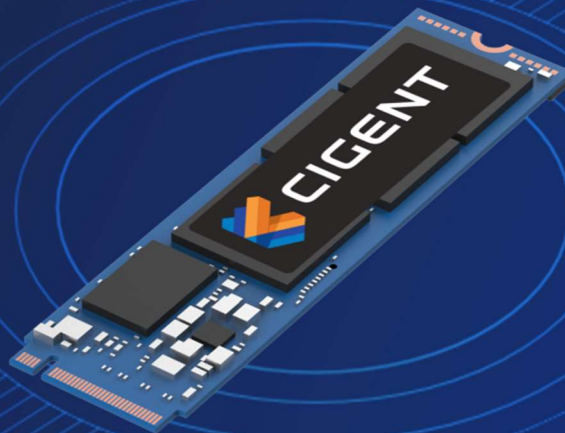




CIGENT DATA DEFENSE FOR CIGENT SECURE SSDs

USER GUIDE v1.0



November 2022

V1

Cigent Secure SSD

Cigent Data Defense Version 3.2.10

Contents

1 Introduction..... 3

2 Purpose..... 3

3 Setup and Installation..... 4

 3.1 Compatibility with Cigent PBA software 4

4 Using Always On and Dynamic Drives 12

 4.1 Locking and Unlocking Drives..... 12

 4.2 Accessing Always On Files 13

 4.3 Accessing Dynamic Files 15

5 Manage Cigent Settings..... 16

6 Authentication..... 18

7 License 20

8 Folder Protections 21

9 Network Manager 23

10 Cigent Secure SSD Advanced Features..... 26

 10.1 KeepAlive..... 26

 10.2 Command Log Audit 27

 10.3 True Erase 30

1 Introduction

The Cigent Secure SSD operating firmware includes cybersecurity defenses that repel ransomware attacks and data theft — even when all other cybersecurity protections fail. In conjunction with Cigent Data Defense software (Cigent), Cigent Secure SSDs protect data throughout the entire device lifecycle—from provisioning to end-of-life—defending against a vast number of threat vectors.

Cigent Secure SSDs 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 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 threat containment 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.

2 Purpose

This document is a guide to help you install and configure your Cigent Secure SSD and associated Cigent Data Defense 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.

3 Setup and Installation

This guide is applicable to Cigent Secure SSDs installed internally as primary or secondary drives or externally.

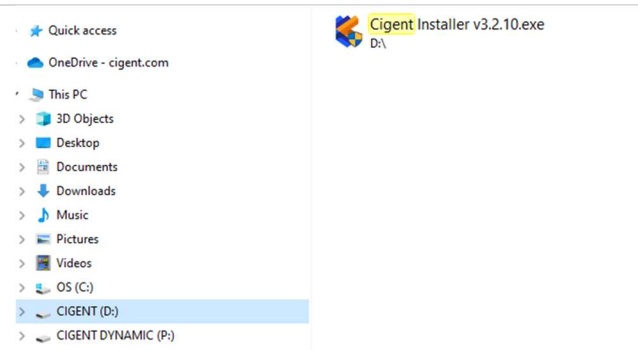
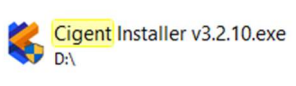
3.1 Compatibility with Cigent PBA software

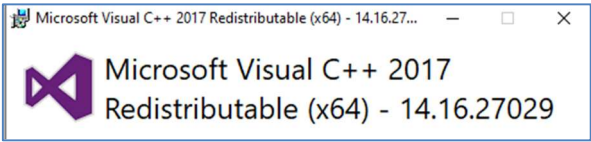
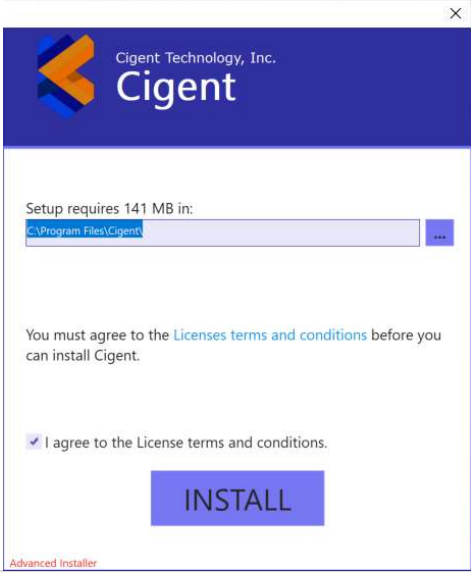

Cigent Data Defense software can be used on systems with or without Cigent PBA software, however there are some requirements and differences when used together. The main requirements and differences are listed below and will also be noted throughout the guide.

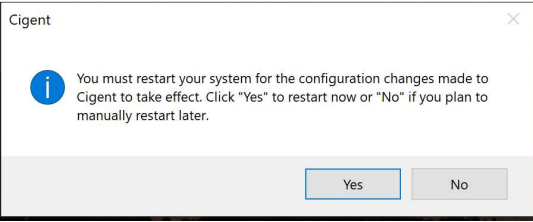
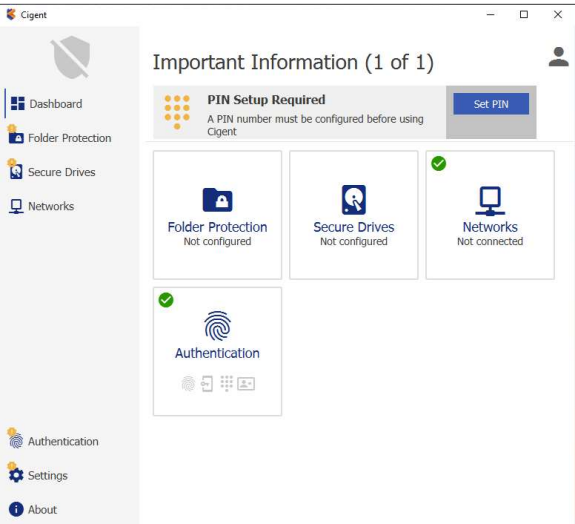
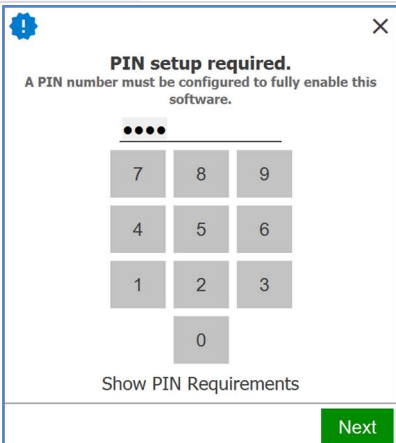
1. Cigent PBA software must be installed before installing Cigent Data Defense software.
2. Authentication for Secure Drive operations (creation, deletion and unlocking) uses Cigent PBA credentials instead of Cigent Data Defense authentication.
3. Creation and deletion of Secure Drives requires a Cigent PBA administrator account.

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

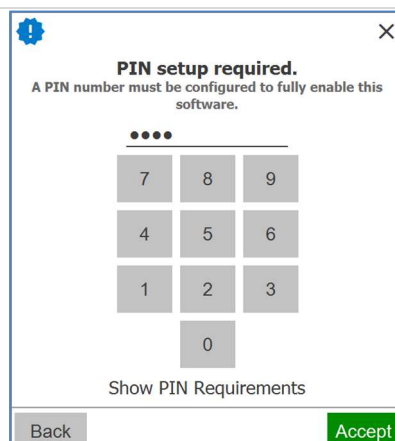
The latest versions of Cigent software can always be found at <https://www.cigent.com/support>

1. Install the Cigent Secure SSD into your system.	
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	

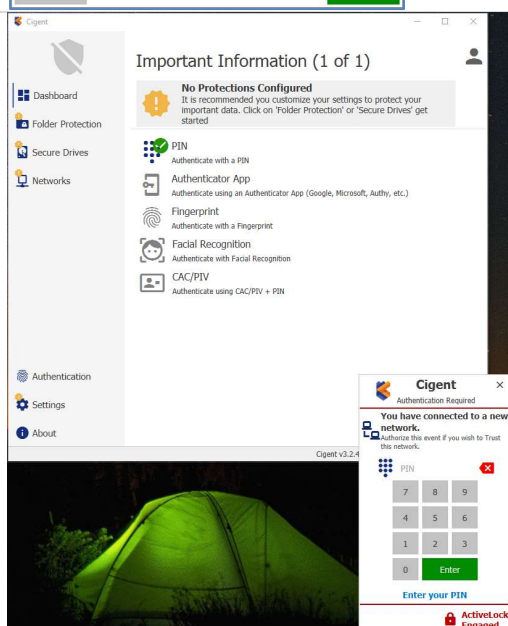
<p>slightly different.</p>	
<p>Note : If Microsoft's Visual C++ Redistributable (x64) package is not already installed, you may be prompted to install it during the Cigent installation process. Please follow the simple instructions to complete the install of the package before proceeding.</p>	 <p>The screenshot shows a Windows window titled "Microsoft Visual C++ 2017 Redistributable (x64) - 14.16.27029". It features the Microsoft logo and the text "Microsoft Visual C++ 2017 Redistributable (x64) - 14.16.27029".</p>
<p>4. Select an installation location, accept the License terms then click Install.</p>	 <p>The screenshot shows the "Cigent" Advanced Installer window. It displays the Cigent logo and "Cigent Technology, Inc." at the top. Below, it states "Setup requires 141 MB in:" followed by a text box containing "C:\Program Files\Cigent\" and a browse button "...". A message says "You must agree to the Licenses terms and conditions before you can install Cigent." There is a checked checkbox "I agree to the License terms and conditions." and a large blue "INSTALL" button. The text "Advanced Installer" is visible in the bottom left corner.</p>
<p>5. Wait for the installation to complete. Click Finish to close the installer.</p>	 <p>The screenshot shows the "Cigent" Advanced Installer window after successful installation. It displays the Cigent logo and "Cigent Technology, Inc." at the top. The main text says "Cigent has been successfully installed." There is a blue "Finish" button in the bottom right corner. The text "Advanced Installer" is visible in the bottom left corner.</p>

<p>6. Click Yes to reboot for Cigent's changes to take effect.</p>	
<p>After rebooting, the Cigent dashboard will automatically open and request a PIN to be set.</p>	
<p>7. Click Set PIN.</p>	
<p>8. Enter your PIN, click Next.</p>	

9. Re-enter your PIN and click **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.

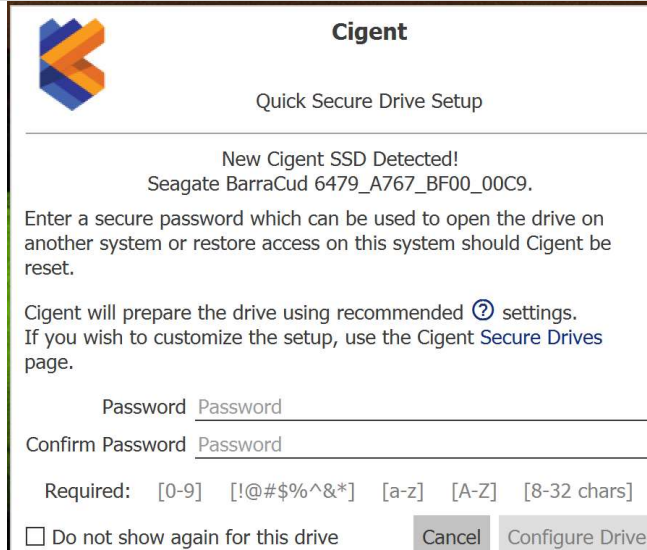



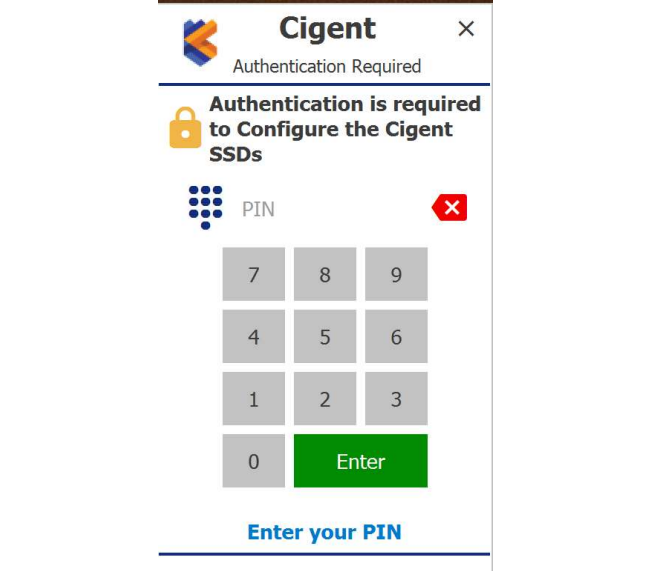
11. If you have an external Cigent Secure SSD inserted or your internal Cigent Secure SSD installed, the Quick Secure Drive Setup popup should appear.


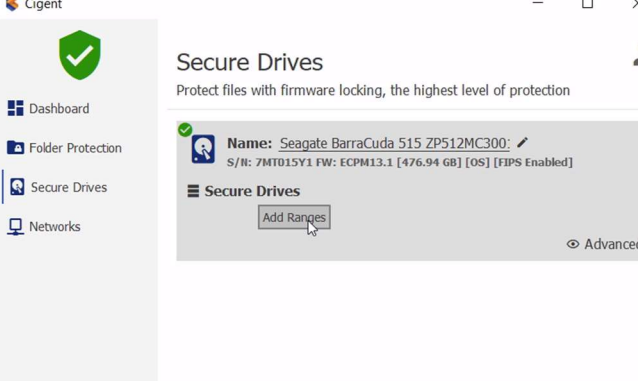
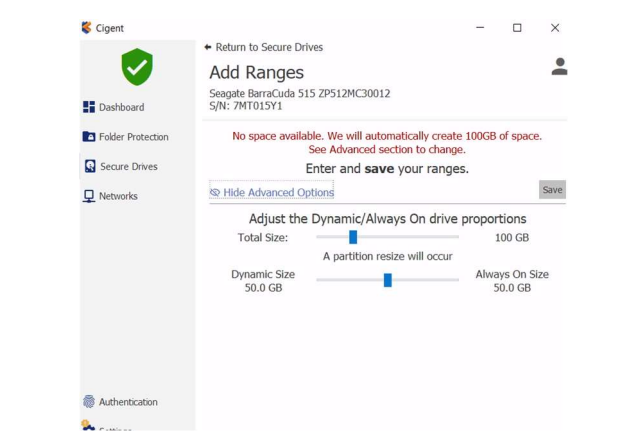


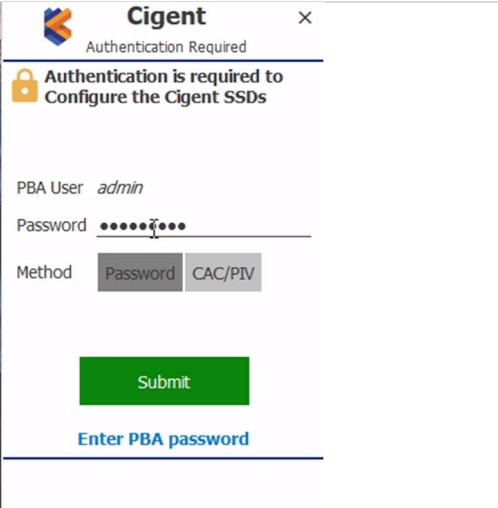
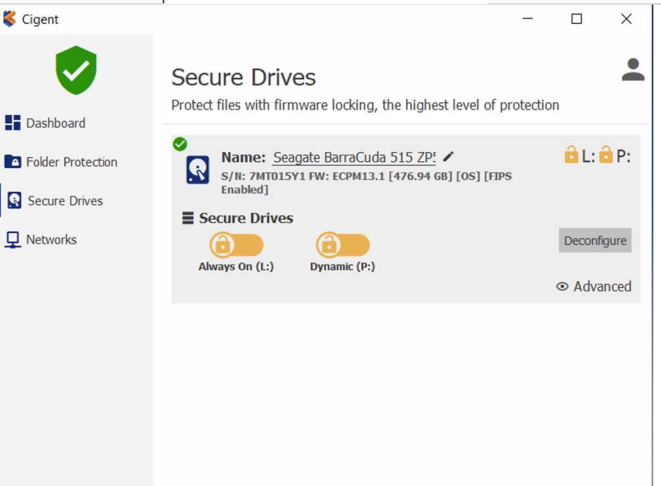
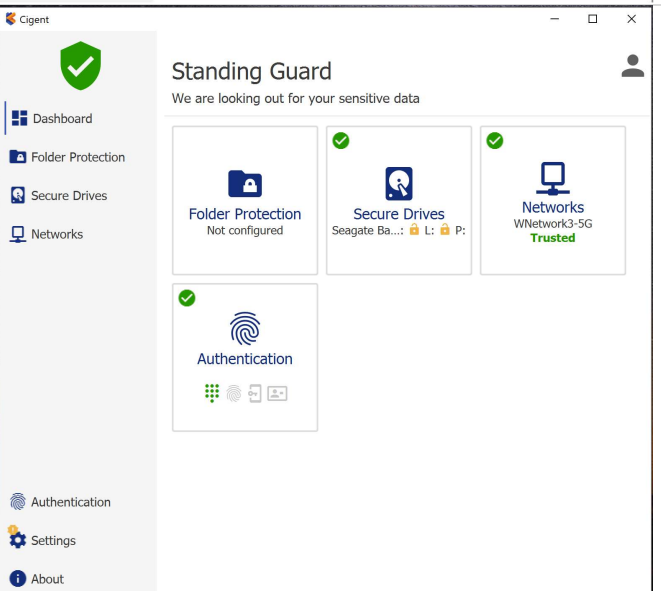
If Cigent PBA is installed, the Quick Secure Drive Setup will not be displayed. You must configure the drives using the Secure Drive page.

Skip to Step 15.



<p>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.</p>	
<p>13. Enter your authentication PIN and click Enter to approve the SSD setup.</p>	

<p>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. Skip to Step 20</p>	 <p>Cigent</p> <h3>Quick Secure Drive Setup</h3> <p>Cigent SSD Configuration Complete!</p> <p>A backup file containing your encrypted password has been saved to: C:/Users/dwolf/Desktop/6479_A767_BF00_00C9._backup.k3y</p> <p>IMPORTANT: You should move this file to a safe, external location like a USB flash drive and keep it in a safe place. It can be used to restore access to your drive should you forget your password.</p> <p>If you wish to lock/unlock your secure drives, use the tray menu or the Cigent Secure Drives page.</p> <p>Close</p>
<p>15. On the Secure Drives page select your Cigent Secure SSD then click Add Ranges.</p>	 <p>Cigent</p> <h3>Secure Drives</h3> <p>Protect files with firmware locking, the highest level of protection</p> <p>Name: Seagate BarraCuda 515 ZP512MC300: S/N: 7MT015Y1 FW: ECPM13.1 [476.94 GB] [OS] [FIPS Enabled]</p> <p>Secure Drives</p> <p>Add Ranges</p> <p>Advanced</p>
<p>16. Its likely that your entire drive has been allocated to the C: partition. If so, Cigent will offer to reduce the C: partition by 100GB (or 10% of unused space) on which to create the Secure Drives. You can adjust the total size of the reduction along with the proportion of Dynamic to Always On anywhere from 0 to 100%. Click Save to begin creation.</p>	 <p>Cigent</p> <h3>Add Ranges</h3> <p>Seagate BarraCuda 515 ZP512MC30012 S/N: 7MT015Y1</p> <p>No space available. We will automatically create 100GB of space. See Advanced section to change.</p> <p>Enter and save your ranges.</p> <p>Hide Advanced Options</p> <p>Adjust the Dynamic/Always On drive proportions</p> <p>Total Size: 100 GB</p> <p>A partition resize will occur</p> <p>Dynamic Size: 50.0 GB</p> <p>Always On Size: 50.0 GB</p> <p>Save</p>

<p>17. Enter the password for the PBA user who logged in to unlock the full drive.</p>	 <p>The dialog box titled 'Cigent' with a close button (X) in the top right corner. Below the title bar, it says 'Authentication Required'. A lock icon is followed by the text 'Authentication is required to Configure the Cigent SSDs'. Below this, it shows 'PBA User: admin' and a 'Password' field with masked characters. There are two buttons for 'Method': 'Password' (selected) and 'CAC/PIV'. A green 'Submit' button is at the bottom, and a link 'Enter PBA password' is below it.</p>
<p>18. If successful, Cigent will return to the Secure Drives page showing both drives.</p>	 <p>The 'Cigent' dashboard window. On the left is a sidebar with a green checkmark icon and menu items: 'Dashboard', 'Folder Protection', 'Secure Drives' (selected), and 'Networks'. The main area is titled 'Secure Drives' with the subtitle 'Protect files with firmware locking, the highest level of protection'. It shows a drive 'Seagate BarraCuda 515 ZP' with status 'Enabled'. Below are two toggle switches for 'Secure Drives': 'Always On (L:)' and 'Dynamic (P:)', both turned on. A 'Deconfigure' button and an 'Advanced' link are on the right.</p>
<p>19. 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. You should see these drives in File Explorer.</p>	 <p>The 'Cigent' dashboard window. On the left is a sidebar with a green checkmark icon and menu items: 'Dashboard', 'Folder Protection', 'Secure Drives' (selected), 'Networks', 'Authentication', 'Settings', and 'About'. The main area is titled 'Standing Guard' with the subtitle 'We are looking out for your sensitive data'. It displays four status cards: 'Folder Protection' (Not configured), 'Secure Drives' (Seagate Ba...: L: P:), 'Networks' (WNetwork3-5G Trusted), and 'Authentication' (with icons for various authentication methods).</p>

CONGRATULATIONS

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

If you want to learn more about how to use your Cigent Secure SSD and Cigent proceed further in this guide.

4 Using Always On and Dynamic Drives

There are two types of file protection modes available:

Files on Always On 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 Drives

- 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).

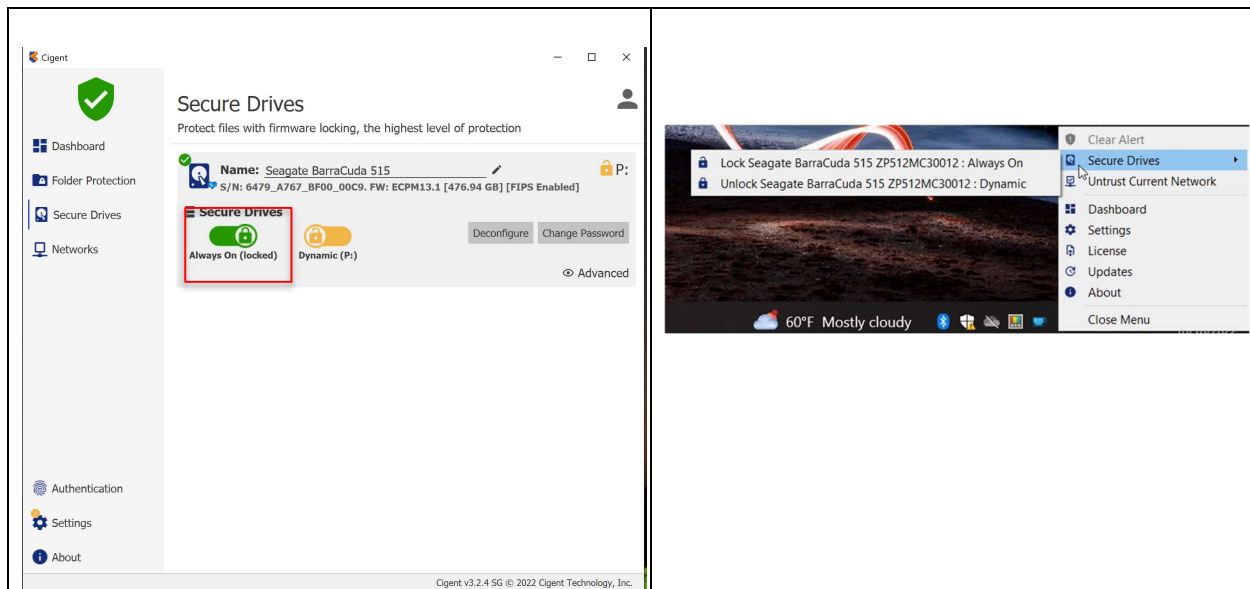
4.1 Locking and Unlocking Drives

You can lock and unlock Secure Drives using either the Secure Drives page of the 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.

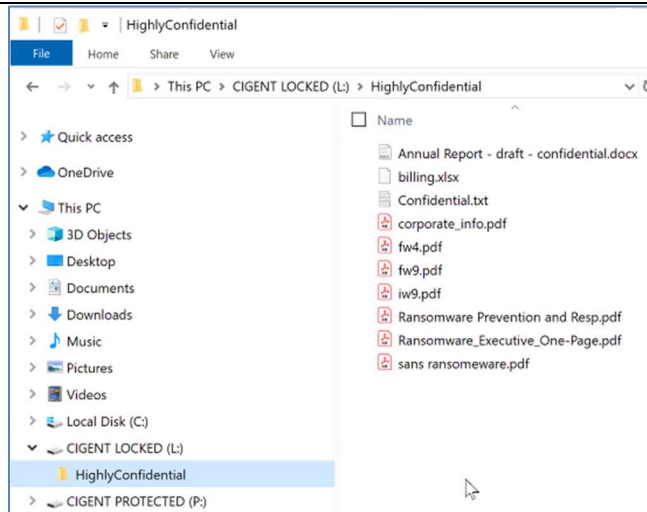


When Cigent PBA is also installed, automatic unlocking of Secure Drives is disabled.

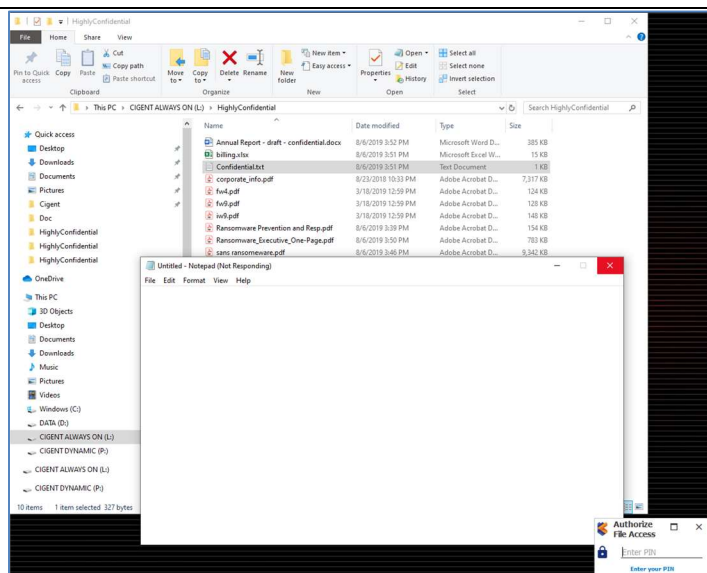


4.2 Accessing Always On Files

1. In windows explorer, browse to your AlwaysOn drive (usually L:) (If your L: drive is not visible, you must unlocked it before proceeding.)



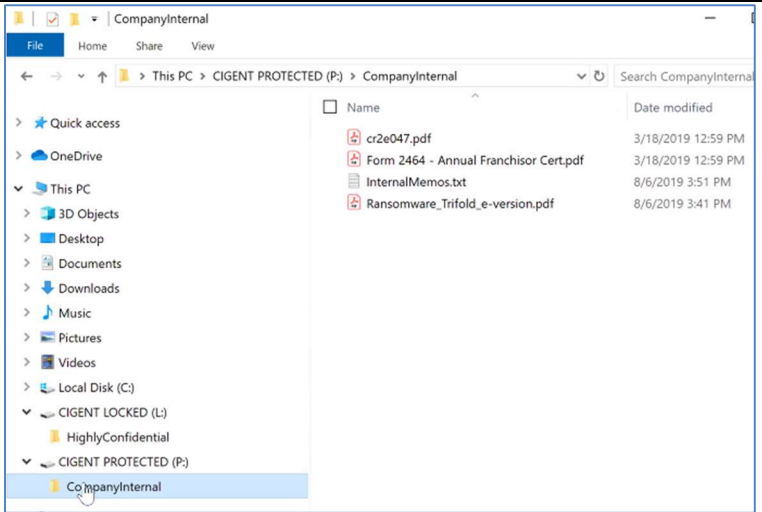
2. Double click on a file to open it. Regardless of the Active Lock state, Cigent will require authentication to open any file on the Locked drive.



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

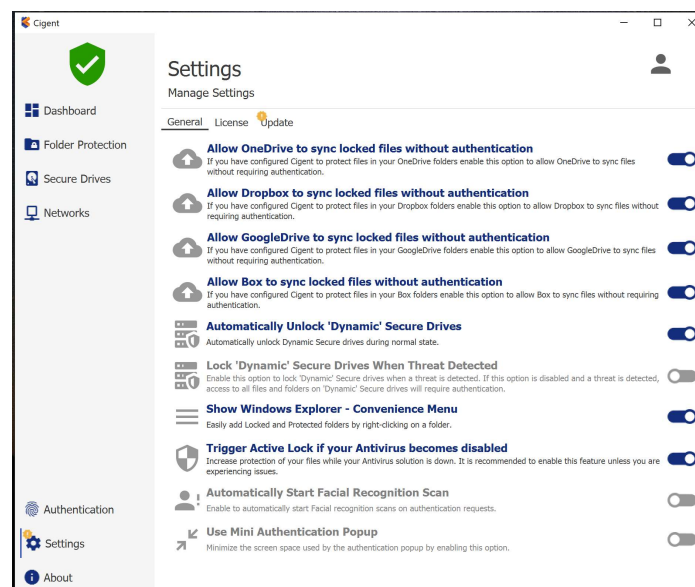


4.3 Accessing Dynamic Files

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.	

5 Manage Cigent Settings

The Cigent Settings page allows you to customize different aspects of Cigent and Cigent Secure SSD operations. This section explains each setting. Those preceded by an asterisk(*) are particularly important or useful.



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.

- **Allow OneDrive to sync locked file without authentication**
- **Allow Dropbox to sync locked files without authentication**
- **Allow GoogleDrive to sync locked files without authentication**
- **Allow Box to sync locked files without authentication**

* **Automatically Unlock Dynamic Secure Drives**

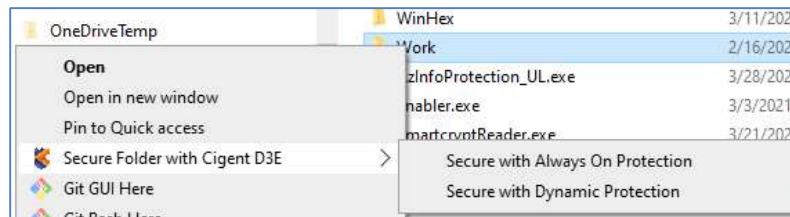
Enable to have Cigent automatically unlock(mount) your Dynamic drive (if configured) after system restarts and a threat clears.

* **Lock 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 that files will be protected by requiring a second factor authentication similar to AlwaysOn files until the threat is cleared.

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

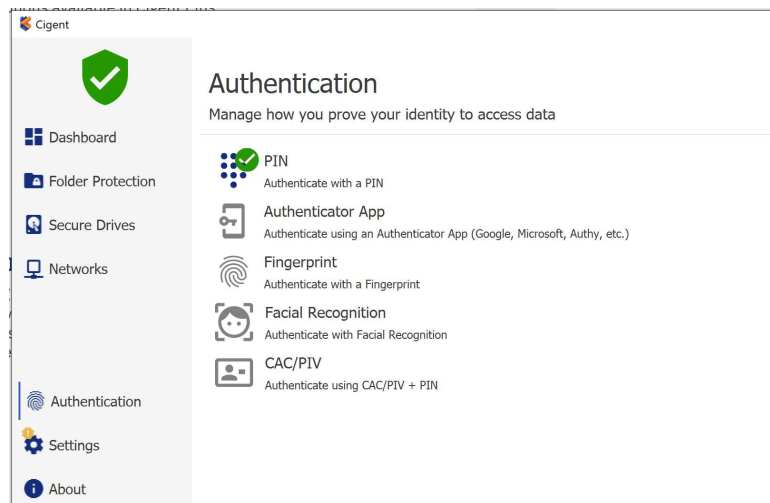
Scanning automatically starts when Facial Recognition is enabled.

* Use Mini Authentication Popup

This setting reduces the size of the popup authentication window and includes minimal information. When the PIN is enabled, users can enter their PIN with the keyboard.

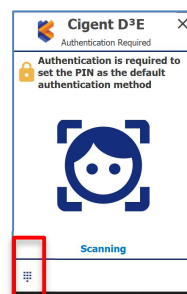
6 Authentication

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



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

You can use your favorite authenticator application from Google, Microsoft and more as a primary authentication factor. To begin setup, click the Setup button next to Authenticator app and enter your PIN. Cigent will then provide a QR code to scan using your application. Click OK to close the window and then Default to make Authenticator app your default method.

Fingerprint

Facial Recognition

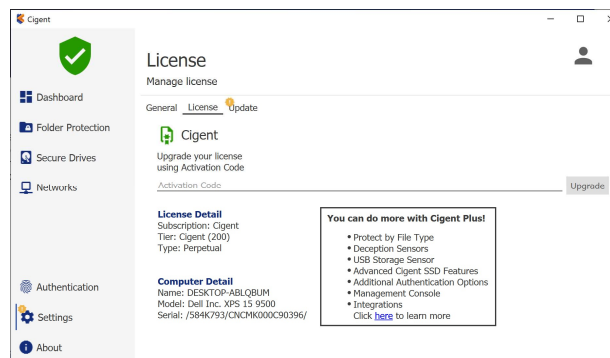
Both Fingerprint and Facial recognition use the Windows Hello APIs to work. If your system supports either of these options, click the Setup button to complete the configuration through the Hello UI. Once complete, return to Cigent and select Default to change to this form of authentication to be used.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

PIV/CAC

You can use your government or company issued smartcard as your primary authentication using the smartcard PIN each time. To begin setup, make sure your card is inserted into the reader and attached, then click Setup. Enter your Cigent PIN, and the smartcard PIN. Once complete, leave your smartcard attached and enter your 8 digit smartcard pin during authentication requests.

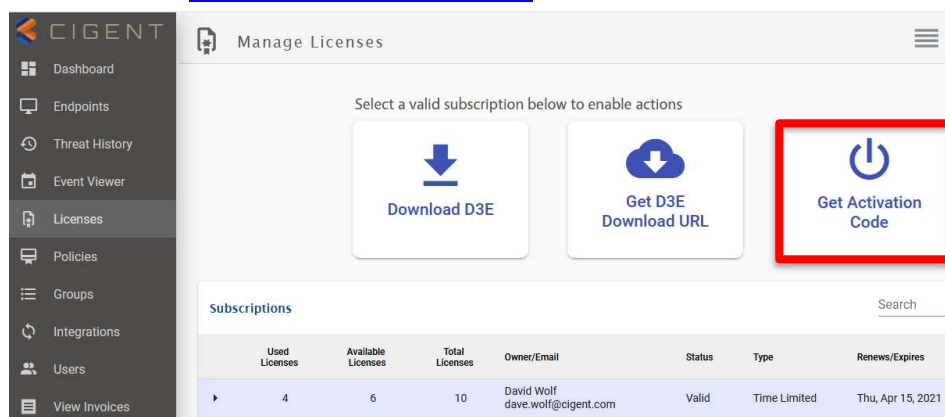
7 License

Cigent can be upgraded to Cigent Select or Cigent Plus to gain access to additional protections, integrations, and enterprise management features.



Activation Code

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 so they can enter into the Cigent license page. Cigent will automatically register to the subscription and start enforcing settings specified by configured policies.

8 Folder Protections

Cigent can also provide protection to files residing in folders not located on 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.

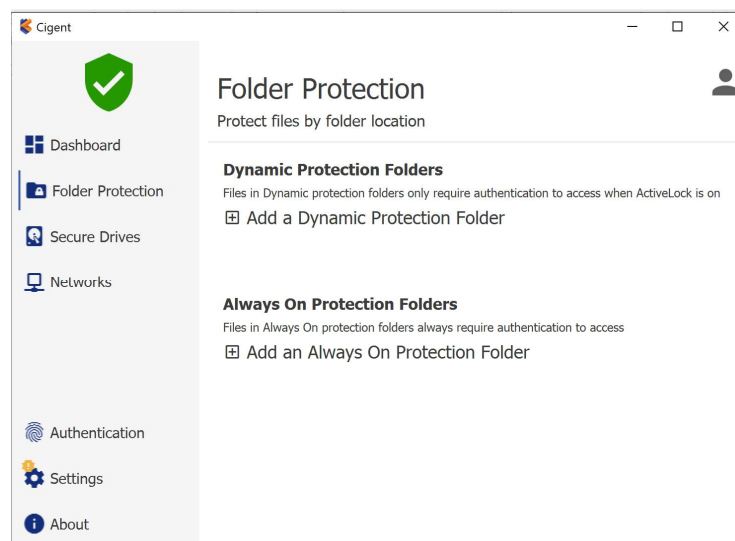
Folder protections follow the same paradigm as Secure Drives.

Always On

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

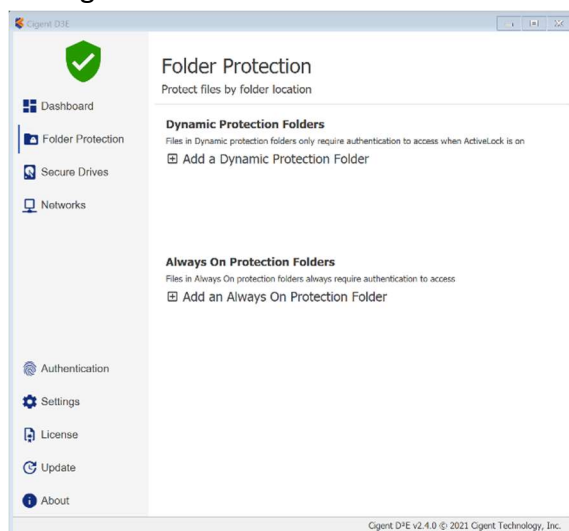
Dynamic

- 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 bulk access like Source code.

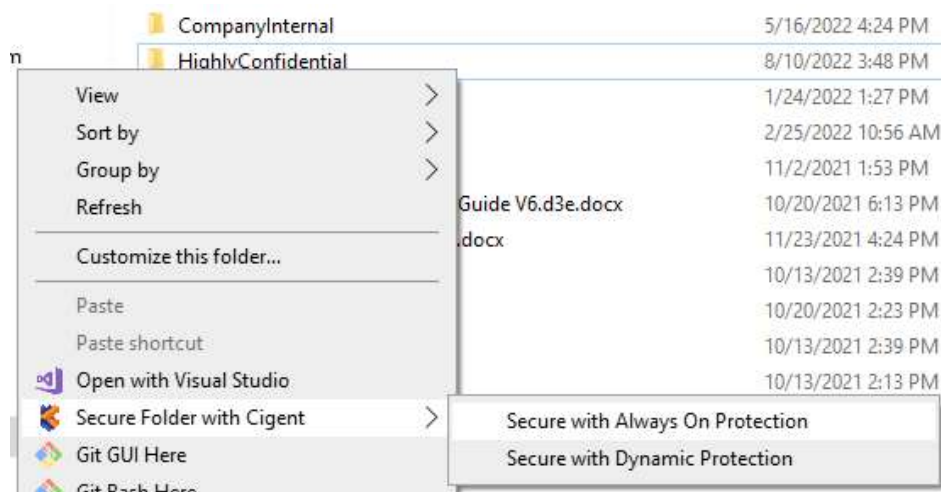


Folder protection can be added in two ways:

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



2. Using the Convenience 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.



9 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:

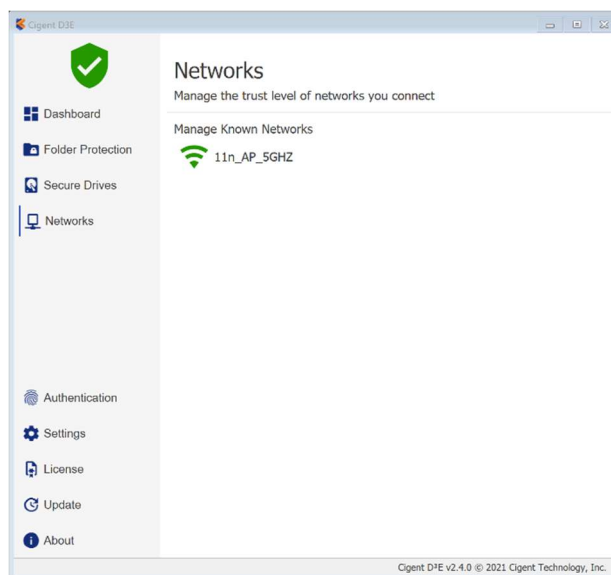
- You join a network that has not been previously trusted.
- A network device scans your host for open ports and connects to a Cigent deception port.
- An untrusted network device attempts to connect to your device on any port.

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.

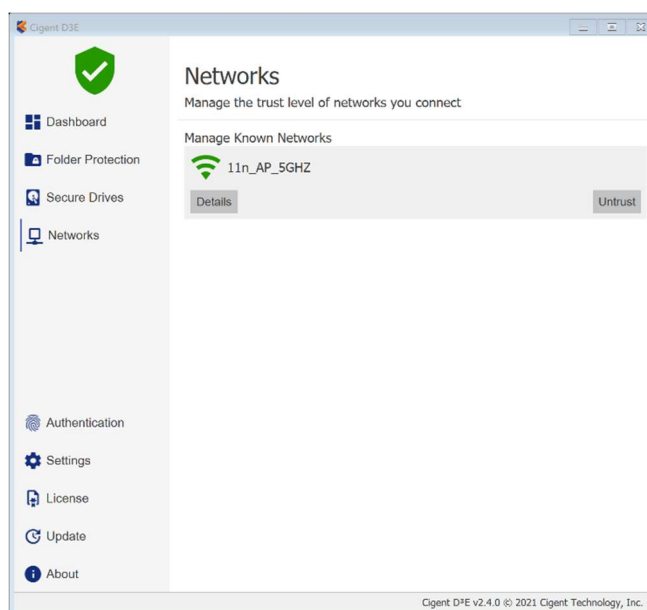
Untrusting your current network

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.

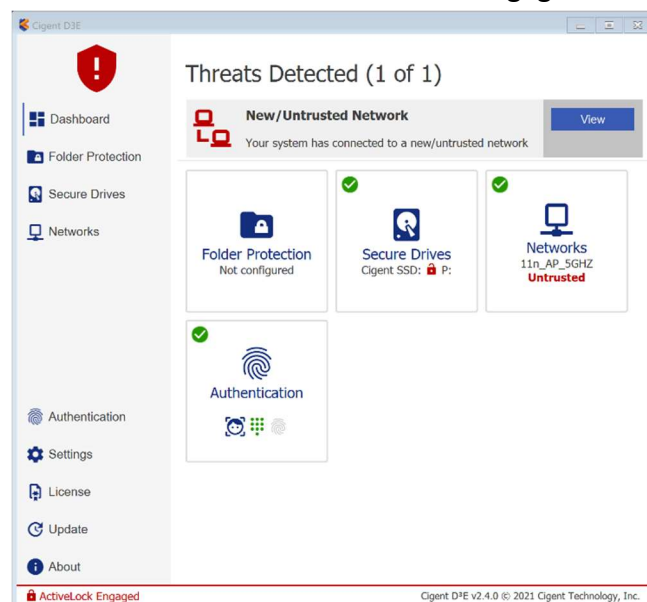
1. Open the Cigent and select the Networks menu.



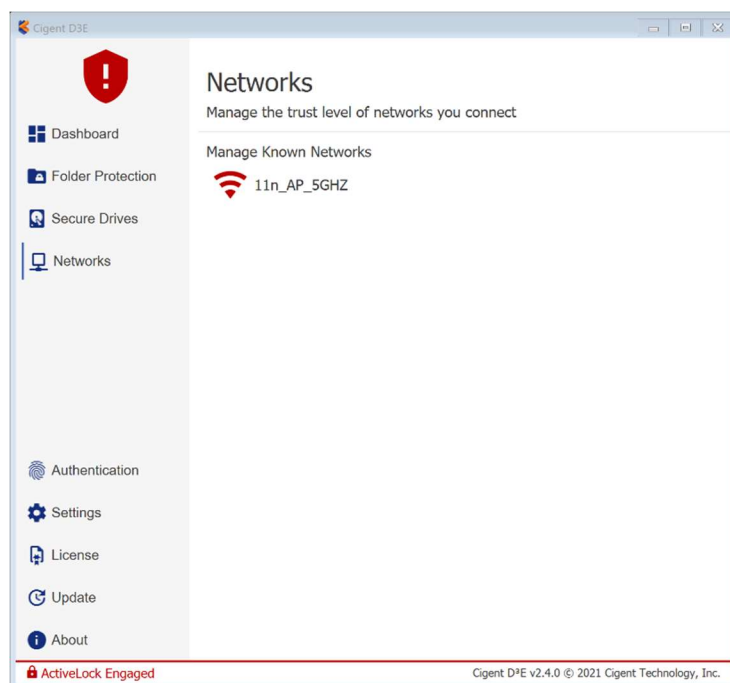
2. Select the active network and click on the Untrust button.



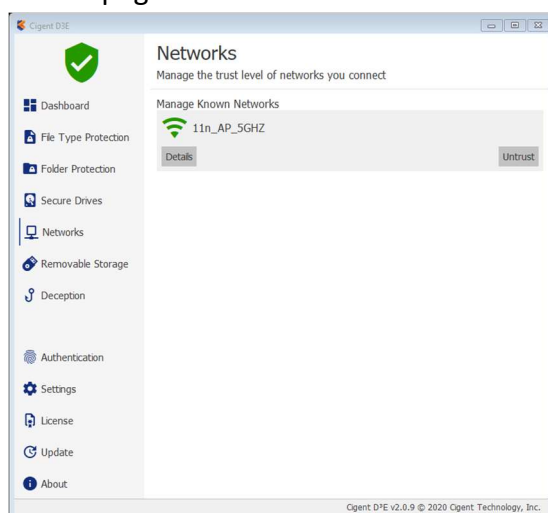
3. Switch back to the Dashboard. Note that Active Lock is engaged.



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.

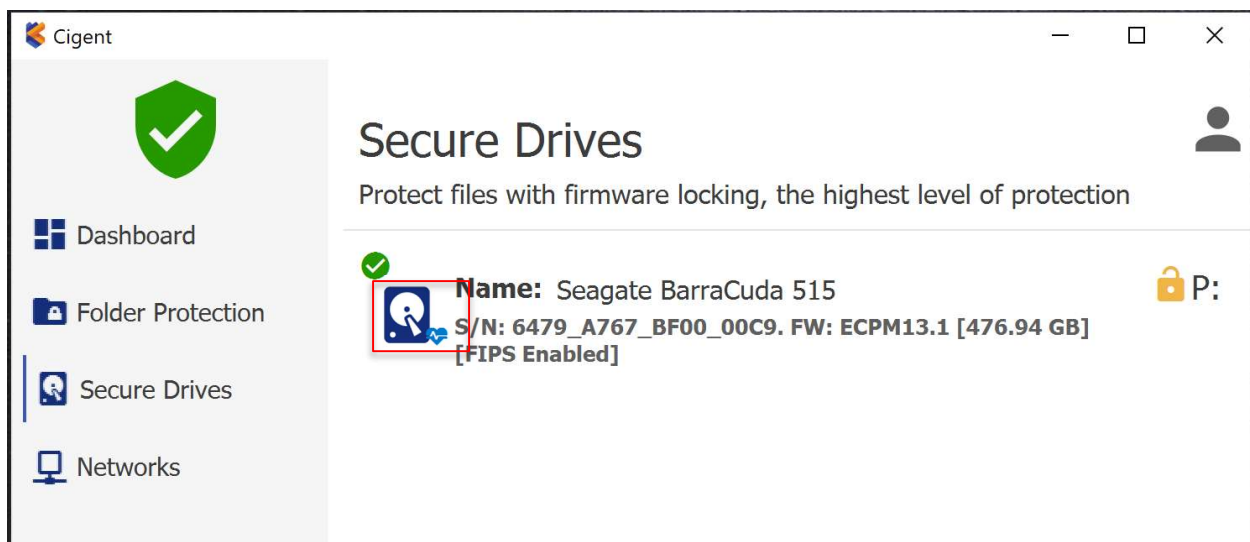


10 Cigent Secure SSD Advanced Features

10.1 KeepAlive

KeepAlive provides an extra layer of protection by creating a tighter trust connection between the Cigent Secure SSD firmware 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.

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

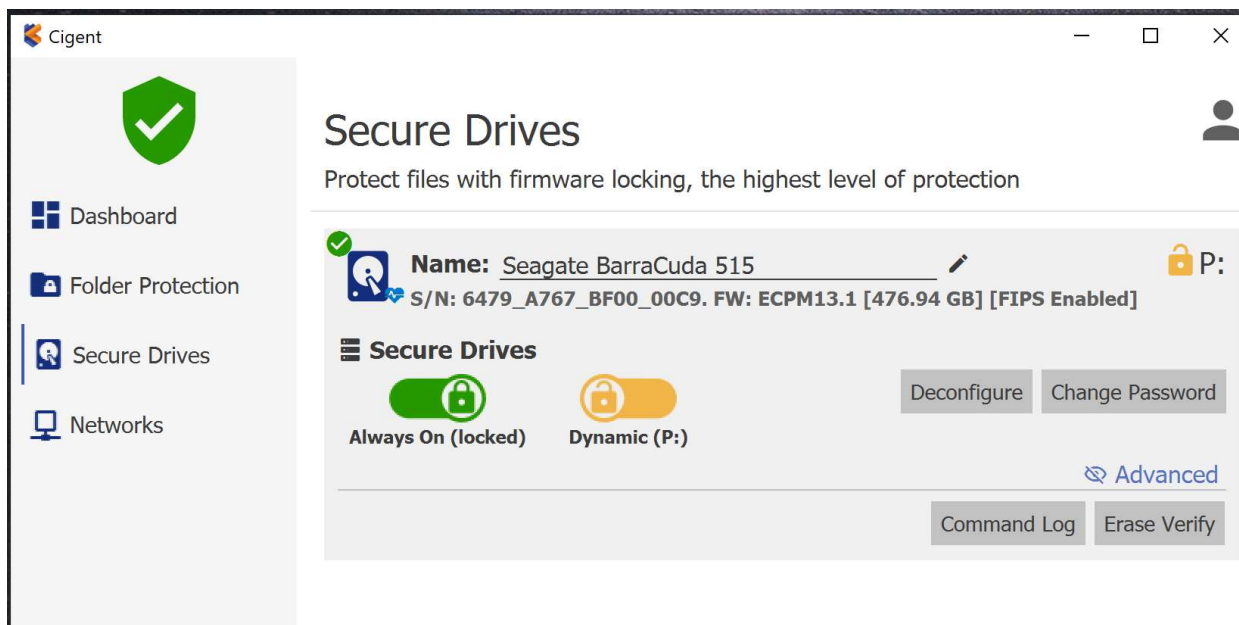


10.2 Command Log Audit

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.

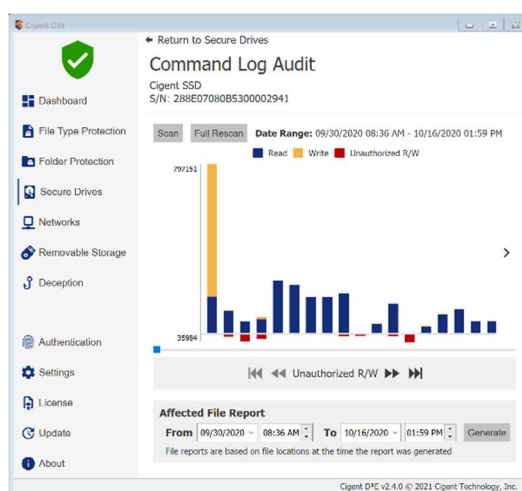
This command log can be used to audit drive activity to capture attempts to read information from the drive without Cigent possibly indicating attempts to circumvent file protection. Further, the command log can be used to report on files accessed with or without Cigent running by mapping the accessed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

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

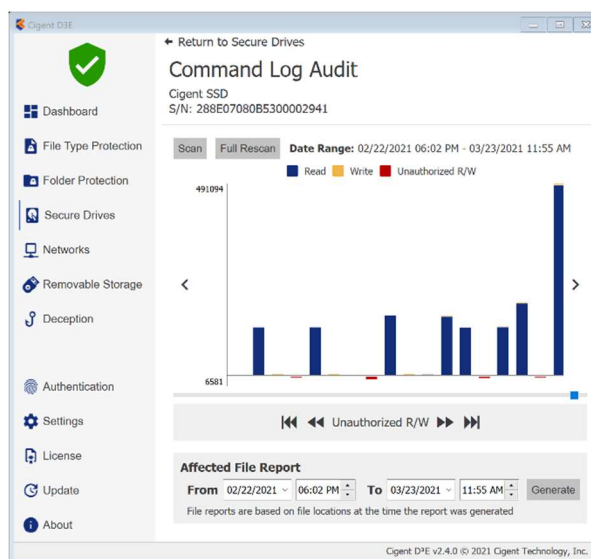


2. Click **Command Log** to open the Command Log Audit page. Click **Scan** to start the reading of the command log.

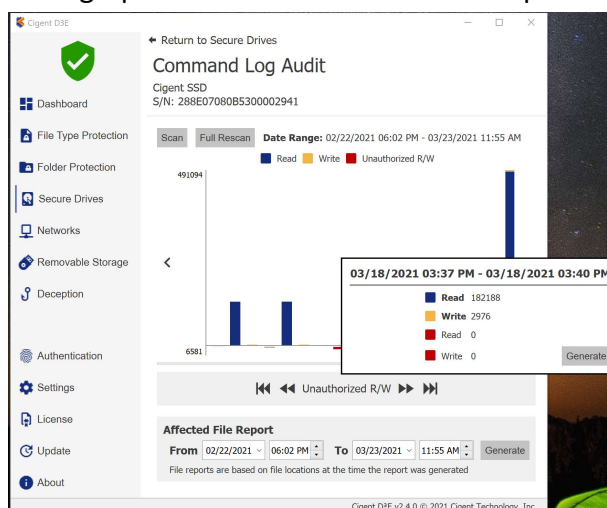
Note: Reading the command log from the drive over USB especially can take several minutes.



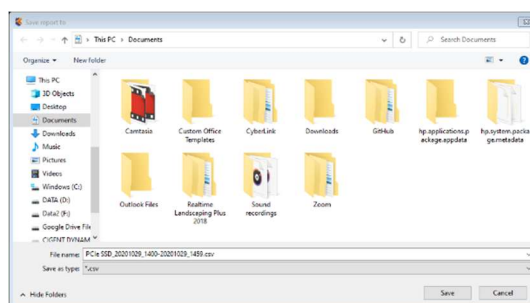
3. If this is a newer drive, you may have only a few data points. If this drive has been in use for a while, you may need to scroll the graph to the right to get to the newest information.



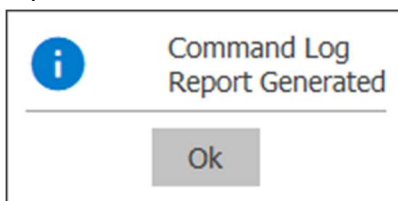
- Click on a shorter bar in the graph to detailed results of each operation.



- 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.



6. Click OK once the operation completes.



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

	A	B	C	D	E	F	G
1	Time	Monitored	Volume	Letter	File ID	Parent File ID	File Name
2	2020-10-29 18:00:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
3	2020-10-29 18:01:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
4	2020-10-29 18:02:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
5	2020-10-29 18:03:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
6	2020-10-29 18:04:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
7	2020-10-29 18:05:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
8	2020-10-29 18:06:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
9	2020-10-29 18:07:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
10	2020-10-29 18:08:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
11	2020-10-29 18:09:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
12	2020-10-29 18:10:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
13	2020-10-29 18:11:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
14	2020-10-29 18:12:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
15	2020-10-29 18:13:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
16	2020-10-29 18:14:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
17	2020-10-29 18:15:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
18	2020-10-29 18:16:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
19	2020-10-29 18:17:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
20	2020-10-29 18:18:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
21	2020-10-29 18:19:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
22	2020-10-29 18:20:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
23	2020-10-29 18:21:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT
24	2020-10-29 18:22:27 UTC	Yes	{6de3007b-bc52-4fdb-8df9-I-L		0	5	\$MFT

The columns of major importance are:

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

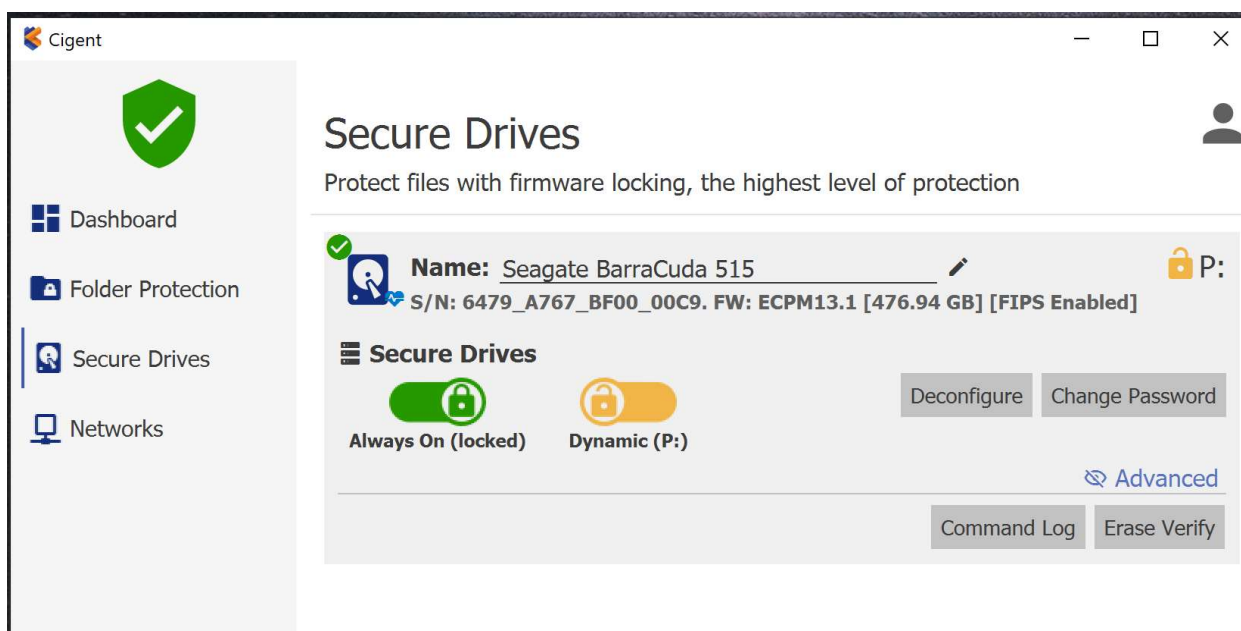
Note : You will see many files used by Windows that are usually hidden from users.

10.3 True Erase

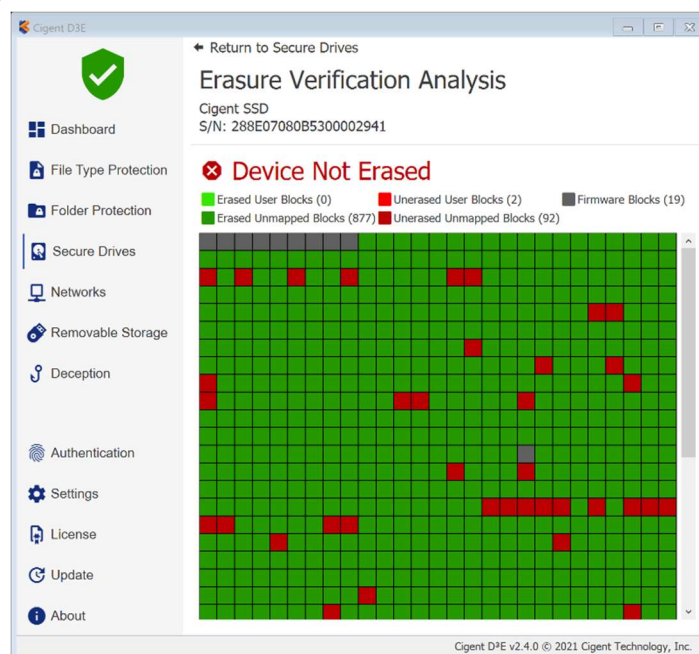
Secure data erasure is an important process for many commercial and governmental organizations preventing classified information from unauthorized access. Short of costly and wasteful physical destruction, users earlier had to depend on outdated erasure programs originally written for magnetic media. SSDs 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 mapped and unmapped block to verify the data

has been removed. Any blocks reporting data will result in an erasure verification failure. Once D3E confirms the drive has been truly erased, it can be safely and securely reused.

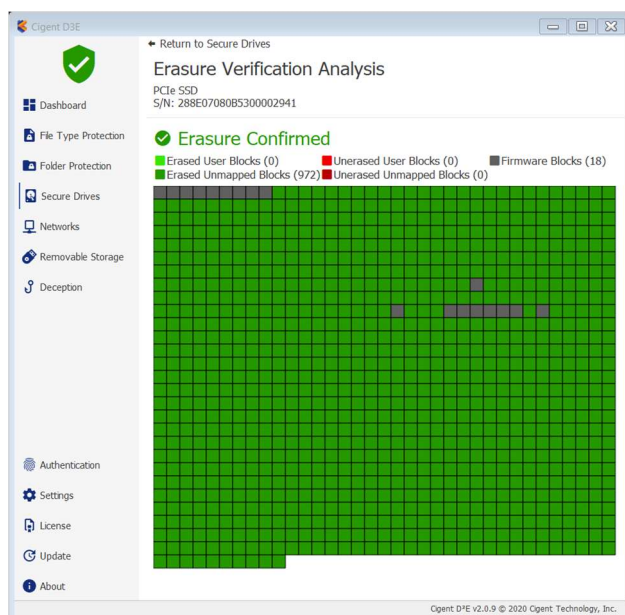
1. Select the Cigent Secure SSD and click **Advanced** to reveal the advanced features.



2. Click Erase Verify.



Cigent 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.



For more information about Cigent Secure SSDs please visit www.cigent.com

©2022 Cigent Technology Inc. All rights reserved. Cigent is a registered trademark of Cigent Technology Inc. in the United States and other jurisdictions.