleshooting.
* **Viewing Multiple Logs:**
  + Multiple log files can be opened simultaneously and arranged in various layouts (cascade, horizontal, vertical) for comparative analysis.
  + The "Merge" option allows combining multiple log files into a single view.

By utilizing these features, administrators can effectively review Configuration Manager log files for troubleshooting, monitoring, and understanding system behavior.

**What is CMTrace and What is it Used For? The Ultimate Guide**

CMTrace is a real-time log file viewer for Microsoft Configuration Manager (ConfigMgr). I originally wrote a blog post about CMTrace back in 2014, so I thought that it was time to update it with new information about running it you can learn from. In this post, I’ll tell you why I like using CMTrace because you may have noticed that I often refer to it when I need to review ConfigMgr log files. I’ll also tell you where you can find CMTrace and I’ll give you a couple of helpful tips on how to use CMTrace to its full potential!

**What Makes CMTrace a Must-Have Tool?**

There are numerous reasons to use this tool, but here are a few of my favorites:

-Log files can be reviewed in real time as they are updated, which can save you time.  
-Multiple log files can be merged together to be viewed as one file.  
-You can highlight text based on your own needs as you work through the logs. Don’t underestimate this feature.  
-Ability to look-up error codes.

**CMTrace Reads All ConfigMgr Log Files**

After working with ConfigMgr for a while you will realize that there are almost 200 different Configuration Manager log files. To help you understand what each log file does, the ConfigMgr documentation team listed and documented each one.

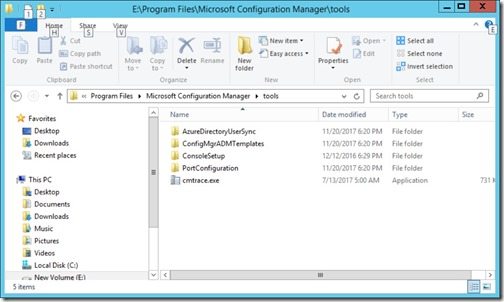
In order to open and view the complete list, here’s a link to the [documentation](https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/log-files). One of the things that you will notice on the update learning site, is that the logs are broken down by CM roles and functions. Making it easier for you to understand what logs to look at when troubleshooting an issue. This is particularly helpful when you are starting out with ConfigMgr.

Given that CMTrace can read each log file, I strongly encourage you to give CMTrace a try!

**Where Can I Find CMTrace?**

**ConfigMgr**

A while back the Microsoft Product team, included CMTrace as part of the CM client install. You no longer need to locate and install the Toolkit, just to find CMTrace. From a Run window type cmtrace and it should show up. If it doesn’t, you will find it under c:\windows\ccm\cmtrace.exe.

For completeness, the toolkit tools still exist and are now included in the installation of ConfigMgr. These tools, which include CMTrace, are updated as required with each cumulative update (CU).  
  
The toolkit is found under the Tools folder. In my case the path to cmtrace.exe is:  
E:\Program Files\Microsoft Configuration Manager\tools.  
  


Don’t worry. When you first try to access the Tools folder, you will receive the following message: You don’t currently have permission to access this folder. Simply click on the Continue button, adjust the folder permissions and grant yourself access to the folder.  
  


**Usage notes about CMTrace:**

A line highlighted in yellow generally indicates that there is a warning message, and a line highlighted in red generally indicates that there is an error message. BUT remember just because a line is highlighted in yellow or red doesn’t mean that it is a problem. You need to read the whole log file in context to determine if it is a problem.



For example, if you look at the purple arrow and noticed the red highlighted line, you will assume that the hardware inventory failed. But if you looked closely a few lines later you will see that the inventory was sent to your MP correctly. Context is important when reviewing the log files.

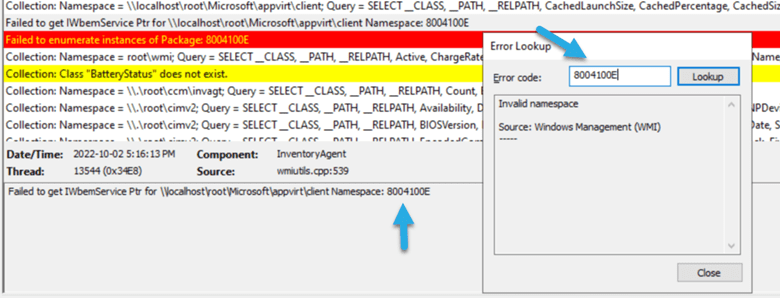
**Revolutionize your reporting.**

Access information not natively available in ConfigMgr and other ITSMs with Endpoint Insights.

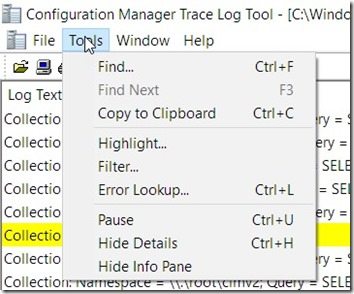
[LEARN MORE](https://www.recastsoftware.com/endpoint-insights/)

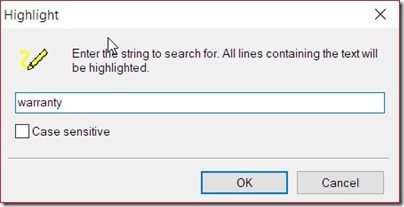
**Error Message Lookup**

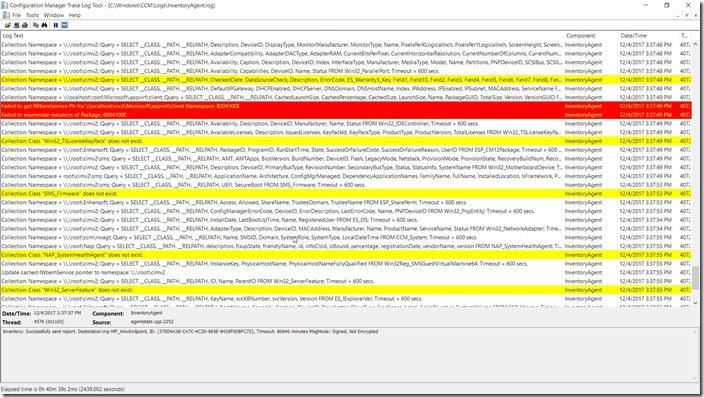
In CMTrace, using the log snippet below as an example, I copied the 8004100E error code and open Error Lookup window using the Ctrl-L command. Then pasted the error code before click Lookup button. From there I can see what this error message means in plain text. Thereby pointing me in the right direction. In this case I already know that App-V is not installed and therefore the WMI namespace doesn’t exist, so this error is to be expected. Which makes it not really an error.



**Highlight Lines**

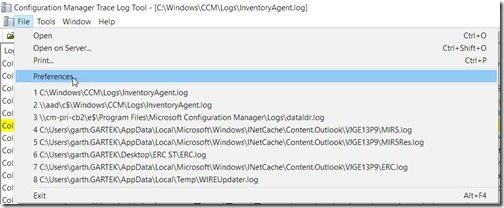
If you are troubleshooting something within the ConfigMgr logs it can be useful to highlight the item in order to see it happen in real-time.  
  


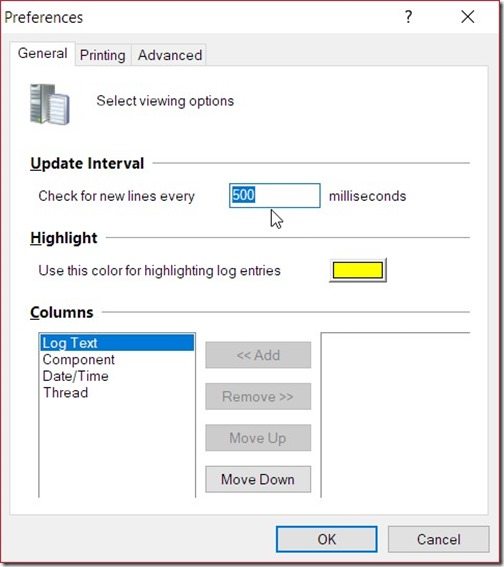
To do this within CMTrace, click on the Tools and Highlight… menu items.  
  


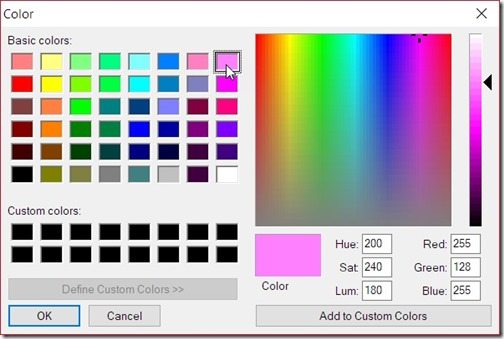
In the Highlight text box enter the text that you want to highlight and then click on the OK button.  
  


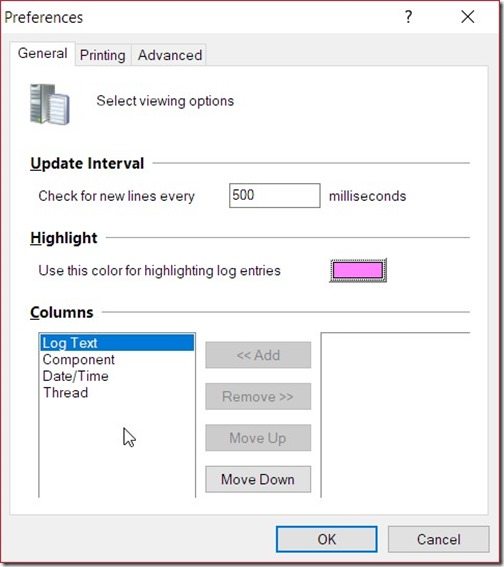
All instances of the text will be highlighted within the log file.  
  
By default, the highlighted text will be shown in yellow. Since this can lead to some confusion because warning messages are also in yellow, I recommend changing the color to something different. See my next section on how to do that.  
  
Without changing any of the colors, can you tell which one of the lines above has the highlighted text?

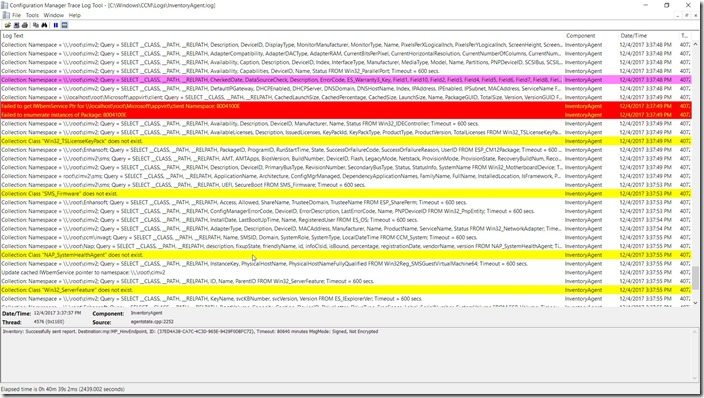
**Pink Highlighted Lines**

****

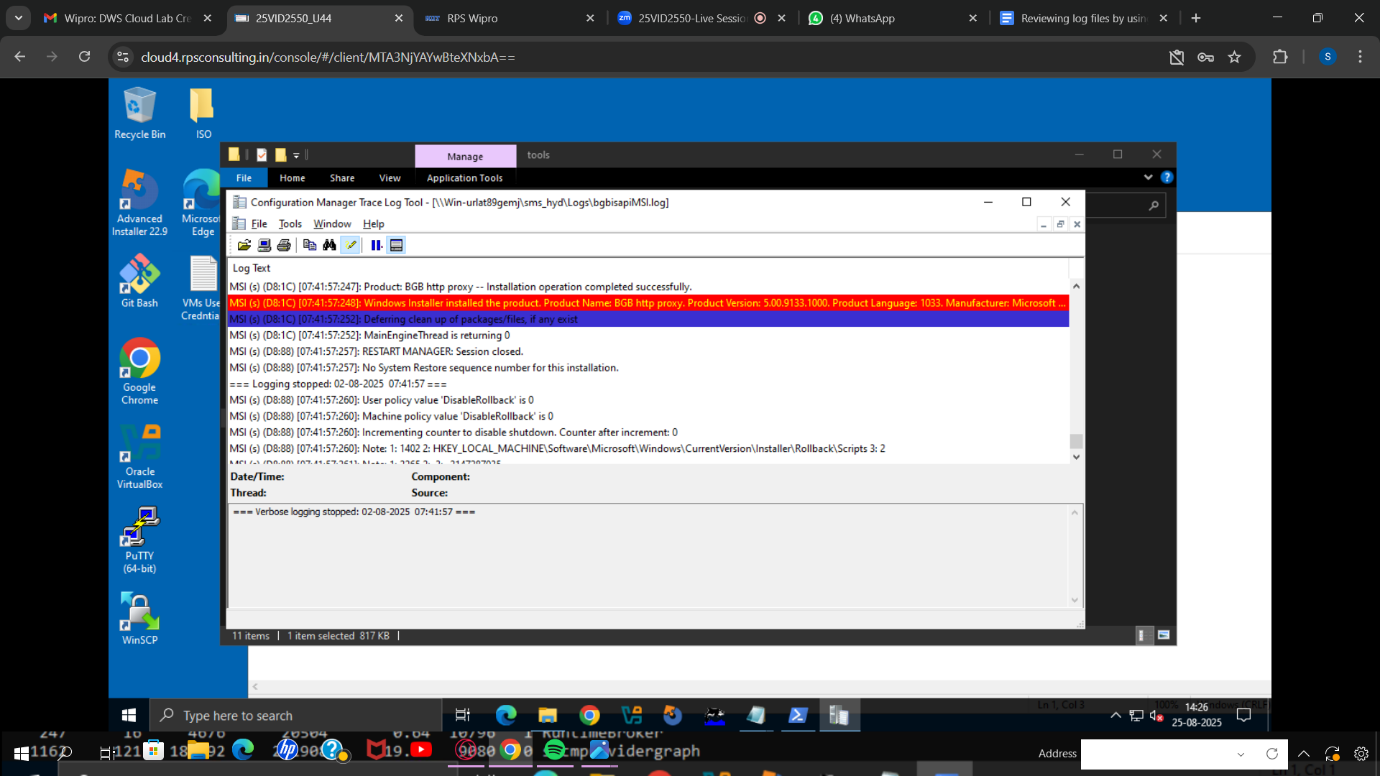
To change the default highlighted color, select the File and Preferences… menu items.  
  


Click on the yellow box next to Use this color for highlighting log entries.  
  


I find that using the color pink really stands out! However, you can use whatever you like, so choose a color and click OK.  
  


Finally, click on the OK button. Now all of my highlighted text will be displayed in pink.  
  


Now you can tell from the screenshot above what line has the highlighted text! In my opinion, you need to change the color of the highlighted text in order to quickly see it, and I think that the color pink is a great alternative.



**Introduction to queries in Configuration Manager**

You can create and run queries to locate objects in a Configuration Manager hierarchy that match your query criteria. These objects include items like specific types of computers or user groups. Queries can return most types of Configuration Manager objects, which include sites, collections, applications, and inventory data.

**Query creation overview**

When you create a query, you must specify a minimum of two parameters: where you want to search and what you want to search for. For example, to find the amount of hard drive space that's available on all computers in a Configuration Manager site, you can create a query to search the **Logical Disk** attribute class and the **Free Space (MB)** attribute for available hard drive space.

After you create an initial query, you can specify additional query criteria. For example, you can specify that the query results include only computers that are assigned to a specified site. You can also change how results are displayed so you can view the results in an order that's meaningful to you. For example, you can specify that the results are sorted by the amount of free hard drive space, in either ascending or descending order.

When you create a query, it's stored by Configuration Manager and displayed in the **Queries** node in the **Monitoring** workspace. From this location, you can create new queries and run, update, and manage existing queries.

Queries and reports work together in a database: **a query is a request to retrieve, filter, and organize specific data from one or more tables, while a report is a formatted, organized, and presentation-ready output of that data, often based on a query**. Queries act as the engine for finding the desired information, and reports serve as the polished presentation of that information for analysis and viewing by others.

**Queries**

* **Purpose:** To extract and manipulate data from a database.
* **Functionality:**
  + **Retrieve specific records:** You can ask for, say, all customers in a particular city.
  + **Filter data:** You can apply criteria to narrow down results, showing only records that meet your conditions.
  + **Perform calculations:** Queries can sum, average, or otherwise process data.
  + **Combine data:** They can pull information from multiple tables and present it in a single datasheet.
  + **Update data:** Some queries are "updateable," allowing you to edit data in the underlying tables.
* **Example:** A query could find all sales made by "Region A" in the last quarter.

**Reports**

* **Purpose:** To present the data retrieved by queries in a professional, formal, and easily digestible format.
* **Functionality:**
  + **Formal design:** Reports are designed for presentation, often with a formal look and feel for meetings or updates.
  + **Calculations and formatting:** They can include custom calculations, summaries, and visual elements like fonts and branding.
  + **Printing:** Reports are heavily integrated with printers and are designed to produce well-formatted outputs on paper.
  + **Data freshness:** Each time a report is opened, it displays the most current data available in the database.
* **Relationship to Queries:** A report typically uses a pre-existing query as its data source, meaning it displays only the specific, filtered information the query provides.
* **Example:** A report based on the sales query would show a formal summary of "Region A" sales, potentially with totals and percentages.

In Summary

Think of a query as a powerful search and selection tool, and a report as a final brochure or document that showcases the search results. You first use a query to find the data you need, and then you create a report to display that data in a structured, visually appealing way.

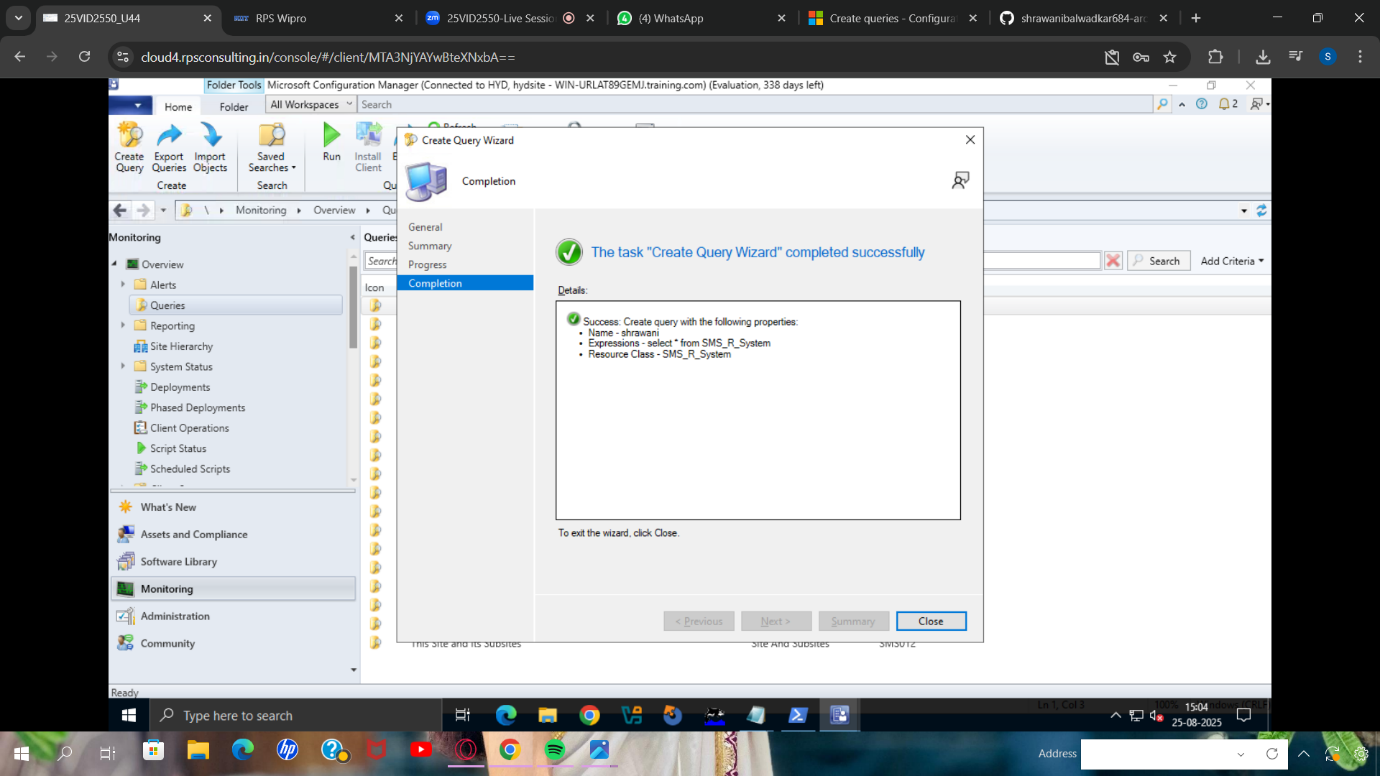
**Create queries in Configuration Manager**

This article describes how to create and import queries in Configuration Manager.

**Create a query**

Use this procedure to create a query in Configuration Manager.

1. In the Configuration Manager console, select **Monitoring**.
2. In the **Monitoring** workspace, select **Queries**. On the **Home** tab, in the **Create** group, select **Create Query**.
3. On the **General** tab of the **Create Query Wizard**, specify a unique name and, optionally, a comment for the query.
4. If you want to import an existing query to use as a basis for the new query, select **Import Query Statement**. In the **Browse Query** dialog box, select a query that you want to import, and then select **OK**.
5. In the **Object Type** list, select the type of object that you want the query to return. This table describes some examples of the types of objects you can search for:



**Health attestation for Configuration Manager**

**How to enable health attestation service communication on Configuration Manager client computers**

Use this procedure to enable device health attestation monitoring for devices that connect to the internet.

1. In the Configuration Manager console, choose **Administration** > **Overview** > **Client Settings**. Select the tab for **Computer Agent** settings.
2. In the **Default Settings** dialog box, select **Computer Agent** and then scroll down to **Enable communication with Health Attestation Service**.
3. Set **Enable communication with Health Attestation Service** to **Yes**, and then select **OK**.
4. Target the collections of devices that should report device health.

