

# CIGENT SECURE SSD ADVANCED

USER GUIDE v1.2



PROUDLY FUNDED BY



## Table of Contents

Introduction.....	2
Purpose.....	2
Setup and Cigent for Windows Installation.....	3
Using Always On and Dynamic Drives.....	8
Locking and Unlocking Drives.....	8
Accessing Always On Files.....	9
Accessing Dynamic Files.....	10
Manage Cigent Settings.....	11
Authentication.....	13
License.....	14
Folder Protections.....	15
Microsoft Defender and Antivirus Integration.....	17
Network Manager.....	21
Cigent Secure SSD Advanced Features.....	23
Keep Alive.....	23
Command Audit Log (Cigent Plus Only).....	24
Verified Data Destruction (Cigent Plus Only).....	25

# CIGENT SECURE SSD ADVANCED USER GUIDE

## Introduction

The advanced cybersecurity defenses built into the operating firmware of Cigent Secure SSDs™ repel ransomware attacks and prevent data theft even when all other cybersecurity protections fail or are bypassed. When used in conjunction with Cigent® for Windows, Cigent Secure SSDs protect data throughout the entire device lifecycle—from provisioning to end-of-life—defending against a vast number of threat vectors.

Available in NVMe internal and external FIPS and non FIPS configurations, the Cigent Secure SSD Advanced is offered in four sizes—512GB, 1TB, 2TB, and 4TB (non FIPS only). It can be installed as the primary storage device on a Windows PC where the O/S runs, as secondary internal storage (such as in a desktop tower), or as external media plugged into a USB port.

Cigent for Windows (Cigent) is a new approach to data security, one that complements existing solutions and places the importance of protecting data above all else. Cigent takes concepts used in zero trust and continuous authentication and applies them as close to the data stream as possible, bringing proactive protection directly to your data. Cigent 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.

## Purpose

This document is a guide to help you install and configure your Cigent Secure SSD and associated Cigent software so you can start using it as quickly as possible. It also provides a basic operation overview and explanation for some of the security sensors if you are interested in learning more.

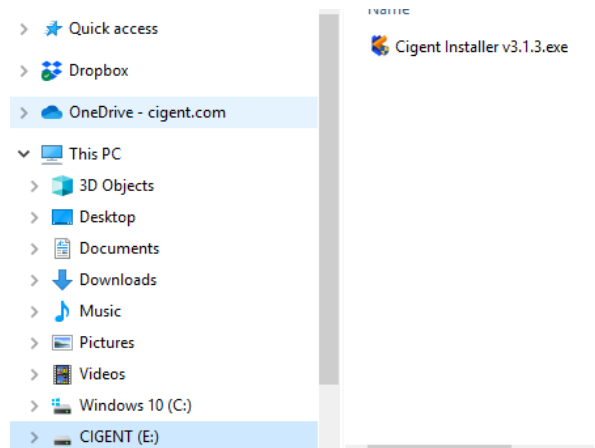
# SETUP AND CIGENT FOR WINDOWS INSTALLATION

This guide is applicable to either external or internal Secure SSD Advanced installed as secondary drives. Installing your Secure SSD Advanced as a primary (OS) drive will require cloning your existing installation to the Secure SSD Advanced or installing a fresh OS. These configurations are outside the scope of this guide, but setup and configuration are the same once installed.

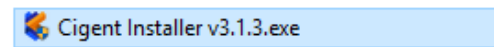
A copy of the Cigent installer is placed onto each Cigent Secure SSD before shipping.

1. Plug in your External Secure SSD or install the Internal Secure SSD into your system as a secondary drive.

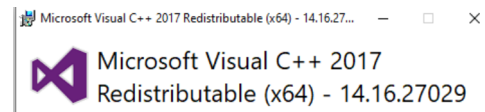
2. Open Windows Explorer and select the **CIGENT** partition.



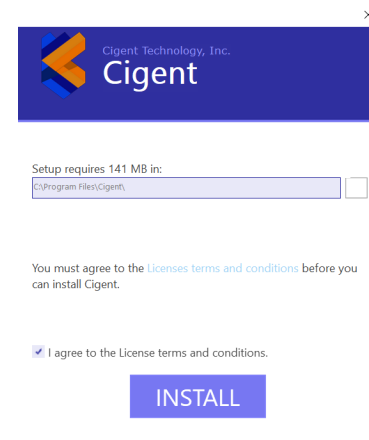
3. Double click the Cigent installer executable to begin the installation process. Note: The name of the installer may be slightly different.



**Note:** If Microsoft's Visual C++ Redistributable (x64) package is not already installed, you may be prompted to install it during the Cigent installation process. Please follow the simple instructions to complete the install of the package before proceeding.

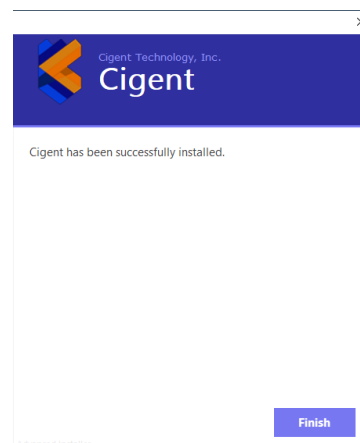


4. Select an installation location, accept the License terms then click Install.

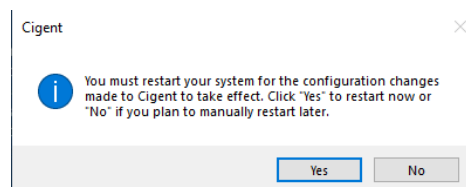


# SETUP AND CIGENT FOR WINDOWS INSTALLATION

5. Wait for the installation to complete. Click Finish to close the installer.

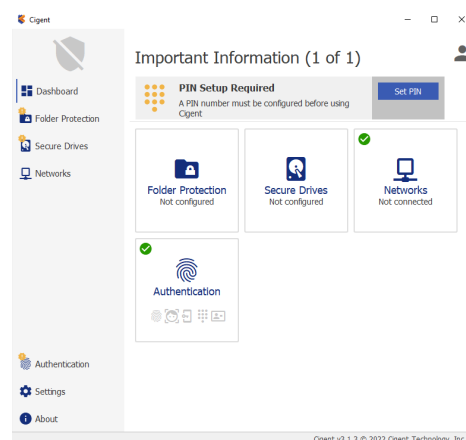


6. Click Yes to reboot for Cigent's changes to take effect.



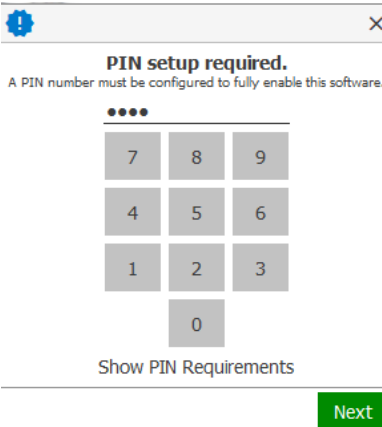
After rebooting, the Cigent dashboard with automatically open and request a PIN to be set.

7. Click Set PIN.

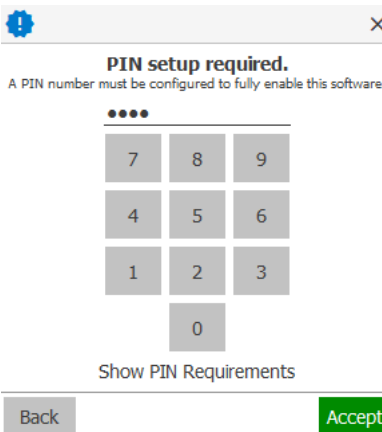


# SETUP AND CIGENT FOR WINDOWS INSTALLATION

8. Enter your PIN, click Next.

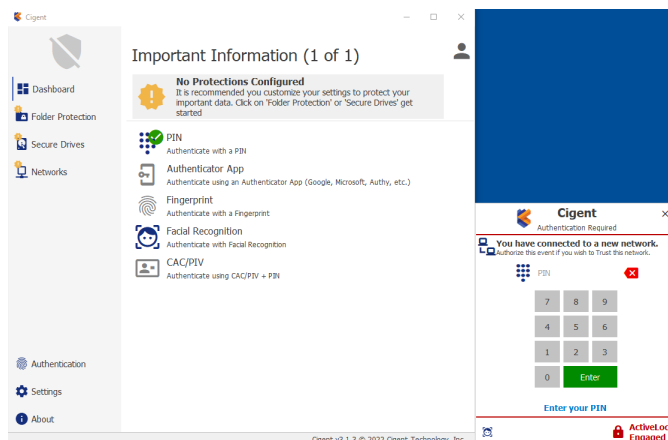
A dialog box titled "PIN setup required." with a blue information icon in the top left and a close button in the top right. The text inside says "A PIN number must be configured to fully enable this software." Below this is a 3x3 grid of buttons for digits 7, 8, 9, 4, 5, 6, 1, 2, 3, and a single button for 0. Above the grid are four dots indicating the PIN length. Below the grid is a link that says "Show PIN Requirements". At the bottom right is a green button labeled "Next".

9. Re-enter your PIN and click Accept.

A dialog box titled "PIN setup required." with a blue information icon in the top left and a close button in the top right. The text inside says "A PIN number must be configured to fully enable this software." Below this is a 3x3 grid of buttons for digits 7, 8, 9, 4, 5, 6, 1, 2, 3, and a single button for 0. Above the grid are four dots indicating the PIN length. Below the grid is a link that says "Show PIN Requirements". At the bottom left is a grey button labeled "Back", and at the bottom right is a green button labeled "Accept".

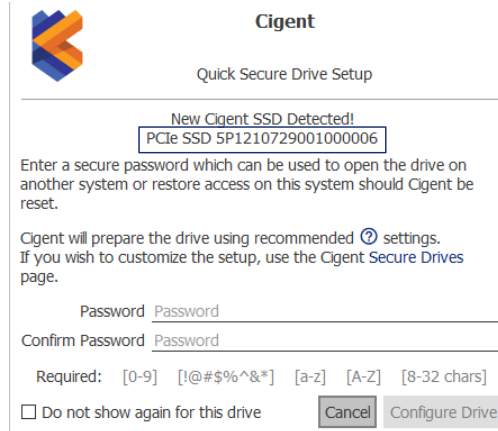
10. If you are currently connected to a network and your network is NOT set to Private in Windows, Cigent will engage Active Lock. If the network is secure, simply enter your PIN and click Enter to add the current network as Trusted. If you are not connected to a network at the time of installation, please just proceed to the next step.

**Note:** Cigent will automatically trust your first network if it is configured as Private in Windows.



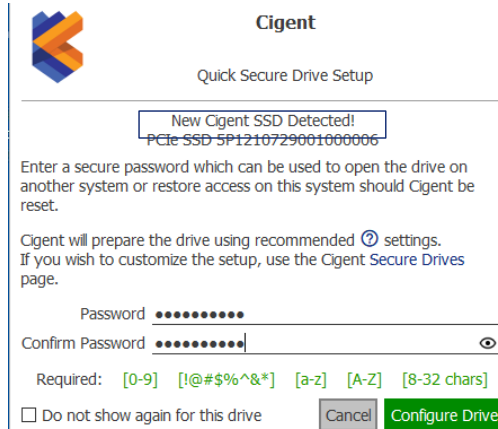
# SETUP AND CIGENT FOR WINDOWS INSTALLATION

**11.** If you have an external Cigent Secure SSD inserted or your internal SSD installed, the Quick Secure Drive Setup popup should appear.



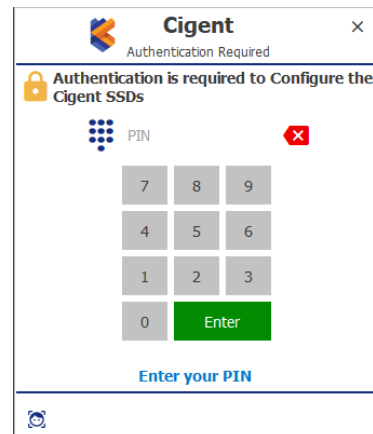
The screenshot shows the 'Cigent Quick Secure Drive Setup' window. At the top, it says 'New Cigent SSD Detected!' and displays the device ID 'PCIe SSD 5P1210729001000006'. Below this, it prompts the user to 'Enter a secure password which can be used to open the drive on another system or restore access on this system should Cigent be reset.' It then states 'Cigent will prepare the drive using recommended settings. If you wish to customize the setup, use the Cigent Secure Drives page.' There are two password input fields labeled 'Password' and 'Confirm Password'. Below the fields, it lists requirements: '[0-9] [!@#\$%^&\*] [a-z] [A-Z] [8-32 chars]'. At the bottom, there is a checkbox 'Do not show again for this drive', a 'Cancel' button, and a 'Configure Drive' button.

**12.** Enter a secure password twice and click Configure Drive to automatically configure the SSD to Cigent default configuration. If you wish to customize the settings, you can click Cancel and configure the drive from the Secure Drives page of the Cigent Dashboard.



This screenshot is similar to the previous one, but the password fields are now filled with dots. The 'Configure Drive' button is now highlighted in green, indicating it is the next step in the process.

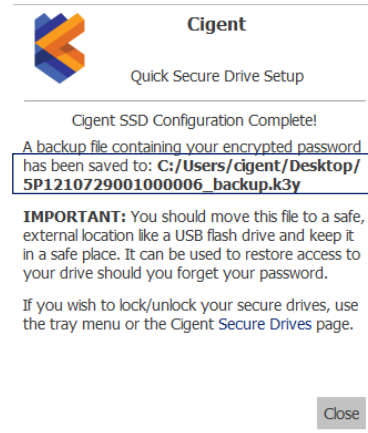
**13.** Enter your authentication PIN and click Enter to approve the SSD setup.



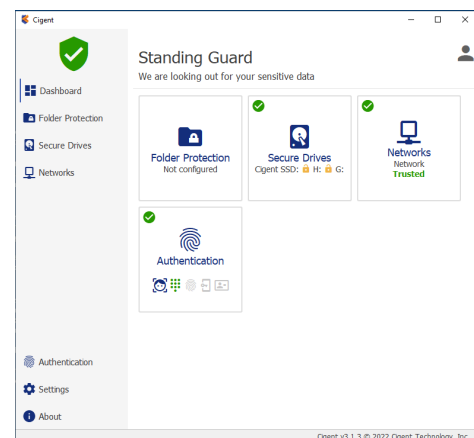
The screenshot shows the 'Cigent Authentication Required' window. It features a lock icon and the text 'Authentication is required to Configure the Cigent SSDs'. Below this is a PIN input area with a grid of numbers (0-9) and an 'Enter' button. A red 'X' icon is visible next to the PIN input area. At the bottom, there is a blue link that says 'Enter your PIN'.

# SETUP AND CIGENT FOR WINDOWS INSTALLATION

**14.** Note the location of the encrypted password file. This file should be moved to a secure location off of the host for security purposes. Click Close when you are ready.



**15.** Once complete, the Cigent dashboard will show the drive letters of the newly created Secure Drives. They are automatically unlocked after setup to allow you to start copying files to them immediately.



## Congratulations

You have completed the steps necessary to begin using your Cigent Secure SSD and Cigent software.

# USING ALWAYS ON AND DYNAMIC DRIVES

There are two types of file protection modes available.

## Files on Always Drives

- Files remain locked under all conditions
- Step-up authentication is required to access the file every time
- Designed for extremely sensitive information
- Drive is locked (unmounted) when a threat has been detected and must be manually unlocked afterwards

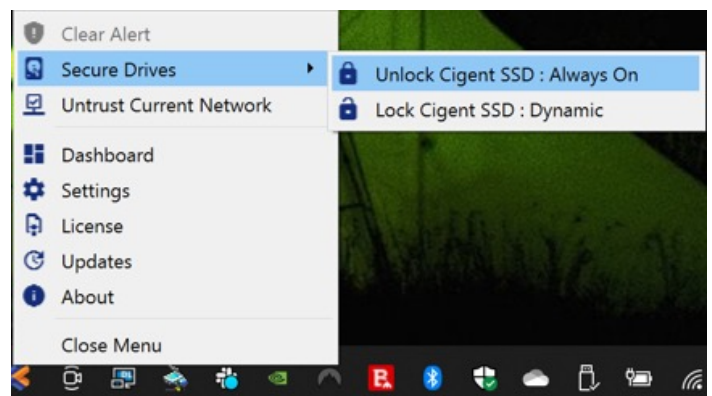
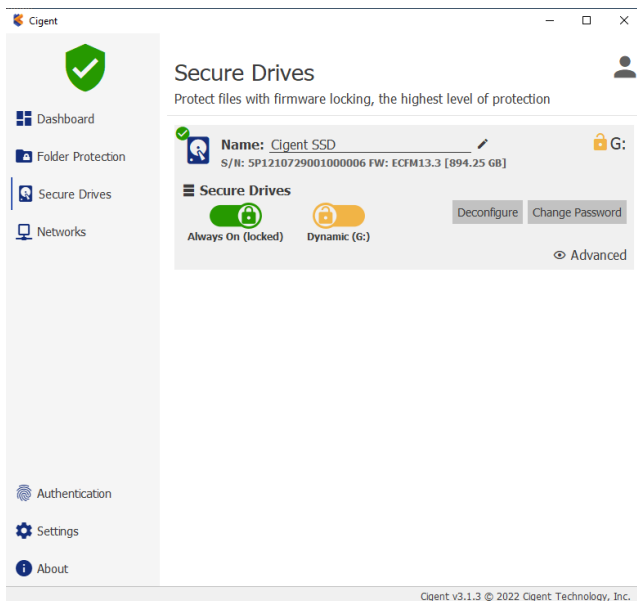
## Files on Dynamic Drive

- Files are locked only if a threat has been detected
- Provides strong protection in a minimally invasive manner—the user is prompted to authenticate only if access to a locked file is attempted
- Designed for files that require frequent or bulk access like Source code.
- Drive is locked (unmounted) when a threat has been detected and automatically unlocked (by default.)

## Locking and Unlocking Drives

You can lock and unlock Secure Drives using either the Secure Drives page of the Cigent Dashboard or the quick menu (right click Cigent tray icon.)

- Unlocking a drive always requires authentication but locking does not.
- By default the Dynamic drive will automatically unlock on startup and after a threat clears. This can be changed in the settings.

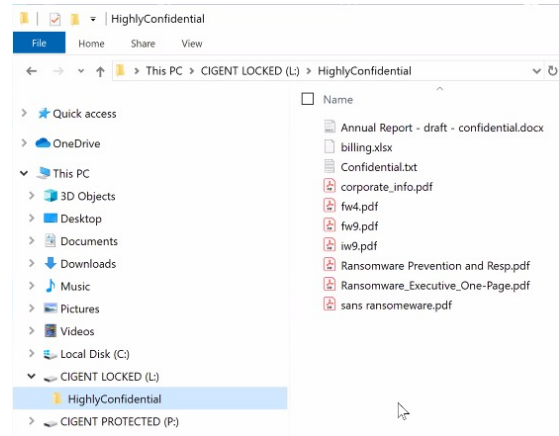




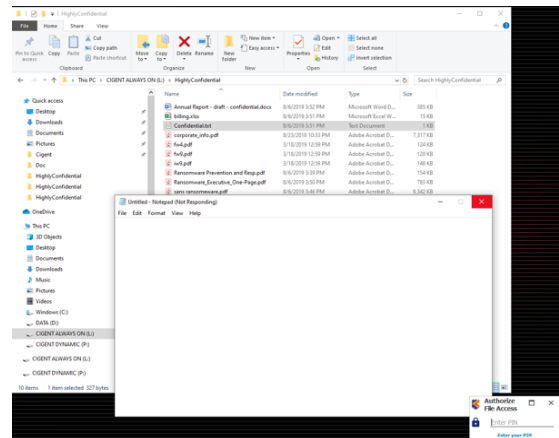
# USING ALWAYS ON AND DYNAMIC DRIVES

## Accessing Always On Files

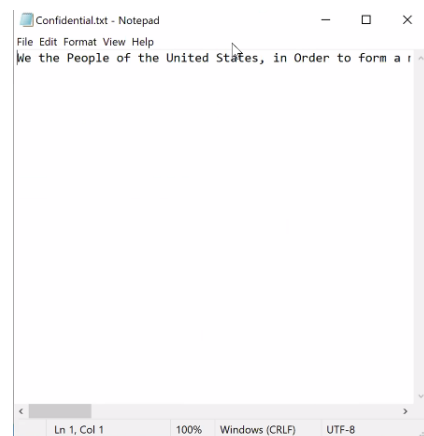
1. In Windows Explorer, browse to your Always On drive (usually L:) (If your L: drive is not visible, you must unlocked it before proceeding.)



2. **Double click** on a file to open it. Regardless of the Active Lock state, Cigent will require authentication to open any file on the Locked drive.



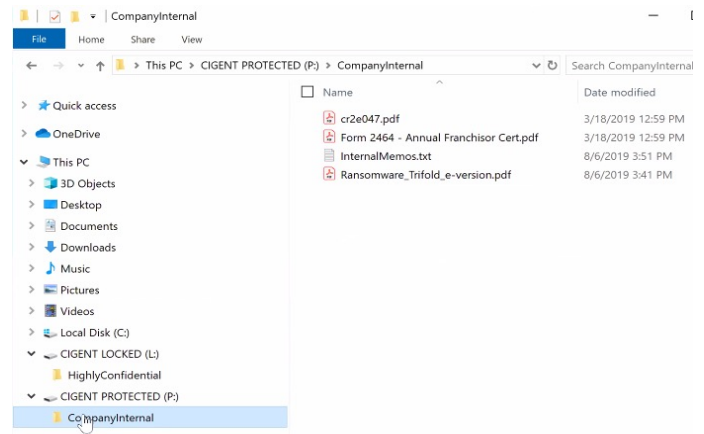
3. Enter your PIN and click **Enter**. Your file will then open.



# USING ALWAYS ON AND DYNAMIC DRIVES

## Accessing Dynamic Files

1. In Windows Explorer, browse to your Dynamic Drive (usually P:)

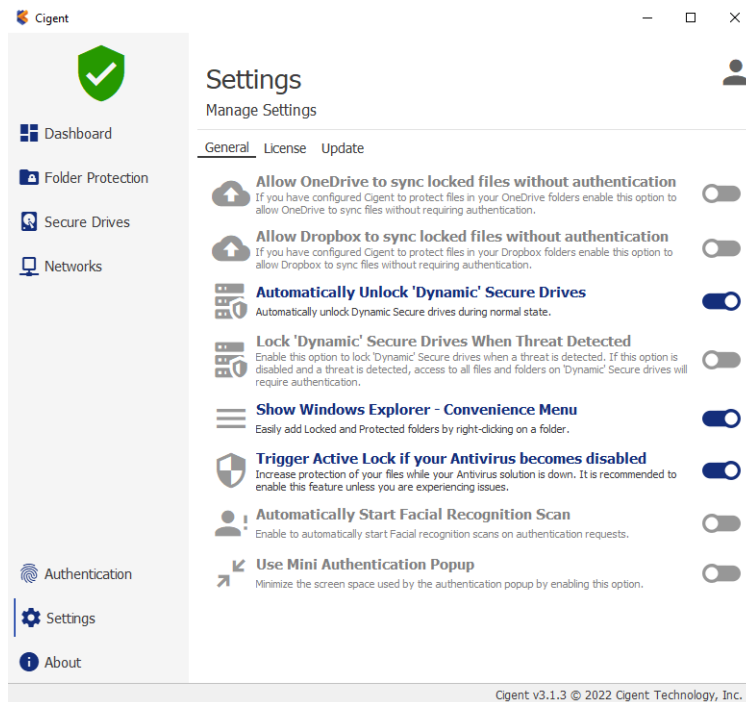


2. **Double click** on a file to open it.

3. Since the file resides on the Dynamic drive, the file will open without requiring a second factor authentication unless there is an Active threat and the system is in Active Lock.

# MANAGE CIGENT SETTINGS

The Cigent Setting page allows you to customize different aspects of Cigent and Cigent Secure SSD operations. This section is a quick explanation of each setting. Those proceeded with an asterisk(\*) are particularly important or useful.



## Allow OneDrive to sync locked file without authentication

Enable these options if you use either of these Cloud File storage solutions and have added an Always On folder being synchronized by these applications.

## \*Automatically Unlock Cigent Dynamic Secure Drives

Enable to have Cigent automatically unlock (mount) your Dynamic drive (if configured) after system restarts and a threat clears.

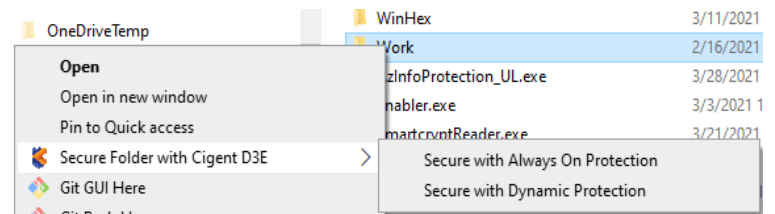
## \*Lock Cigent Dynamic Secure Drives When Threat Detected

Disable this option if you want the Dynamic drive to remain unlocked (mounted) even during a threat state. Note however that files will still be protected by requiring a second factor authentication similar to Always On files until the threat is cleared.

# MANAGE CIGENT SETTINGS

## Show Windows Explorer – Convenience Menu

This setting determines if the right-click convenience menu is active in Windows Explorer. Users can easily add protections to folders using this method.



## Trigger Active Lock if your Antivirus becomes disabled

This setting determines if Cigent should engage Active Lock should your AV become disabled. You should ONLY disable this setting if your AV is not detected by Cigent for some reason.

## Automatically Start Facial Recognition Scan

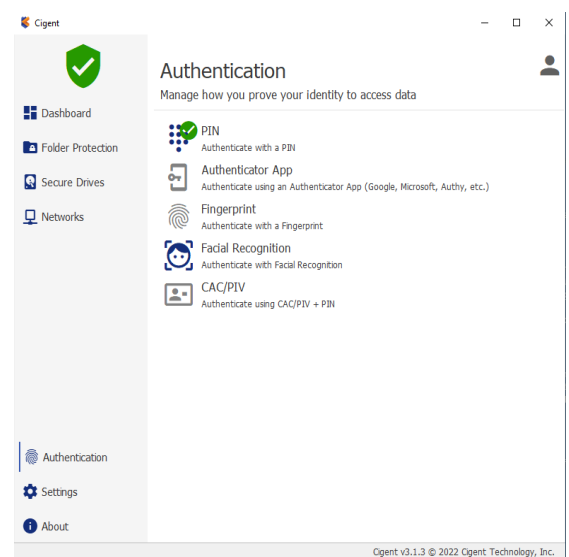
When Facial Recognition is being used for authentication, scanning will automatically start when this setting is enabled.

## \*Use Mini Authentication Popup

When enabled, this setting reduces the size of the popup authentication window and include minimal information. When PIN is enabled, users can type their PIN using the keyboard instead of clicking the numbers using a mouse.

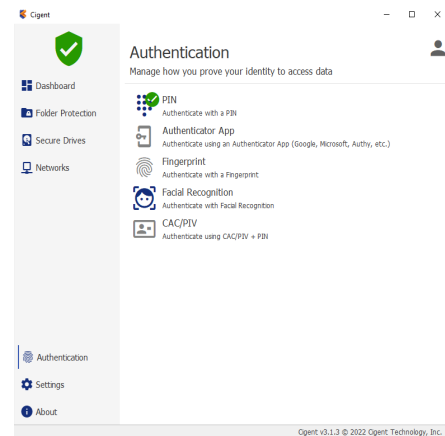
## Authentication

Opening protected files, unlocking Cigent Secure Drives and making configuration changes all require providing a second factor of authentication. Cigent provides several options with additional enterprise options available in Cigent Plus.



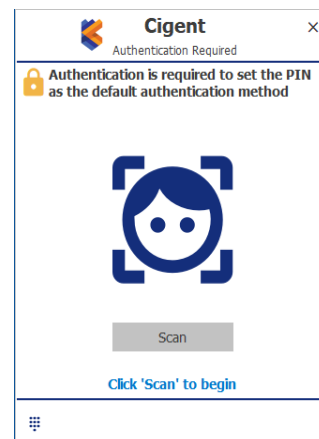
# AUTHENTICATION

Opening protected files, unlocking Cigent Secure Drives and making configuration changes all require providing a second factor of authentication. Cigent provides several options with additional enterprise options available in Cigent Plus.



## PIN

PIN is the default and must be at least 4 numbers in length. Even if you change the primary authentication to something else, you can always switch back to PIN by clicking the keypad icon in the authentication popup



## Authenticator App

Authenticator App enables the use of popular mobile authentication applications from Google, Microsoft, Authy and more. Once configured, application will display a rotating six digit PIN that must be entered into Cigent before it changes (usually 1 minute.)

## Fingerprint and Facial Recognition

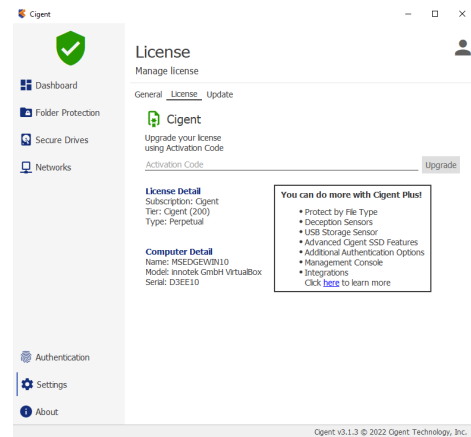
Both Fingerprint and Facial recognition use the Windows Hello APIs to work. If your system supports either of these options, click the Setup button to complete the configuration via the Hello UI. Once complete, return to Cigent and select Default to change to this form of authentication to be used. Again, you can always use PIN by selecting the keypad in the authentication popup.

## CAC/PIV

Common Access Card/Personal Identity Verification is an identification card issued by a federal agency that contains a computer chip which can be used to identify and validate a user using a PIN stored on the card. A CAC card reader is required and the CAC must be activate and valid.

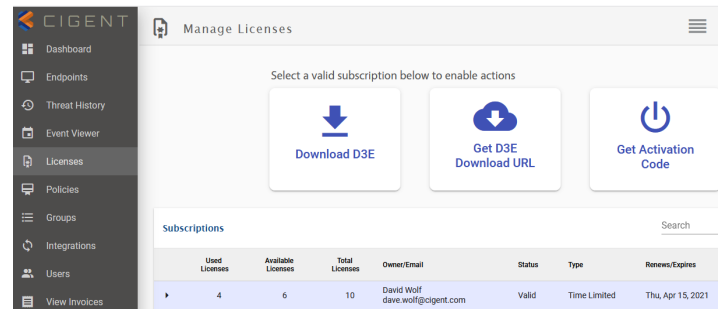
# LICENSE

Cigent can be upgraded to Cigent Select or Cigent Plus to gain access to additional protections, integrations and enterprise management features. For more information on Cigent Select and Cigent Plus, please visit: <https://www.cigent.com/product>



## PIN

Administrators of Cigent Plus can obtain an Activation Code from the Licenses page of the Central Cigent console at <https://central.cigent.com>.



Provide this Activation code to users to enter into the Cigent license page. Cigent will automatically register to the subscription and start enforcing settings specified by configured policies.

# FOLDER PROTECTIONS

Cigent can also provide protection to files residing in folders not located on Cigent Secure Drives however these files are not protected when Cigent is not running or present. This can be useful for protecting the portion of your important files that must reside on your OS (C:) drive for example.

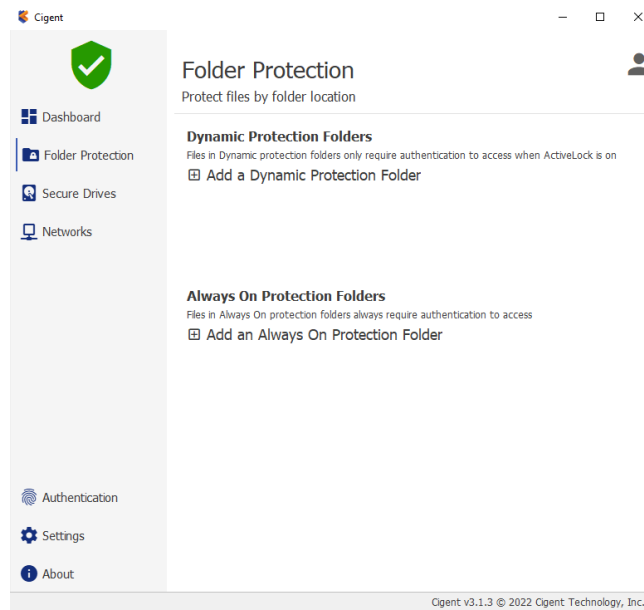
Folder protections follow the same paradigm as Cigent Secure Drives.

## Files on Always Drives

- Files remain locked under all conditions
- Step-up authentication is required to access the file every time
- Designed for extremely sensitive information

## Files on Dynamic Drive

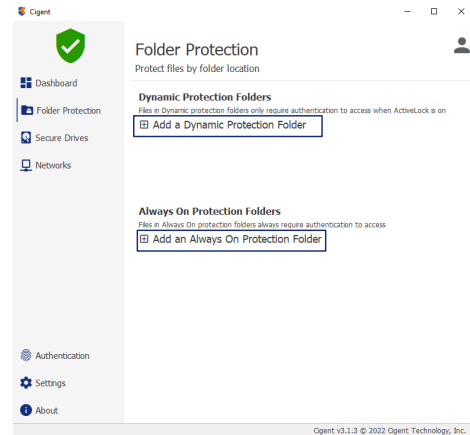
- Files are locked only if a threat has been detected
- Provides strong protection in a minimally invasive manner—the user is prompted to authenticate only if access to a locked file is attempted
- Designed for files that require frequent or bulk access like Source code.



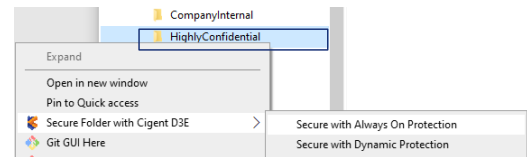
# FOLDER PROTECTIONS

Folder protection can be added in two ways:

1. By clicking on the desired “Add ...” link on the Folder Protection page, selecting the folder in the Explorer window and clicking Select folder.



2. Using the menu from Windows Explorer itself. Right click on the folder, select “Secure Folder with Cigent” menu and the desired protection level from the sub menu.





# MICROSOFT DEFENDER AND ANTIVIRUS INTEGRATION

In the following optional sections, we will explore Cigent sensors and their impact on Dynamic and Always On drives and files stored on them.

Cigent is integrated with Microsoft Defender® and other Antivirus solutions registered with Windows Security Center adding additional protection in case of a threat or attack. Cigent will initiate Active Lock if:

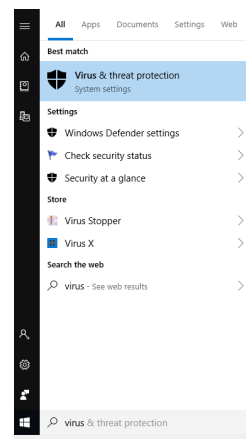
1. Microsoft Defender detects a threat
2. Microsoft Defender or AV is shutdown or disabled

## Disabling Microsoft Defender or other Antivirus solution

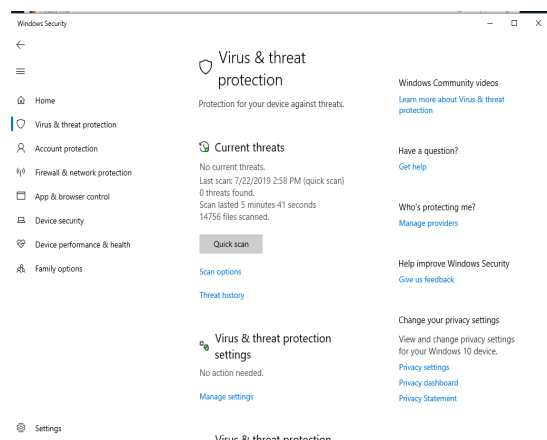
Attackers will often first disable the existing AV solution in order to make it easier to proceed with the attack. Cigent constantly monitors the status of Microsoft Defender or other AV solutions and will initiate Active Lock when it is no longer running or has detected a threat. This section details the steps for exercising this sensor using Microsoft Defender but you can accomplish the same using whatever your AV solution.

### Manually stopping Microsoft Defender

1. Search in the start menu for “Virus & threat protection”. Select the item to open System Settings.

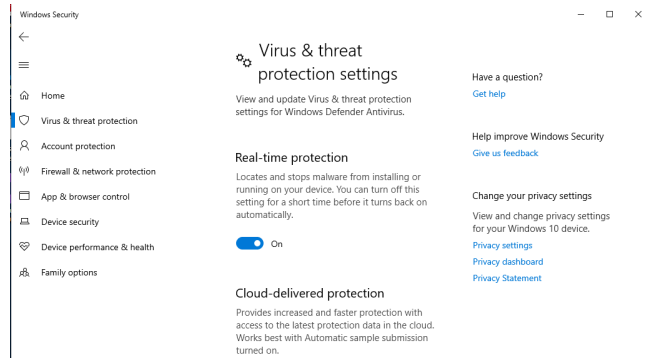


2. Select “Manage Settings”



# MICROSOFT DEFENDER AND ANTIVIRUS INTEGRATION

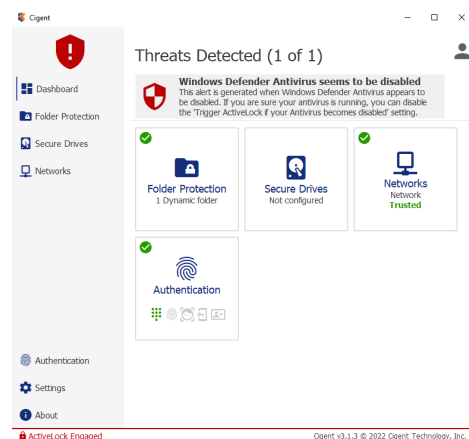
3. Turn off Real-Time protection using the slider.



4. Select Yes to allow the action to complete.

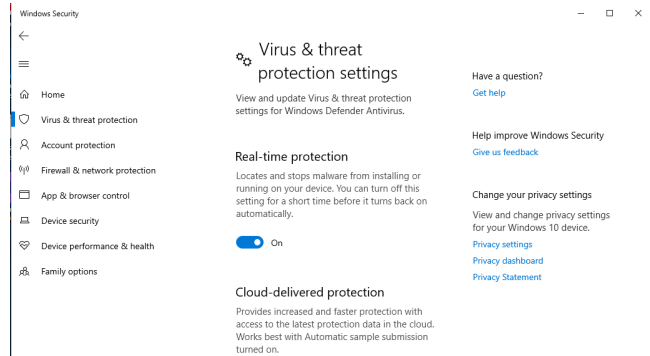


5. Minimize the Windows Security window and return to the Cigent dashboard. Note that Active Lock was immediately engaged. The Dynamic and Always On drives have automatically been locked.

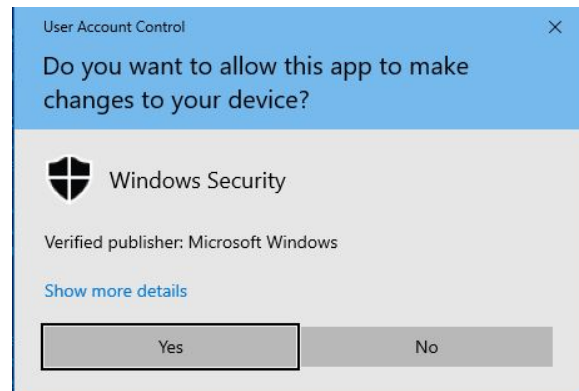


# MICROSOFT DEFENDER AND ANTIVIRUS INTEGRATION

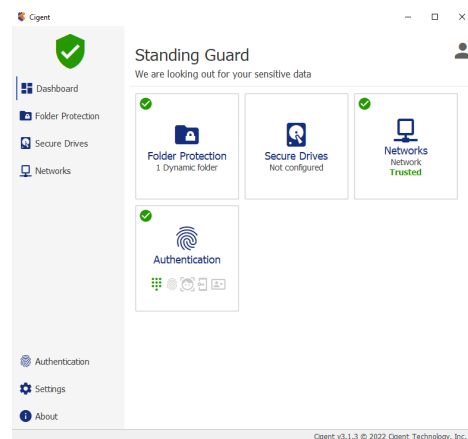
6. Return to the Windows Security window and re-enable Real-time.



Select Yes to allow the action to complete.

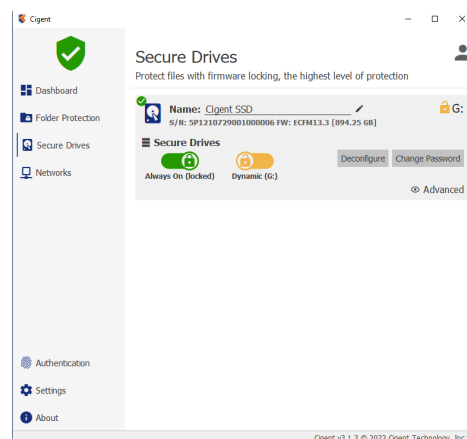


7. The security status is now clear. Notice the Cigent icon in the tray has returned to normal.

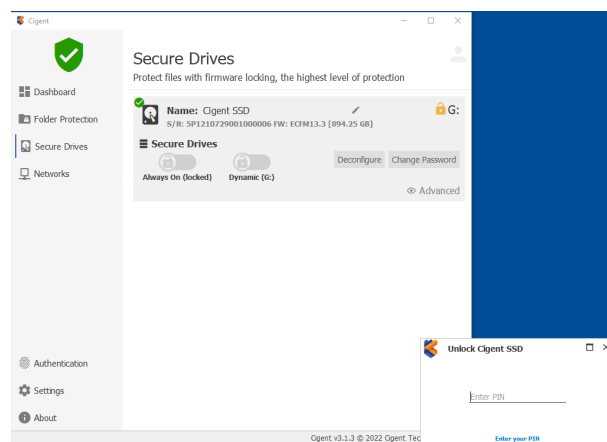


# MICROSOFT DEFENDER AND ANTIVIRUS INTEGRATION

1. Select the Secure Drives tile and select your drive. Notice that P: has automatically been unlocked but L: remains in locked state.



2. Unlock the L: drive. Slide the switch next to L:, enter your PIN and click Enter.



# NETWORK MANAGER

The Network Manager system prevents unauthorized network devices from establishing connections to your protected system. Among the many events that will engage Active Lock are:

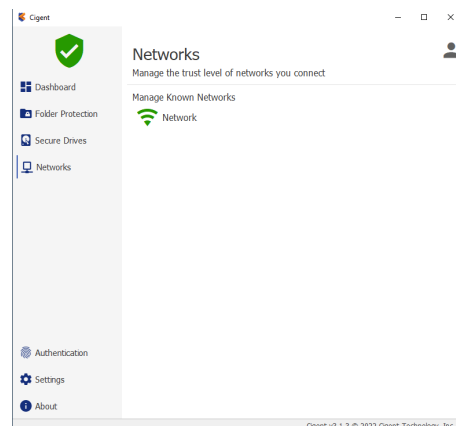
- You join a network that has not been previously trusted
- A network device scans your host for open ports and connects to a Cigent deception port.
- An untrusted network device attempts to connect to your device on any port.

Note: This entire section can only be completed if your installation is connected to a network. It does NOT need internet access but simply a valid network IP address.

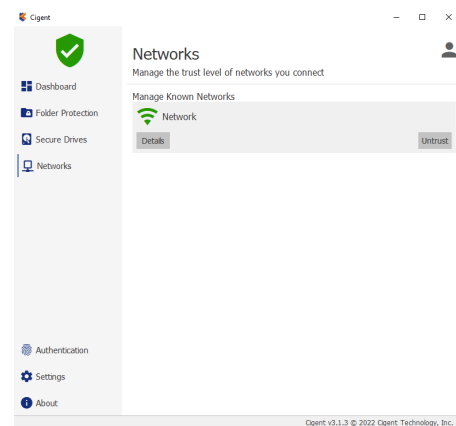
## Untrusting your current network

You can simulate the effects of joining a network that has not previously been trusted by simply untrusting the network on which you are currently connected. This will cause Active Lock to be engaged.

1. Open Cigent and select the Networks menu.

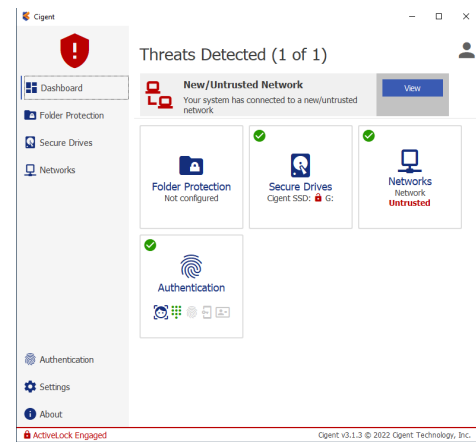


2. Select the active network and click on the Untrust button.

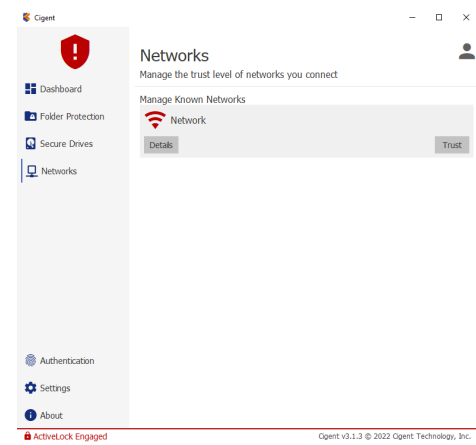


# NETWORK MANAGER

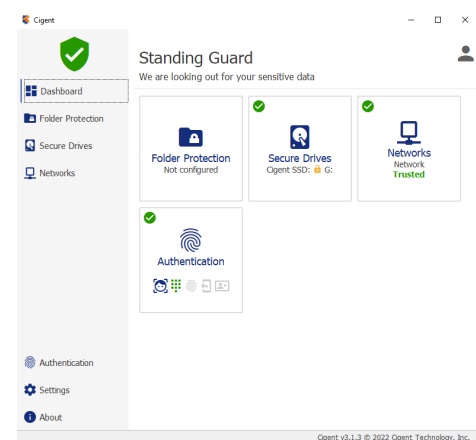
3. Switch back to the Dashboard. Note that Active Lock is engaged.



4. Return to the Networks page and click TRUST under your current network. You will need to enter your PIN.



5. Switch back to the Dashboard page and note that Active Lock is disengaged.

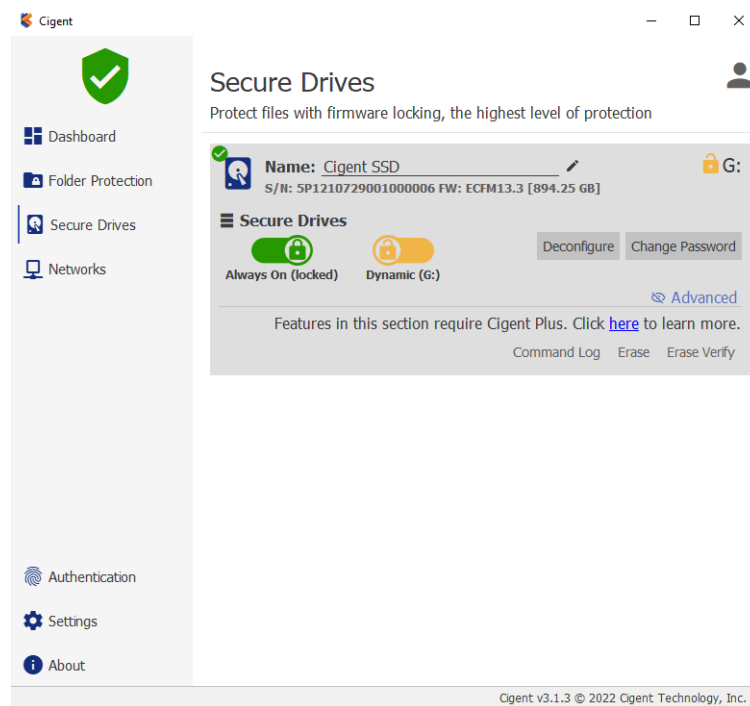


# CIGENT SECURE SSD ADVANCED FEATURES

## Keep Alive

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

Keep Alive is automatically enabled by the Quick Secure Drive setup process. You can confirm Keep Alive is enabled by the presence of a heart icon on the drive icon on the Secure Drives page.



Testing Keep Alive functionality is beyond the scope of this document. You can find information on testing this feature in the larger Cigent Evaluation Guide found on the Cigent website resources page: <https://www.cigent.com/resources>

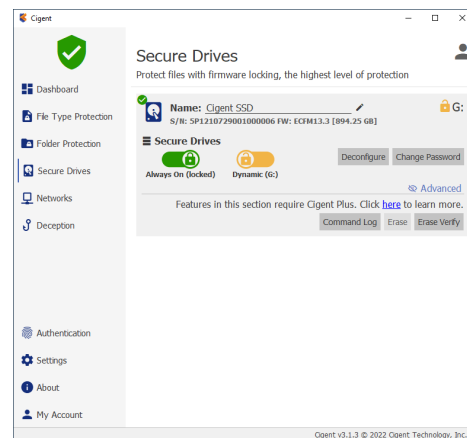
# CIGENT SECURE SSD ADVANCED FEATURES

## Command Log Audit (Cigent Plus Only)

Cigent Secure SSDs automatically store every command sent to the drive in a tamperproof location in memory on the drive. Cigent also periodically writes markers to the log to indicate the activity was performed with Cigent running and that the activity was properly authorized. Commands are stored for all partitions including unsecured locations should the user have configured a portion of the drive as a normal NTFS partition.

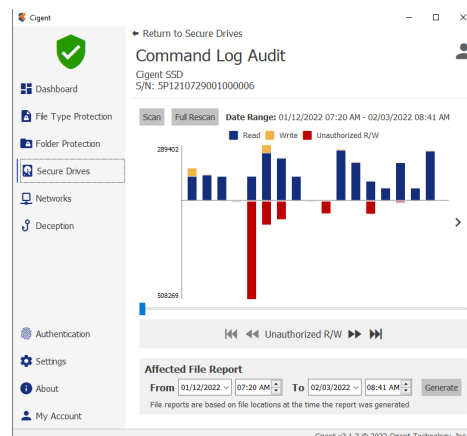
This command log can be used to audit drive activity to capture attempts to read information from the drive while not under the protection of Cigent, possibly indicating attempts to circumvent file protection. Further, the command log can be used to report on files accessed with or without Cigent running 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 what files were attempted to be accessed.

1. Select the Cigent Secure SSD and click Advanced to reveal the advanced features.



2. Click Command Log to open the Command Log Audit page. Click Scan to initiate the reading of the command log.

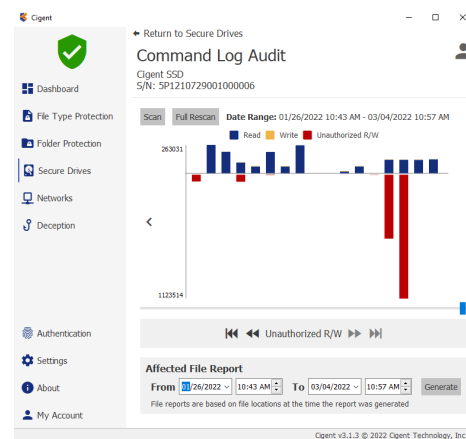
**Note:** Reading the command log from the drive over USB especially can take several minutes.



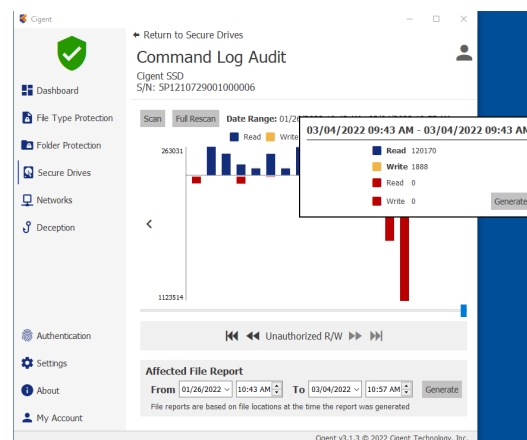


# CIGENT SECURE SSD ADVANCED FEATURES

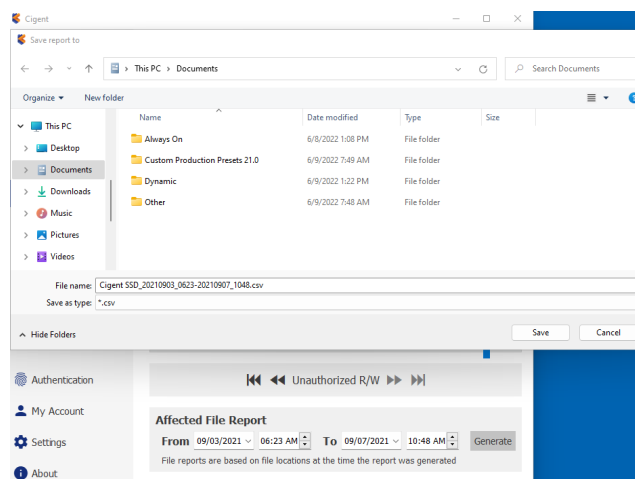
3. If this is a relatively new drive, you may have only a few data points. If this drive has been in use for a while, you may need to scroll the graph to the right using slider to get to the newest information.



4. Click on a shorter bar in the graph to receive some details as the counts of each operation.

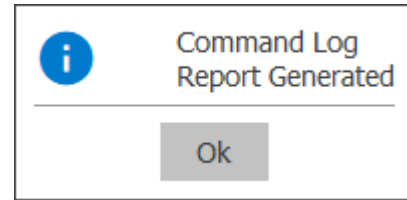


5. Click the Generate button to create a CSV file containing files to which the commands log entries currently map. Click Save and enter your PIN to authorize the action.



# CIGENT SECURE SSD ADVANCED FEATURES

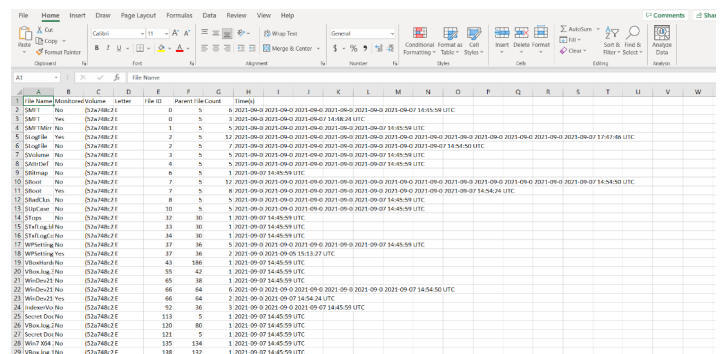
6. Click OK once the operation completes.



7. Open the file using a text editor or Excel.

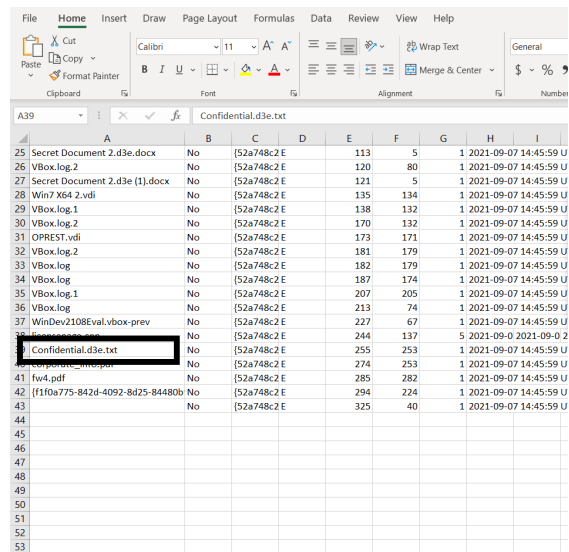
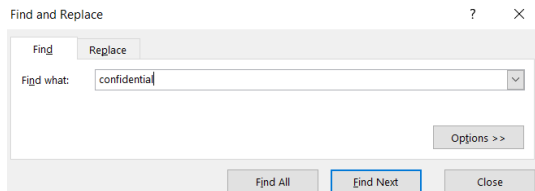
The columns of major importance are:

- A. Time - In UTC that the activity occurred.
- B. Monitored – If Cigent was active or not.  
(Filter to No for unauthorized activity)
- C. File Name – Name of the file accessed.



File Name	Monitored	File Size	Parent File Count	Time (UTC)
...	...	...	...	...

**Note:** You will see many files used by Windows that are usually hidden from users.



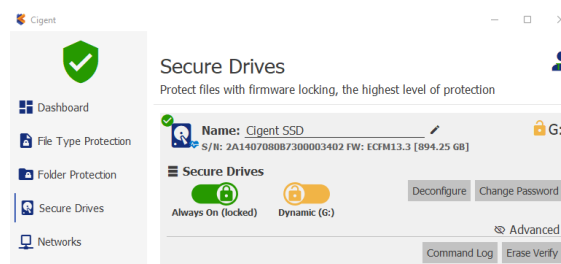
File Name	Monitored	File Size	Parent File Count	Time (UTC)
...	...	...	...	...

# CIGENT SECURE SSD ADVANCED FEATURES

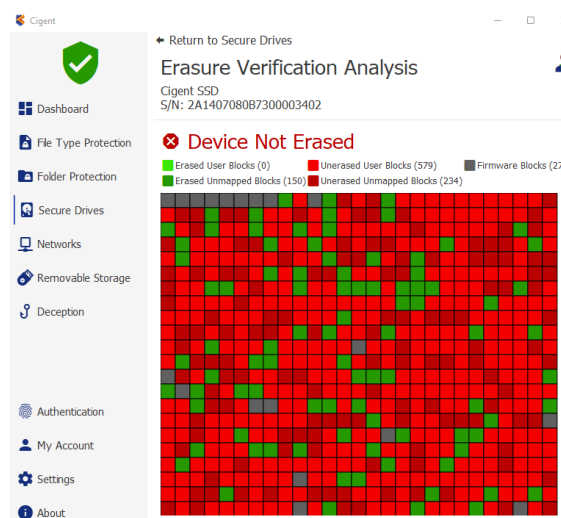
## Verified Data Destruction (Cigent Plus Only)

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 Secure SSDs 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 Cigent confirms the drive has been truly erased, it can be safely and securely reused.

1. Select the Cigent Secure SSD and click Advanced to reveal the advanced features.



2. Click Erase Verify.



# CIGENT SECURE SSD ADVANCED FEATURES

1. Cigent will indicate Drive Not Erased (as expected) with a count of erased and non-erased blocks from the unmapped and user areas. The map at the bottom is a logical display of the blocks by block number and color coded by its status.

Testing complete data erasure is beyond the scope of this document however feel free to experiment with different data destruction methods and see if you are able to achieve the 'Erasure Confirmed' message as seen below.

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

