Clue tool usage guide

By Clint Huffman

Contents

[What is Clue tool? 3](#_Toc446658135)

[Features 3](#_Toc446658136)

[Prerequisites 3](#_Toc446658137)

[Download and Installation (administrator rights required) 3](#_Toc446658138)

[Silent installation 7](#_Toc446658139)

[Uninstallation (administrator rights required) 8](#_Toc446658140)

[Silent uninstallation 8](#_Toc446658141)

[Common Usage 8](#_Toc446658142)

[Clue Tasks in Task Scheduler 8](#_Toc446658143)

[Clue Performance Monitor Data Collectors 10](#_Toc446658144)

[Config XML file 11](#_Toc446658145)

[PalCollector 11](#_Toc446658146)

[User initiated data collection 12](#_Toc446658147)

[Frequently Asked Questions 12](#_Toc446658148)

[Feedback and Support 12](#_Toc446658149)

## What is CLUE tool?

C.L.U.E. (Collection of Logs and the User Experience) is a fully automate data collection tool for performance problems that may cause system delays. It is best used on Microsoft Windows where the end user does not have administrator rights or to capture difficult problems on Windows Server.

## Features

* Automatically collects data during critical events with no human intervention.
* Configurable to collect any data through Powershell 2.0.
* Survives reboots. In the event that the server is rebooted, the Task Scheduler service automatically reinitializes Clue data collectors.
* Gathers the optimal performance counters for Performance Analysis of Logs (PAL) analysis. <http://pal.codeplex.com>.
* Allows users without administrator rights to initiate data collection.

## Prerequisites

This tool is supported on x86 (32-bit) and x64 (64-bit) versions of Windows 6.1 (Win7|WS2008R2) through Windows 10.

* Powershell 2.0 or later must be installed and functional. The “ByPass” feature is used to by-pass the Powershell execution policy. This means that there is no need to change the system’s Powershell execution policy, but administrator rights is needed during initial installation.
* Windows Task Scheduler
* Windows Performance Monitor

## Download and Installation (administrator rights required)

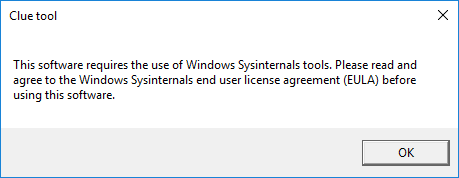
Availability of the Clue tool is current limited to beta users. Contact [clinth@microsoft.com](mailto:clinth@microsoft.com) for the latest location.

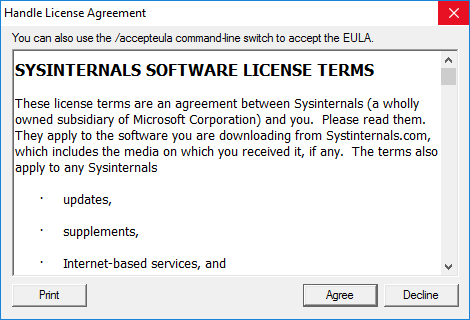
Log onto the target server with administrator rights and copy the zip file to your desktop or My Documents folder. Go to Properties of the zip file and click or check Unblock and then OK. Extract the zip file to a folder. Right-click and run Setup.bat with administrator rights.

The setup might prompt you for an installation directory and/or an output directory if they are not already defined in config.xml. For security purposes, the installation folder is hardcoded to “C:\ProgramData\Clue”, to prevent non-administrators from modifying the commands.

**Microsoft Windows Sysinternals End User License Agreement (EULA)**

This software requires the use of Windows Sysinternals tools. The EULA must be agreed to in order to proceed.

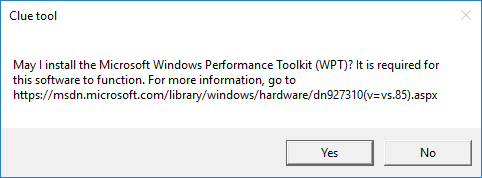




**Note:** A silent installation will assume agreement to the end user license agreement.

**Installation of the Windows Performance Toolkit (WPT)**

This software requires the use of the Windows Performance Toolkit. A response of Yes will silently install the WPT to the default folder of **C:\Program Files (x86)\Windows Kits\10** regardless of the architecture of the system. A response of No will stop installation of this software.



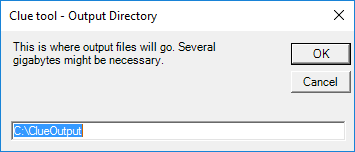
**Note:** A silent installation will assume agreement to the WPT end user license agreement.

**Installation Directory**

This is where all of the Clue related files will be copied. All Clue operations will run from this directory. Once installed, the installation files are no longer needed. The size of this directory is relatively small (less than 100 MB). This is hard-coded to C:\ProgramData\Clue to prevent non-administrator tampering.

**Output Directory**

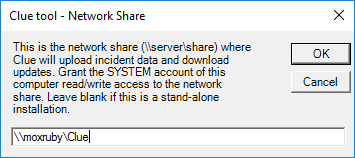
This is where all of the collected data will be saved. Files such as ETL and BLG files can be very large (often larger than 500 MB). Ensure that the logical disk hosting the Output Directory has enough free space to accommodate the potential data.



For a silent installation, edit config.xml and set the value of OutputDirectory to the file system location you desire.

**Network Share**

This is a network share where the \Microsoft\Windows\Clue\IncidentFolderManagement scheduled task will move incident data periodically. It is transferred using Robocopy.exe at a throttled speed of roughly 100 KB/s.



For a silent installation, edit config.xml and set the value of UploadNetworkShare to the network share path that you desire.

The scheduled task is running as System by default. If a Clue network share is used, then the IncidentFolderManagement scheduled task may need to be updated with a domain\user account. This account requires read/write access to the network share.

Use the following commands to change the credentials for the IncidentFolderManagement job. Use /S parameter to apply it to a remote system:

schtasks /Change /TN \Microsoft\Windows\Clue\IncidentFolderManagement /RU MyDomain\MyUser /RP "My password"

**WARNING: This method is a high security risk due to how the password is stored by the Task Scheduler. It is recommended to set the network share to allow the SYSTEM account write access to the share.**

Next, restart the scheduled task:

schtasks /End /TN \Microsoft\Windows\Clue\IncidentFolderManagement

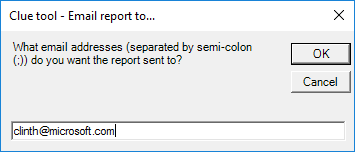
schtasks /Run /TN \Microsoft\Windows\Clue\IncidentFolderManagement

And then, check its status:

schtasks /Query /TN \Microsoft\Windows\Clue\IncidentFolderManagement

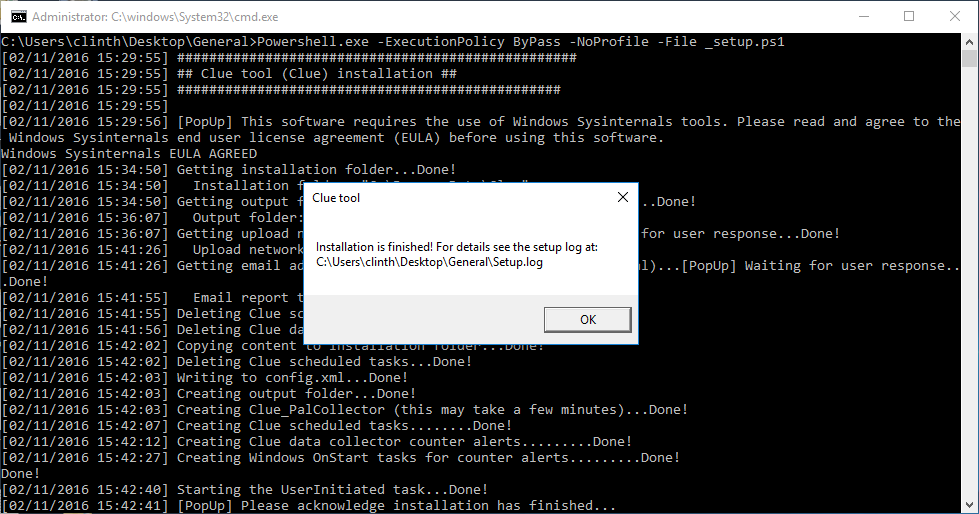
**EmailReportTo**

This is an optional field. This is the email address or email addresses (separated by semi-colons) that will be emailed a report by the analysis services, if applicable.



For a silent installation, edit config.xml and set the value of EmailReportTo to the email addresses you desire.

In less than a few minutes, a dialog box should show that installation was successful.



If Setup.bat fails to run from Windows Explorer, then open an administrator command prompt and run Setup.bat. Administrator rights is required in order to create performance counter data collectors and scheduled tasks.

If an error occurs, then look at Setup.log in the folder where Setup.bat was executed. If help is still needed, then report the error to me at [clinth@microsoft.com](mailto:clinth@microsoft.com) with a screenshot or detailed description of the exact error.

Once installation is complete, you may log off of the system. Data collection will be automatic. Periodically, watch the Output folder and Network Share folder for “incident” data.

## Silent installation

A “silent” installation will not prompt for anything. If installation fails, then see setup.log.

The silent option assumes that installation questions (attributes in the first node) have been answered in Clue.xml in the installation folder such as, but not limited to:

* InstallationDirectory
* OutputDirectory
* UploadNetworkShare
* EmailReportTo

<Clue InstallationDirectory="C:\ProgramData\Clue" OutputDirectory="C:\ClueOutput" UploadNetworkShare="" EmailReportTo="">

To install Clue silently, fill in the attribute fields in Clue.xml and then run SetupSilent.bat with administrator rights. Check setup.log for success or failure.

## Uninstallation (administrator rights required)

To remove or uninstall Clue, run Uninstall.bat with administrator rights from the original zip file or from the Clue installation folder. This action removes the Performance Monitor data collectors, Scheduled Tasks, and installation folder.

Note: Data in the Output folder will remain untouched to prevent data loss. This could be a significant amount of disk usage, so check it while uninstalling.

Note: The Microsoft Windows Performance Toolkit is \*not\* removed by Clue uninstallation.

## Silent uninstallation

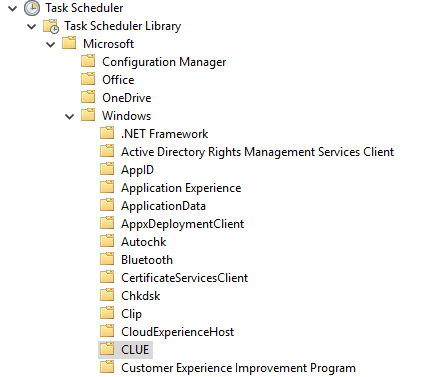
This is the same as uninstallation, but there are no prompts. Run UninstallSilent.bat to uninstall silently.

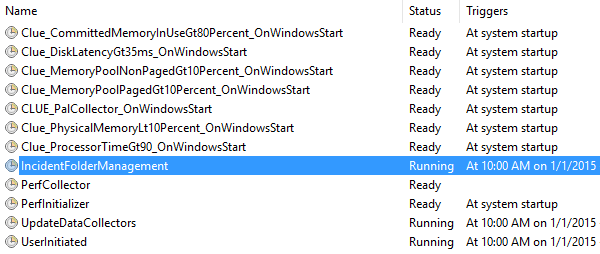
## Common Usage

The best use of Clue is to collect ETW events using xperf.exe to create ETL trace files, to collect event log data, and to collect performance counter data when a performance condition occurs.

## Clue Tasks in Task Scheduler

Open Windows Task Manager (part of the operating system) and navigate to “\Microsoft\Windows\Clue” folder.





The installation of Clue creates tasks at this location only.

All performance counter data collector triggers use the same Clue task, “PerfCollector”, which executes PerfCollector.ps1.

All tasks with the naming convention of “Clue\_<Name>\_OnWindowsStart” are tasks that will start Performance Monitor related data collectors upon reboot of Windows.

PerfInitializer executes PerfInitializer.ps1 upon start of Windows. It executes all enabled “OnStart” actions defined in Clue.xml.

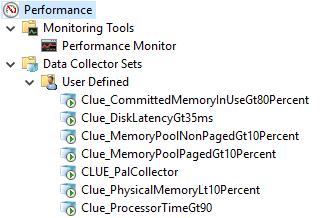
All scheduled tasks should be in a Ready state except for IncidentFolderManagement, UpdateDataCollectors, and UserInitiated which run in a continuous loop.

IncidentFolderManagement compresses resultant incident folders into zip files and moves completed Clue incident data to the designated network share. In addition, it resets run limits each day at a random hour|minute as long as the Clue output folder does not have any incident zip files – meaning the data has been moved off of the system and is ready for more.

UserInitiated watches %public%\Documents\UserInitiated.txt for content changes. Content changes initiates data collection.

## Clue Performance Monitor Data Collectors

Clue creates Performance Monitor data collectors to collect performance counter data. Open Performance Monitor by running “perfmon.exe”.



Data Collector Sets with the naming convention of “Clue\_<Name>” are counter alerts related to Clue (except for Clue\_PalCollector). They gather the respective counters defined in Clue.xml and execute the PerfCollector scheduled task when the counter alert threshold is broken. The Clue task executes PerfCollector.ps1 which gathers the respective counters based on the SampleInterval, MaxSample, and AnyOrAll criteria.

**SampleInterval:** This is how often in seconds that the defined counters will be gathered by PerfCollector.ps1.

**MaxSamples:** This is how many samples of the counters will be collected before the collected data is analyzed. For example, if the sample interval is 1 second and MaxSamples is 5, then the defined counters are collected every 1 second for 5 seconds.

**AnyOrAll:** If set to “Any”, then if any of the counters defined break the threshold, then the data collector will execute the “OnTrigger” action defined in Clue.xml. If set to “All”, then the data collector will execute the “OnTrigger” action only if all of the defined counters exceed the threshold.

**Operator:** This uses the Powershell operators (Example: “gt” is greater than) comparing the values of the defined counters to the value of the Threshold attribute.

**PalCollector** is a performance counter data collector set with the performance counters detected on the local system and optimized for analysis with the [PAL](http://pal.codeplex.com/) tool. This means that if the system has Microsoft Exchange Server and a named instance of SQL Server installed, then performance counters for the operating system, and both products will automatically be added. In addition, the data collector is configured to be a binary circular log file of 100 MB – meaning it will never be larger than 100 MB. Furthermore, a scheduled task is created to automatically start this data collector set upon the start of Windows allowing it to “survive” reboots.

## Config XML file

The config.xml file is the heart of the tool in which the rest of the scripts and tasks follow.

**DataCollecollectorSet node:** This is a logical grouping of DataCollector nodes and Action nodes. The Name field is not used at this time, but will be implemented when a user interface is created. Enabled supports “True” or “False” and is ignored when set to False.

**DataCollector node:** These are the data collectors that “trigger” one of the Action nodes.

Type CounterAlert creates a Performance Monitor Data Collector alert. When the alert is triggered in Performance Monitor, the PerfCollector.ps1 script collects more samples of the counter and determines if the one or more of the counters are exceeding thresholds.

**Action nodes:** Actions nodes with a Name of “OnStart” run as soon as Clue is installed and when Windows is started. Nodes with the name “OnTrigger” execute whenever one of more of the DataCollector nodes exceeds or matches a threshold. Node with the name “OnEnd” execute when the PerfOnEnd.ps1 script is executed which is recommended to run before uninstalling Clue.

If you only want an action to occur x amount of times, then x can be specified in the RunLimit attribute of the Action node. Once the Ran attribute (increments when ran) reaches the RunLimit, the action will no longer execute unless Ran is set to 0 manual or RunLimit is increased.

## PalCollector

The Performance Analysis of Logs (PAL) tool is a popular open source project that is analyzes performance counter logs. Clue uses the threshold files of the PAL tool to create a Performance Monitor data collector that optimizes the analysis of the PAL tool by collection every performance counter that could be analyzed in the PAL tool.

During installation of Clue, the PalCollector.ps1 script executes and creates a performance counter data collector as a binary circular log file – meaning this data collector can run indefinitely and not cause the system to run out of disk space because it is hard coded to a specific size.

For more information, see the PAL tool at <http://pal.codeplex.com>.

## User initiated data collection

Clue has automated data collectors, but there may be a “hang” situation that needs to be captured. Any user such as non-administrator users can initiate general data collection. Simply open %public%\Documents\ClueUserInitiated.txt, write a description of the problem and/or symptoms, and then save the changes.

Once the change is saved, data collection should be immediate. Check the output folder for an incident folder with “UserInitiated” in the folder name.

## Frequently Asked Questions

**If the server is rebooted, will Clue continue to function?**

Yes, Clue creates scheduled tasks to restart itself in the event of a reboot.

**How do I remove this tool when done?**

Run Uninstall.bat or UninstallSilent.bat using an administrator command prompt.

**How do I prevent Clue from creating too many files?**

Set the RunLimit attribute on the respective Action nodes to the number of times you wish it to run. This is reset at a random time each day as long as there are no zip files in the output folder.

## Feedback and Support

Clue is not supported at this time. Please contact me directly for support at [clinth@microsoft.com](mailto:clinth@microsoft.com).