



CIGENT Data Defense Setup and Evaluation Guide



Date: September 2024

Version: 1

Data Defense Version 5.0.6

Contents

Introduction	3
Purpose	3
Related Evaluation Material	3
Data Defense Basic Installation	4
Quick Start Wizard	6
Understanding Invisible vs Visible Drive state	9
Understanding Always vs During Threat protection	10
Understanding threat sensors and their impact	14
Cigent firmware features	18
Erase Verify	19
KeepAlive	21
Command Log	25

Introduction

The Cigent Data Defense is a new approach to data security, one that complements existing solutions and places the importance of protecting data above all else. Data Defense takes concepts used in threat containment and continuous authentication and applies them as close to the data stream as possible, bringing proactive protection directly to your data. Data Defense allows users to safely and easily access critically important information, even if the system is already compromised. The result is an unprecedented level of protection, detection, and response to cyberattacks, insider threats, and lost or stolen devices.

Data Defense employs key concepts of the Zero Trust security model to ensure access to protect all the way down to the file level. Users are presented with a step up authentication challenge before accessing files based on the protection level and threat status of the host.

Discrete sensors are deployed to monitor suspicious network, system, and deception events for indications of compromise. These sensors, along with ingested security events from Windows Defender,™ and other leading endpoint and network security solutions, are fed into our AI-based Analysis Engine. When the threat level is elevated, Data Defense responds by securely locking files, blocking suspicious devices, or sending an alert to a SIEM or SOC.

Purpose

This document is a guide to help you quickly install and configure the Data Defense software so you can see it working in your own environment. The guide describes each Data Defense sensor and how to simulate their activation using manual steps or programs provided by Cigent. By the end, you will have a good understanding of the power of Data Defense and its sensor network and how it can complement your existing data security solutions.

Related Evaluation Material

Additional material in the form of sample files are available for download at the link below. These items are referred to throughout the guide and can be used to replicate the steps for a consistent result.

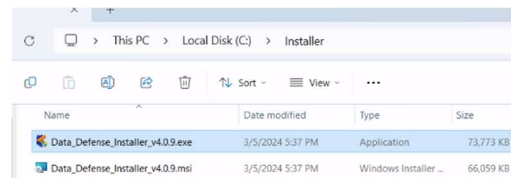
<https://cigent.blob.core.windows.net/download/SampleFiles.zip>

Data Defense Basic Installation

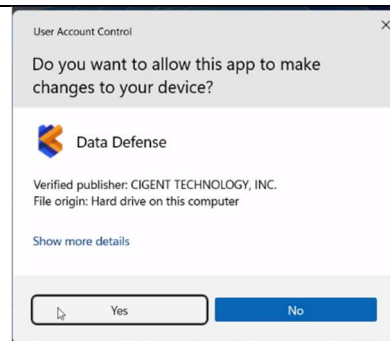
The latest versions of Data Defense can always be found on the Cigent support site (<https://support.cigent.com>). They can also be found on the downloads page of the Cigent management console (<https://central.cigent.com>) if you have a subscription. Note that activating Data Defense to a subscription enables additional features and capabilities not covered in this tutorial. This tutorial will just be covering the features available in the stand-alone version.

There are two types of installation packages available. The executable (EXE) is a user interactive installation while the Microsoft Standard Installer (MSI) is typically used for remote deployments requiring no user interaction. For this tutorial, we will be using the executable.

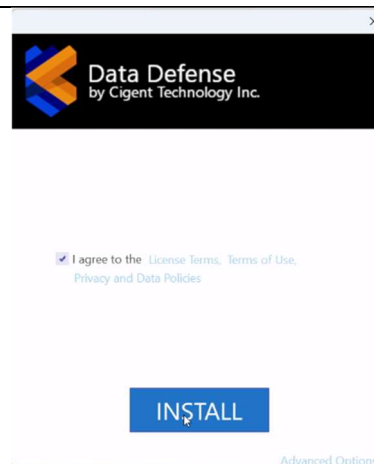
1. Double click the EXE to start the installation.



2. Select Yes on the User Account Control popup.



3. Click the checkbox and click INSTALL.



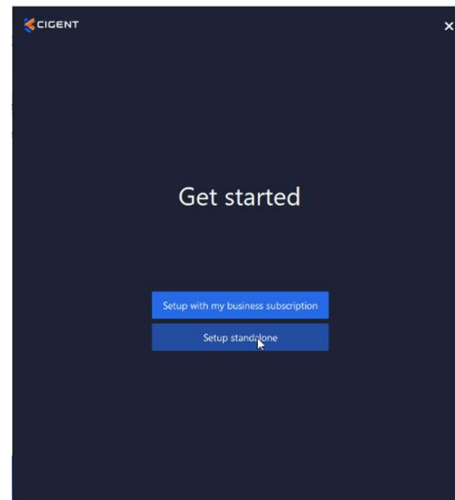
4. Click Finish to complete the installation.



Quick Start Wizard

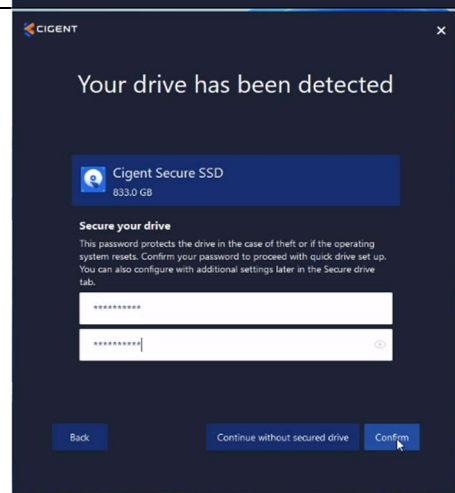
1. Shortly after the installation completes, a setup wizard will appear that will guide the user through basic setup of a Secure Drive (if present) and folder protection.

Click Setup standalone to begin.



2. If discovered, the setup wizard will present an option to configure a single secure drive.

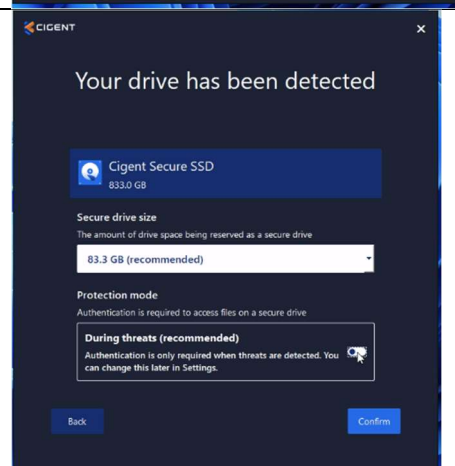
Enter a password twice and click Confirm.



3. Accept or change the Secure drive size.

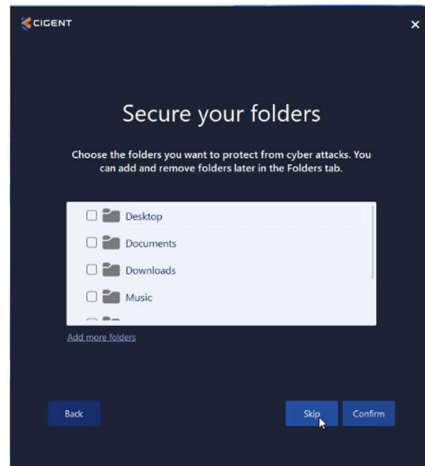
Change the Protection mode to NOT be During threats. This results in an Always secure drive which will be used for this tutorial.

Click Confirm.

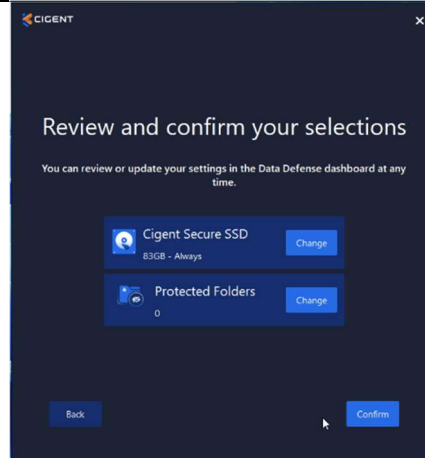


4. You may optionally add protected folders from the list of predefined values or your own custom locations. However, this tutorial will not be covering this protection feature.

Click Skip.

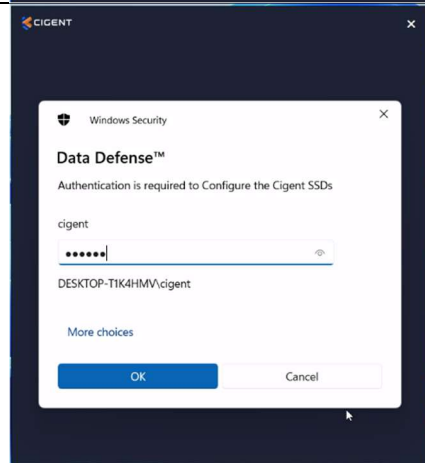


5. Click Confirm to complete setup wizard.

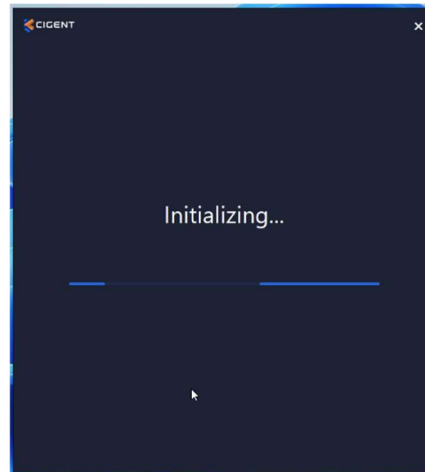


6. To complete the setup, Data Defense requests a step up authentication. By default, the authentication type is whatever the current Windows Hello sign in method is. Typically, this is password. However, any of the available options (Facial recognition, fingerprint, etc are supported.)

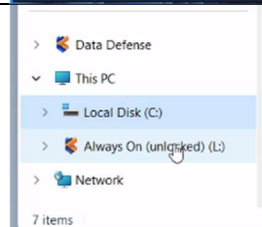
Click OK to continue.



7. It may take a few minutes to initialize the Secure drive. During this time you may see Windows display notifications regarding a new drive being available.



8. Once complete, you should have an Always On drive (typically L:) viewable in your File Explorer.

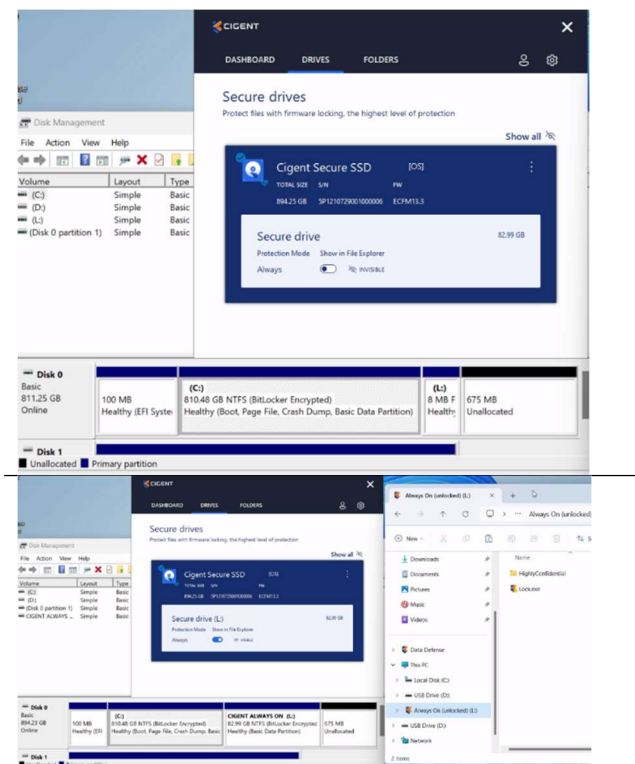


Understanding Invisible vs Visible Drive state

The first layer of data protection we will cover is invisible data. The secure drive you just created is special in that it can be either visible or invisible to the operating system. When invisible, all data stored on the drive is protected from threats like ransomware, malware and even malicious insiders simply because it cannot be accessed. To gain access to data on the drive, users can manually make the drive visible using step up authentication. As an additional layer of protection, secure drives will also automatically become invisible if a threat is detected. (More on this later.)

When a secure drive is invisible the drive appears to the OS as a small read only partition containing only a convenient program (unlock.exe) to make the drive visible. When visible, the full drive appears to the OS exposing all data stored on the drive. The drive letter remains the same in both states.

1. Open Windows Disk Management, Windows Explorer and Data Defense as shown.



2. Click the toggle icon to change the drive to Visible. Notice how the partition appears in Disk Management and Explorer and you can now see your data.

Understanding Always vs During Threat protection

Each type of data protection including secure drive, folder and file type in Data Defense supports two modes, Always and During Threats. End users or administrators can choose the option that best suits the level of protection based on the type of data being protected.

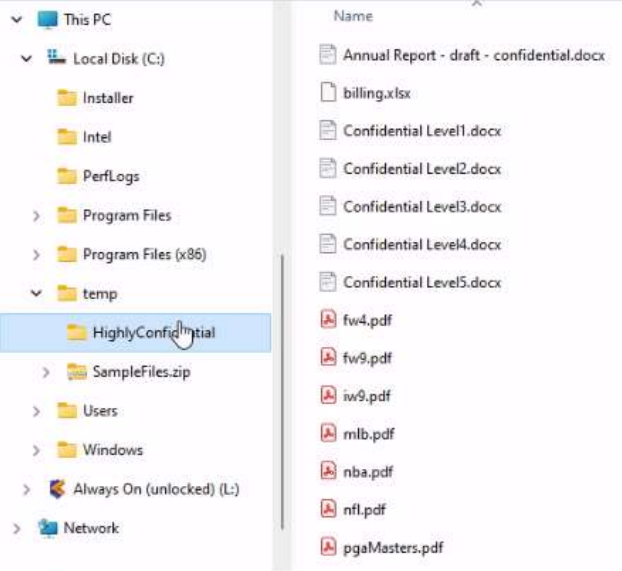
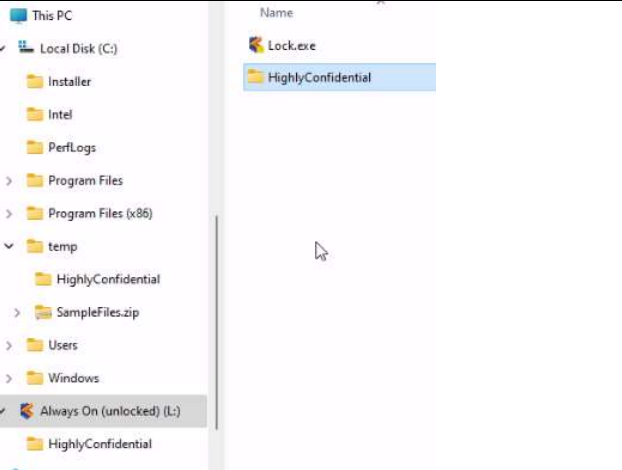

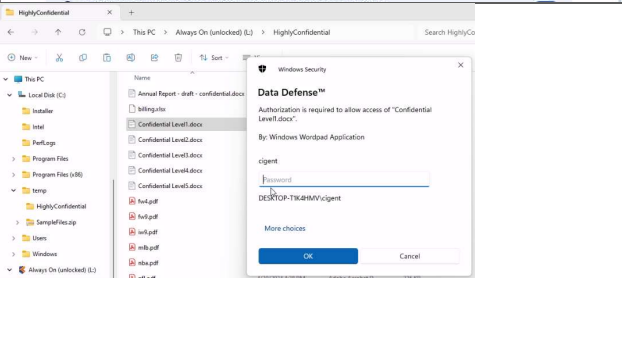
During Threats protection only requires step up authentication to access protected files when the threat state of the endpoint is elevated. The threat state can become elevated by an internal Data Defense sensor or by an externally integrated source. The standalone version of Data Defense has a Trusted Network and Anti-virus sensor. If a sensor detects a potential threat, users must authenticate each file access until the threat is remediated.

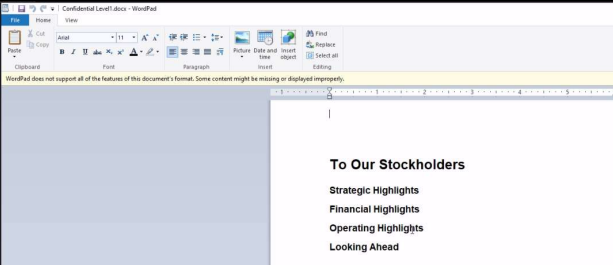
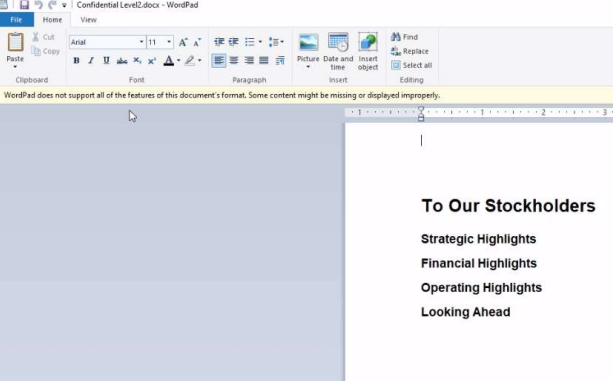
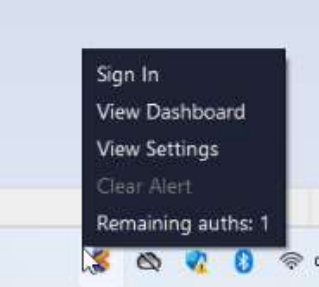
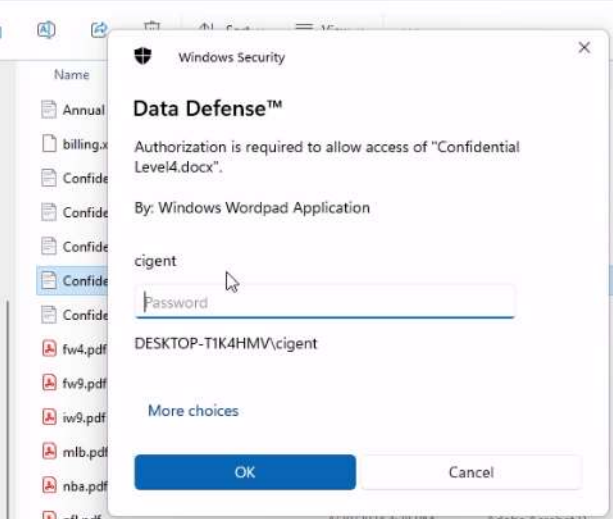
Always protection requires step up authentication to access protected files every time by default. The File Reauthentication Frequency setting allows changing the access authentication to occur after a predetermined number of accesses over a period of time. This greatly reduces the impact on the user of accessing protected files while balancing the risk of unauthorized access.

The use of Always protection and File Reauthentication Frequency is the recommended mode of protection by Cigent.

In this section we will start interacting with files to see the file protection in action. You can either use some of your own files or you can download the files used in this guide.

<https://cigent.blob.core.windows.net/download/SampleFiles.zip>

<p>1. Create a folder C:\temp and copy SampleFiles.zip into it. Right click to Extract All. files. Change location to C:\temp. When complete, you should have a HighlyConfidential folder in C:\temp.</p>	
<p>2. Make sure your Always On Secure Drive is Visible and the copy the HighlyConfidential folder to L:\.</p>	
<p>3. Open Data Defense -> Settings. Change the File Reauthentication Frequency to 2. The changes the requirement to authenticate from every time to every third time.</p>	
<p>4. In Windows Explorer, navigate to L:\HighlyConfidential. Double-click to open Confidential Level1.docx. Since this is the first file being opened today, authorization is required. Notice the name of the file and requesting application is indicated letting the user know</p>	

<p>what is accessing the particular file.</p>	
<p>5. Enter your credential and the file will open.</p>	
<p>6. Double click on Confidential Level2.docx. Notice the file opens without authentication. This is because you set the reauthentication frequency greater than zero.</p>	
<p>7. You can see how many pre-authenticated file access you have left by right clicking on the Data Defense tray icon.</p>	
<p>8. Open Confidential Level3.docx and then open Confidential Level4.docx. Upon attempting to open Confidential Level4.docx, you are again required to authenticate because you had no remaining pre-authentications.</p>	

Understanding threat sensors and their impact

As mentioned earlier, the threat state of Data Defense is determined by its sensors. These sensors are either internal or external. The standalone version of Data Defense has two sensors available, Trusted Network and Anti-virus tethering. Additional sensors are available with the Data Defense subscription and are not covered in this guide.

The Trusted Networks sensor (inactive by default) looks for connections to newly connected networks and increases the threat level of Data Defense until the user trusts the network. This can occur if a user joins an open wifi network at a coffee shop for example. Users can also not trust a network leaving the threat state elevated for increased file protection.

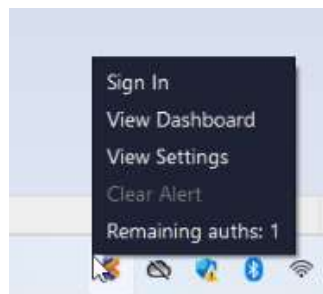
The Anti-Virus tethering sensor monitors the state and status of the active anti-virus application in Windows. If the anti-virus program detects a virus or becomes disabled, Data Defense will elevate the threat level.

When the threat level is elevated by a sensor, the following occurs:

1. Always On secure drives are automatically made invisible.
2. During Threat secure drives are conditionally locked based on the settings in Data Defense.
3. The Remaining pre-authentication count is reset to zero.
4. Files on During Threat secure drives or in During Threats folders will require authentication for each file access.

In the following section, we will trigger the Data Defense Anti-virus sensor to see the effect.

1. Open files on the Always On secure drive so you have at least 1 pre-authentication remaining.

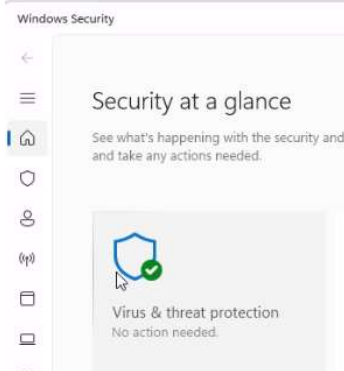


2. We will assume Windows Defender is the active anti-virus. If you are using something else, you should be able to

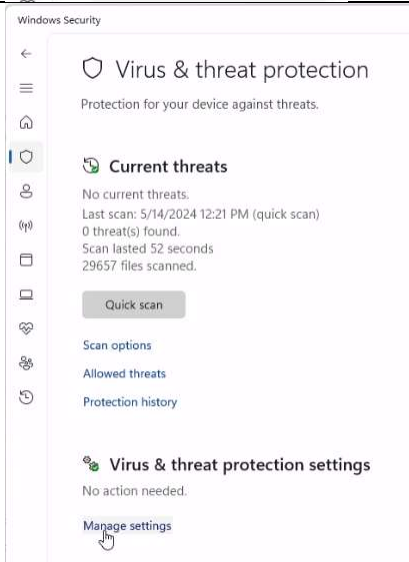


accomplish the same but the steps will vary. Open Windows Security control by clicking the tray icon.

3. Click Virus & threat protection



4. Select Manage settings



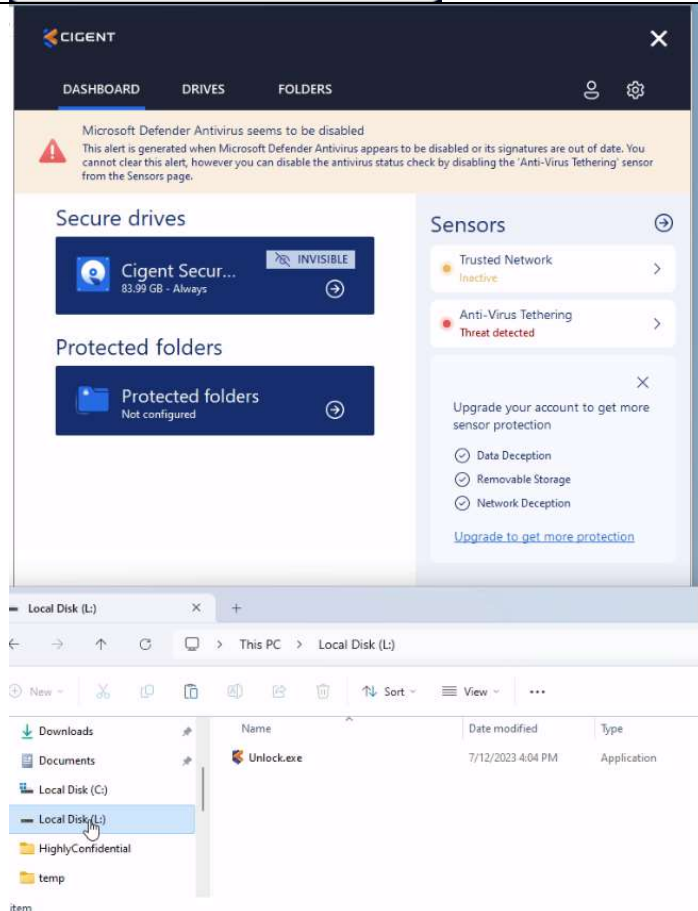
5. Click on the toggle to turn off the real-time protection



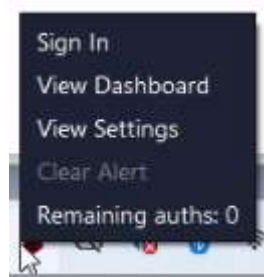
6. Select Yes.


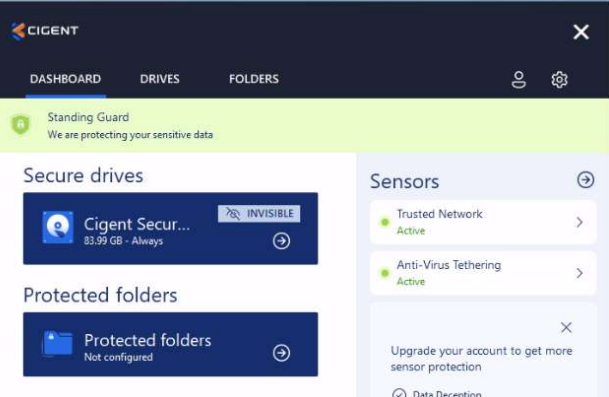
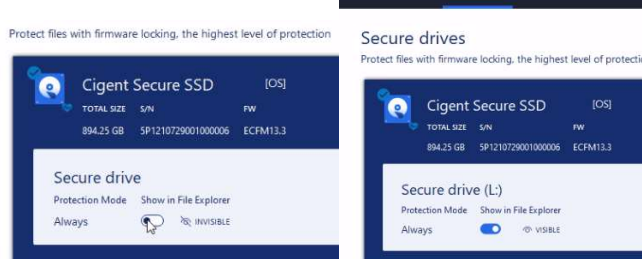


7. Return to the Data Defense dashboard on notice the red banner indicating the elevated threat state due to the Antivirus sensor. Also notice that the Always On secure drive is now locked (safeguarding the files on the drive.)



8. Notice the Data Defense tray icon is now red indicating an active threat. Right click on the icon and also notice the remaining auths is reset to 0.



<p>9. Re-enable the real-time protection.</p>	 <p>Windows Security</p> <h2>Virus & threat protection</h2> <p>View and update Virus & threat protection settings. Antivirus.</p> <h3>Real-time protection</h3> <p>Locates and stops malware from installing or can turn off this setting for a short time before automatically.</p> <p><input checked="" type="checkbox"/> On</p>
<p>10. Notice the Data Defense dashboard threat state returns to Standing guard.</p>	 <p>CIGENT</p> <p>DASHBOARD DRIVES FOLDERS</p> <p>Standing Guard We are protecting your sensitive data.</p> <p>Secure drives</p> <p>Cigent Secure SSD [OS] 83.99 GB - Always INVISIBLE</p> <p>Protected folders</p> <p>Protected folders Not configured</p> <p>Sensors</p> <ul style="list-style-type: none"> Trusted Network: Active Anti-Virus Tethering: Active <p>Upgrade your account to get more sensor protection</p> <p>Data Deception</p>
<p>11. Unlock your Always On secure drive manually.</p>	 <p>Protect files with firmware locking, the highest level of protection</p> <p>Cigent Secure SSD [OS] TOTAL SIZE: 894.25 GB S/N: SP1210729001000006 FW: ECFM13.3</p> <p>Secure drive</p> <p>Protection Mode: Always Show in File Explorer: INVISIBLE</p> <p>Secure drives</p> <p>Protect files with firmware locking, the highest level of protection</p> <p>Cigent Secure SSD [OS] TOTAL SIZE: 894.25 GB S/N: SP1210729001000006 FW: ECFM13.3</p> <p>Secure drive (L)</p> <p>Protection Mode: Always Show in File Explorer: VISIBLE</p>

Cigent firmware features

So far, we have covered the first three layers of data protection provided by Data Defense when combined with a supported SED to create Secure Drives.

1. Invisible data
2. Step up authentication
3. Threat sensors and response

Although these protections are strong, they are primarily enabled in software which a sophisticated adversary could attempt to bypass or find a vulnerability. For example, should a threat actor gain administrative control of the host, they could disable Data Defense and its components. If the secure drive was currently unlocked, the data would be accessible.

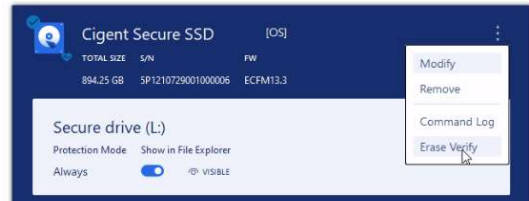

That is where the Cigent firmware enhancements come into play to close those threat vectors. The three firmware features available in the Cigent Secure SSD are:

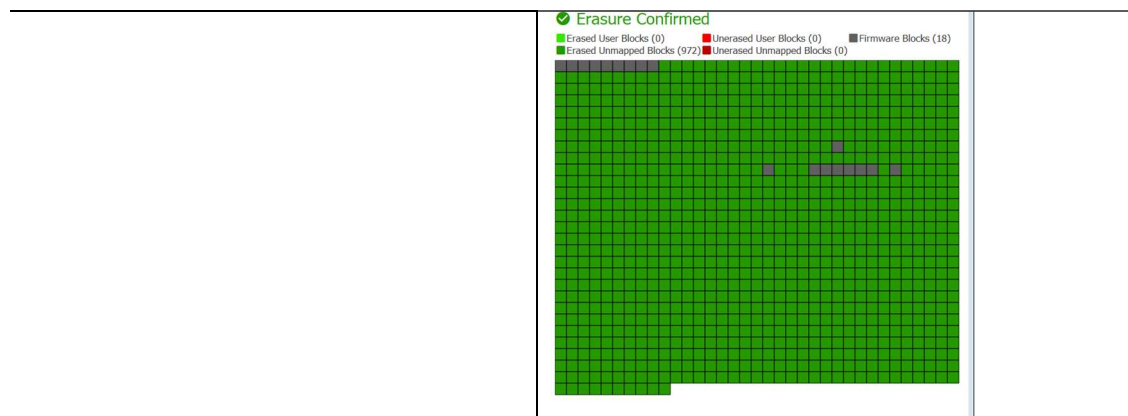
1. Erasure Verification
2. Keep-Alive heartbeat
3. Command Log

Next we will examine and test each of these features to get an understanding of how they work.

Erase Verify

Secure data erasure is an important process for many commercial and governmental organizations preventing classified information from unauthorized access. Short of costly and wasteful physical destruction, users had to depend on outdated erasure programs originally written for magnetic media. Solid State Drives require different methods of erasure to prevent recovery by today's advanced tools and technique. Cigent Drives support extended erasure verification commands to check each and every mapped and unmapped block to verify the data has been removed. Any blocks reporting data will result in an erasure verification failure. Once Data Defense confirms the drive has been truly erased, it can be safely and securely reused.

<p>1. Select Erase Verify from the menu on the Drives page.</p>	<p>Secure drives</p> <p>Protect files with firmware locking, the highest level of protection</p> 
<p>2. The resulting map displays the logical blocks color coded as to their state. The overall state of the drive (Erased or not Erased) is indicated at the top.</p> <p>Of importance are the unmapped blocks which may be missed by some erasure programs and processes. The process of erasing a drive completely is beyond the scope of the document but is more easily tested using an external drive.</p>	
<p>3. Example after a successful data erasure procedure.</p>	



If you have questions on how best to accomplish complete data erasure, please contact Cigent support for some guidance.

KeepAlive

KeepAlive provides an extra layer of protection by creating a tighter trust connection between the firmware (SSD) and the software (Data Defense). When enabled, a non-replayable heartbeat continuously plays between Data Defense and the Cigent Secure SSD such that if the drive fails to receive the proper response in time, the drives will automatically lock. This prevents any chance a hacker could stop Data Defense protection once a drive is unlocked. This makes it impossible to access the files on the Cigent Secure SSD without Data Defense running.

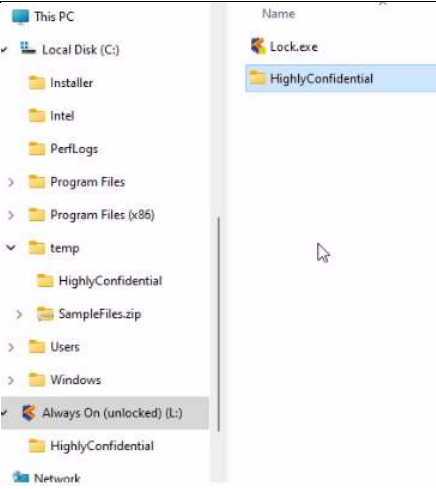
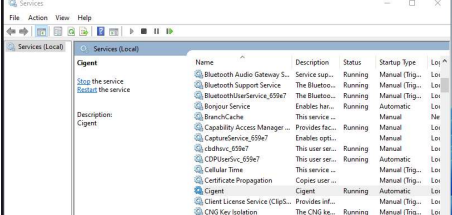
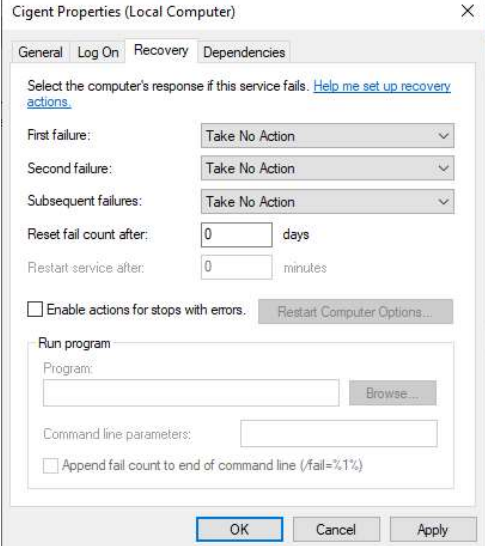

KeepAlive was automatically setup and enabled when you configured your Secure Drive. Indication it is enabled can be seen on the secure drive panel:

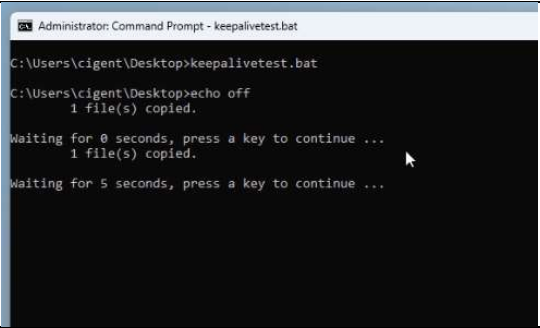
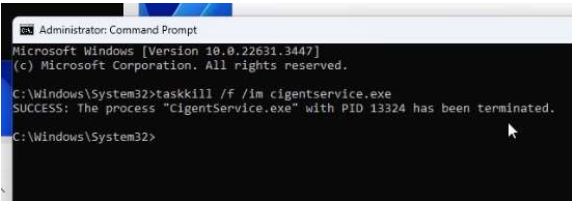
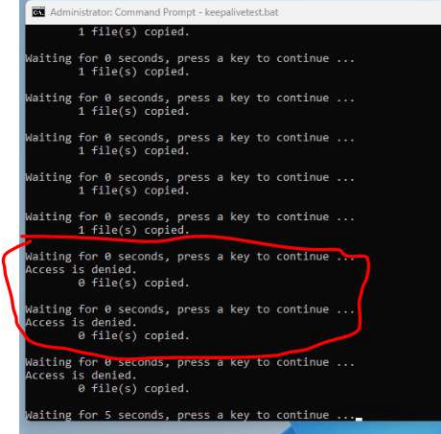
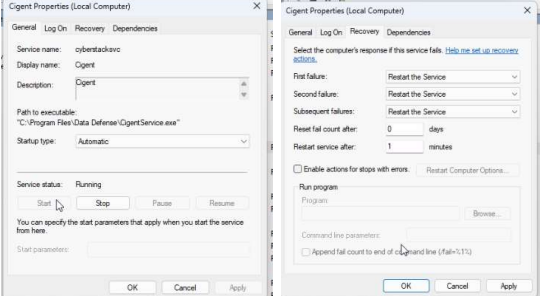
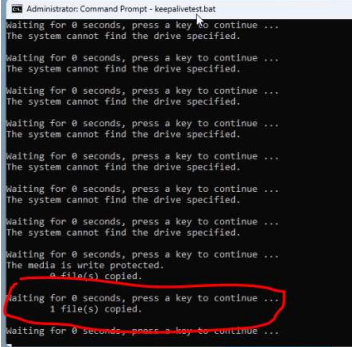
Secure drives

Protect files with firmware locking, the highest level of protection



Since Windows caches a significant amount of file and directory information, testing Keepalive can be a bit of a challenge just using windows explorer. The best method is using a simple batch script to continuously write a test file to the secure drive and then stop the Data Defense service. After about 30 seconds the script will no longer be able to write to the secure drive because the firmware automatically locked it. d, it will eventually fail to create new files.

<p>1. Ensure the Secure Drive is unlocked.</p>	
<p>2. Open Services application and locate the Cigent service.</p>	
<p>3. Right-Click on the row and select Properties. Change all of the failure actions to "Take No Action" then click ok.</p>	
<p>4. Create a batch file called keepalivetest.bat on your C: drive with the following contents:</p>	 <pre> echo off echo "This is a test" >> test.txt :start copy test.txt L: /v timeout 5 goto start </pre>

<p>5. Open a command prompt (Administrator) and run batch file and leave it running</p>	 <pre> Administrator: Command Prompt - keepalivetest.bat C:\Users\cigent\Desktop>keepalivetest.bat C:\Users\cigent\Desktop>echo off 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 5 seconds, press a key to continue ... </pre>
<p>6. Open another command prompt(Administrator) and run the command 'taskkill /f /IM cigentservice.exe' to forcibly shutdown the Cigent Service.</p>	 <pre> Administrator: Command Prompt Microsoft Windows [Version 10.0.22631.3447] (c) Microsoft Corporation. All rights reserved. C:\Windows\System32>taskkill /f /im cigentservice.exe SUCCESS: The process "CigentService.exe" with PID 13324 has been terminated. C:\Windows\System32> </pre>
<p>7. Notice that soon the writes begin to fail. This is an indication that the keepalive timed out and the firmware locked the drive. Windows explorer may not even notice the drive is locked until you attempt to access it but eventually it will.</p>	 <pre> Administrator: Command Prompt - keepalivetest.bat 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue ... Access is denied. 0 file(s) copied. Waiting for 0 seconds, press a key to continue ... Access is denied. 0 file(s) copied. Waiting for 5 seconds, press a key to continue ... </pre>
<p>8. Restart the service using services and reset the failure actions to restart service.</p>	
<p>9. Unlock the Always On drive using Data Defense. (Note, you may have to lock and unlock the drive twice to return the drive to its previous drive letter (L:)) Notice that after unlocking the drive, the script is once again able to write to the secure drive.</p>	 <pre> Administrator: Command Prompt - keepalivetest.bat Waiting for 0 seconds, press a key to continue ... The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue ... The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue ... The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue ... The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue ... The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue ... The system cannot find the drive specified. Waiting for 0 seconds, press a key to continue ... The media is write protected. 0 file(s) copied. Waiting for 0 seconds, press a key to continue ... 1 file(s) copied. Waiting for 0 seconds, press a key to continue ... </pre>

10. Terminate the batch file using Control-C.	
--	--


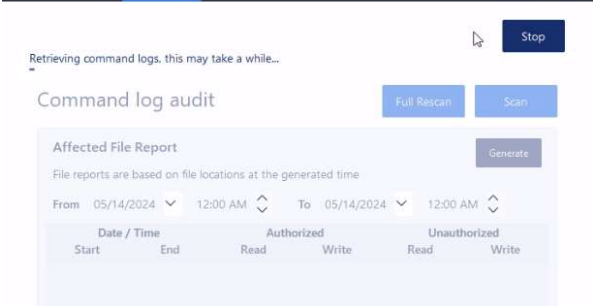
Command Log

Cigent Secure SSDs automatically store every command sent to the drive in a tamperproof location in memory on the drive. Cigent Data Defense also periodically writes markers to the log to indicate the activity was performed with Data Defense running and that the activity was properly authorized. Commands are stored for all partitions including unsecured locations (for example the C: drive.)

This command log can be used to audit drive activity to capture attempts to read information from the drive without Data Defense possibly indicating attempts to circumvent file protection. Further, the command log can be used to report on files accessed with or without Data Defense running by mapping the accessed locations to the current file system layout. This can reveal important information to investigators attempting to understand what was accessed or at least attempted to be accessed.

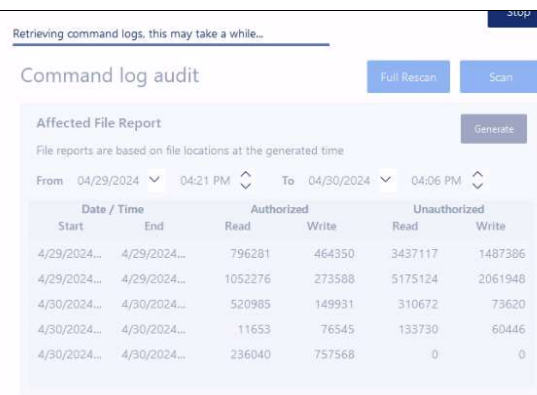
Retrieving the command log would normally only be done during an forensic investigation or to understand if a drive has been tampered with.

Command logs also form the basis for the machine learning ransomware detection capability of the Cigent Secure SSD+ drive.

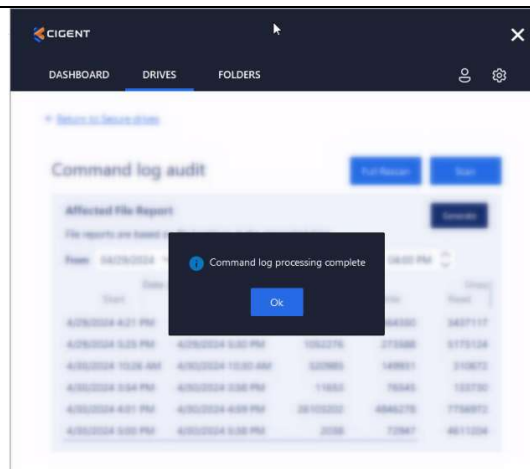
1. In Data Defense->Drives, select Command Log.	 <p>The screenshot shows the 'Secure drives' window with a list of drives. The 'Secure drive (L:)' is selected, and a context menu is open showing options: 'Modify', 'Remove', 'Command Log', and 'Erase Verify'. The 'Command Log' option is highlighted.</p>
2. Select Scan. NOTE: This process can take 30 minutes or more. You can always stop the process by click Stop. Any data retrieved up to that point will be viewable.	 <p>The screenshot shows the 'Command log audit' window. It has a 'Full Rescan' button and a 'Scan' button. Below the buttons is a section for 'Affected File Report' with a 'Generate' button. At the top right of the window, there is a 'Stop' button.</p>

- Eventually, you will start to see rows start appearing in the table starting with the oldest dates available.

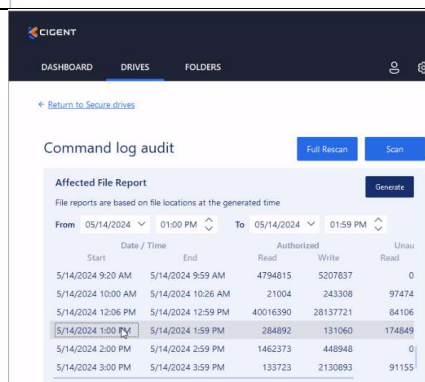
Once data is displayed, you can stop the retrieval, but it is suggested you wait until it is complete to see data from your previous activities as a result of following this guide.



- Once complete a popup will appear. Click Ok.

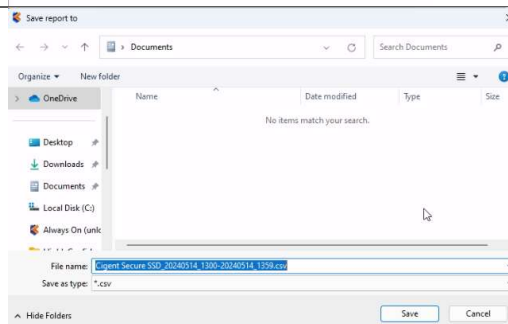


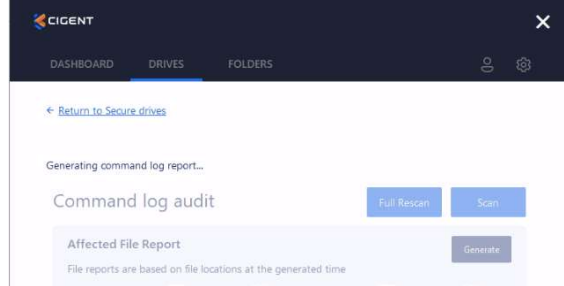
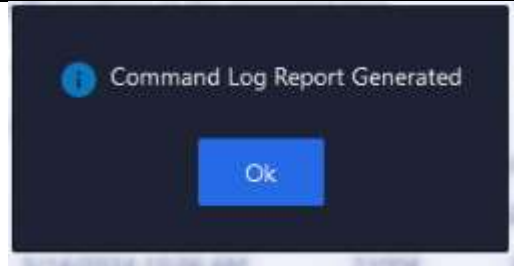
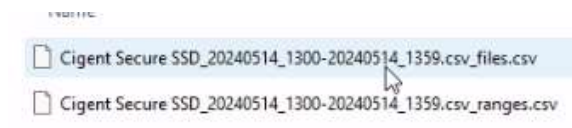
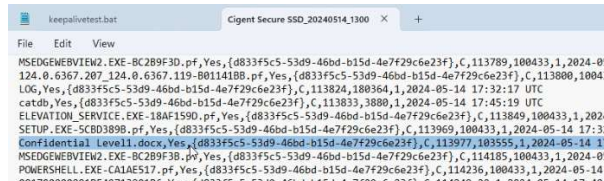
- Scroll to the end of the table and select a row that encompasses the times during which you were following this guide. Then click Generate.



- Click Save after choosing the report location and name.

You will be asked to authenticate.



<p>7. Data Defense will then process the command long and cross reference the file system with the access blocked to create an affected file report.</p>	
<p>8. Click Ok</p>	
<p>9. Find and open the file ending in csv_files.csv.</p>	
<p>10. Search the file for "Level1". Hopefully you will see an entry for the file used during this evaluation.</p>	

Authorized activities occurred while Data Defense was running. Unauthorized activities occurred without Data Defense running which can be during system start up or perhaps if the drive was accessed from another system while in an external enclosure. It does not necessarily mean the activity was malicious but can give clues as to how it was accessed.

