Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Application Control Verification Tool – User Guide

FEBRUARY 2024

Introduction

The Essential Eight Strategies to Mitigate Cyber Security Incidents (abbreviated to the Essential Eight) is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of adversaries. As a part of enabling Australian entities to benefit from the increased security protections afforded when using the Essential Eight, the Australian Cyber Security Centre (ACSC) has developed the 'Cyber Toolbox', a set of tools designed to be used independently by an organisation to assist in assessing and uplifting their cyber security maturity.

The Application Control Verification Tool (ACVT) is one of the Cyber Toolbox tools, and has been developed by the ACSC to test application control policies applied to an operating system. The tool accesses the operating system, simulates a user with standard privileges, and tests and reports on weaknesses and misconfigurations in the system's application control policies. Currently it assists with testing Level One of the November 2023 Essential Eight Maturity Model Application Control mitigation strategy by testing execution of multiple file types including executables, scripts, batch files and libraries.

When the tool is double-clicked it runs in its default configuration, and will begin from the root of the file system (for example "C:\") from which it is run. If the tool is on a network drive it will assess from the root of that network drive (e.g. "E:\"). Once started it will:

- Identify all directories that exist on the system;
- Copy a small executable, script or library file to each directory;
- Run the file;
- Remove the file.

The ACVT will create a Comma Separated Values (CSV) file that outlines the result of all of the above attempts, which a security practitioner can use to diagnose any issues with their application control policies.

The ACVT is not intended to be used as an audit tool. Entities considering making use of this tool should assess whether it is appropriate for their needs.

Usage

Caution: This tool should not be run on production or essential systems, including network file shares. System resources are monopolised as it runs, and the tool may leave test files scattered across the file system.

Preparing to run ACVT

Identify the system to run on

As per the caution note preceding this section, care should be taken to ensure the tool is not run on production systems and that network file shares are not accidentally included in the paths to be scanned. An ideal system to test would be a standalone Standard Operating Environment (SOE) that provides a representative system on which the ACVT can be run without posing any risk to other systems.

The tool will attempt to stay on the system that it is run on, but more complex file system setups may include links to external file shares. The risk is that these external file systems may see their performance degraded if the ACVT is accessing them repeatedly in order to drop, execute and then remove the small test files. There is the potential that the small executables that ACVT drops may be left on the file systems upon which it is run.

Obtain and Verify the ACVT

The latest version of the ACVT can be obtained from the ACSC Portal. To access the ACSC Portal, you must be an ACSC Partner.

Once you have obtained the ACVT, verify that you have a legitimate copy of the ACVT application. You should have received the ACVT application along with this document. Validate that the executable files and scripts are correctly signed by checking the “Digital Signatures” tab of the file properties that they were signed by ASD. You can also verify that the binary is signed with ASD’s certificate using the PowerShell “Get-AuthenticodeSignature” function.

Once you have verified ACVT, place the executable somewhere on the system drive that you wish to test. For most users the drive that they wish to test will be “c:\”, and so placing the binary anywhere in the normal user directories will be sufficient (e.g. “c:\Users\Username\Desktop\acvt\acvt.exe”).

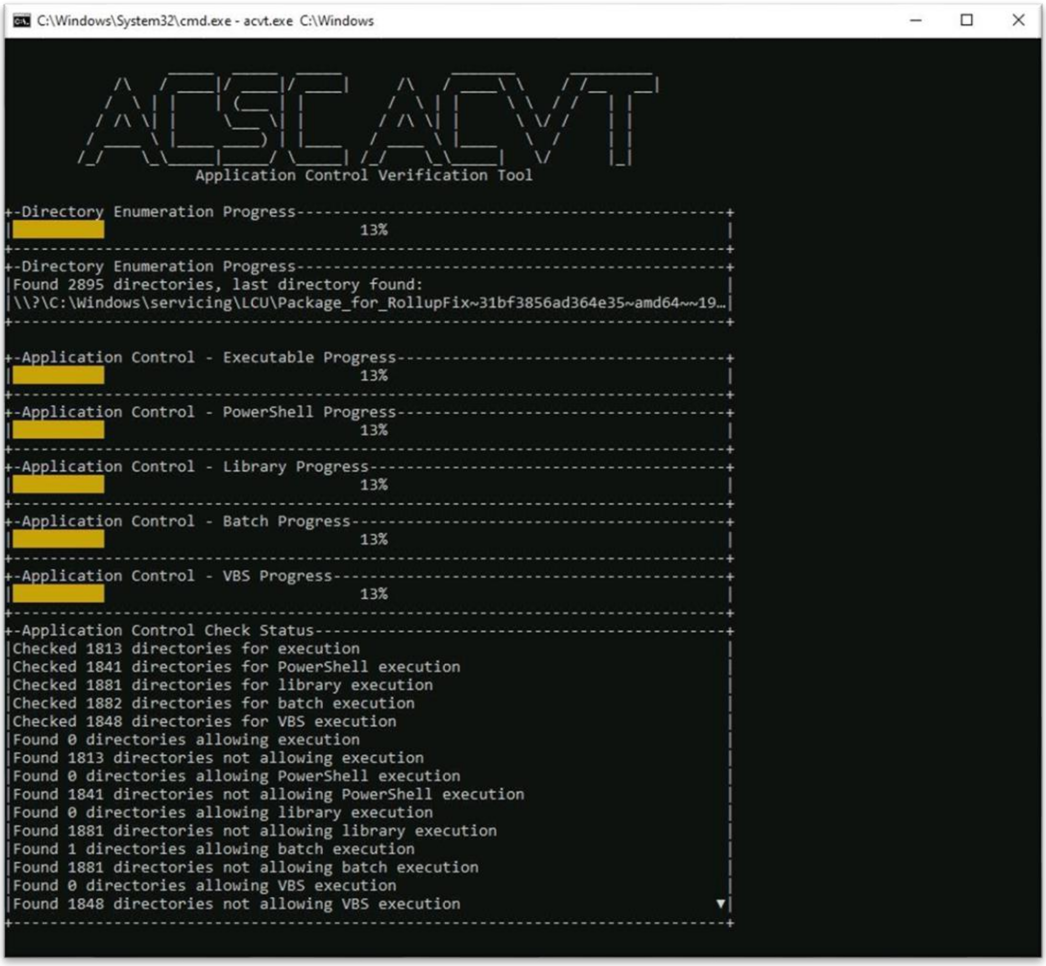
Prepare the Application Control policy

If you have a robust application control policy in place, you may need to configure a policy exemption for ACVT to run on the target system. How the exception is implemented depends on your product and configuration, though note that ACVT is signed with an ASD code signing certificate. Specific guidance on creating exceptions within your application control policy is outside the scope of this document. Consult your application control product manuals or the vendor for detailed instructions.

Note that ACVT does not require additional programs or services to be installed for it to work. However, the tool will only run on **64-bit versions of Windows 7 and higher, or Windows Server 2008 and higher**.

Running ACVT

Once you have prepared the system, locate and double click the executable file. This will start the tool and ask for confirmation that the tool is running on a non-production system, and that you accept the risk of running the tool. Once this confirmation is received from the user, ACVT will start testing the application control policy applied to the system. A window will display the progress of the tool as it runs (as per Figure 1). Additional command line arguments can be supplied, with detail provided by running “acvt.exe -h” or “acvt.exe --help” from a command line prompt.



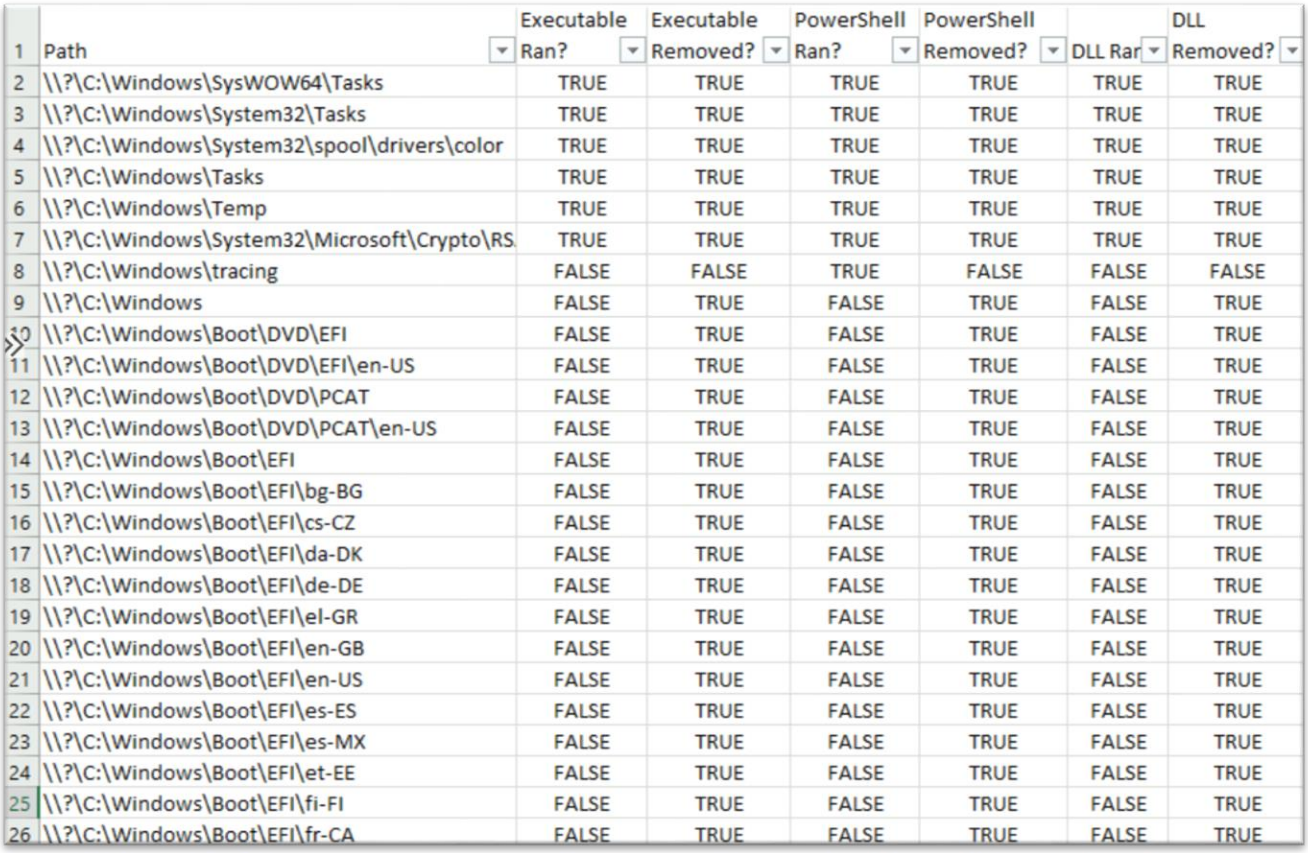
```
C:\Windows\System32\cmd.exe - acvt.exe C:\Windows

                    Application Control Verification Tool

+-Directory Enumeration Progress----------------------------------------+
|                                    13%                                |
+-----------------------------------------------------------------------+
+-Directory Enumeration Progress----------------------------------------+
|Found 2895 directories, last directory found:                          |
|\\?\C:\Windows\servicing\LCU\Package_for_RollupFix~31bf3856ad364e35~amd64~~19…|
+-----------------------------------------------------------------------+

+-Application Control - Executable Progress-----------------------------+
|                                    13%                                |
+-----------------------------------------------------------------------+
+-Application Control - PowerShell Progress-----------------------------+
|                                    13%                                |
+-----------------------------------------------------------------------+
+-Application Control - Library Progress--------------------------------+
|                                    13%                                |
+-----------------------------------------------------------------------+
+-Application Control - Batch Progress----------------------------------+
|                                    13%                                |
+-----------------------------------------------------------------------+
+-Application Control - VBS Progress------------------------------------+
|                                    13%                                |
+-----------------------------------------------------------------------+
+-Application Control Check Status--------------------------------------+
|Checked 1813 directories for execution                                 |
|Checked 1841 directories for PowerShell execution                      |
|Checked 1881 directories for library execution                         |
|Checked 1882 directories for batch execution                           |
|Checked 1848 directories for VBS execution                             |
|Found 0 directories allowing execution                                 |
|Found 1813 directories not allowing execution                          |
|Found 0 directories allowing PowerShell execution                      |
|Found 1841 directories not allowing PowerShell execution               |
|Found 0 directories allowing library execution                         |
|Found 1881 directories not allowing library execution                  |
|Found 1 directories allowing batch execution                           |
|Found 1881 directories not allowing batch execution                    |
|Found 0 directories allowing VBS execution                             |
|Found 1848 directories not allowing VBS execution                     ▼|
+-----------------------------------------------------------------------+
```

Figure 1: ACVT User Interface

Once the tool has finished running, it will produce a CSV file in the same directory from which it was run, and then exit. If you run the test several times, the CSV file name will change for every scan, and it will not overwrite the results of previous scans.

Examining the Results

Opening the CSV file will show your directory paths, and whether any test files were able to be run and removed from each directory (see Figure 2).



1	Path	Executable Ran?	Executable Removed?	PowerShell Ran?	PowerShell Removed?	DLL Rar	DLL Removed?
2	\\?\C:\Windows\SysWOW64\Tasks	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
3	\\?\C:\Windows\System32\Tasks	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
4	\\?\C:\Windows\System32\spool\drivers\color	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
5	\\?\C:\Windows\Tasks	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
6	\\?\C:\Windows\Temp	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
7	\\?\C:\Windows\System32\Microsoft\Crypto\RS	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
8	\\?\C:\Windows\tracing	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
9	\\?\C:\Windows	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
10	\\?\C:\Windows\Boot\DVD\EFI	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
11	\\?\C:\Windows\Boot\DVD\EFI\en-US	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
12	\\?\C:\Windows\Boot\DVD\PCAT	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
13	\\?\C:\Windows\Boot\DVD\PCAT\en-US	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
14	\\?\C:\Windows\Boot\EFI	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
15	\\?\C:\Windows\Boot\EFI\bg-BG	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
16	\\?\C:\Windows\Boot\EFI\cs-CZ	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
17	\\?\C:\Windows\Boot\EFI\da-DK	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
18	\\?\C:\Windows\Boot\EFI\de-DE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
19	\\?\C:\Windows\Boot\EFI\el-GR	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
20	\\?\C:\Windows\Boot\EFI\en-GB	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
21	\\?\C:\Windows\Boot\EFI\en-US	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
22	\\?\C:\Windows\Boot\EFI\es-ES	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
23	\\?\C:\Windows\Boot\EFI\es-MX	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
24	\\?\C:\Windows\Boot\EFI\et-EE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
25	\\?\C:\Windows\Boot\EFI\fi-FI	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE
26	\\?\C:\Windows\Boot\EFI\fr-CA	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE

Figure 2: Example ACVT Output

The figure above shows the following information:

- Column 1 (*Path*) shows the file system path that was tested.
- Column 2 (*Executable Ran?*) shows whether the tool was able to copy and execute an executable file to that path. If "*True*" is displayed, you should investigate that path as a file was able to be written and executed.
- Column 3 (*Executable Removed?*) shows whether the tool was able to delete the executable file after it was written. If this column displays "*false*", then the tool was unable to remove the file from this directory, and you should remove the file manually.
- The remaining columns are a repeat of columns 2 and 3 for the additional file types covered by ACVT.

In the above example, the output shows that all file types were not able to run in “C:\Windows\”, but were able to run in several sub directories, such as “C:\Windows\Temp” and “C:\Windows\Tasks\”. It also shows that executable files could not run in “C:\Windows\tracing\”, however PowerShell scripts were able to run in this location, but could not be deleted. In this example, the administrator would know that they:

- Need to consider adjusting their application control policy to prevent execution within these directories;
- Should remove the ACVT test file in C:\Windows\tracing, and;
- Should re-run the ACVT to ensure that any policy change made is effective.

Once you have completed testing and remediation work, ACSC recommends secure storage (or disposal) of reports and data generated by this tool.

Known Issues

Slow Run

ACSC has observed ACVT taking an excessive amount of time to assess some systems, seeming to pause indefinitely. If this occurs, consider running the tool from the command line and providing a more targeted set of directories to assess. Please advise us if this occurs via the ASD Assist mailbox (asd.assist@defence.gov.au), with any additional context.

Antivirus

In moving across the file system and making a large number of file changes quickly, ACVT displays behavior that is similar to ransomware applications. As such, ACSC has observed some security products to identify it as malware and block it from running. The ACVT is not malware, and it has undergone an internal security review to ensure that its components are free from security issues. If you are concerned about any behavior please contact us.

Paths with semicolons

There is a known issue with the csv report that ACVT produces after running. Paths containing semicolons are not quoted in the output csv file, and the default behavior by common spreadsheet software will be to split the semicolons into an extra column. The end result will be that the output csv will have an extra column for each semicolon in a path, and that row will not properly align with the table headings. Users will need to be aware of this when examining results, as results with semicolons will be harder to read in the report.

Application control popups

Some application control products will inform the user if a particular file type was blocked from execution. Suppression of these messages may require configuration within your application control solution. Alternatively, if the popup issue resides with a particular file type checker, this can be explicitly disabled using –e flag to remove a particular checker.

Non-existent path bypasses

ACVT can only check for execution within paths that exist on the system. An application control policy may contain exceptions for directories that do not exist on the test system, but could be created by an adversary to allow code execution. For example, an adversary may use inbuilt PowerShell commands to analyse the effective AppLocker policy on a system and discover a user writeable location that will allow execution. ACVT is unable to duplicate this behaviour to check for these bypasses and will not be reported by the tool.

Feedback

If you identify issues using the ACVT, ACSC would appreciate this receiving this feedback so that we can guide any further development actions. If you encounter issues such as error messages or crashes, please run the tool from the command line with the “--debug” option enabled, and provide the log file produced along with the details of the problem to the ASD Assist mailbox (asd.assist@defence.gov.au). The ACSC would appreciate your feedback, comments, and details of any errors you encounter while running the tool.

Further information

1. Implementing Application Control https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-application-control

Warnings

The ACSC recommends against running ACVT on business critical or production systems. Testing has been performed with government entities to identify issues, and due care has been taken by the developers to reduce the likelihood of errors or failures, but they cannot be ruled out.

Legal

Redistribution of the software (in either source or binary form) is not permitted. The software is provided on an ‘as is where is’ basis by the Australian Cyber Security Centre (ACSC) and may be updated over time. Neither the ACSC nor the Commonwealth have any liability whatsoever in connection with use of the software.

Contact details

For questions regarding this advice, email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).