CIGENT WINDOWS FOR SEAGATE® BARRACUDA™ 515 SSD

USER GUIDE v1.0

FIPS VALIDATED 140-2

November, 2022

V1

Seagate® BarraCuda™ 515

Cigent Windows Version 3.2.9

Contents

1   Introduction

The BarraCuda™ 515 SSD operating firmware includes cybersecurity defenses that repel ransomware attacks and data theft — even when all other cybersecurity protections fail. In conjunction with Cigent Windows software (Cigent), BarraCuda™ 515 SSDs protect data throughout the entire device lifecycle—from provisioning to end-of-life—defending against a vast number of threat vectors.

BarraCuda 515 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 BarraCuda 515 SSD and associated Cigent Windows 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

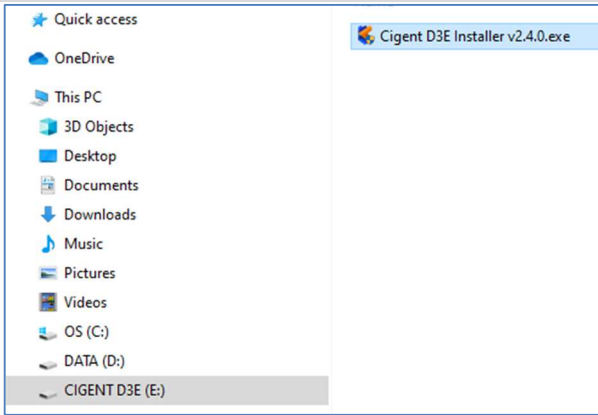This guide is applicable to Seagate BarraCuda 515 SSDs installed internally as primary or secondary drives or externally.

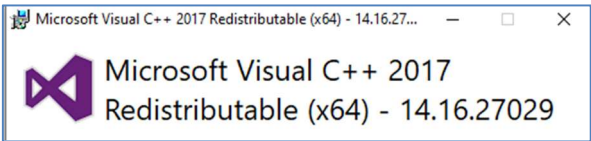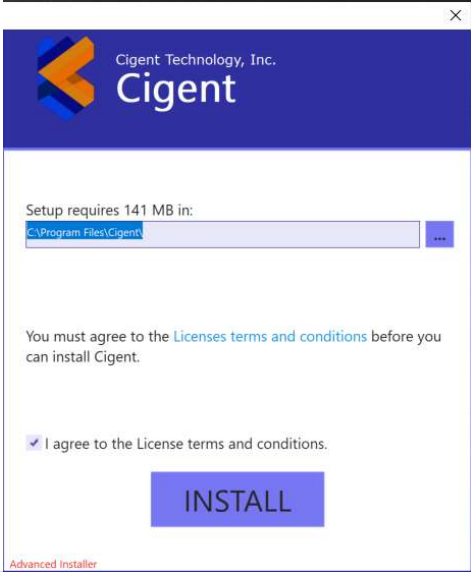## 3.1   Compatibility with Cigent PBA software

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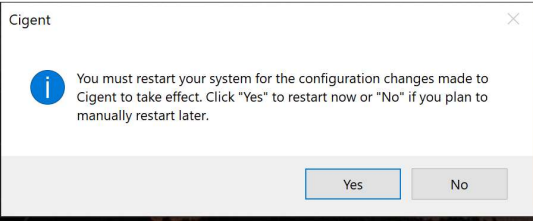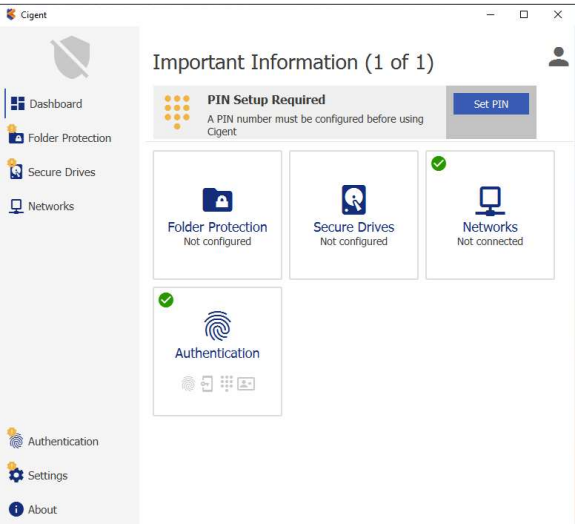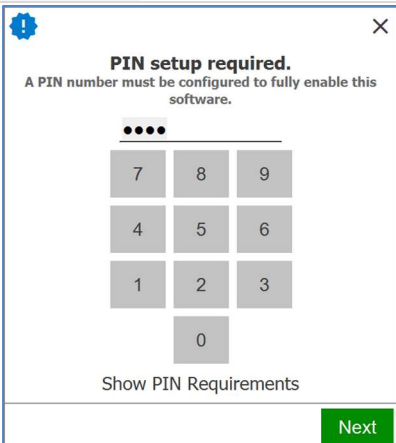
1. Cigent PBA software must be installed before installing Cigent Windows software.
2. Authentication for Secure Drive operations (creation, deletion and unlocking) uses Cigent PBA credentials instead of Cigent Windows authentication.
3. Creation and deletion of Secure Drives requires a Cigent PBA administrator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

A copy of the Cigent Windows installer is placed onto each Seagate BarraCuda 515 SSD before shipping.

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

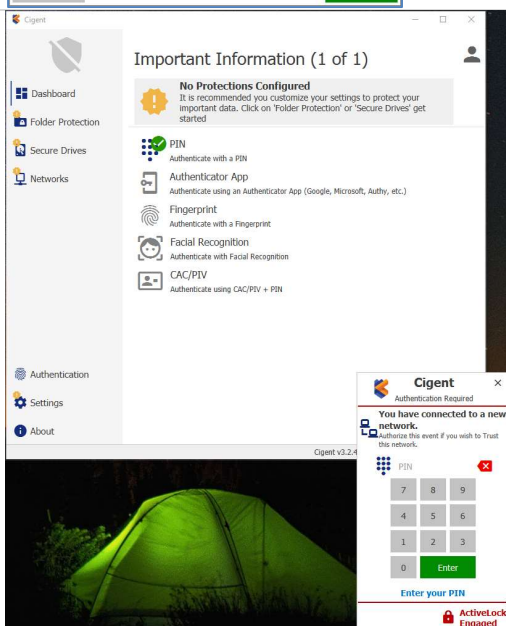|	
1. Install the BarraCuda 515 SSD into your system.	
2. Open Windows Explorer and select the CIGENT partition.	
3. Double click the Cigent installer executable to begin the	

installation process. Note: The name of the installer may be 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**.	
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 will automatically open and request a PIN to be set.	
7. Click **Set PIN**.	
8. Enter your PIN, click **Next**.	

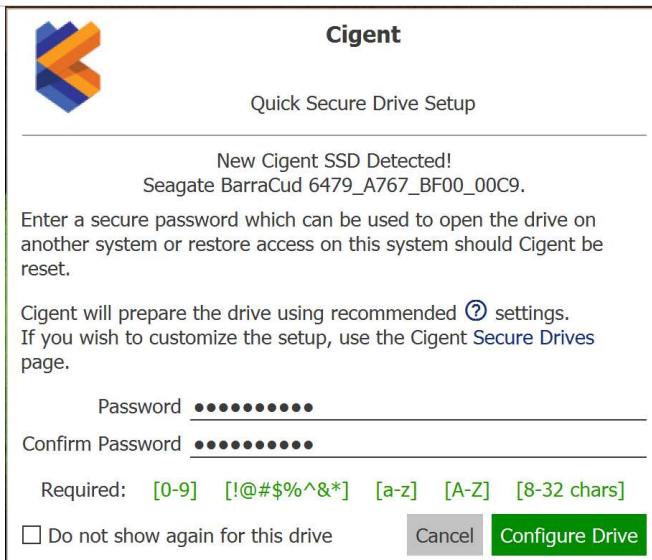|	
9. Re-enter your PIN and click **Accept**.	
10. If you are currently connected to a network and your network is NOT set to Private in Windows, Cigent will engage Active Lock. If the network is secure, simply enter your PIN and click **Enter** to add the current network as Trusted. If you are not connected 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 BarraCuda 515 SSD inserted or your internal BarraCuda 515 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.**	
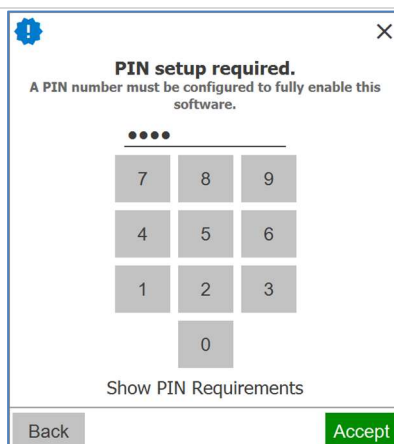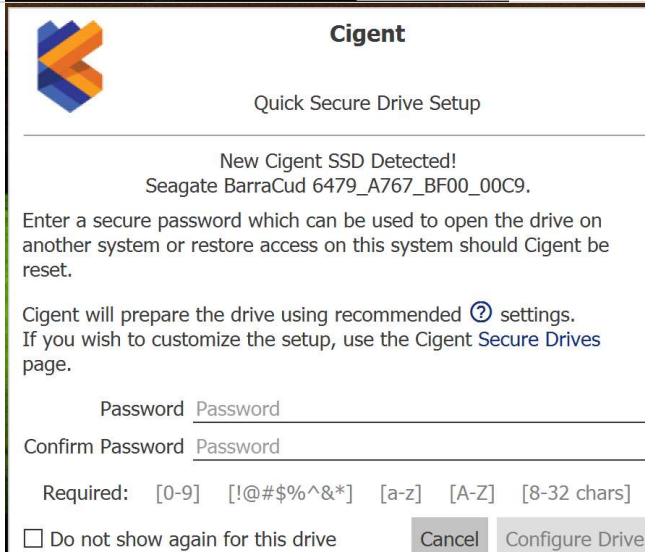
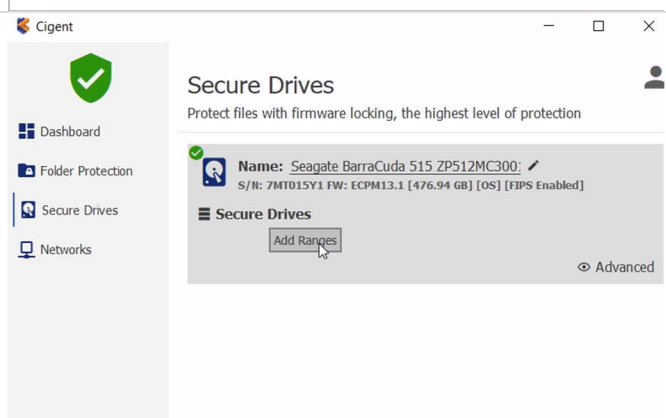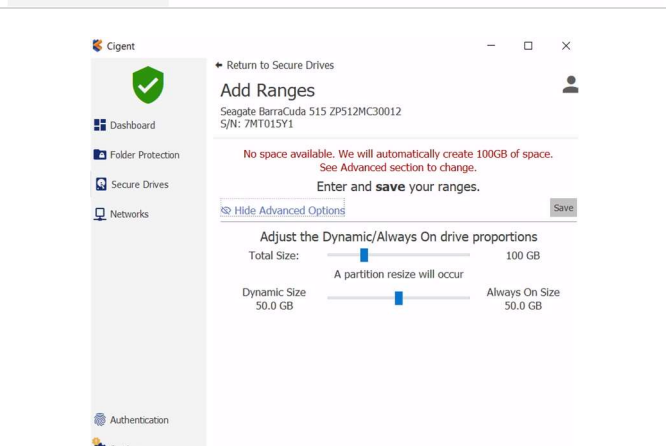|	
12. Enter a secure password twice and click **Configure Drive** to automatically configure the SSD to Cigent default configuration. If you wish to customize the settings, you can click Cancel and configure the drive from the Secure Drives page of the Cigent Dashboard.	**Cigent** Quick Secure Drive Setup New Cigent SSD Detected! Seagate BarraCud 6479_A767_BF00_00C9. 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. Cigent will prepare the drive using recommended ⑦ settings. If you wish to customize the setup, use the Cigent Secure Drives page. Password ●●●●●●●●●● Confirm Password ●●●●●●●●●● Required: [0-9] [!@#$%^&*] [a-z] [A-Z] [8-32 chars] ☐ Do not show again for this drive Cancel Configure Drive
13. Enter your authentication PIN and click **Enter** to approve the SSD setup.	**Cigent** ✕ Authentication Required **Authentication is required to Configure the Cigent SSDs** PIN ❌ 7 8 9 4 5 6 1 2 3 0 Enter **Enter your PIN**

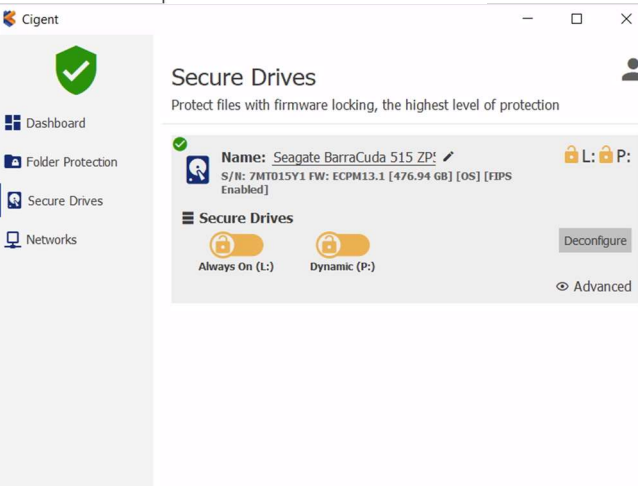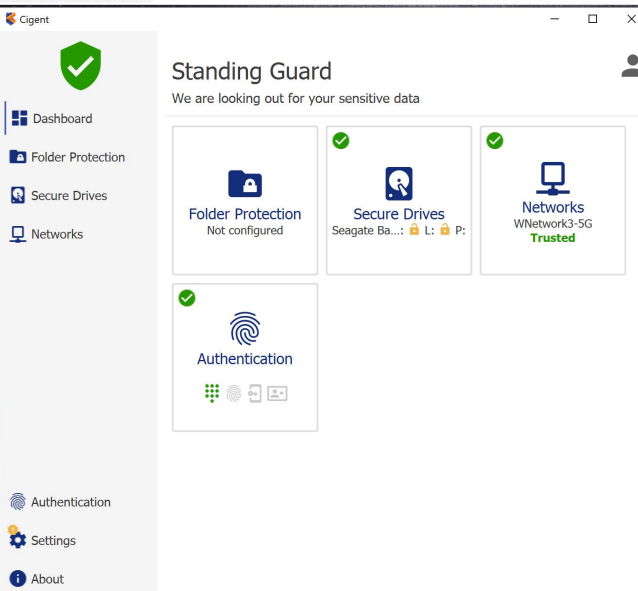|	
14. Note the location of the encrypted password file. This file should be moved to a secure location off of the host for security purposes. Click **Close** when you are ready. **Skip to Step 20**	**Cigent** — Quick Secure Drive Setup Cigent SSD Configuration Complete! A backup file containing your encrypted password has been saved to: **C:/Users/dwolf/Desktop/ 6479_A767_BF00_00C9._backup.k3y** **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. If you wish to lock/unlock your secure drives, use the tray menu or the Cigent Secure Drives page. Close
15. On the Secure Drives page select your BarraCuda 515 SSD then click **Add Ranges**.	Cigent — Secure Drives. Protect files with firmware locking, the highest level of protection. **Name:** Seagate BarraCuda 515 ZP512MC300: S/N: 7MT015Y1 FW: ECPM13.1 [476.94 GB] [OS] [FIPS Enabled]. Secure Drives — Add Ranges. Advanced. Dashboard / Folder Protection / Secure Drives / Networks
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.	Cigent — Return to Secure Drives. Add Ranges. Seagate BarraCuda 515 ZP512MC30012 S/N: 7MT015Y1. No space available. We will automatically create 100GB of space. See Advanced section to change. Enter and save your ranges. Hide Advanced Options. Save. Adjust the Dynamic/Always On drive proportions. Total Size: 100 GB. A partition resize will occur. Dynamic Size 50.0 GB. Always On Size 50.0 GB. Dashboard / Folder Protection / Secure Drives / Networks / Authentication

17. Enter the password for the PBA user who logged in to unlock the full drive.	
18. If successful, Cigent will return to the Secure Drives page showing both drives.	
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.	

CONGRATULATIONS

You have completed the steps necessary to begin using your BarraCuda 515 SSD and Cigent Windows software.

If you want to learn more about how to use your BarraCuda 515 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.
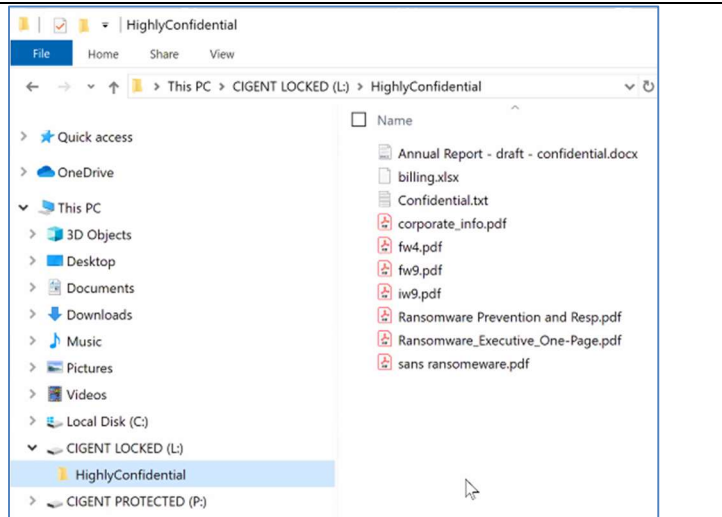
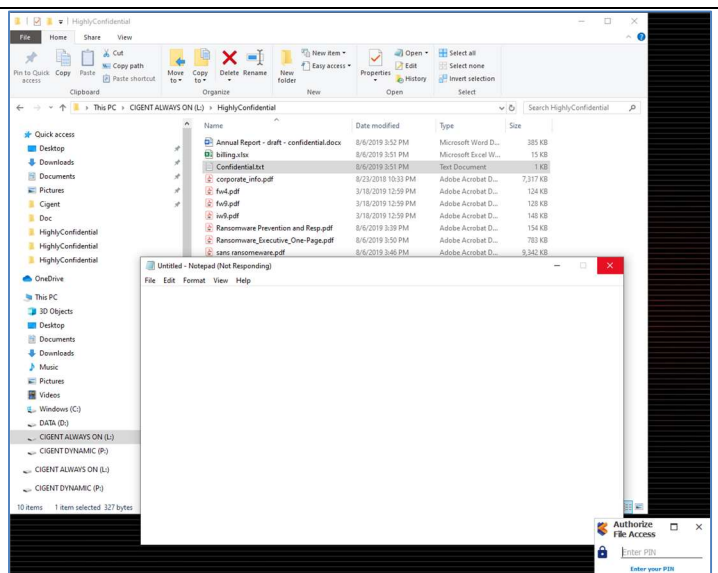When Cigent PBA is also installed, automatic unlocking of Secure Drives is disabled.
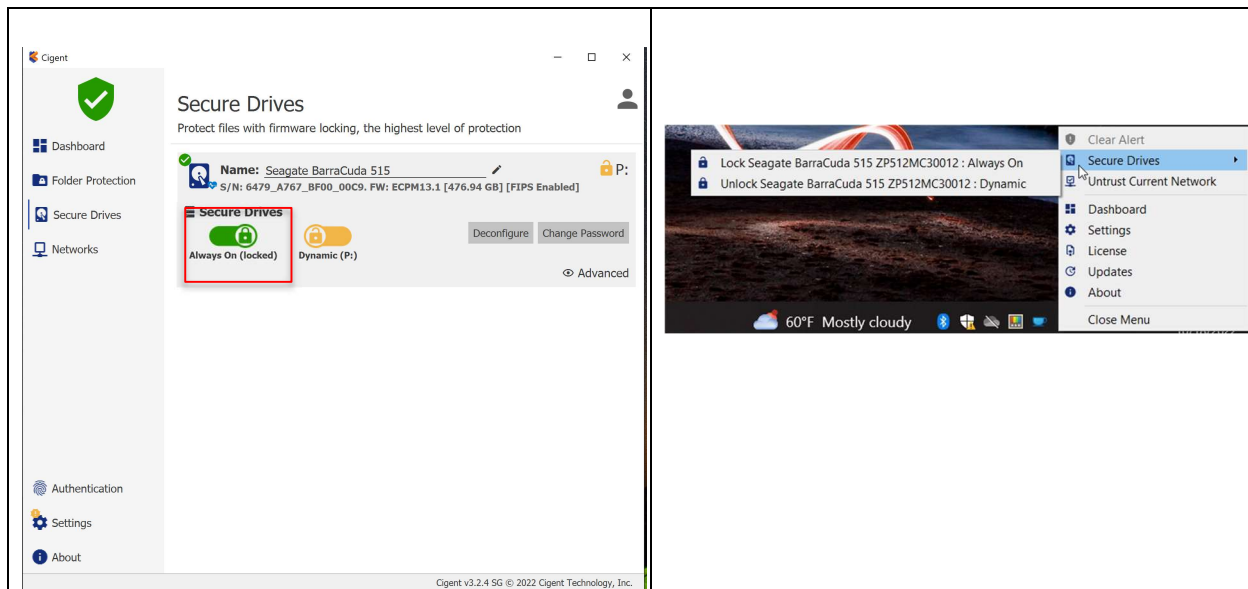
4.2   Accessing Always On Files

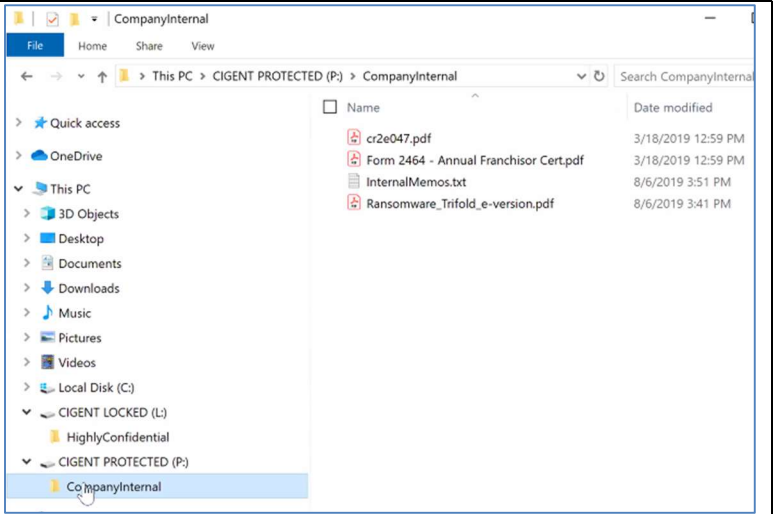|	
1. In windows explorer, browse to your AlwaysOn drive (usually L:) (If your L: drive is not visible, you must unlocked it before proceeding.)	

|	
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 BarraCuda 515 SSD operations. This section explains each setting. Those preceded by an asterisk(*) are particularly important or useful.
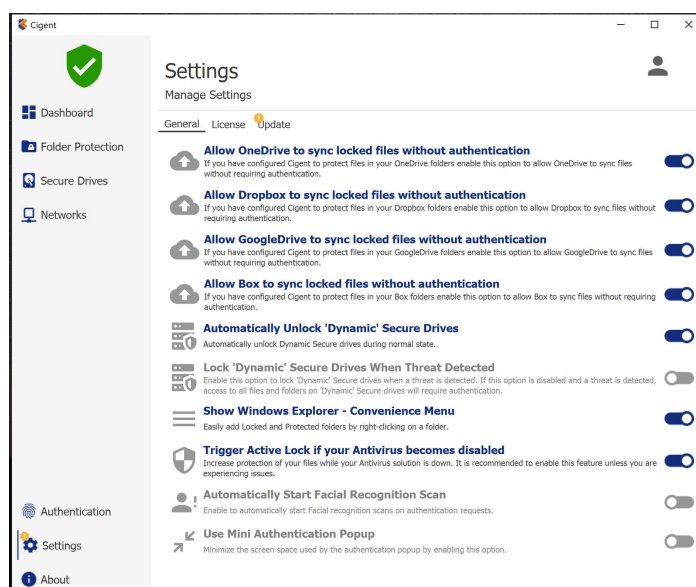
Enable these options if you use either of these Cloud File storage solutions and have added an Always On folder being synchronized by these applications.

- **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.
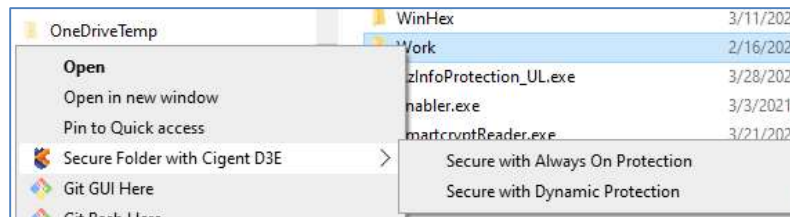
Trigger Active Lock if your Antivirus becomes disabled
This setting determines if Cigent should engage Active Lock should your AV become disabled. You should *only* disable this setting if your AV is not detected by Cigent for some reason.

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 BarraCuda 515 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.
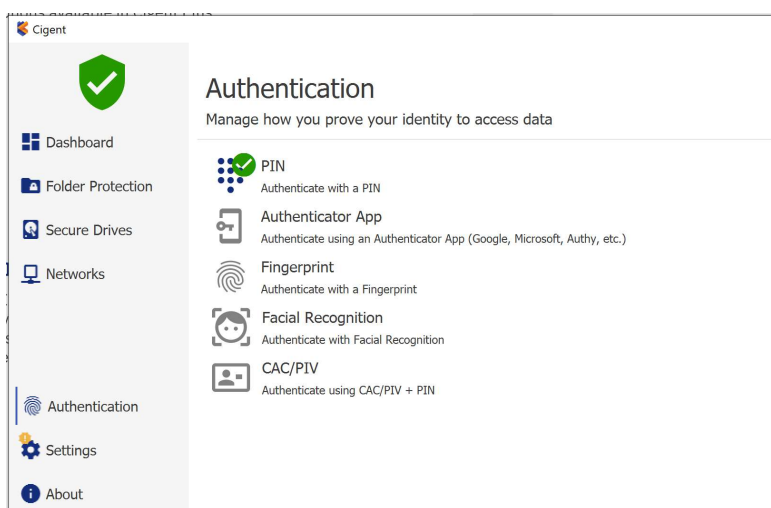
PIN

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
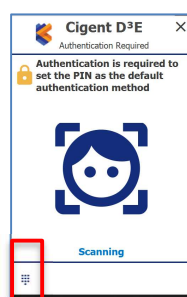
Authenticator App

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 you 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 of Cigent Plus to gain access to additional protections, integrations, and enterprise management features.
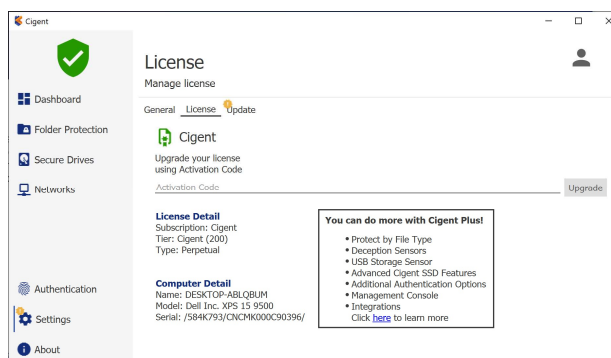
Activation Code

Administrators of Cigent Plus can obtain an Activation Code from the Licenses page of the Central Cigent console at https://central.cigent.com.
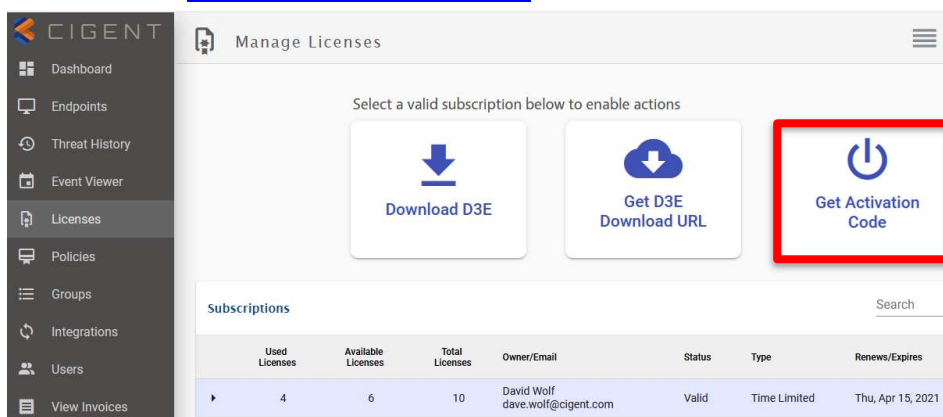
Provide this Activation code to users so they can enter into the Cigent license page. Cigent will automatically register to the subscription and start enforcing settings specified by configured policies.

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.
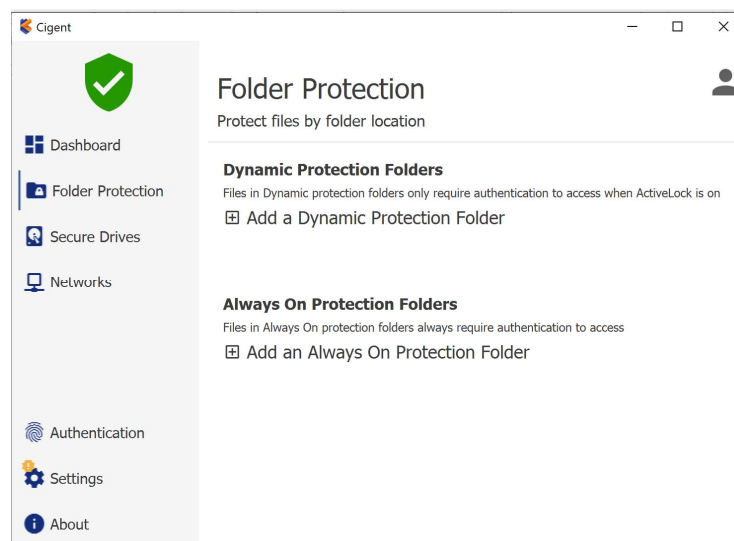
Folder protection can be added in two ways:

1. Click on the desired "Add …" link on the Folder Protection page, selecting the folder in the explorer window and clicking Select folder.
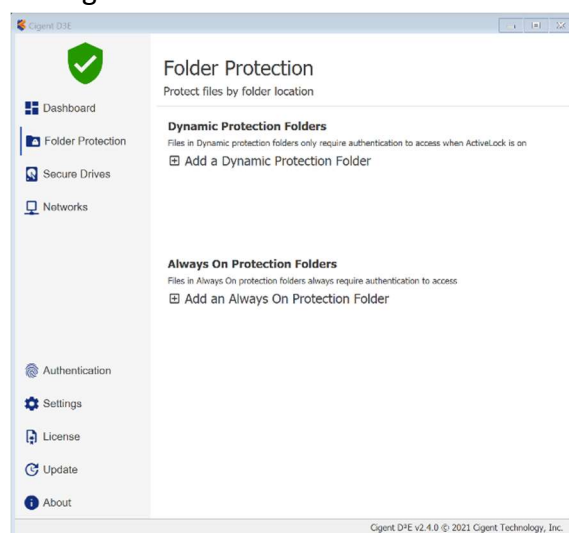
2. Using the Convience menu from Windows Explorer itself. Right click on the folder, select "Secure Folder with Cigent" menu and the desired protection level from the sub menu.
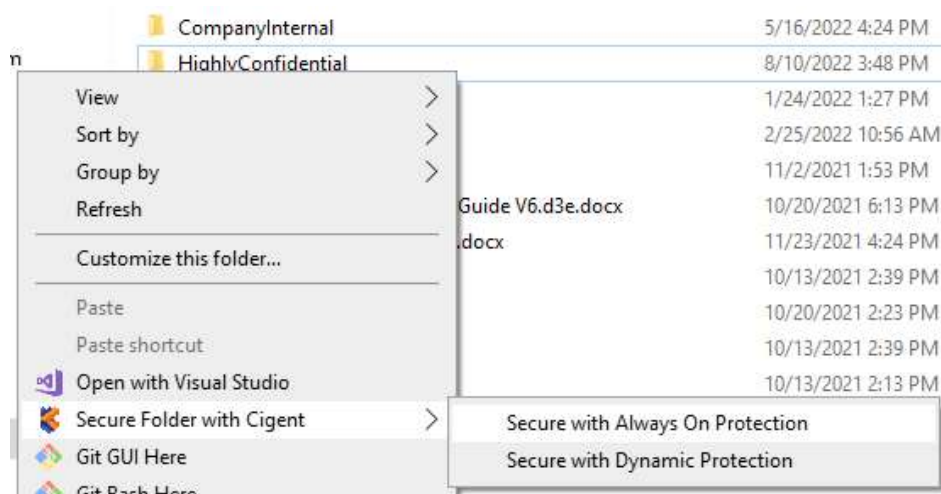
9   Network Manager

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.
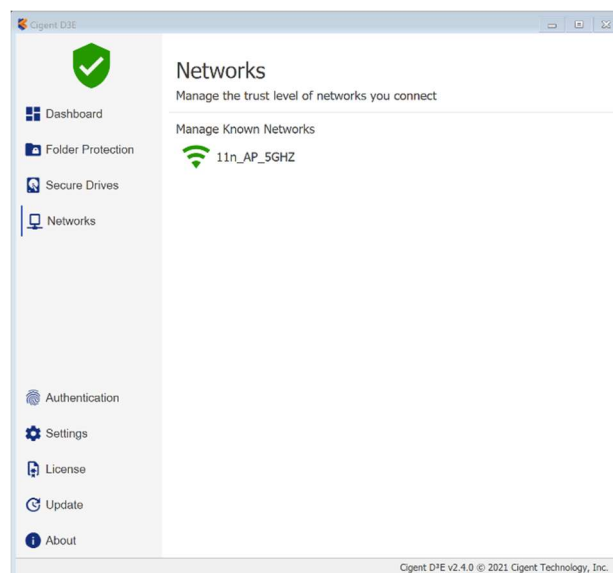
2. Select the active network and click on the Untrust button.
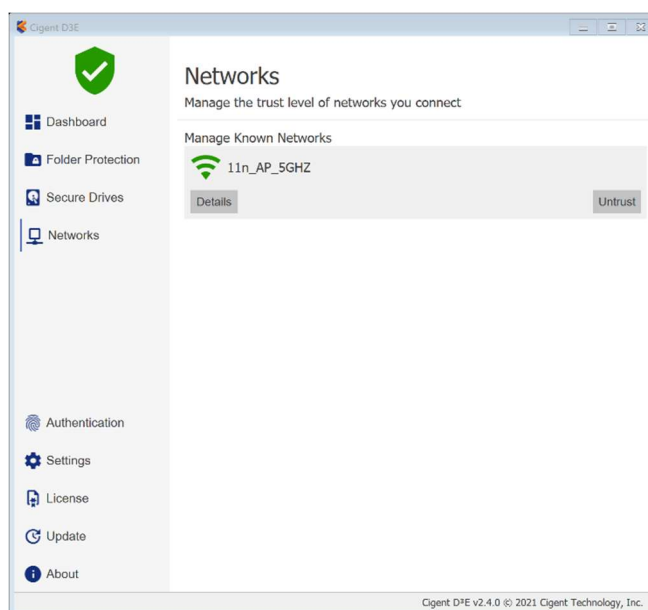
3. Switch back to the Dashboard. Note that Active Lock is engaged.
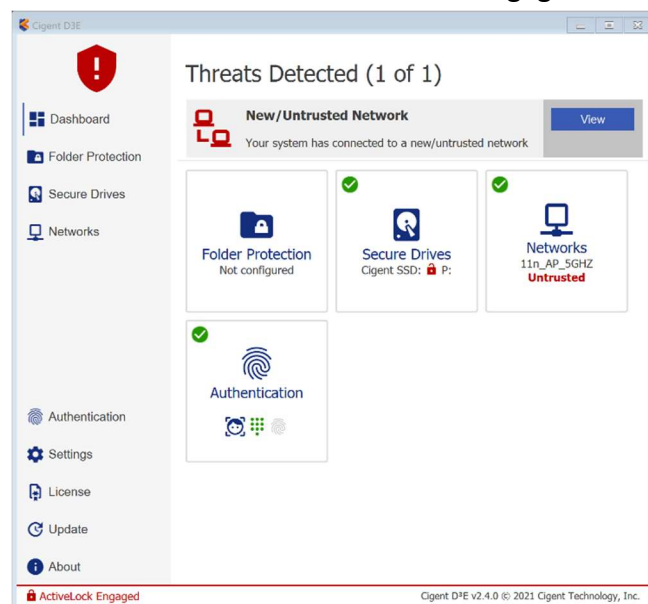
4. Return to the Networks page and click TRUST under your current network. You will need to enter your PIN.
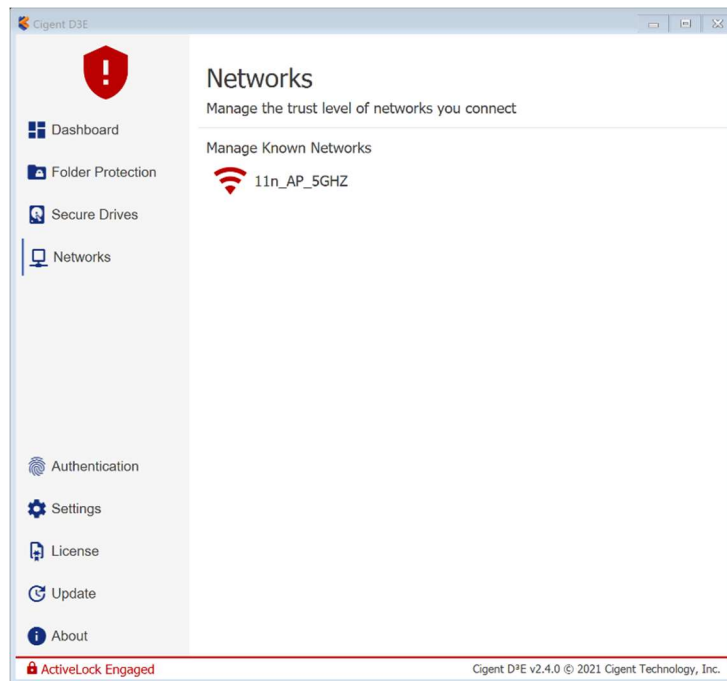
5. Switch back to the Dashboard page and note that Active Lock is disengaged.
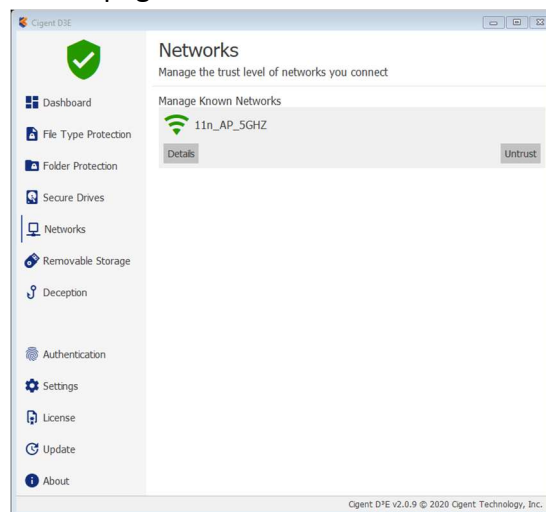
10   BarraCuda 515 SSD Advanced Features

10.1 KeepAlive

KeepAlive provides an extra layer of protection by creating a tighter trust connection between the BarraCuda 515 SSD firmware and the software (Cigent). When enabled, a non-replayable heartbeat starts between Cigent and the BarraCuda 515 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 BarraCuda 515 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.
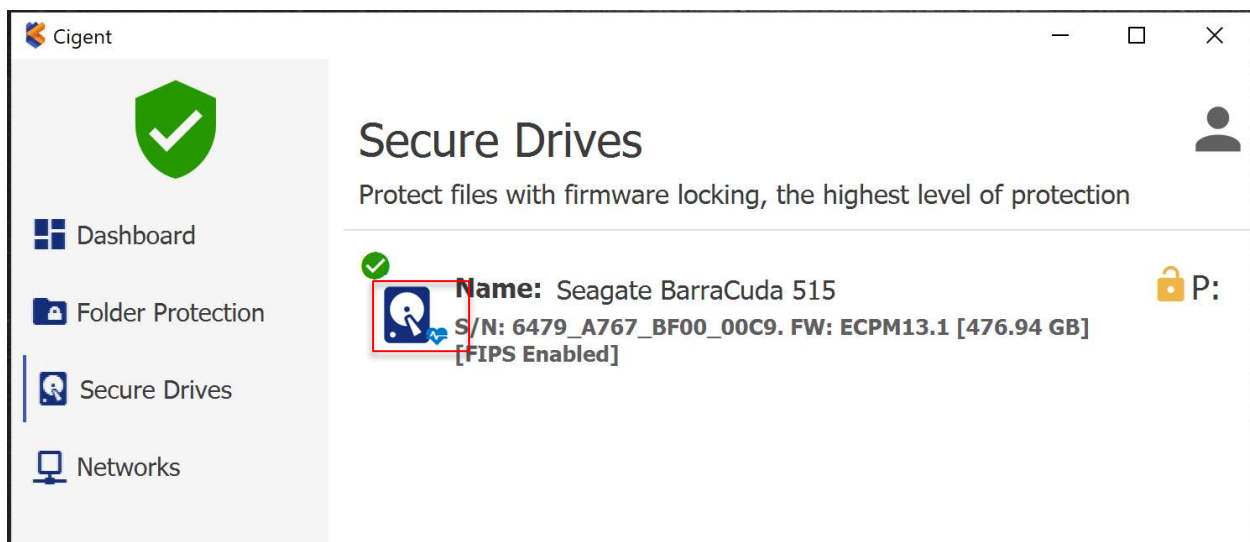
10.2   Command Log Audit

BarraCuda 515 SSDs automatically store every command send 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 BarraCuda 515 SSD and click **Advanced** to reveal the advanced features.
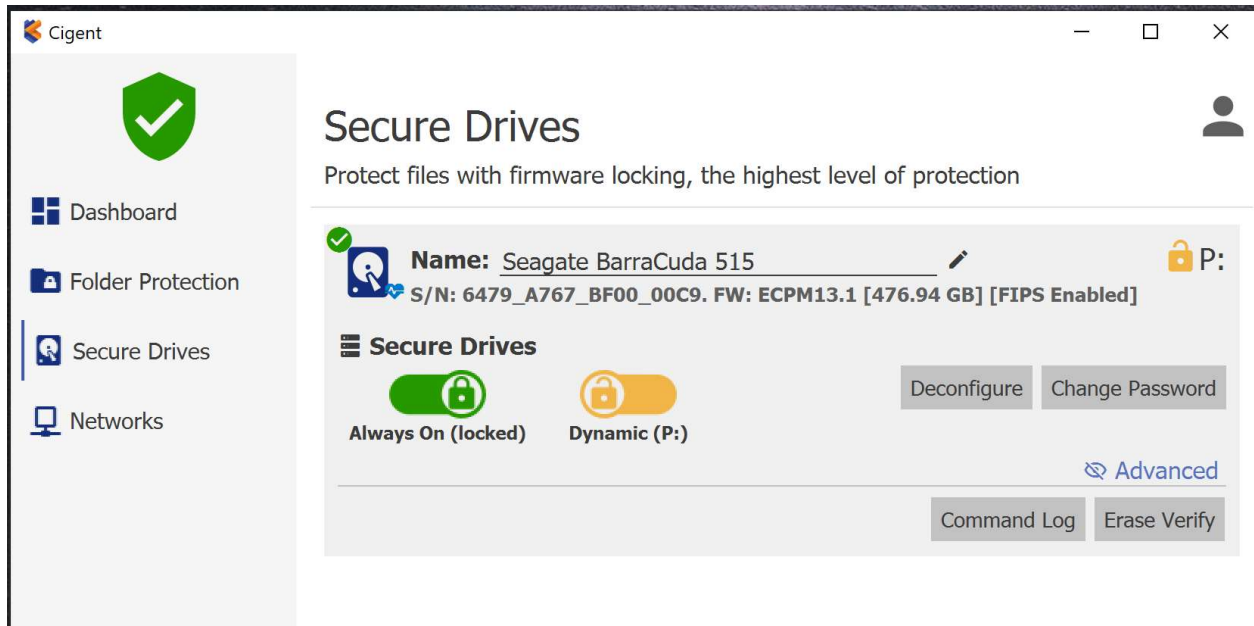
2. Click **Command Log** to open the Command Log Audit page. Click **Scan** to start the reading of the command log.
    Note: Reading the command log from the drive over USB especially can take several minutes.
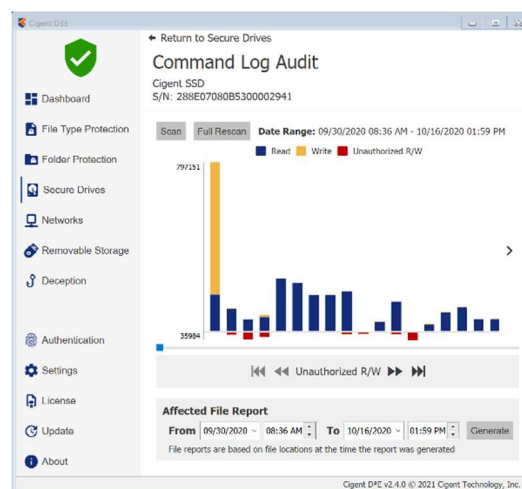
3. If this is a newer drive, you may have only a few data points. If this drive has been in use for a while, you may need to scroll the graph to the right to get to the newest information.
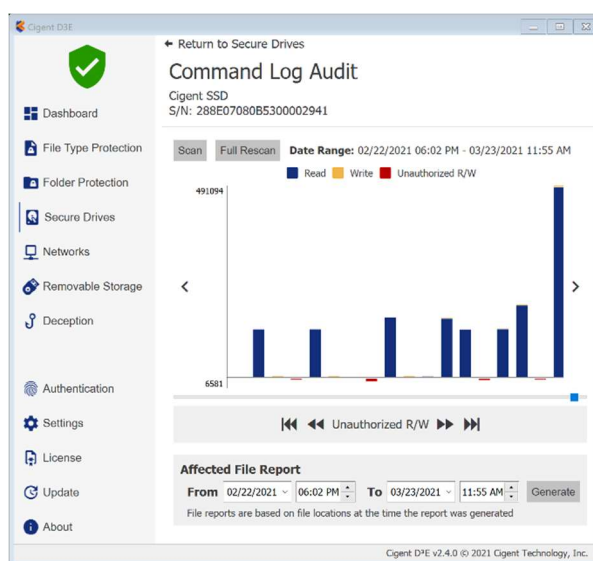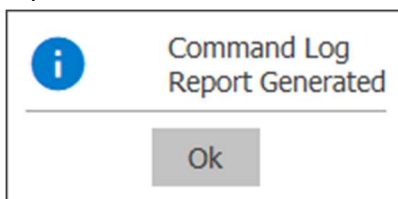
4. Click on a shorter bar in the graph to detailed results of each operation.
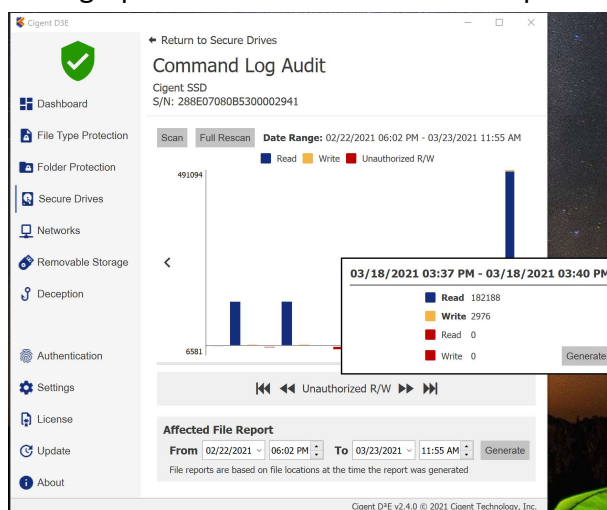
5. Click the Generate button to create a CSV file containing files to which the commands log entries currently map. Click Save and enter your PIN to authorize the action.
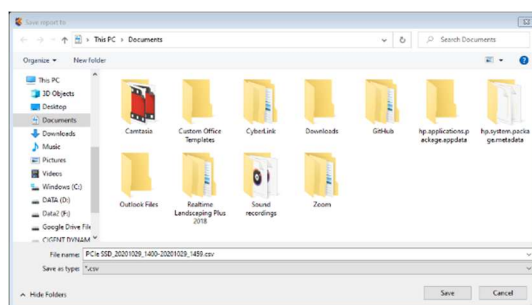
6. Click OK once the operation completes.

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.

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. BarraCuda 515 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.
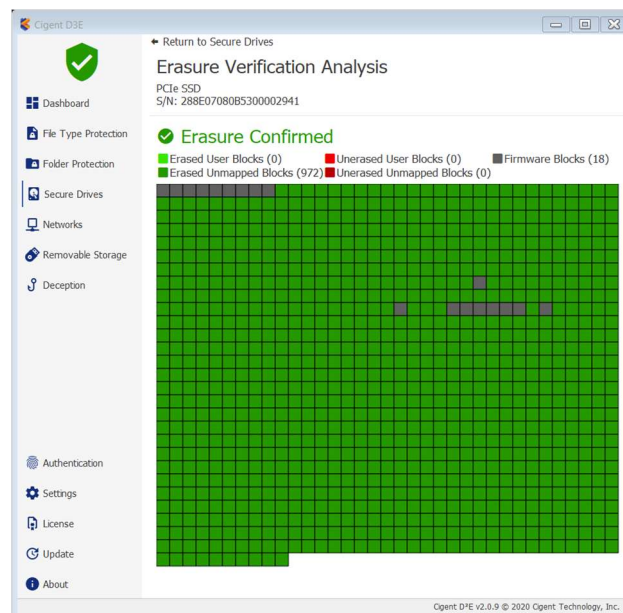
1. Select the BarraCuda 515 SSD and click **Advanced** to reveal the advanced features.
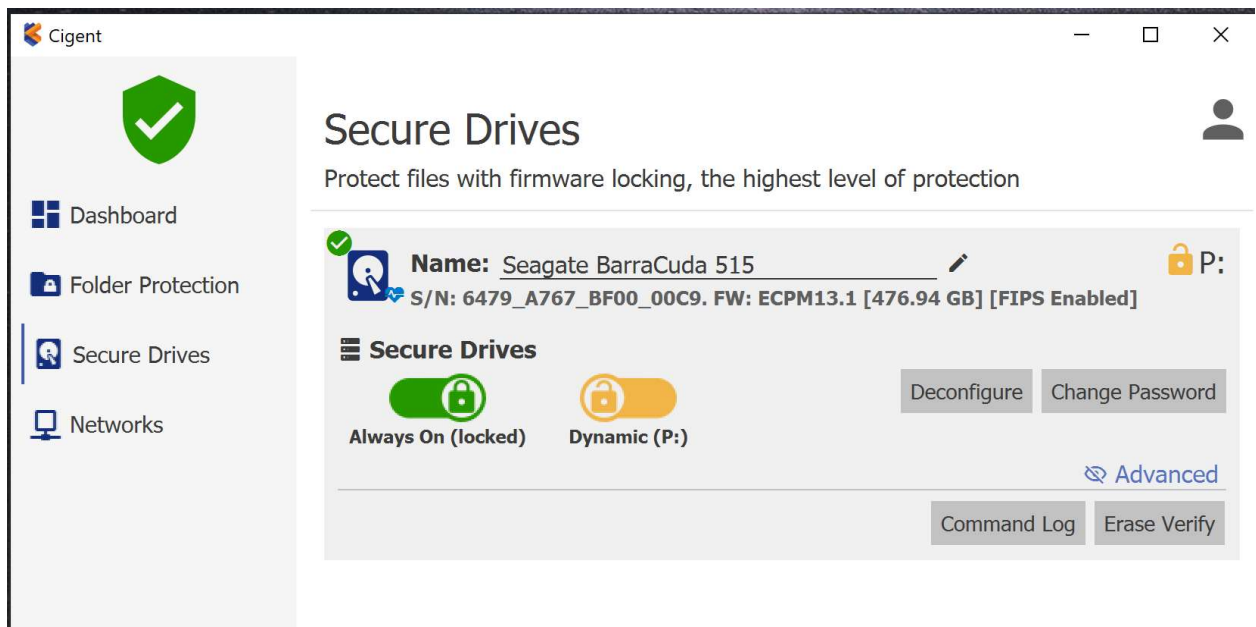
2. Click Erase Verify.
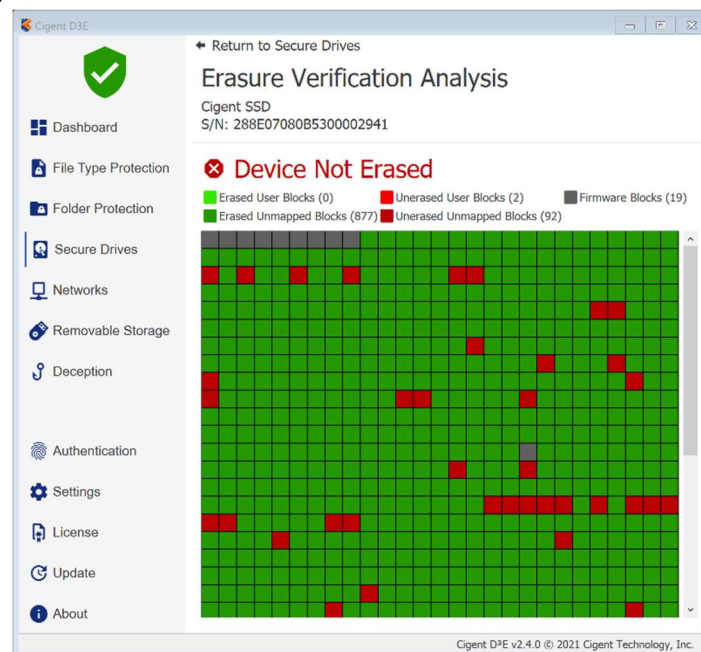
Cigent will indicate Drive Not Erased (as expected) with a count of erased and non-erased blocks from the unmapped and user areas. The map at the bottom is a logical display of the blocks by block number and color coded by its status.

For more information about Seagate BarraCuda 515 SSDs please visit ww.seagate.com