MP210372

MITRE PRODUCT

MITRE

Sponsor: AFLCMC/CROWS
Dept. No.: N141
Contract No.: FA8702-21-C-0001
Project No.: 03214PA0-SG

Bedford, MA

USAF Cyber Resiliency Office for Weapon Systems (CROWS) Evaluation of the Cigent Dynamic Data Defense Engine (D3E) App and Self-Encrypting Solid-State Drive

Feature Verification and Assessment of D3E on USAF Windows Platforms

Author: John G. Mulrey

July 2021

Approved By

Christian E Fiore II (CFIORE)

Digitally signed by Christian E Fiore II (CFIORE)
Date: 2021.07.22 15:55:55 -04'00'

22JUL2021

Christian E. Fiore II
CROWS Task Leader

Date

Abstract

At the request of the United States Air Force Cyber Resiliency Office for Weapons Systems (USAF CROWS) program, MITRE evaluated Cigent Technology's data-protection solution consisting of (1) Dynamic Data Defense Engine (D3E) software version 2.4.4 and (2) firmware protection afforded by D3E-equipped self-encrypting Solid-State Drives (SSDs).

D3E Software Protection

The purpose of the D3E app is to protect any endpoint files designated as sensitive, even when endpoint cybersecurity protection has been bypassed and user credentials have been compromised [1]. D3E supplements a platform's DoD CAC[1]/login authentication, requiring the use of additional authentication to access designated sensitive information under prescribed conditions.

Cigent D3E software lets administrators assign protection levels to file types and folders, based on the sensitivity of the data. The table below provides a brief overview of the D3E protection afforded for each data-sensitivity designation, as well as the locked status and authentication requirements for each data-protection level.

D3E Data-Protection Levels

Sensitivity of Data	Most Sensitive	Sensitive	Considered Not Sensitive
Data-Protection Requirements	Highest	High	Protection Unnecessary
D3E Protection Designation	***Always On***	***Dynamic***	None
D3E Locked Status	Locked by Default	Locked Conditionally When D3E Detects Threat	Unlocked
Requires MFA/PIN to Unlock Data	Always	Under Threat Conditions	N/A

D3E software currently does not encrypt files or folders to protect them. Instead, D3E uses "a mini-filter driver which blocks access to protected files, asking for authentication before allowing access. In the near future, there will be an option in D3E to encrypt files in protected folders. These can then be shared with others in a protected manner via email/cloud file systems/etc." [2]. Cigent is seeking FIPS[2] 140-2 certification for the future D3E encryption [3].

Cigent tailored their D3E software to work with the following Air Force platform types[3]:

- Windows 10 (Win10), 64-bit Operating System (OS)

[1] DoD CAC = Department of Defense Common Access Card
[2] FIPS = Federal Information Processing Standard(s)
[3] D3E also works with Windows 8, but the Air Force did not cite that as a needed D3E platform.

- Windows 7 (Win7), 64-bit OS
- Win7, 32-bit OS

MITRE evaluated D3E on each of these platform types. An overview of the evaluation results is contained in Section 3 and details are described in Appendix A.

D3E did an admirable job of protecting sensitive data. File types and folders requiring the highest level of security were marked for *Always On* protection, meaning that the information's default state was locked and inaccessible. Such information could be unlocked only by the user's entry of a PIN[4]. Sensitive information requiring a slightly lower level of security was marked for *Dynamic* protection. Files and folders with *Dynamic* protection normally are unlocked and accessible; such information was locked automatically only when D3E sensed a threat and engaged *ActiveLock*. When D3E's AI[5]-driven Analysis Engine determines that the threat level is elevated, "D3E responds by securely locking files, blocking suspicious devices, or sending an alert to a SIEM[6] or SOC[7]" [4]. Under *ActiveLock*, file types or folders designated for protection, whether *Dynamic* or *Always On*, are accessible only after authentication has been used.

We executed a variety of tests at each of the three laptops to ensure that D3E (1) triggered *ActiveLock* status when appropriate and (2) allowed or disallowed file access in accordance with data sensitivity and the threat status at the protected computer.

Cigent Firmware Protection

Cigent also supports *Firmware Locking* by means of D3E-equipped self-encrypting SSDs. The primary roles of Cigent firmware protection are data protection and information hiding. Cigent secure SSDs also support such features as undetectable data-access logs and verification of drive-erasure status. Cigent's K2 SSD "is in the process of FIPS 140-2 certification with expected timeframe of September this year" [3].

Important features of the self-encrypting SSDs are summarized below. We evaluated *Firmware Locking* using a Cigent-provided Win10 laptop.

- Data Protection: Firmware in the Cigent self-encrypting SSDs checks continuously to ensure that D3E and host security are running. If the firmware detects that security agents[8] are missing or have stopped, D3E engages *ActiveLock* and locks any files marked for *Dynamic* protection. (Files with *Always On* protection are locked by default; however, if any *Always On* files happen to be open when a security incident occurs, those files will be locked, as well.)
    - Among the ways Cigent SSDs protect information is the *KeepAlive* feature. *KeepAlive* tethers Cigent Secure SSDs to the D3E software running on them by means of a non-replayable heartbeat between the drive and D3E. When the feature is activated, Secure SSDs will enact *ActiveLock* and prevent file access if

[4] PIN = Personal Identification Number
[5] AI = Artificial Intelligence
[6] SIEM = Security Information and Event Management system
[7] SOC = Security Operations Center
[8] D3E is integrated with Windows Defender and other antivirus solutions registered with Windows Security Center [8].

the drive fails to receive the heartbeat signal in time. The feature is designed to prevent hackers from stopping D3E protection on unlocked Secure Drives.

- Information hiding: Secure drives/partitions become "invisible" when threats are detected. With *Always On* security, secure drives are locked. They remain unmounted and invisible to the Operating System (OS) until the administrator unlocks (mounts) them by following the prescribed authentication method. Similarly, secure drives marked for *Dynamic* security "disappear" from the Windows OS when a detected threat triggers D3E to lock them [1].
- Undetectable Data-Access Logs: Data access logs stored securely in SSD firmware cannot be detected or erased, yielding a valuable tool for post-breach analysis.
- Verification of Drive Erasure Status: Cigent's *True Erase* feature is useful for assessing the erasure status of attached SSDs. *True Erase* provides reliable feedback on whether a previously-wiped drive has, in fact, been erased, "report(ing) each block's erased or un-erased state after a wipe attempt" [1].

A detailed summary of the *Software & Firmware Locking* evaluations is contained in Appendix A to this report. Each of the D3E functions performed well, meeting the performance capabilities advertised in Cigent documentation. There were a few instances of anomalous or unexpected behavior, however, which MITRE identified to Cigent. Anomalies are listed below and summarized in greater detail in Appendix B. MITRE also offered suggestions about how to make D3E more convenient for the end user. Our recommendations are contained in Section 4 of this report.

Anomalies[9]:

1. Password/PIN reuse is allowed.
2. Honeypot files can be moved, changed, and deleted.
3. Windows Service host process periodically tries to access the default honeypot file.[10]
4. APPCRASH condition occurred on the Win7 64-bit laptop.

Summary:

The Cigent products performed well. MITRE recommends that Cigent D3E and Secure SSDs be considered for further evaluation. An Air Force *Innovation Pitch* event would be an excellent venue for Cigent to showcase its products. We believe that, in addition to its data-protection role, the Cigent solution could be beneficial for defensive and offensive cyber operations.

[9] The first two anomalies are attributable to D3E software, and modifications are expected to be easy to implement. Items three and four will require further testing.

[10] MITRE is working with Cigent to determine which process is attempting to access the *Deception* file. If the application is deemed legitimate, it could be designated a "Safe App." This would put a stop to the unwanted alarm conditions. Note that the Safe App feature requires a special license from Cigent, available to premium customers upon request.

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

1 Introduction

MITRE evaluated Cigent Technology's Dynamic Data Defense Engine (D3E) endpoint-protection application at the request of the United States Air Force Cyber Resiliency Office for Weapons Systems (USAF CROWS). This report documents MITRE's D3E evaluation.

Cigent data security has two modes of operation: (1) D3E *Software Locking* mode and (2) *Firmware Locking* mode for selected types of solid-state drives (SSDs)[11] with D3E software running on the SSD. *Software Locking* works on any Windows 10 (Win10) or Windows 7 (Win7) installation and protects files in "user-specified folders on any non-removable storage device" [4]. Cigent's *Firmware Locking* mode works with SATA[12]- and NVMe[13]-specific APIs[14] to secure dedicated partitions, which Windows view as drives. "Firmware locking mode is supported on HDDs[15] and SSDs supporting TCG[16] OPAL[17] [5] 2.0 and Cigent Secure SSDs" [4]. Also referred to as Cigent Secure SSD Storage, the product is compatible with Windows 10, 8, and 7 operating systems [6]. D3E software locks user-specified folders, and file types on Windows computers to protect the information from unauthorized access. *Firmware Locking* provides protection to entire drives (partitions). The locking/unlocking of these partitions is under the control of the D3E administrator.

We used three personal computers (PCs) and one external Universal Serial Bus (USB) drive in our assessment, as described below.

Cigent loaned a Windows 10 64-bit laptop for the MITRE assessment. The Cigent laptop was delivered with D3E version 1.6.10. We later upgraded this to version 2.4.4. We installed the machine on the NERVE[18] network, so that it would be accessible from remote locations. The Cigent PC was equipped with a CTI[19] SSD drive suitable for testing the Cigent firmware-based protection feature discussed in Sections 3.1 and 3.2 and in Sections 1 and 2 of Appendix A. It was possible to test D3E's software- and firmware-locking features on this laptop. Cigent also provided a secure USB external drive for our evaluation.

MITRE provided a pair of Win7 laptops, one with a 64-bit processor, and a second with a 32-bit processor. We installed D3E version 2.4.4 on each of the Win7 machines.

The hard drives in the MITRE PCs were not compatible with Cigent firmware-based protection; i.e., they did not match any of the SSD drive types listed in Section 2.2.1.1. Consequently, only D3E software-based protection was assessed on the MITRE laptops.

Section 2 contains a brief overview of the D3E application and firmware-locking data protection, identifying the Cigent solution's important features and benefits. Section 3 summarizes results of

[11] Refer to Section 2.2.1.1 for a list of SSD drive types that can support Cigent firmware locking.
[12] SATA = Serial Advanced Technology Attachment
[13] NVMe = Non-Volatile Memory Express
[14] API = Application Programming Interface
[15] HDD = Hard Disk Drive
[16] TCG = Trusted Computing Group
[17] OPAL is a TCG security standard for storage devices.
[18] NERVE = Networked Experimentation, Research, & Virtualization Environment
[19] CTI = Cigent Technology, Inc.

our evaluation. For brevity and ease of reading of the main document, the detailed, step-by-step examination of D3E and SSD features was deferred to Appendix A. Section 4 contains conclusions and recommendations for the D3E endpoint-security product. Appendix B contains a brief summary of the few anomalies that we encountered. Finally, Appendix C contains a brief description of D3E's central management console.

2 Cigent D3E Overview

Cigent data-protection solutions help prevent unauthorized access to sensitive files, while ensuring that authorized users can always access important data, even when the host system is already compromised.

D3E uses machine learning (ML) and user-behavior-analytics (UBA) techniques to authenticate user identity. D3E also continuously checks for malware intrusion, deploying sensors to monitor events and integrating with Windows Defender or other antivirus (AV) solutions registered with Windows Security Center. D3E feeds its sensor data and the AV-derived inputs into D3E's AI-based[20] Analysis Engine. When the Analysis Engine determines that the threat level is elevated, "D3E responds by securely locking files, blocking suspicious devices, or sending an alert to a SIEM[21] or SOC[22]" [4]. D3E sensors are listed in Section 2.1.1.1.

As mentioned earlier, Cigent data security has two operating modes, (1) D3E *Software Locking* mode and (2) *Firmware Locking* mode on approved SSDs. These two modes are described in Sections 2.1 and 2.2, respectively. The bulk of our assessment pertains to D3E software-based protection (for results and details, refer to Section 3.3 and Appendix Section A.3); however, we also evaluated Cigent firmware-based protection, using the Cigent loaner laptop and external USB drive, as described in Sections 3.1 and 3.2 and in Appendix Sections A.1 and A.2.

2.1 D3E – Software-Based Data Protection

D3E software-based protection employs two locking modes, ***Always On*** and ***Dynamic***, to render sensitive information impervious to data theft or ransomware when locked. The D3E administrator has control over which folders and file types fall into the ***Always On*** and ***Dynamic*** protection categories.

Section 2.1.1 describes D3E data protection for different sensitivity levels.

2.1.1 D3E Software Protection for Sensitive Data

- As its name implies, the *Always On* locking mode always requires one or more unlocking techniques (Multi-Factor Authentication, or MFA[23]) to access; i.e., file types, folders, and partitions[24] marked for *Always On* protection stay locked until a user fulfills the prescribed authentication requirements and unlocks the data. Typically, a system's most sensitive information would be marked for *Always On* protection. With *Always On* protection, "sensitive files are accessible for a very limited time and only on an as needed basis by the trusted user" [6]. Refer to Table 2-1.

[20] AI – Artificial intelligence
[21] SIEM = Security Information and Event Management system
[22] SOC = Security Operations Center
[23] The user's device login credentials serve as the first means of authentication; D3E authentication requirements constitute the second factor.
[24] Drives/partitions are marked for *Dynamic* or *Always On* protection only in *Firmware Locking* mode. With software-only protection, only folders and file types can be given *Dynamic* or *Always On* protection.

- If a file type, folder, or partition is marked for *Dynamic* protection, *ActiveLock* will engage and lock those entities whenever D3E determines that a threat has been encountered. (Refer to Section 2.1.1.1 for a discussion of the types of events that will trigger employment of *Dynamic* protection.) For file types, folders and partitions marked for *Dynamic* protection, the normal status is unlocked and accessible. *Dynamic* mode would be used to protect sensitive data that does not require the same level of privacy or security as information marked for *Always On* protection. Refer to Table 2-1.

Table 2-1 provides a brief overview of the D3E protection afforded for each data-sensitivity designation, as well as the locked status and authentication requirements for each data-protection level.

Table 2-1. D3E Data-Protection Levels

Sensitivity of Data	Most Sensitive	Sensitive	Considered Not Sensitive
Data-Protection Requirements	Highest	High	Protection Unnecessary
D3E Protection Designation	***Always On***	***Dynamic***	None
D3E Locked Status	Locked by Default	Locked Conditionally When D3E Detects Threat	Unlocked
Requires MFA/PIN to Unlock Data	Always	Under Threat Conditions	N/A

Note: In cases of dual assignment or overlap, ***Always On*** *protection supersedes* ***Dynamic*** *(Sometimes-On/Conditional) protection. Refer to Appendix Section A.3.6.2 for further discussion about protection overlap.*

The methods for unlocking data are the same in both the *Always On* and the *Dynamic* modes: the user/administrator uses an approved means of authentication. (Refer to Section 2.3 for a brief discussion of D3E authentication.) For our evaluation, we used only the PIN[25] method of authentication.

D3E also supports a *Group Lock* feature that locks files on multiple PCs in a preconfigured group of devices if a threat is detected on any member of the group [7]. MITRE did not evaluate D3E's *Group Lock* feature.

2.1.1.1 How D3E Protects Information

D3E software currently does not encrypt files or folders to protect them. Instead, D3E uses "a mini-filter driver which blocks access to protected files, asking for authentication before

[25] PIN = Personal Identification Number

allowing access. In the near future, there will be an option in D3E to encrypt files in protected folders. These can then be shared with others in a protected manner via email/cloud file systems/etc." [2]. Cigent is seeking FIPS[26] 140-2 certification for the forthcoming D3E encryption [3]. Cigent should expedite the certification process so that D3E can be considered for the protection of CUI[27] and FOUO[28] information.

2.1.2 Triggers for D3E *Dynamic* Protection

As noted above, D3E locks information whenever a threat is detected.

In *Dynamic* mode, D3E uses threat-detection sensors to monitor for the following [4, 8] [7]:

- Malware
- Fileless attacks
- Privilege escalation
- Endpoint security agent, e.g., Windows Defender, disabled
- Untrusted network detected (e.g., an attached network has not been explicitly trusted in D3E)
- An untrusted network device scans the Cigent-protected machine for open ports and connects to a Cigent *Deception* port
- External-media insertion detected (e.g., unauthorized USB drive inserted)
- Network and file *Deception* engines (e.g., port-scans or attempts to access honeypot files)
- Keyboard typing cadence, network usage (User Behavior Analytics (UBA))

2.1.3 *Deception*

D3E includes Network and File System *Deception* engines that detect attempts to access user-configured honeypot files or network scanning for open ports. When such attempts are detected, D3E automatically locks all file types and folders marked for *Dynamic* or *Always On* protection[29]. Cigent claims that the D3E *Deception* engines "provide virtually zero false-positive indications of hacking activity" [1]. *Note: Care should be taken when naming and situating honeypot files, to ensure that they are not inadvertently accessed by innocent users; such accidental accesses would cause inconvenience for users and administrators.*

2.1.3.1 *Deception* Files

Deception files are honeypots that help track unauthorized access to the host system; they are intended to attract would-be attackers with enticing file names and locations. D3E creates a

[26] FIPS = Federal Information Processing Standard(s)
[27] CUI = Controlled Unclassified Information
[28] FOUO = For Official Use Only
[29] As noted elsewhere in this document, file types and folders marked for *Always On* protection are usually in a locked state. If they happen to be unlocked when *ActiveLock* is triggered, D3E will lock them.

default *Deception* file called *passwords.xls* in local users' ***Documents*** directories. D3E users can create other *Deception* files in locations of their choice. Attempts to open *Deception* files trigger *ActiveLock*, so that all file types/folders/partitions marked for *Dynamic* or *Always On* protection will be locked, and the prescribed authentication method for the device will be required to access protected information.

The D3E Dashboard hides *Deception* files for security, but D3E administrators can display their locations and file names by clicking on the ***Show All*** icon and using the prescribed authentication method. The left side of Figure 2-1 shows the normal, obfuscated *Deception*-file view at the D3E desktop, while the right side of the figure displays the post-authentication version.

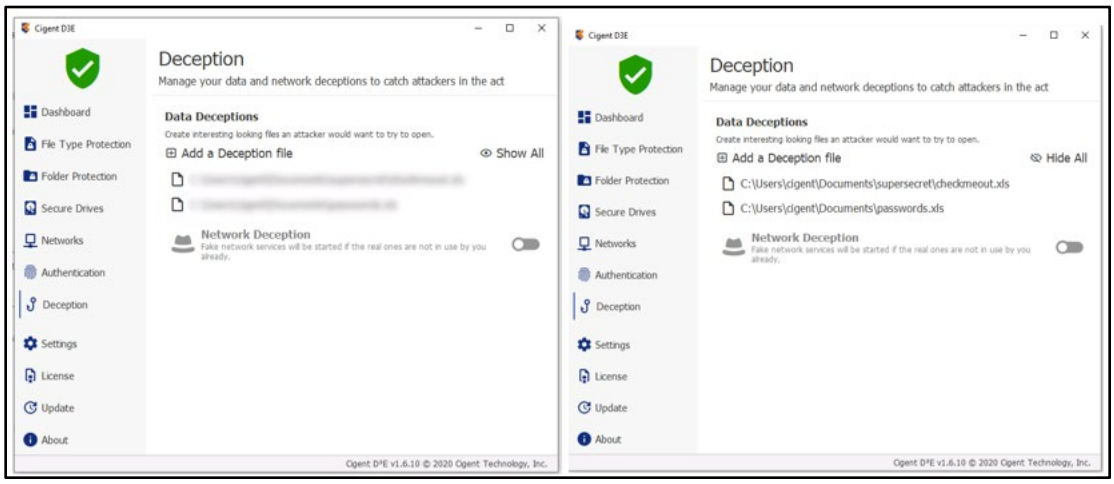


Figure 2-1. *Deception* File Locations – Obfuscated and Displayed

2.1.3.2 *Network Manager* – Cigent *Deception* Ports

Network Manager starts fake services on commonly attacked ports if they are not already in use. Examples include illusory copies of commonly hacked File Transfer Protocol (FTP) or Telnet[30] services.

If a network device scans a D3E-protected host for open ports and connects to a Cigent *Deception* port, D3E will trigger *ActiveLock* to protect sensitive information.

2.2 Firmware-Based Data Protection

D3E's robust software-based file-protection capabilities notwithstanding, software-only protection has known limitations that allow built-in protections to be bypassed [7]:

- Disabling of the endpoint's security applications, e.g., Windows Defender
- Theft of cryptographic keys
- Physical removal of the hard drive

[30] Telnet stands for Terminal Network.

- Bypassing the PC's OS by booting from another OS

Cigent's firmware-locking features supplement the software-locking capability cited in Section 2.1. The *Firmware Locking* mode works with SATA- and NVMe-specific APIs to secure dedicated partitions cryptographically. Section 2.2.1 below contains further information about Cigent firmware-based protection and self-encrypting SSDs.

2.2.1 Self-Encrypting SSDs

Cigent claims that its self-encrypting SSDs address the vulnerabilities of software-only protection itemized above. Self-encrypting SSDs running D3E software automatically become undetectable to attackers as soon as a threat is detected by the Analysis Engine. Files on such drives can be accessed only when the administrator uses the approved means of authentication to unlock them.

Section 2.2.1.3 provides more details about the features of Cigent's self-encrypting SSDs.

2.2.1.1 How Cigent Self-Encrypting SSDs Protect Data

Cigent secure SSDs protect data by means of encryption. "The SSD provides the encryption for every file stored on it. On top of that, the partitions are 'locked' using a key derived from the password used during configuration. To unlock a drive, D3E authenticates the user via the chosen auth method, and then unlocks the drive using the key. … So, the PIN is not related to the key itself. That is how we can switch between PIN and other auth methods like CAC[31] in the future" [2].

Cigent's K2 SSD is scheduled to be certified as FIPS 140-2 compliant in September 2021 [3]. Cigent should make every effort to ensure that this effort stays on track, so that the SSDs can be considered for protection of CUI and FOUO data.

2.2.1.2 Drive Types Supporting Cigent *Firmware Locking* Mode [4] [6] [7] [9]

Firmware Locking is supported on the following drive types [4]:

- HDDs and SSDs that support TCG OPAL 2.0
- Cigent Secure SSDs

The following three TCG OPAL 2.0 drive configurations currently are supported, each in sizes of 512GB, 1TB, and 2TB:

(1) NVMe[32] M.2 Internal SSD

(2) SATA M.2 2½" Internal SSD

(3) USB External SSD

Cigent summarizes the hardware options of their Secure SSD as follows: "*Available in K2 NVMe internal and external configurations, the Cigent Secure SSD comes in three sizes —512GB, 1TB,*

[31] CAC = Common Access Card
[32] NVMe = Non-Volatile Memory Express

and 2TB. 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" [6].

In each configuration, the self-encrypting SSD includes D3E's software-based functionality, as well.

2.2.1.3 Important Features of the Self-Encrypting SSDs [7]

- Custom firmware continuously checks to make sure D3E and host security agents are running. If they aren't, files marked for protection are locked.
- Data access logs are stored securely in firmware for post-breach analysis. Audit trails cannot be wiped [1]. This represents a significant Defensive Cyber Operations (DCO) capability.
- The *KeepAlive* (tethering) feature binds Cigent Secure SSDs to the D3E software running on them by means of a non-replayable heartbeat between the drive and D3E. When the feature license is turned on, Secure SSDs will enact *ActiveLock* and prevent file access if the drive fails to receive the heartbeat signal in time. The feature is intended to prevent hackers from stopping D3E protection on unlocked Secure Drives.
- Cigent's *True Erase*™ firmware feature indicates whether an erased Cigent SSD hard drive still contains data. *True Erase* supports "extended erasure verification commands to check each and every mapped and unmapped block to verify the data has been removed" [8]. Secure, verifiable data erasure from hard drives helps prevent unauthorized access to sensitive or classified information.
- With *Always On* security, secure drives are locked by default. They remain unmounted and invisible to the OS until the administrator unlocks (mounts) them by following the prescribed authentication method. Similarly, secure drives marked for *Dynamic* security "disappear" from the Windows OS when a detected threat triggers D3E to lock them [1].

2.2.1.4 Automatic Detection of Supported Self-Encrypting SSDs

D3E detects automatically whether a supported drive is installed and displays the information in the D3E Dashboard. Click on ***Secure Drives*** in either panel of the dashboard screen. See Figure 2-2.

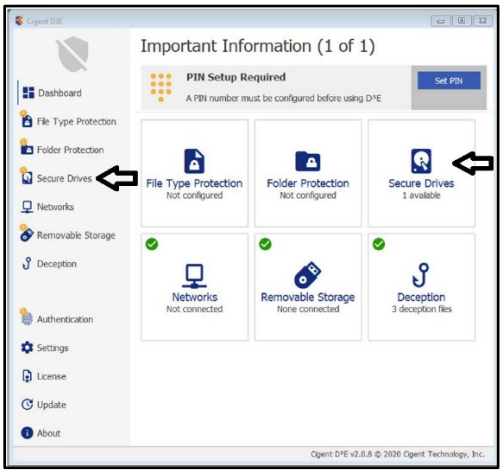


Figure 2-2. D3E Dashboard [4]

When D3E detects a supported drive type, clicking on ***Secure Drives*** yields a screen like the one in Figure 2-3. If no supported drive type is found, the display will appear as shown in Figure 2-4.

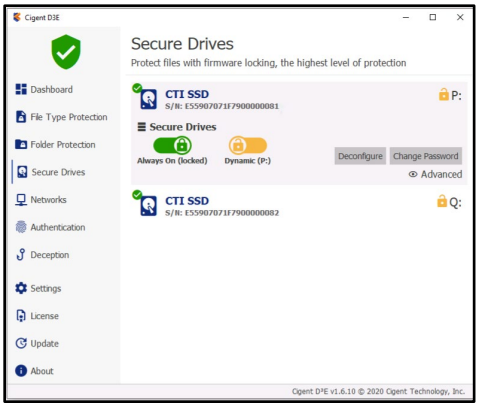


Figure 2-3. Supported Drive Type Found

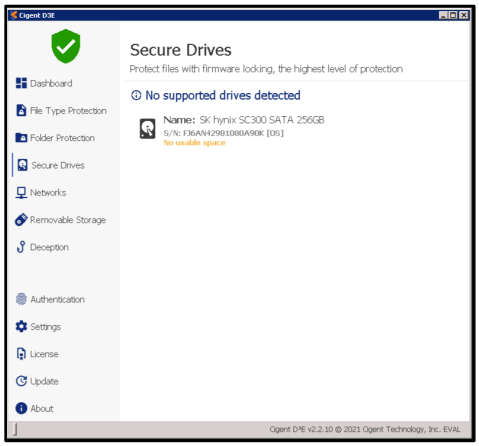


Figure 2-4. Supported Drive Type Not Found

2.3 D3E Authentication (Unlocking) Methods

D3E supplements a platform's DoD CAC/login authentication, requiring the use of additional authentication to access designated sensitive information under prescribed conditions.

In our evaluation, the supplementary authentication method was PIN[33] entry. D3E also supports facial recognition and fingerprint scans as means of authentication and accommodates *Windows Hello*[34] and *Google Authenticator*[35]. Cigent also is working with the Air Force to add DoD CAC as a means of MFA[36] for D3E.

[33] PIN = Personal Identification Number
[34] *Windows Hello* allows access to Win10 devices by means of fingerprint, facial recognition, or a secure PIN [10].
[35] *Google Authenticator* provides two-step authentication that supplements a user's password with a Google-provided one-time authentication code [11].
[36] The user's device login credentials serve as the first means of authentication; D3E authentication requirements constitute the second factor.

3 Functionality Testing Highlights

This section summarizes results of the D3E evaluation. A detailed, step-by-step examination of the D3E features is contained in Appendix A.

3.1 Cigent *Firmware Locking* Mode

The evaluation steps in this subsection were performed only on the Cigent Win10 laptop.

A high-level summary of the Cigent *Firmware Locking* Mode Evaluation is contained in Table 3-1 below.

Table 3-1. Cigent *Firmware Locking* Mode Evaluation – Results

Feature Name	Results	Comments	✓ / X
SSD Config/ De-Config	Configuring and de-configuring Secure SSDs was straightforward. Performance satisfied advertised capabilities.	D3E permitted reuse of an old SSD provisioning password. We recommend that Cigent use NIST SP 800-63-3 as a guide for constructing robust digital identities.	✓
***Always On* and *Dynamic* Protection**	The feature performed well and met advertised capabilities. There were no issues accessing or manipulating *Dynamic* and *Always On* files on the Cigent Secure Drive.		✓
***Deception* Files**	D3E File *Deception* behaved as advertised, triggering *ActiveLock* whenever an attempt was made to access a *Deception* file.	Although attempts to open user-created and system-generated *Deception* files triggered the appropriate responses, it was possible to move and edit those files and copy them back to the honeypot location. Cigent has identified a fix for the issue, which will be resolved in the next D3E build.	✓/?

AV Integration	D3E performed as expected, in that it triggered *ActiveLock* when Windows Defender was turned off.	After we ran the feature evaluation and re-activated *Real-time protection* in the host laptop, D3E persisted in detecting an antivirus-disabled threat, even though virus and threat-protection settings had been restored to their original state. This turned out to be appropriate behavior, because the protection definitions at the Win10 laptop were out of date.	✓
Network Manager	The *Network Manager* feature functioned as advertised on the Win10 Cigent laptop equipped with Secure Drives.		✓

3.2 Cigent Secure SSD Features

The evaluation steps in this subsection were performed only on the Cigent Win10 laptop.

A high-level summary of the Cigent Secure SSD Features Evaluation is contained in Table 3-2 below.

Table 3-2. Cigent Secure SSD Features Evaluation – Results

Feature Name	Results	Comments	✓ / X
Command Log Audit	The *Command Log Audit* feature functioned as advertised on the Win10 Cigent laptop equipped with Secure Drives.		✓

True Erase	The D3E *True Erase* feature functioned as advertised on the Win10 Cigent laptop equipped with Secure Drives.		✓
***KeepAlive* (Tethering)**	The *KeepAlive* SSD feature generally performed as advertised. When the heartbeat tether between the SSD and D3E was severed, firmware in the drive locked the *Always On* drive, so that it was not possible to open files or write to that drive. In other words, when the heartbeat stopped, the *Always On* drive was protected, even though the D3E service had stopped. It was possible to open the *Dynamic* Drive and write to it, but that was expected.	We did notice an anomaly in the Cigent documentation. Reference [8] states that "In less than 30 seconds, the script output will start indicating 0 files copied and you will receive a Windows error indicating Write Protect Error. Press Ctrl-C to terminate the script." In fact, Windows gave the ***ERROR Verify*** message shown in Figure A-69.	✓

3.3 D3E *Software Locking* Mode

We ran *Software Locking* procedures on the two Win7 test laptops. In a few instances, we supplemented earlier testing on the Cigent SSD-equipped Win10 laptop and ran the software-locking tests on that machine, as well.

A high-level summary of the D3E *Software Locking* Mode Evaluation is contained in Table 3-3 below.

Table 3-3. D3E *Software Locking* Mode Evaluation – Results

Feature Name	Results	Comments	✓ / X
Folder Protection	The D3E folder-protection feature met expectations. Segregating important information into *Always On* and *Dynamic* folders is an excellent means of protecting sensitive data.	This feature was tested on all three evaluation laptops.	✓
***Always On* and *Dynamic* Protection**	The feature performed well and met advertised capabilities.	This part of the evaluation was done on the Win7 laptops. Earlier testing on the Cigent Win10 laptop yielded similar good results. (See Table 3-1.)	✓
***Deception* Files**	D3E File *Deception* behaved as advertised, triggering *ActiveLock* whenever an attempt was made to access a *Deception* file.	The anomalies cited during the Cigent Win10 laptop evaluation recurred during the Win7 testing. Refer to Table 3-1.	✓ Refer to Table 3-1.
AV Integration	D3E performed as expected, triggering *ActiveLock* when Windows Defender was turned off.		✓
Network Manager	The *Network Manager* feature functioned as advertised on the MITRE Win7 laptops.	The "untrust" and network-scanning components of the *Network Manager* feature both performed well.	✓
File Extension Protection	*File Extension protection* worked well, performing as advertised.	We evaluated this feature on all three laptops.	✓

3.4 *Removable Storage Protection*

We tested *Removable Storage Protection* on each of the three evaluation laptops. A high-level summary of the evaluation results is contained in Table 3-4 below.

Table 3-4. *Removable Storage Protection* Evaluation – Results

Feature Name	Results	Comments	✓ / X
Removable Storage Protection	The feature behaved appropriately. It was possible to access files on a storage device only when the device was trusted in D3E. *Removable Storage Protection* prevented access to files on an untrusted removable-storage device without affecting access to files on the laptop itself.	We noticed slightly different behavior when evaluating *Removable Storage Protection* on the SSD-equipped Cigent Win10 laptop. The SSD-equipped laptop provides the option to "forget" a removable storage device after it has been untrusted. The next time the storage device is connected to the laptop, the user must make an explicit choice to trust the device.	✓

4 Conclusions and Recommendations

4.1 Overall Impression

Our impression of the data-protection features of Cigent's D3E software and self-encrypting SSDs was favorable. The dual firmware- and software-protection approaches combine to form a strong defense against tampering and theft of sensitive data. The *Always On* protection designation was assigned to our test systems' most sensitive information. As the name implies, file types and folders with *Always On* security were locked and inaccessible until the D3E administrator explicitly granted access to the information. Sensitive information requiring less protection than the *Always On* variety was marked for *Dynamic* protection, which locked the data only when D3E or the host detected threat conditions.

The D3E tool is flexible. The system administrator has complete control over which folders and file types are assigned *Always On* or *Dynamic* protection status. Similarly, when configuring Secure SSDs, the administrator gets to choose what percentage of each drive is given full-time, *Always On* protection.

The benefits of Secure SSDs, beyond data protection, are covered in Sections 2.2 and A.2, but the advantages of a couple of SSD features bear repeating.

- Self-encrypting SSD drives/partitions designated for *Always On* protection are unmounted and "invisible" until they are unlocked (temporarily) by the D3E administrator. This capability has obvious benefits for data security, because information on the protected drive cannot be seen, let alone accessed, by malefactors. Looking beyond data protection, the feature could yield additional cybersecurity benefits and should be investigated further.
- Among the ways Cigent SSDs protect information is the *KeepAlive* feature. *KeepAlive* tethers Cigent Secure SSDs to the D3E software running on them using a non-replayable heartbeat between the drive and D3E. Secure SSDs with the *KeepAlive* feature will enact *ActiveLock* and prevent file access if the drive fails to receive the heartbeat signal within a specified time. The feature is designed to prevent hackers from stopping D3E protection on unlocked Secure Drives.
- Cigent Secure SSDs also have a *Command Log Audit* feature that automatically stores every command sent to the drive. Commands are kept in a tamperproof location in the SSD's memory for post-breach analysis; they cannot be erased. This represents a significant DCO capability. The feature also can detect whether D3E was running at the time each command was issued, letting forensic analysts know whether the command was authorized.

In summary, MITRE recommends that Cigent D3E and Secure SSDs be considered for further evaluation. An Air Force *Innovation Pitch* event would be an excellent venue for Cigent to showcase its products. We believe that, in addition to its data-protection role, the Cigent solution could be beneficial for defensive and offensive cyber operations. We do, however, have some recommendations affecting D3E deployment, as well as a few suggestions for feature enhancements.

4.2 Deployment Recommendations

4.2.1 Use Standardized Data-Protection Designations

As noted above, the D3E tool is very flexible. That flexibility, however, could lead to inconsistencies from system to system. If D3E were deployed on a wide scale throughout the DoD, it would be wise to have a standard in place that defines how information should be categorized. This would help prevent the same data having different designations on multiple systems. The standard should:

- Identify the level of data sensitivity requiring *Always On* protection.
- Determine which level of sensitivity needs to be marked for *Dynamic* protection.
- Classify the types of data that will not require protection, i.e., files that will be afforded neither *Always On* nor *Dynamic* protection.

4.2.2 Deploy a Central Management Console

We evaluated D3E functionality separately on individual laptops to assess performance on different types of platforms. In that deployment mode, however, each laptop's administrator manages threat responses for just the individual machine. This model could lead to inconsistent and potentially unsafe threat handling. A more secure and practical mode of deployment would be to have a centralized D3E manager respond to threats across a network. D3E can be deployed with a central management console capable of monitoring and managing data security throughout a network and responding either manually or automatically. Refer to Appendix C for a brief discussion of the D3E Central Management Console.

4.2.3 Managing Files with *Always On* and *Dynamic* Protection

4.2.3.1 Use File-Extension Protection Only for Uncommon File Types

For common file extensions, such as *docx*, *pdf*, *xlsx*, and *txt*, it is preferable to segregate files needing *Always On* or *Dynamic* protection into folders marked explicitly for the desired treatment and to use D3E's *Folder Protection* feature. Use *File Extension* protection only for less common file-extension types, and only if needed. The extra administrative steps required to collect sensitive information into separate folders may be initially cumbersome, but it will avoid the potential confusion that could result from the *Folder/File Extension* conflict described in Appendix Section A.3.6.2.

4.2.3.2 Purge Extra Copies of Sensitive Files

When moving sensitive information into folders for *Dynamic* or *Always On* protection, make sure that residual copies or variants of the information do not exist in unprotected folders.

4.3 Suggestions for Feature Enhancements

4.3.1 Expedite FIPS 140-2 certification for D3E Software and Cigent SSDs

As noted in Section 2.1.1.1, D3E software does not yet provide FIPS 140-2 certified encryption, though Cigent intends to obtain that certification for their forthcoming file-encryption capability. Similarly, FIPS 140-2 certification for their K2 SSD is on Cigent's agenda. Certification for the K2 drives is expected in September 2021. Cigent should strive to keep these certification efforts on track, so that the Cigent solution can be considered for protection of FOUO and CUI information.

4.3.2 Implement DoD CAC as a Method of D3E Authentication

It was pointed out earlier that Cigent is working on adding DoD CAC as a method of D3E authentication. This is a positive development, as CAC is ubiquitous throughout the DoD and represents a proven means of MFA. Cigent should make every effort to ensure that DoD CAC is incorporated into the D3E solution as soon as possible.

4.3.3 Allow Multiple Administrator Actions per Authentication

The current D3E build requires the system administrator to enter authentication each time an unlock or other change command is issued. This method of operating is secure, and not terribly onerous; however, rather than requiring authentication prior to each administrative action, allowing the D3E administrator to perform multiple operations under a single authentication, should be considered as a time-saving device.

4.3.4 Password and PIN Reuse

As noted in the evaluation details in Appendix A, D3E permitted reuse of an old SSD-provisioning password. This was convenient for the purpose of our evaluation, but National Institute of Standards and Technology (NIST), DoD, and other agencies recommend stricter practices for reuse and strength.

- We recommend that D3E consult NIST Special Publication (SP) 800-63-3 [10] as a guide for constructing robust digital identities.[37]
- Microsoft recommendations [11] for restricting password reuse on Win10 platforms (shown below) offer useful guidance.
    - Under *Security Settings/Account Policies*, set the **Enforce password history** parameter value to 24.
    - The *Maximum password age* should be set to between 60 and 90 days.

[37] Cigent Response: "Cigent will add the ability for password policy enforcement for both the Secure SSD password and authentication PIN in the upcoming release. It is also worth noting that that file authentication via CAC/PIV will be supported in a near term release" [19].

  - The *Minimum password age* should be configured so that passwords cannot be changed immediately.

- Ideally, password policy decisions should be controlled by a single administrator at a Central Management Console, and local users/administrators should not be able to weaken the assigned policy.
- Weaker password enforcement should be allowed only in non-fielded test environments.
- At a minimum, D3E should issue a warning to the user about following DoD password guidance.
- Similar, stricter guidance should apply to setting the D3E PIN, as well.

4.3.5 Consider Implementing *File Name Protection*

MITRE believes that adding a new *File Name Protection* feature to supplement *Folder* and *File Extension Protection*, would enhance D3E. D3E administrators would be able to build an alphabetized list of files that receive either *Always On* or *Dynamic* protection. Such an implementation would avoid the *Folder/File Extension* conflict and confusion described in Appendix Section A.3.6.2.

E.g.,
- Sensitive personnel data.docx *Dynamic Protection*
- Attack plans 2021.pdf *Always On Protection*

- In addition, use of wild-card characters would help to ensure that outdated or other variants of sensitive files receive appropriate protection.

E.g.,
- Sensitive personnel*.* *Dynamic Protection*
- Attack plans 20**.* *Always On Protection*

4.3.6 Alert Users to Potentially Sensitive Information in Unprotected Folders

Section 4.2.3.2 warns users to purge extra copies of sensitive files to ensure that sensitive information is not left unintentionally in unprotected folders. Automating this warning, alerting administrators of unprotected copies or variants of sensitive files, would enhance D3E.

5 References

[1] Cigent Technology, "Cigent D3E - Layer Zero Data Protection," 2021. [Online]. Available: https://www.cigent.com/cigent-d3e.

[2] D. Wolf, *6/17/21 email to John Mulrey: "Question about D3E FIPS 140-2 compliance",* Nashua, NH: Cigent Technology, 2021.

[3] Mulrey and Wolf, *Mulrey/Wolf Correspondence, 16 June 2021,* Amherst, NH: Cigent Technology, 2021.

[4] Cigent Technology, Cigent Technology Dynamic Data Defense Engine (D3E) Quick Start and Evaluation Guide, Version 2, Fort Myers, FL: Cigent Technology, 2020.

[5] Trusted Computing Group, "TCG Storage Security Subsystem Class: Opal; Specification Version 2.01, Revision 1.00," 5 August 2015. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_SSC_v2.01_rev1.00.pdf#page=12.

[6] Cigent Technology, "Cigent Secure SSD Storage," Cigent Technology, 2021. [Online]. Available: https://www.cigent.com/cigent-secure-ssd.

[7] Cigent Technology, "Cigent Solutions Overview - Briefing to USAF 7/2/2020," Cigent Technology, Ft. Myers, FL, 2020.

[8] Cigent Technology, D3E Premium Evaluation Guide, Fort Myers, FL: Cigent Technology, 2021.

[9] Cigent Technology, "Cigent D3E Firmware Locking," Cigent Technology, 21 August 2019. [Online]. Available: https://www.youtube.com/watch?v=1-xk87LXjRs.

[10] National Institute of Standards and Technology, "NIST Special Publication 800-63-3: Digital Identity Guidelines," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html.

[11] Microsoft Corporation, "Enforce Password History," 19 April 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enforce-password-history.

[12] Cigent Technology / Dave Wolf, *Zoom Presentation on D3E Central Management Console,* D. Wolf, Ed., Nashua, NH: Cigent Technology, 2021.

[13] Microsoft, "Microsoft Update Catalog (KB4474419)," Microsoft Corporation , 2021. [Online]. Available: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4474419.

[14] Microsoft Corporation, "Microsoft Update Catalog (KB976932)," Microsoft Corporation, 2021. [Online]. Available: https://www.catalog.update.microsoft.com/Search.aspx?q=KB976932.

[15] Cigent Technology, "Cigent D3E Locking All Connected Drives," Cigent Technology, 19 April 2020. [Online]. Available: https://www.youtube.com/watch?v=SEJfuSZ7nFo.

[16] S. Park and J. Lee, "Analysis of the K2 Scheduler for a Real-Time System with an SSD," 6 April 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/7/865/htm.

[17] Microsoft Corporation, "Learn about Windows Hello and set it up," Microsoft Corp., 2021. [Online]. Available: https://support.microsoft.com/en-us/windows/learn-about-windows-hello-and-set-it-up-dae28983-8242-bb2a-d3d1-87c9d265a5f0.

[18] Google, "Get verification Codes with Google Authenticator," Google, 2021. [Online]. Available: https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=en.

[19] Mulrey and Wolf, *Correspondence - Dave Wolf and John Mulrey, 6 June 2021,* Nashua, NH, 2021.

Haec pagina vacua intentione restat[38].

[38] This page is intentionally blank.

Appendix A D3E Evaluation Details

Result summaries from the evaluation are contained in Section 3 of this report. Details have been moved to this appendix for ease of reading.

The D3E functional testing described below largely follows the outline provided in references [4] and [8].

D3E *Software Locking* mode was tested for each of the three laptop configurations. *Firmware Locking* and Secure Solid-State Drive (SSD) features, however, were evaluated only on the Cigent loaner Win10 machine and the loaner USB drive.

A.1 Cigent *Firmware Locking* Mode

The evaluation steps in this subsection were performed only on the Cigent Win10 laptop.

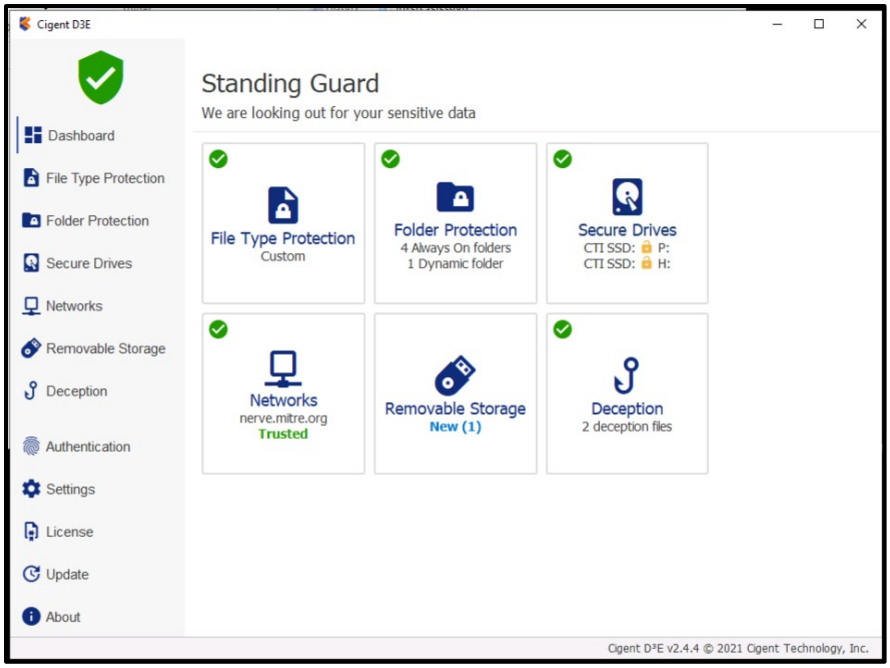


Figure A-1. V2.4.4 Dashboard Indicating that Secure Drives are Installed

The D3E Dashboard shown in Figure A-1 indicates that the computer has at least one secure SSD drive. Therefore, the steps in Sections A.1 and A.2 can be executed.

A.1.1 Configure Cigent Secure SSD Drives

In this evaluation step, we will configure the secure drive labeled E55907071F7900000081.

A.1.1.1 Review Current Secure Drive Configuration

Figure A-1 through Figure A-3 show that the Cigent laptop under evaluation has two physical drives. Note that each drive has a distinct serial number (S/N). Note also that each physical drive

has two partitions, L & P for the …81 drive, and G & H[39] for the …82 drive. Each partition is mounted as a separate drive in Windows. D3E protection was turned off temporarily, so that the *Always On* drives L & G could be seen in the dashboard and in Windows Explorer, as shown in Figure A-2 and Figure A-5.

Drives L & P represent the *Always On* and *Dynamic* drives (partitions), respectively, for the Cigent laptop's internal drive (E55907071F7900000081), while G and H are the *Always On* and *Dynamic* partitions for the external USB drive attached to the Cigent laptop.

Figure A-3 shows that each physical drive has been allocated 447 GB. The 223 GB allocation for the *Dynamic* partition of the …81 drive (Drive P in Figure A-4) indicates that equal space has been given to the *Always On* and *Dynamic* partitions. The same allocation applies to the …82 external drive. The D3E administrator can change drive-space allocations, as will be shown in Section A.1.1.3 below.

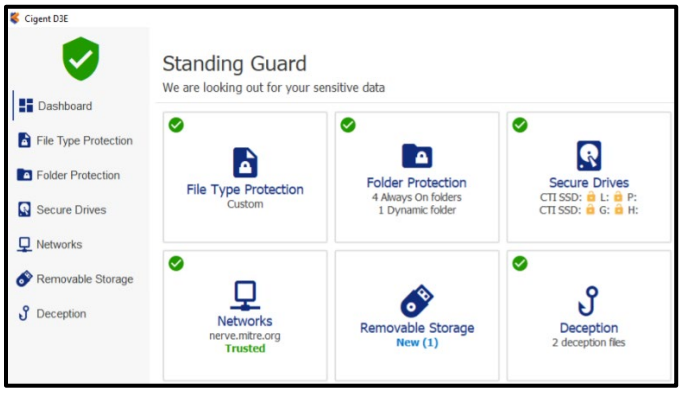


Figure A-2. Two Physical Drives Installed

Figure A-3. Total Drive Space

[39] Labels for the external USB drives can change if the external drive is ejected and later reinstalled.

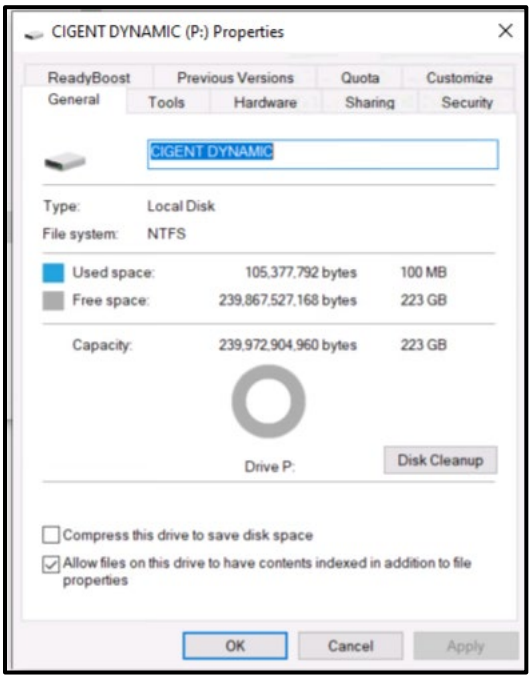


Figure A-4. Equal Allocations for Always On & Dynamic Partitions

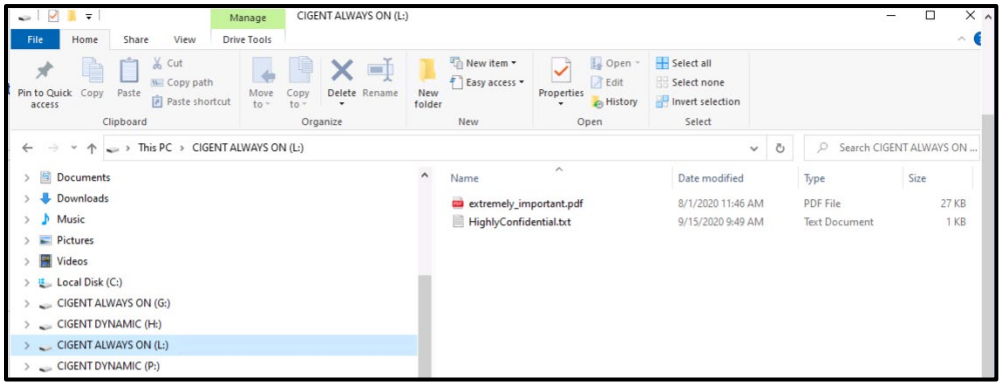


Figure A-5. All Drives Visible in Windows Explorer

In the ***Secure Drives*** window, click on the *Always On* drives for the two physical drives to re-activate protection. Note that it is not necessary to enter a PIN or other authentication type to turn protection back on, though authentication is required when disabling protection.

Figure A-6 shows the results of turning on protection for the partitions. Protection has rendered the two *Always On* partitions, L & G, invisible both in the D3E Dashboard and in Windows Explorer. Had Dynamic partitions P & H been similarly protected (locked), they, too, would have become invisible in Windows. (This attribute applies only to secure SSDs.)

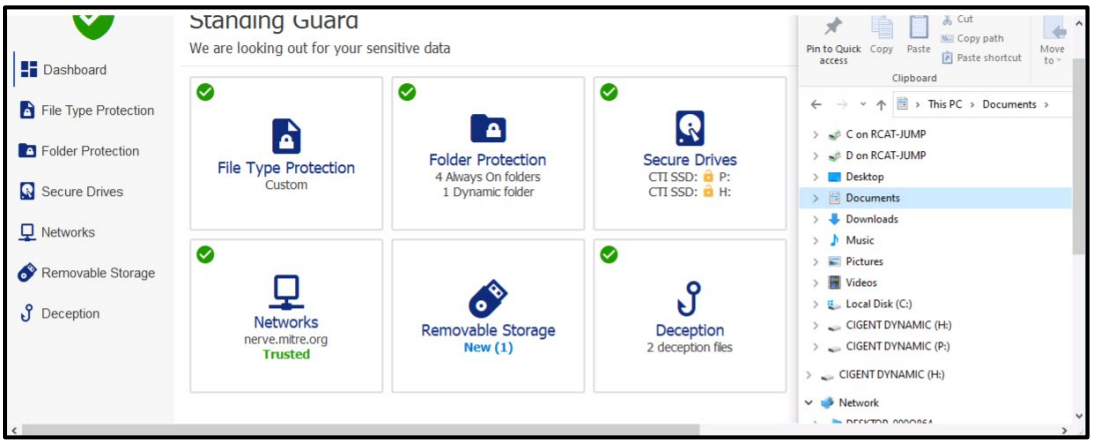


Figure A-6. *Always On* Partitions Not Visible

To demonstrate D3E's ability to reconfigure existing drives, it first was necessary to de-configure a Secure Drive. The …81 Secure Drive will be de-configured in Section A.1.1.2 below.

A.1.1.2 De-Configure a D3E Secure Drive

After making the Secure Drives visible, we copied their file contents to a Backup folder. (It was necessary to enter the authentication PIN each time a secure file was moved.) For the sake of convenience, if not security, a backup folder was located on the Cigent laptop. We also copied the Backup folder to the H: partition of the USB drive, because that drive was not being reconfigured. Note that this Backup folder contains only user-generated files, which we may want to use after the Secure Drive has been reconfigured.

Separate from our backup of user-generated data files, D3E generates a backup file (*.d3e) containing system configuration data for each Secure Drive. In our case, the files were located on the desktop, as shown in Figure A-7. The .d3e backup file will play a role in the de-configuration steps below.

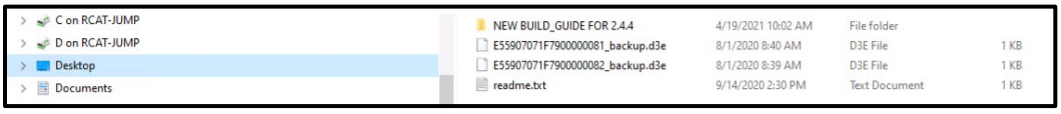


Figure A-7. System-Generated Backup File for Each Drive

- Deconfiguration Step 1:
  - Select the appropriate Secure Drive. For our evaluation, select the ….81 internal drive with partitions L & P.
  - Click the **Deconfigure** button to de-configure the internal Secure Drive of the Cigent laptop. Refer to Figure A-8.

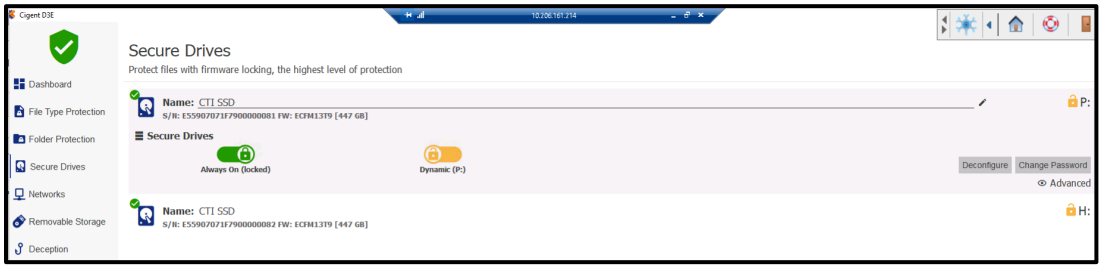


Figure A-8. Click *Deconfigure* for the Selected Drive

- Deconfiguration Step 2:
  - Browse to the desktop location of the desired .d3e backup file, as shown in Figure A-9.

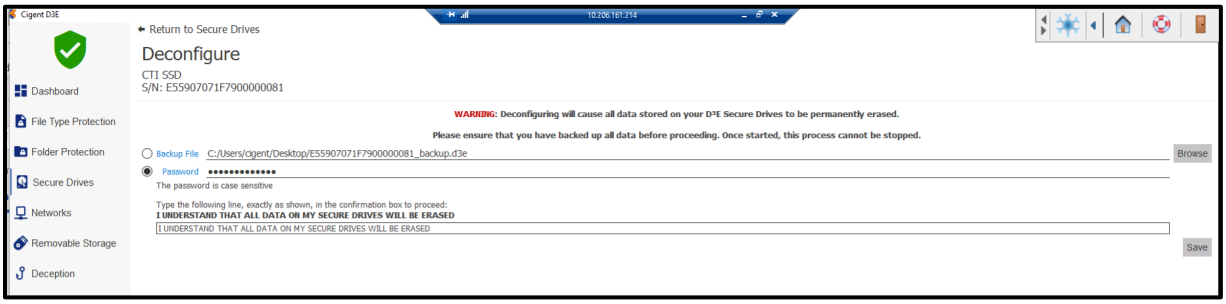


Figure A-9. Enter Backup-File Location and Provision PW to Deconfigure Drive

  - Enter the provisioning password for the Secure Drives.
  - Type the prescribed line in the confirmation box to proceed.
    - Click **Save** to Configure, then execute the prescribed authentication step. (For this system, simply enter the PIN at the D3E prompt.)

A.1.1.3 Reconfigure the Secure Drive

After a successful de-configuration, a screen such as the one in Figure A-10 will be displayed. The internal Secure Drive can now be configured.

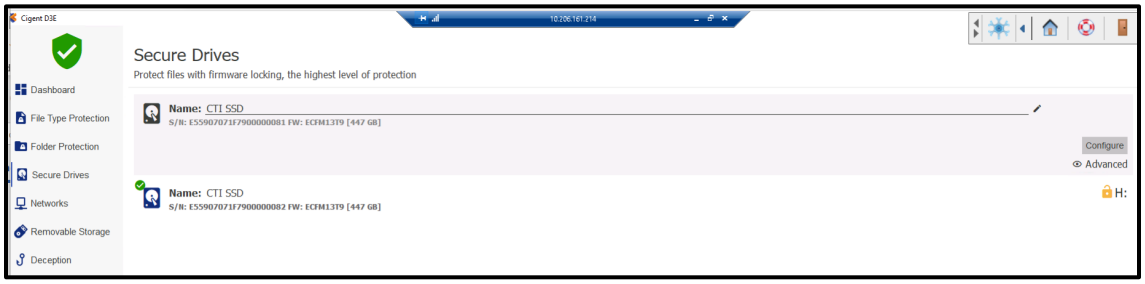


Figure A-10. Configure the Secure Drive

- Configuration Step 1:
  - Click on the **Configure** Button shown in Figure A-10.
- Configuration Step 2:
  - Create/enter password for the Secure Drive d3e configuration file. Refer to Figure A-11.

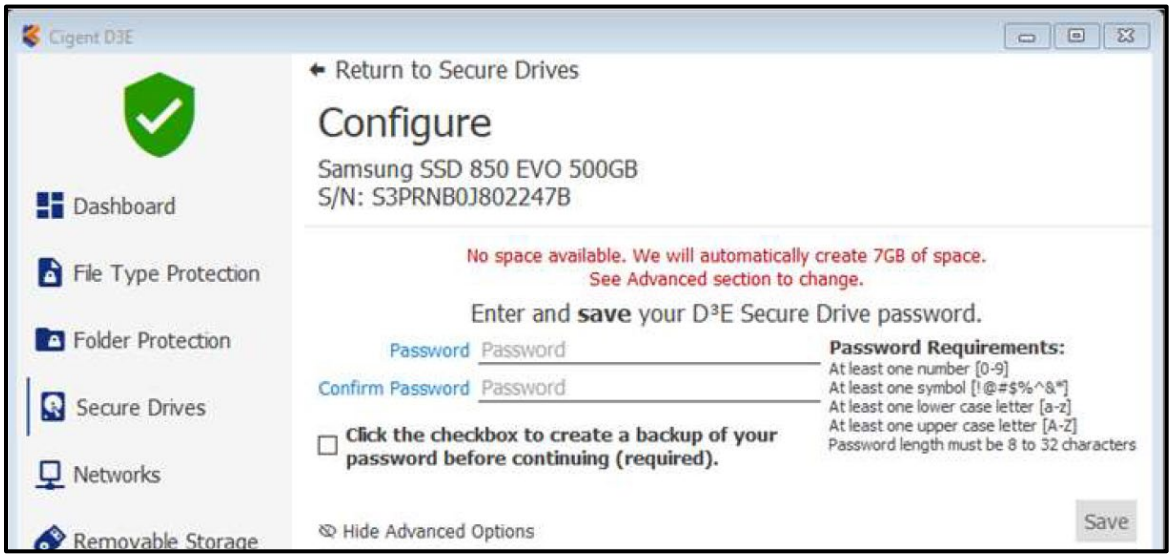


Figure A-11. Enter D3E Secure Drive Password [8]

  - When you click the checkbox to create a password backup file, a screen like the one in Figure A-12 will be displayed.

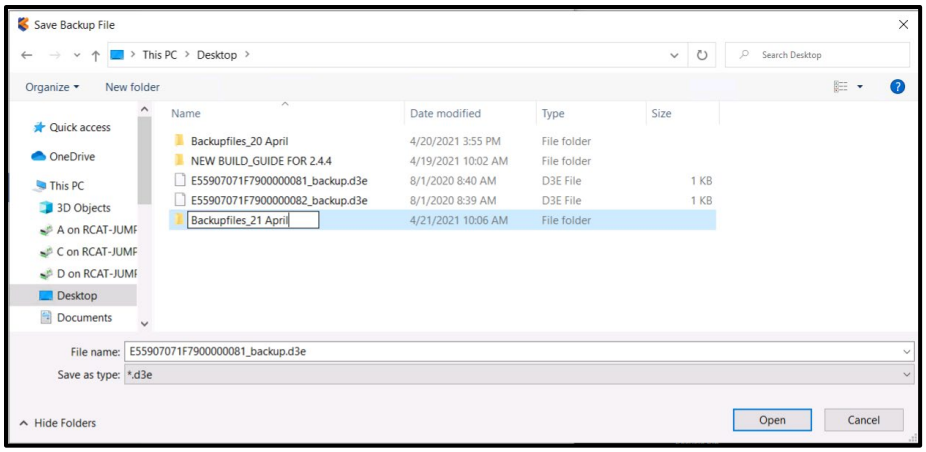


Figure A-12. Select Location for Secure Drive Password Backup

  - After selecting the backup-file location for the Secure Drive password, click the **Save** button shown in Figure A-11.

- Configuration Step 3:
    - The screen in Figure A-13 will be displayed.

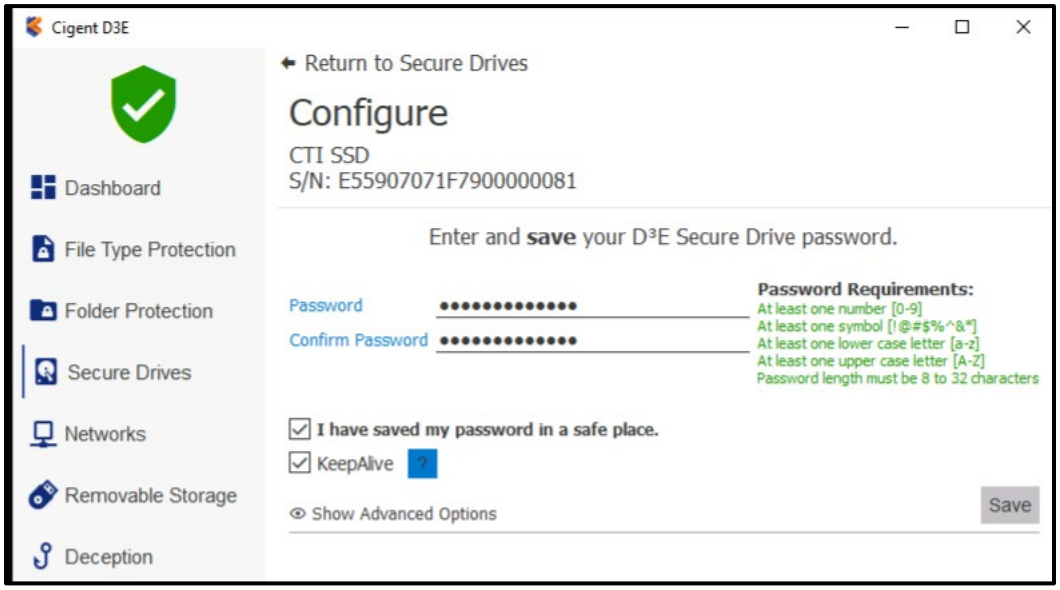


Figure A-13. Select Both Checkboxes

    - Select both checkboxes and click on the **Save** button. D3E displays a notification of the *KeepAlive* security feature. *KeepAlive* protects data if a malware event occurs; the feature is discussed further in Section A.2.3.

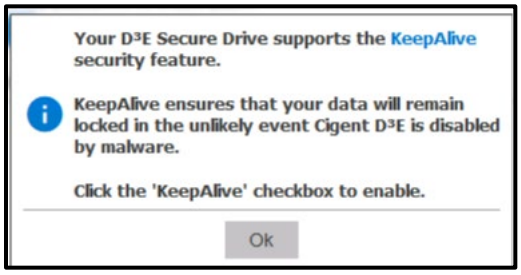


Figure A-14. *KeepAlive* Feature

    - Enter the appropriate authentication (PIN) at the prompt.
    - The post-configuration screen is displayed in Figure A-15.

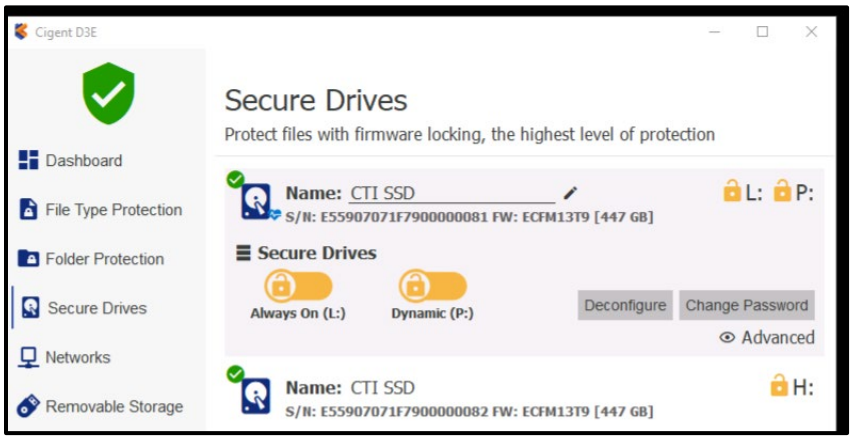


Figure A-15. Post-Configuration L & P Secure Drives

- Configuration Step 4:
    - Allocate Drive Space
        i. Because we intentionally did not erase database files from the C:\users\public\cigent directory, pre-existing configuration data, including drive-space allocations, were carried over from the previous configuration. Consequently, D3E did not prompt us to allocate space for the *Dynamic* and *Always On* partitions. Had we been prompted, a screen like the one in Figure A-16 would have been displayed. To change allocations, simply adjust the *Dynamic*/*Always On* slider.

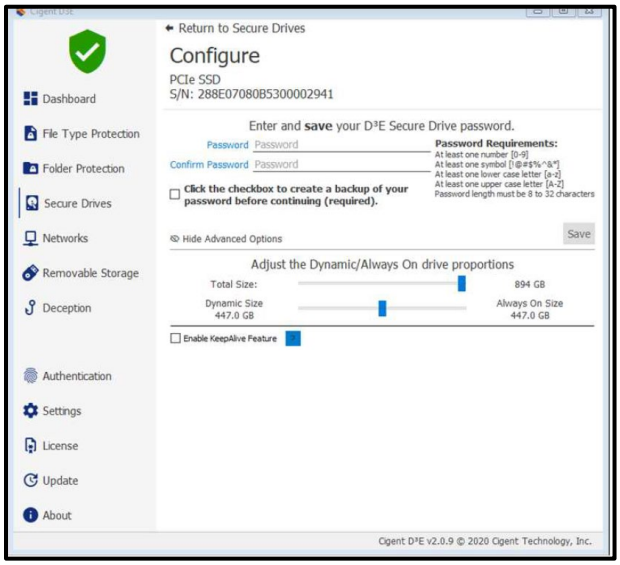


Figure A-16. Allocate Dynamic & Always On Drive Space [8]

A.1.1.4 Enable the Mini Authentication Popup

- At the ***Settings*** Menu of the D3E Dashboard, toggle the slider and enter the appropriate authentication (PIN) to enable the ***Use Mini Authentication Popup*** feature. See Figure A-17.

A.1.1.5 Enable Always On File Type Protection

- At the ***Settings*** Menu of the D3E Dashboard, toggle the slider and enter the appropriate authentication (PIN) to enable ***Allow Always on File Type Protection***. See Figure A-17.

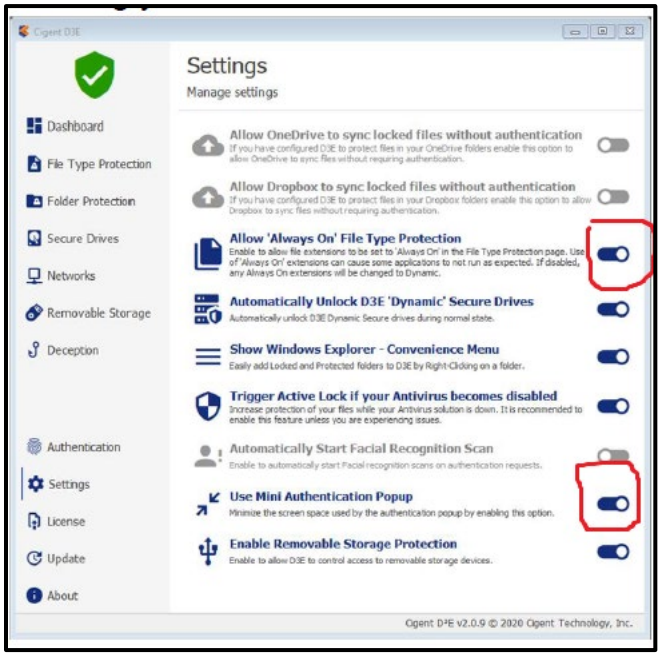


Figure A-17. Toggle D3E Settings

A.1.1.6 Feature Evaluation Results

- The configuration of the Cigent Secure Drive was accomplished according to plan. There were no problems or issues. When a password was created, however, as part of the Secure Drive Configuration (in Section A.1.1.3 above), D3E permitted reuse of the old provisioning PW. This was convenient for the purpose of our evaluation, but Air Force password guidance recommends stricter practices.
    - **Recommendation**: We recommend that Cigent use NIST SP 800-63-3 as a guide for constructing robust digital identities.

A.1.2 *Always On* and *Dynamic* Protection

- Preliminary Steps: Make sure that the recently configured L & P drives contain data files. If the drives are empty, they can be populated with data from the Evaluation Kit that accompanied the D3E build, or from the G & H drives that were not reconfigured. Figure A-18 shows the contents of the ***EvaluationKitAuxFiles*** folder, while Figure A-19 shows the L & P drives with the extracted data.
    - Extract *CompanyInternal.zip* files to the P drive.
    - Extract *HighlyConfidential.zip* files to the L drive.

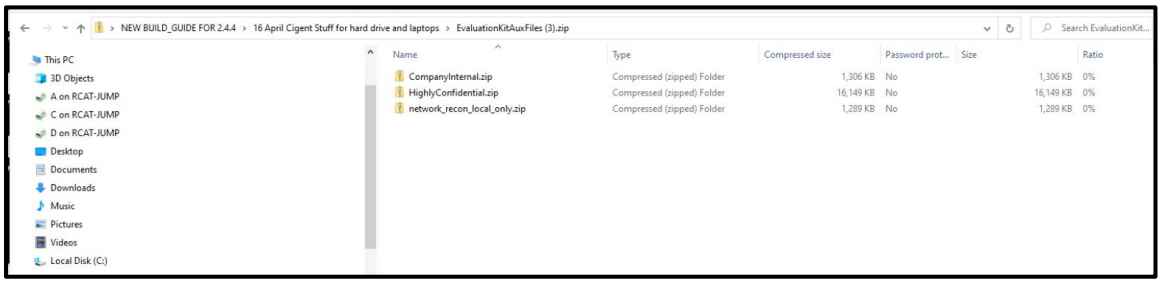


Figure A-18. Extract Zipped Test Data to L & P Drives

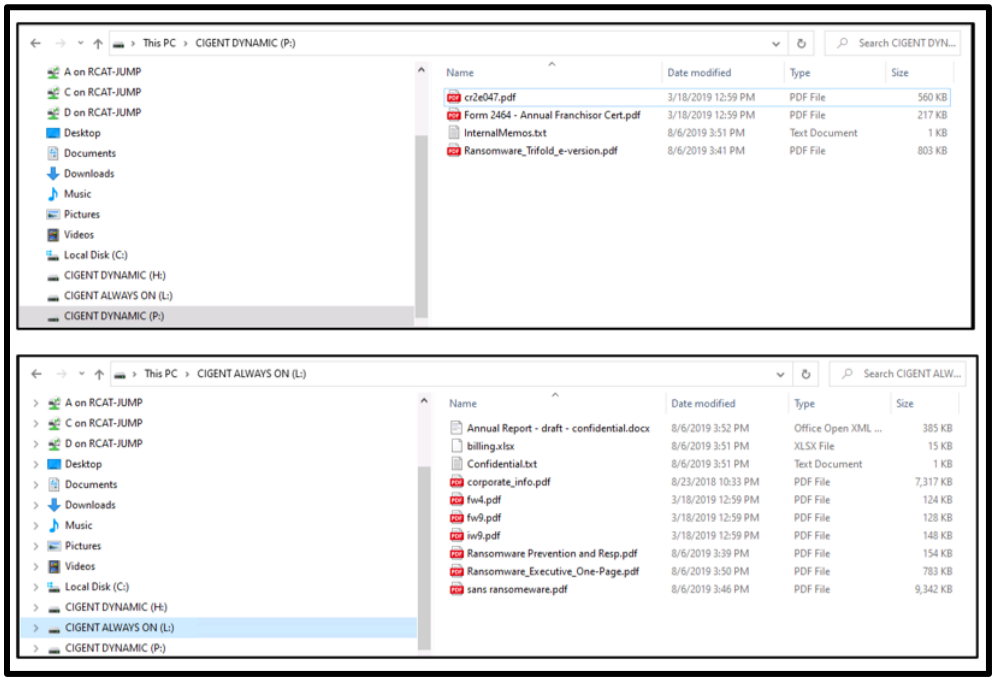


Figure A-19. Contents of P & L Drives with Extracted Data

A.1.2.1 Accessing Always On Files

- Recap of *Always On* Behavior:
    - As we described in Section 2.1 of this paper, files on *Always On* drives remain locked under all conditions, until they are made accessible when a D3E administrator enters the prescribed authentication to unlock the drive temporarily.
        - In other words, step-up authentication is always required to access *Always On* files.
    - Locked *Always On* Secure Drives are not visible in Windows Explorer.
    - If a threat is detected while an *Always On* drive is temporarily unlocked, D3E unmounts (locks) the drive.

- Browse to L:\HighlyConfidential in Windows Explorer. If the drive and file are not visible, simply click on the green portion of the Secure Drive icon in the D3E Dashboard and use the prescribed authentication method. Figure A-20 shows the locked and unlocked states of the *Always On* drive.

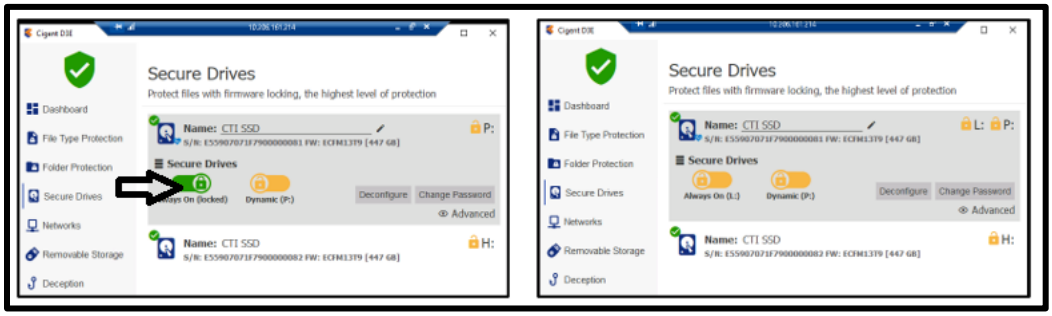


Figure A-20. *Always On* Drive Before and After Unlocking

- Once the Secure Drive has been unlocked, file names will be visible in Windows Explorer. Click on the *Confidential* text file. Regardless of the *ActiveLock* status, the file will appear empty until the appropriate authentication is entered. See Figure A-21.

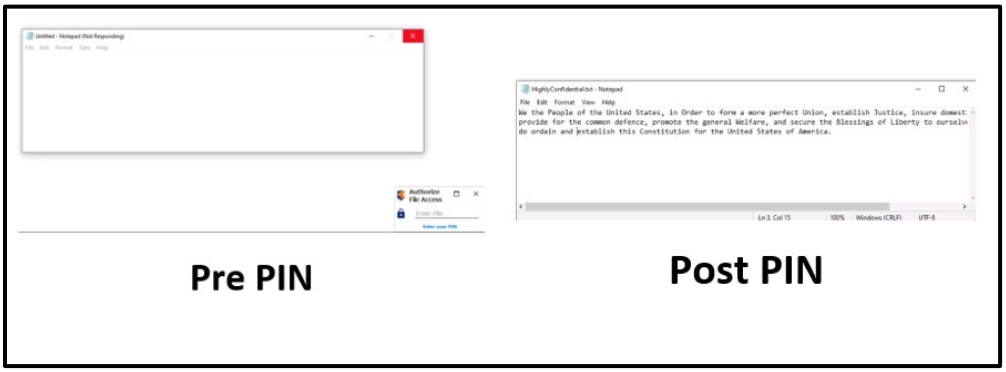


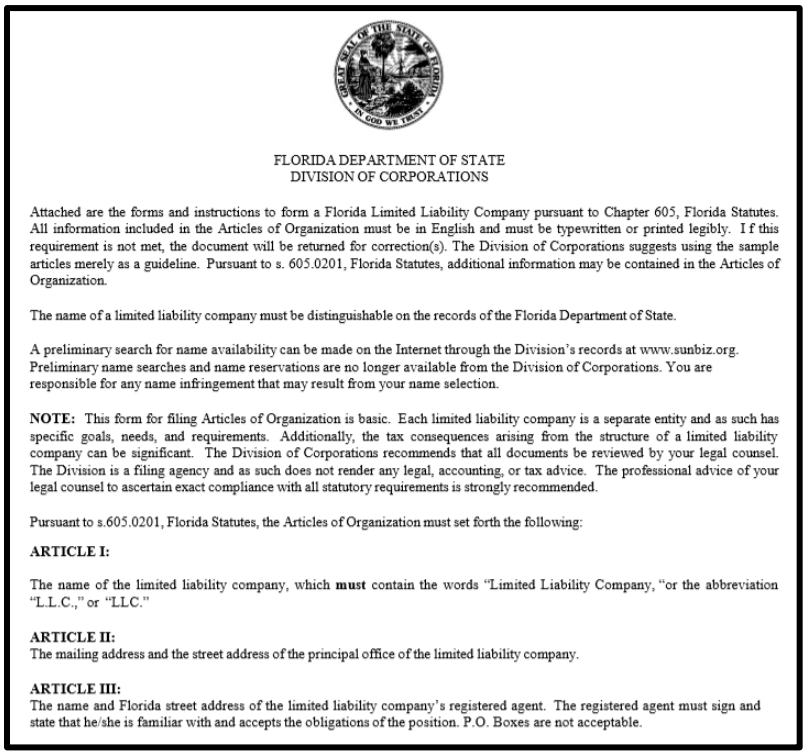
Figure A-21. Files in *Always On* Drive Require PIN to Unlock

- The triggering of ActiveLock to secure the *Always On* drive when a threat is detected is demonstrated and evaluated in Section A.1.3.1 below.

A.1.2.2 Accessing *Dynamic* Files

- Recap of *Dynamic* Behavior:
  - *Dynamic* data normally are unlocked and accessible; however, if a filetype, folder, or partition is marked for *Dynamic* protection, the *Dynamic* locking mode will activate and lock these entities whenever D3E determines that a threat has been encountered. Step-up authentication then will be required to access the information.
  - Locked *Dynamic* Secure Drives are not visible in Windows Explorer.
- Refer to Section 2.1 for further details.

- Browse to P:*cr2e047.pdf* in Windows Explorer. Because the file is on a drive with *Dynamic* protection, second-factor authentication (PIN) will not be required to open it, unless *ActiveLock* has been triggered by a security event. See Figure A-22.



FLORIDA DEPARTMENT OF STATE
DIVISION OF CORPORATIONS

Attached are the forms and instructions to form a Florida Limited Liability Company pursuant to Chapter 605, Florida Statutes. All information included in the Articles of Organization must be in English and must be typewritten or printed legibly. If this requirement is not met, the document will be returned for correction(s). The Division of Corporations suggests using the sample articles merely as a guideline. Pursuant to s. 605.0201, Florida Statutes, additional information may be contained in the Articles of Organization.

The name of a limited liability company must be distinguishable on the records of the Florida Department of State.

A preliminary search for name availability can be made on the Internet through the Division's records at www.sunbiz.org. Preliminary name searches and name reservations are no longer available from the Division of Corporations. You are responsible for any name infringement that may result from your name selection.

NOTE: This form for filing Articles of Organization is basic. Each limited liability company is a separate entity and as such has specific goals, needs, and requirements. Additionally, the tax consequences arising from the structure of a limited liability company can be significant. The Division of Corporations recommends that all documents be reviewed by your legal counsel. The Division is a filing agency and as such does not render any legal, accounting, or tax advice. The professional advice of your legal counsel to ascertain exact compliance with all statutory requirements is strongly recommended.

Pursuant to s.605.0201, Florida Statutes, the Articles of Organization must set forth the following:

ARTICLE I:

The name of the limited liability company, which **must** contain the words "Limited Liability Company, "or the abbreviation "L.L.C.," or "LLC."

ARTICLE II:
The mailing address and the street address of the principal office of the limited liability company.

ARTICLE III:
The name and Florida street address of the limited liability company's registered agent. The registered agent must sign and state that he/she is familiar with and accepts the obligations of the position. P.O. Boxes are not acceptable.

Figure A-22. *Dynamic* Files Open Without MFA

- The triggering of ActiveLock to secure the *Dynamic* files when a threat is detected is demonstrated and evaluated in Section A.1.3.1 below.

A.1.2.3 Feature Evaluation Results

There were no issues accessing or manipulating *Dynamic* and *Always On* files on the Cigent Secure Drive. The feature performed as advertised.

A.1.3 *Deception* Files

As noted earlier, *Deception* files track unauthorized access attempts to the host system by enticing prospective attackers with interesting file names and folders. D3E creates a default *passwords.xls Deception* file in local users' ***Documents*** directories, and D3E users can create other *Deception* files in locations of their choice. Attempts to open *Deception* files trigger *ActiveLock*.

The test cases below demonstrate D3E's response to attempts to access the default and user-created honeypot files.

A.1.3.1 Attempt to Access the Default *passwords.xls Deception* File

- In Windows Explorer, browse to the location of the *passwords.xls* default *Deception* file (C:\Users\cigent\Documents).

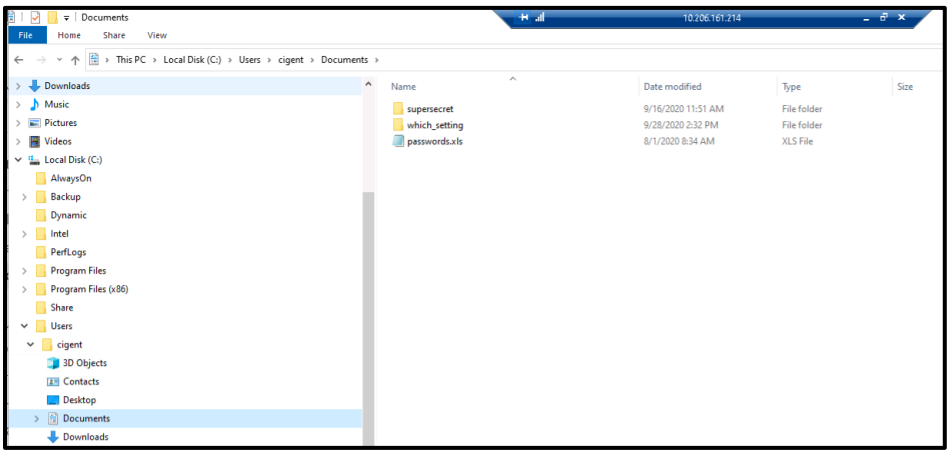


Figure A-23. Locate the passwords.xls *Deception* File

- Double-click on the *passwords.xls* file. Note the following results:
  - A Windows pop-up message informs you that you cannot access the file.
  - The D3E Dashboard displays a ***Threats Detected*** notification.
  - The Cigent task-tray icon turns red.

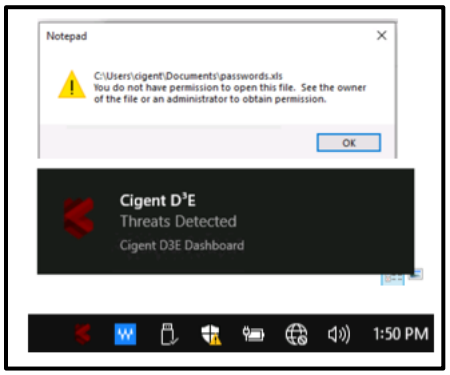


Figure A-24. D3E Threat Notifications

  - The D3E Dashboard indicates that a *Deception* event has occurred. See Figure A-25.

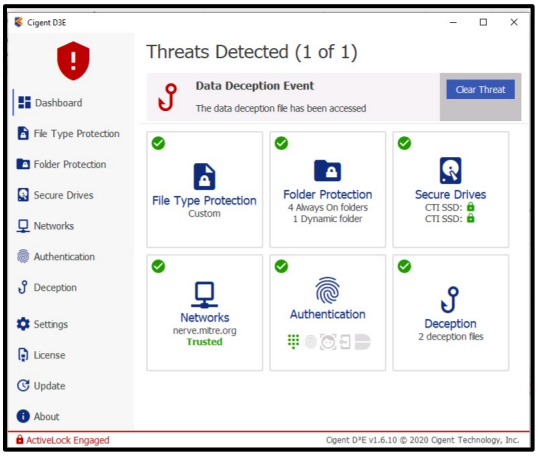


Figure A-25. *Deception* Threat Detected

- The Secure Drives have been locked as a result of the *Data-Deception* attempt.

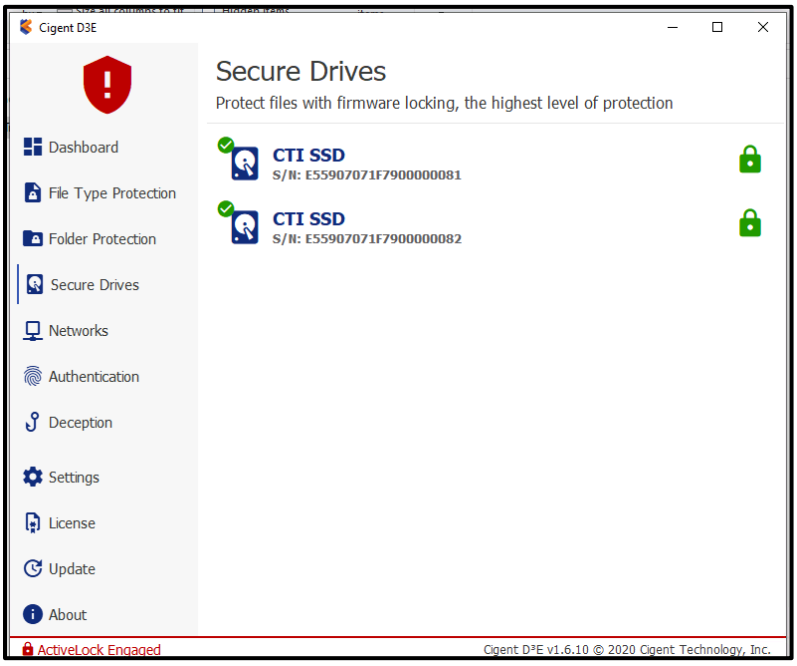


Figure A-26. Secure Drives Locked upon *Deception* Event

- Finally, note that the Secure Drives (G, H, L & P) are no longer visible in Windows Explorer.

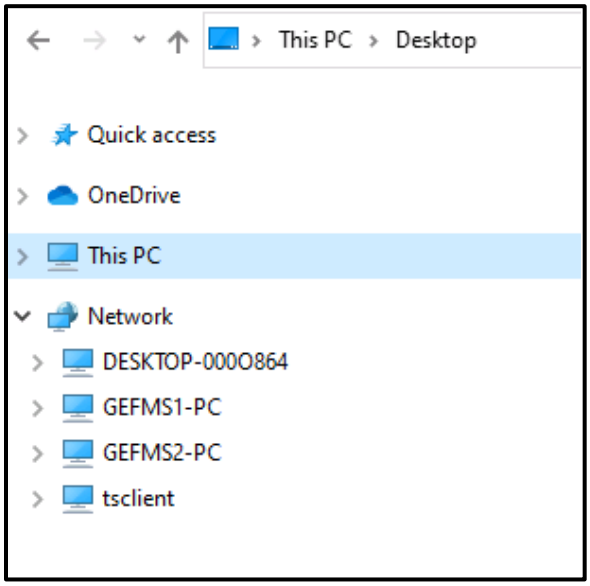


Figure A-27. Secure Drives Invisible in Windows Explorer

- Click on **Dashboard**. Then click on the ***Clear Threat*** button and enter the prescribed authentication method to clear the Cigent warnings and return to normal operation.
    - After the threat has been cleared, note that the *Always On* partitions remain locked (and invisible in Windows Explorer), while the *Dynamic* partitions are visible and unlocked.

A.1.3.2 Attempt to Access User-Created *Deception* File

- To conduct this evaluation, we created a ***Documents\Company Confidential*** folder, because we want the *Deception* file to reside here. (This choice is arbitrary and at the administrator's discretion.)
- Click ***Add a Deception File*** at the D3E Dashboard *Deception* menu.
    - Browse to the folder where you will create the *Deception* file, and thin click **Open**.
    - If you don't wish to use the default *passwords.xls* file name, simply enter the name of a non-existing file (we chose *Ooh lala.txt*), click ***Save***, and implement the prescribed authentication method at the prompt. See Figure A-28.

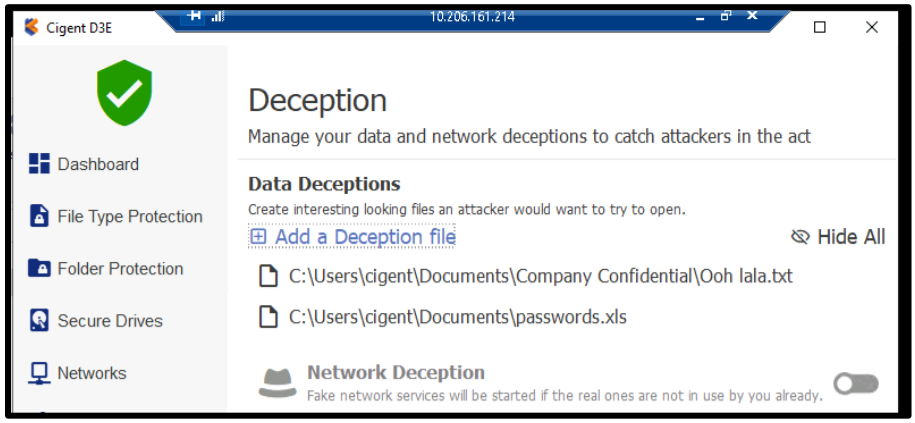


Figure A-28. Add a *Deception* File

- In Windows Explorer, browse to the location of the user-created *Deception* file; then click on the file to access it.
- Note that warnings similar to those shown in Figure A-24 are displayed, and that the D3E Dashboard displays the notification shown in Figure A-25.
- Click on ***Clear Threat*** and use the prescribed authentication method to clear the Cigent warnings.

A.1.3.3 Evaluation Results

Our evaluation demonstrated that D3E File *Deception* behaved as advertised, triggering *ActiveLock* whenever an attempt was made to access a *Deception* file.

We did, however, note the following anomalous behavior:

- Although attempts to open user-created *Deception* files triggered the appropriate responses, it was possible to delete those files from within Windows Explorer. The files also could be moved to another location and subsequently opened/edited.
    - While the *Deception* file is merely a honeypot, and the ability to delete, copy/move, or open it with impunity will not immediately harm the host, such behavior provides an attacker with a means of analyzing and eventually circumventing D3E defenses.
- Moreover, while it was not possible to permanently delete the system-generated *passwords.xls* file, that file could similarly be moved and subsequently opened/examined. See Figure A-29 below. Note that the system-generated *Deception* file has been moved from the *Documents* folder to the desktop prior to opening.

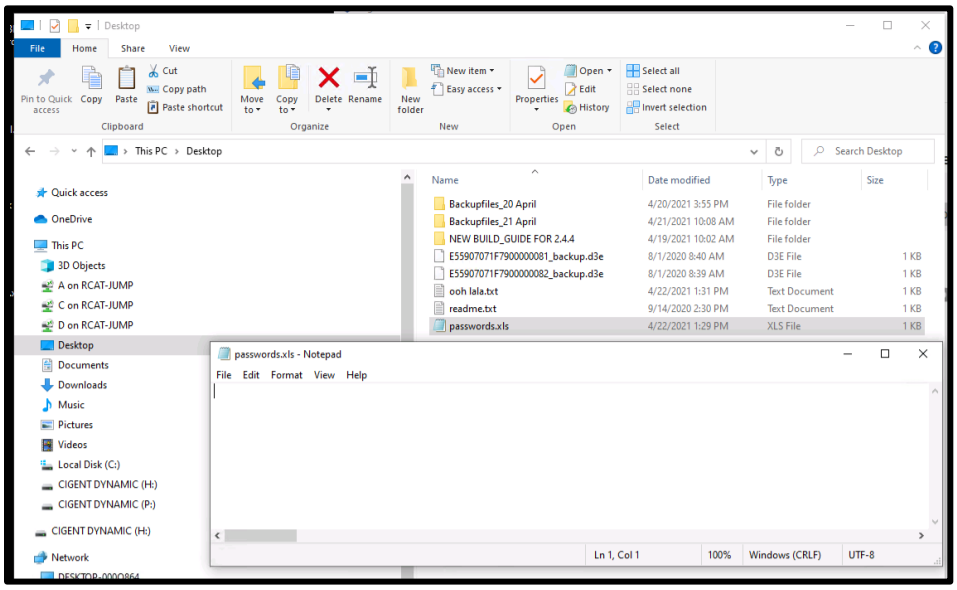


Figure A-29. Successful Attempt to Move and Inspect *Deception* File

- D3E also allowed us to modify the system-generated *passwords.xls* file and replace the default file. Figure A-30 shows the contents of the *passwords.xls* file after moving the file to the desktop, editing the file, and copying it back into the original folder.

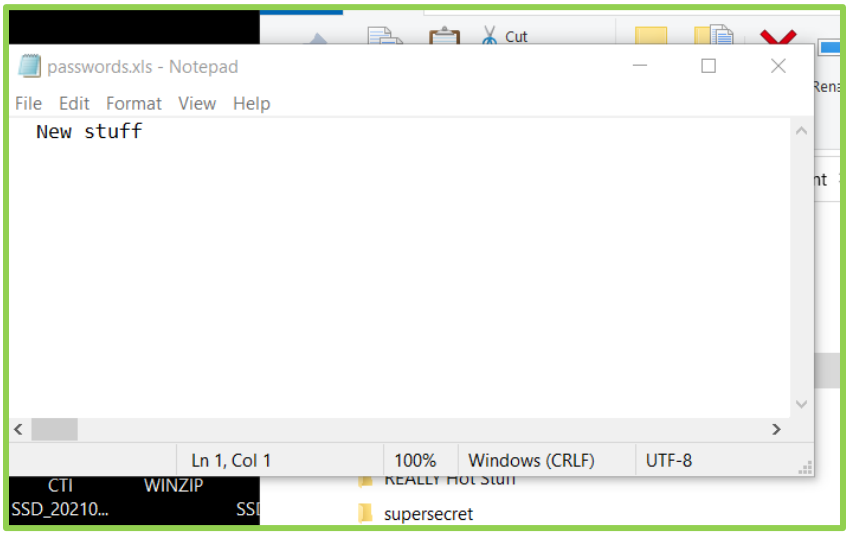


Figure A-30. Modified *Deception* File in Honeypot Location

A.1.4 Windows Defender and Antivirus Integration

D3E works with Windows Defender antivirus (AV) and other AV solutions registered with Windows Security Center; D3E will lock files if Defender detects a threat or if the AV software has been disabled [8].

The subsections below evaluate D3E's integration with Windows' AV protection.

A.1.4.1 Evaluation Steps for Antivirus Integration

- At the D3E Dashboard Settings screen, make sure that *Trigger Active Lock if your Antivirus becomes disabled* is turned on. If it is not enabled, push the slider to the right and enter the appropriate authentication. (See Figure A-31.)

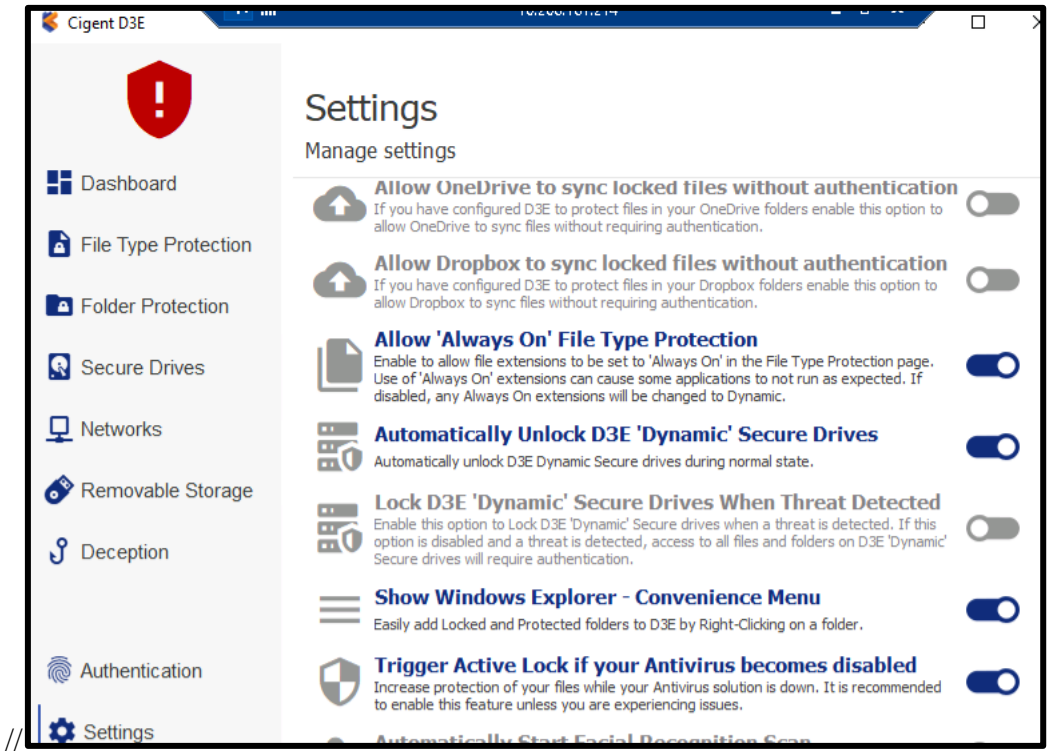


Figure A-31. Setting to Trigger ActiveLock for AV Tampering

- In the Windows start menu, search for *Virus & threat protection*.
  - Click on *Windows Security*.
  - Then click on *Virus & threat protection*. (See Figure A-32.)
  - Click *Manage settings*. (See Figure A-33.)

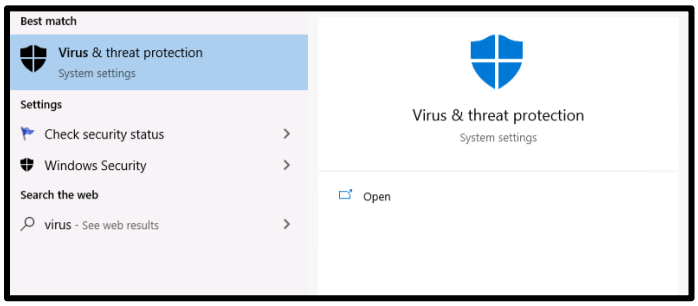


Figure A-32. Disable AV – Step 1

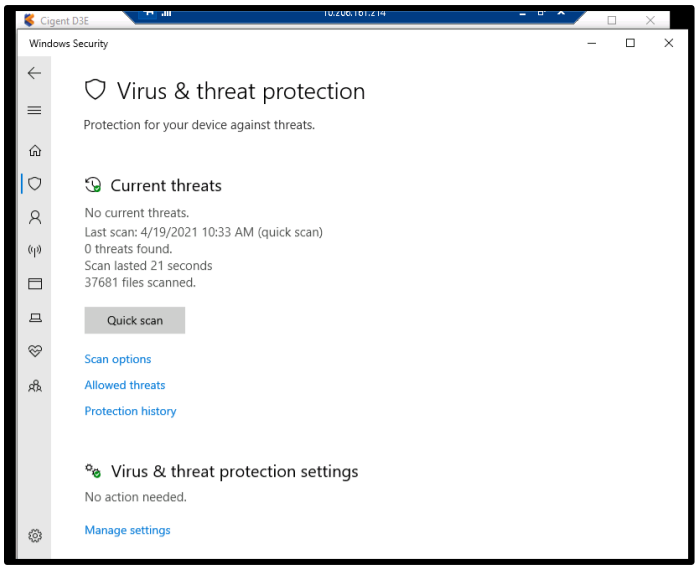


Figure A-33. Disable AV – Step 2

- Turn off *Real-time protection* by pushing the slider to the left. Then click **Yes** to put the action into effect. (See Figure A-34.)

Figure A-34. Disable AV – Step 3

- D3E detects the threat and engages *ActiveLock* (Figure A-35). Note that *Dynamic* drives P & H are visible, but locked, in the D3E Dashboard. *Always On* drives G and L are not visible in the Dashboard or in Windows Explorer. (Refer to Figure A-36.)

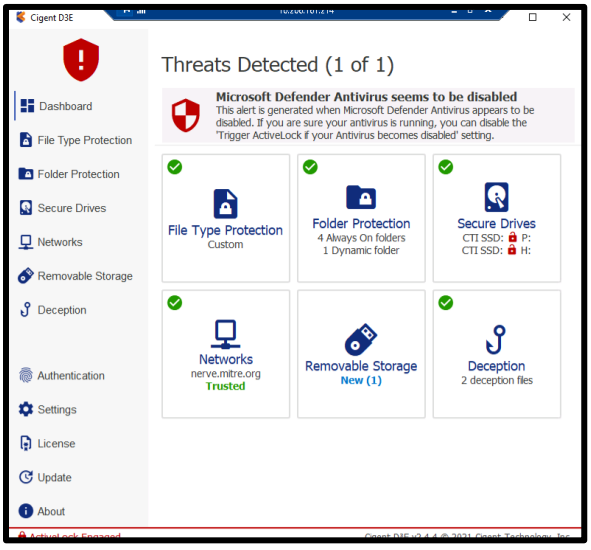


Figure A-35. Tampering with AV Triggers ActiveLock

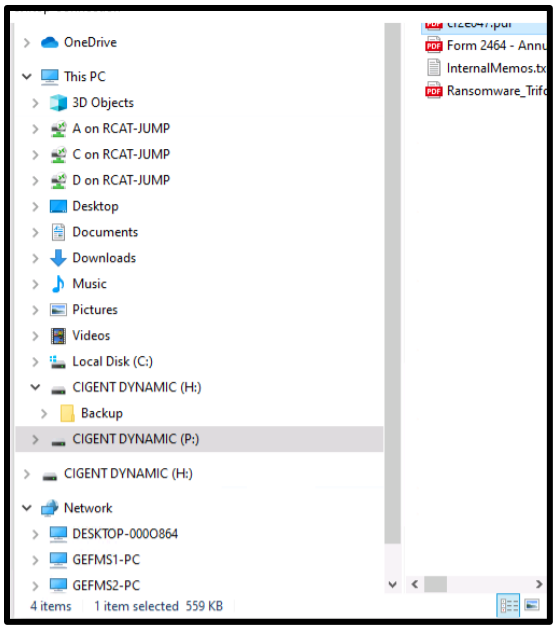


Figure A-36. ActiveLock ➔ Always On Drives Not Visible in Explorer

- Although *Dynamic* drives P & H are visible under *ActiveLock*, files on those drives require PIN authentication to access.
- Repeat earlier steps to manage *Windows Security* settings.
  - Turn *Real-time protection* back on.
  - The *ActiveLock* condition should clear.[40]
- After *ActiveLock* has been cleared, *Always On* drives L & G can be unlocked and made visible in the usual way:
  - Click on ***Secure Drives.***
  - Select either Secure Drive.
  - Toggle the slider from the locked (Green) position and enter the appropriate authentication.

A.1.4.2 Evaluation Results

D3E performed as expected, triggering *ActiveLock* when Windows Defender was turned off. We also noted that D3E properly detected out-of-date virus definitions.

- After we ran the evaluation steps in Section A.1.4.1 and re-activated *Real-time protection* at the host laptop, D3E persisted in detecting an antivirus-disabled threat, even though

[40] As we discovered, D3E will indicate a threat condition if virus protection definitions are not up to date.

virus and threat-protection settings had been returned to normal. (Refer to **Error! Reference source not found.**.) At first we thought that this was an error, so we notified Cigent about the issue. Cigent's response: "D3E uses the Windows Security Center APIs to determine the state and health of the properly registered Anti-Virus applications. In addition to state (enabled/disabled), the APIs will indicate a threat state if the virus definitions are out of date by more than a week (typically)." It turned out that Cigent's suspicion was, in fact, correct. Refer to **Error! Reference source not found.**, which shows that virus protection definitions at the Win10 laptop were out of date.

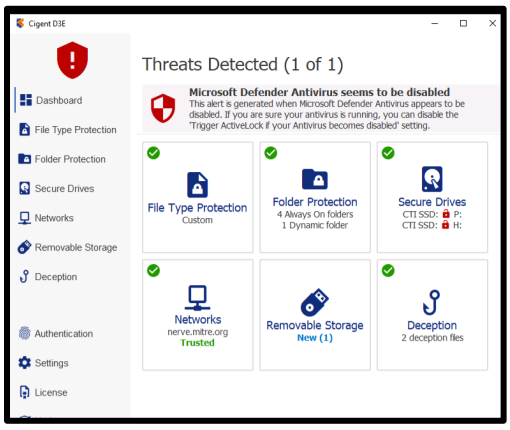


Figure A-37. D3E Indicates Virus Protection Disabled

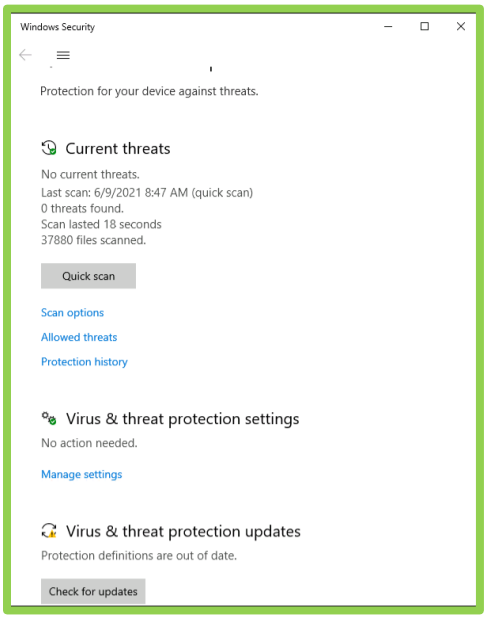


Figure A-38. Protection Definitions are Out of Date

A.1.5 *Network Manager*

Network Manager is designed to prevent unauthorized devices from connecting to the D3E-protected host.

As we stated in Section 2.1.3.2, the D3E *Network Manager* starts fake services on commonly attacked ports if they are not already in use. If a network device scans a D3E-protected host for open ports and connects to a Cigent *Deception* port, D3E will trigger *ActiveLock* to protect sensitive files. *ActiveLock* also is triggered if an unauthorized device tries to connect to the system on any port, or if the system joins a network that has not been previously trusted.

The following two subsections describe the steps we performed to evaluate D3E *Network Manager* functionality.

A.1.5.1 D3E Response to Untrusted Network Connections

- Untrust the Current Network
    - Untrusting an existing network connection will have the same effect as trying to connect the D3E-protected host to an untrusted network.
        - Select *Networks* at the D3 Dashboard.
        - Click on a trusted network.
        - Click the **Untrust** button. Refer to Figure A-39.

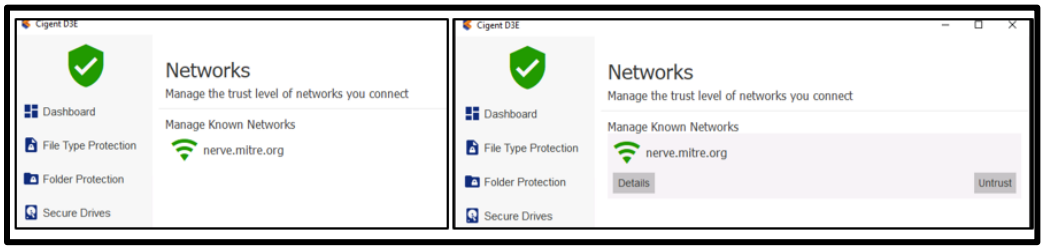


Figure A-39. Untrust an Existing Trusted Network Connection

- Clicking **Untrust** triggers *ActiveLock*. See **Error! Reference source not found.**.

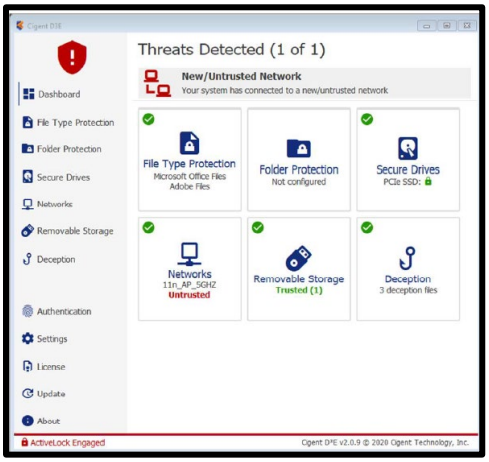


Figure A-40. Untrusting a Network Triggers ActiveLock [8]

- Show that files with *Dynamic* protection cannot be opened under *ActiveLock* condition.

  (*ActiveLock*'s attributes have been demonstrated elsewhere in this report; however, for the sake of completeness, we'll show how D3E protects data after detection of an untrusted-network connection.)

  - Try to open a file that has been assigned *Dynamic* protection. Refer to Figure A-41 below.

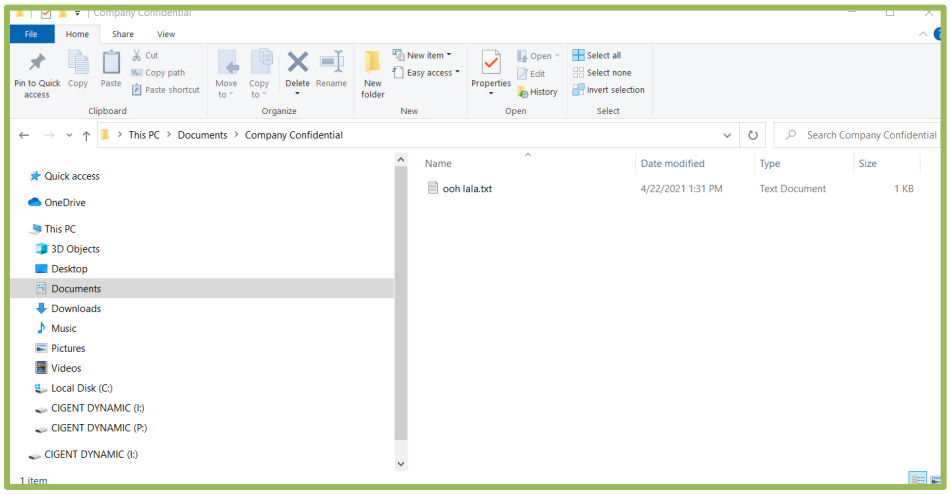


Figure A-41. Try to Open File with *Dynamic* Protection

  - Figure A-42 shows that *ActiveLock* prevents the opening of the file unless the prescribed authentication is used.

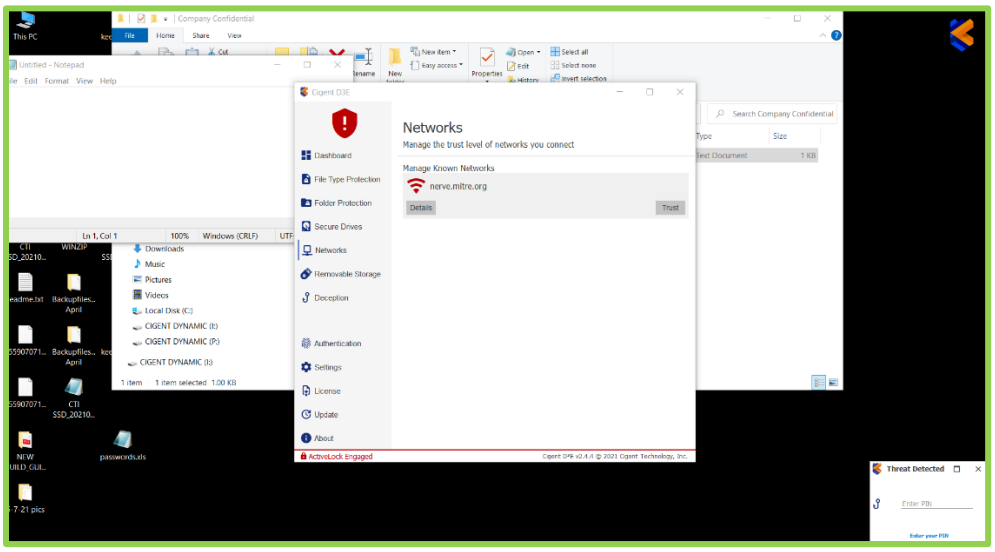


Figure A-42. *ActiveLock* Prevents Opening of File with *Dynamic* Protection

- Clicking **Untrust** also causes the network connection to drop. Refer to Figure A-43.

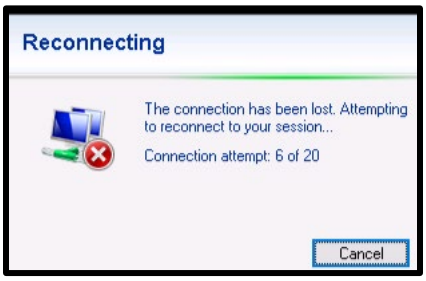


Figure A-43. Untrusted Connection is Lost

- To clear the *ActiveLock* condition and restore the network connection, return to the *Networks* page at the D3E Dashboard and click **Trust** for the network you previously untrusted. Refer to Figure A-44.

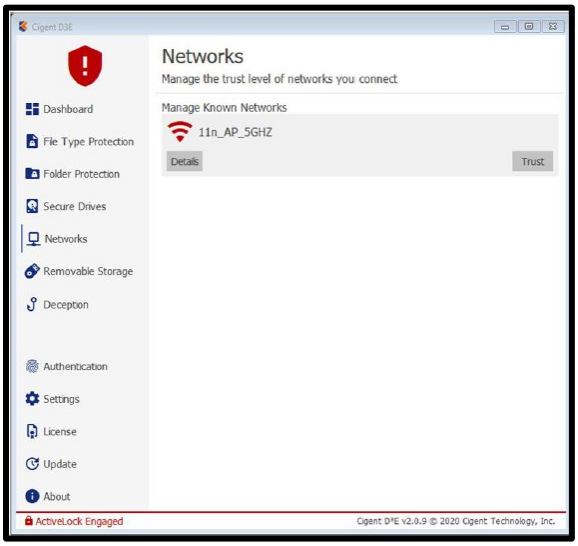


Figure A-44. Return the Network to a Trusted Condition [8]

A.1.5.2 D3E Response to Port-Scanning Attempts

- Scan Network Ports
  - To perform the network-scanning evaluation, we used a port-scanning program provided by Cigent. That file is included on the laptop, as described below and depicted in Figure A-45.
    - The desktop of the evaluation laptop contains a folder called **NEW BUILD_GUIDE FOR 2.4.4.** Open the folder.
    - Next, open the folder called **16 April Cigent Stuff for hard drive and laptops**.
    - Open the **EvaluationKitAuxFiles** folder, which contains the *EvaluationKitAuxFiles* zipped file.

- Clicking on the *EvaluationKitAuxFiles.zip* zipped file reveals the network_recon_local_only.zip file, which we will use to scan network ports.

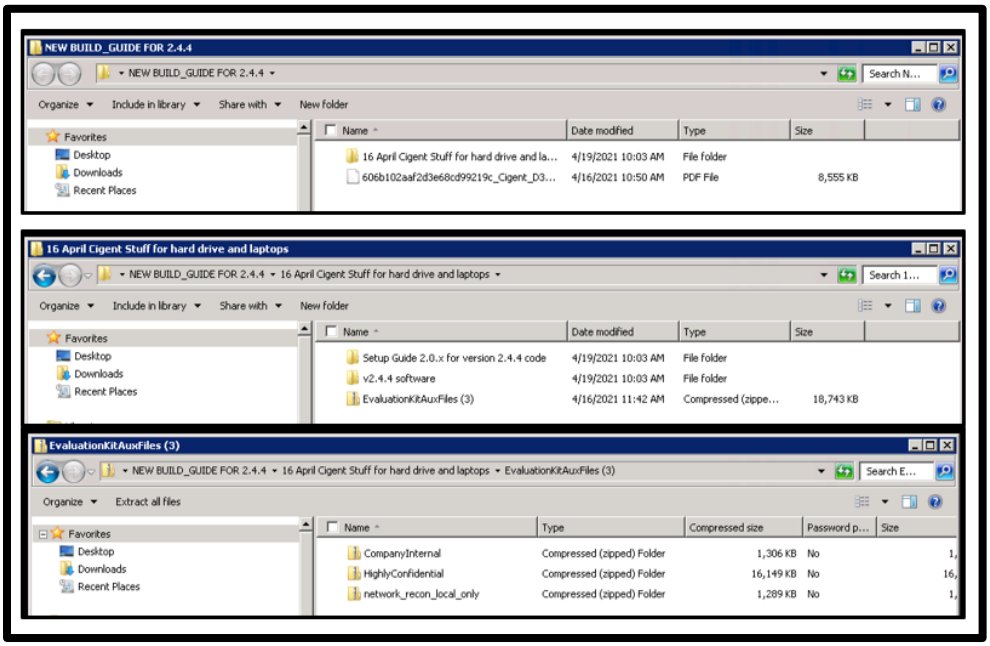


Figure A-45. Locate the Port-Scanning File on the Desktop

- Go to the D3E *Deception* menu and make sure *Network Deception* is turned on.

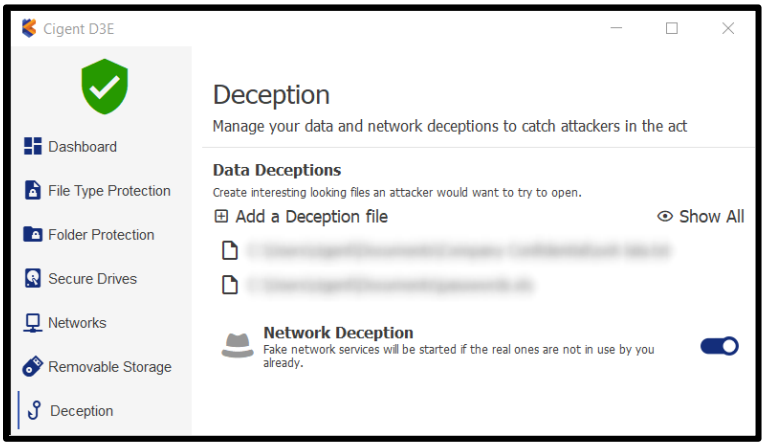


Figure A-46. Make Sure *Network Deception* is Active

- Copy network_recon_local_only.zip to C:\ directory. (The file can be run from anywhere, but it seemed easier to us to execute the command from this location.)
- Open a command prompt; set the current directory to C:\; and run the attack script. Refer to Figure A-47 and Figure A-48.
  - Note that the script attacks ports 3389, 445, 139, and 135. These ports are used for Remote Desktop Protocol (RDP), Transmission Control Protocol

(TCP), Server Message Block (SMB), and Remote Procedure Call (RPC), respectively.

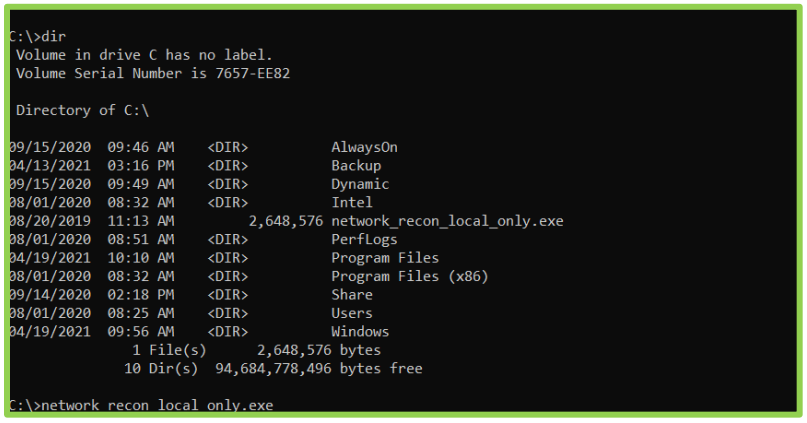


Figure A-47. Run the Attack Script

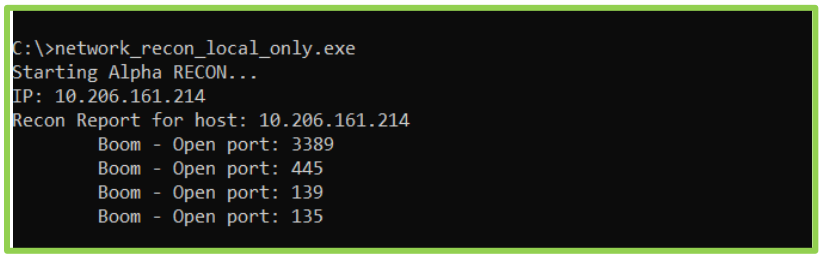


Figure A-48. Execution of Port-Scan Attack Script

- D3E's reaction to the *Network Deception* is shown in Figure A-49.
  - *ActiveLock* is engaged.
  - The D3E icon turns red.
  - The user is prompted to enter authentication to clear the threat.

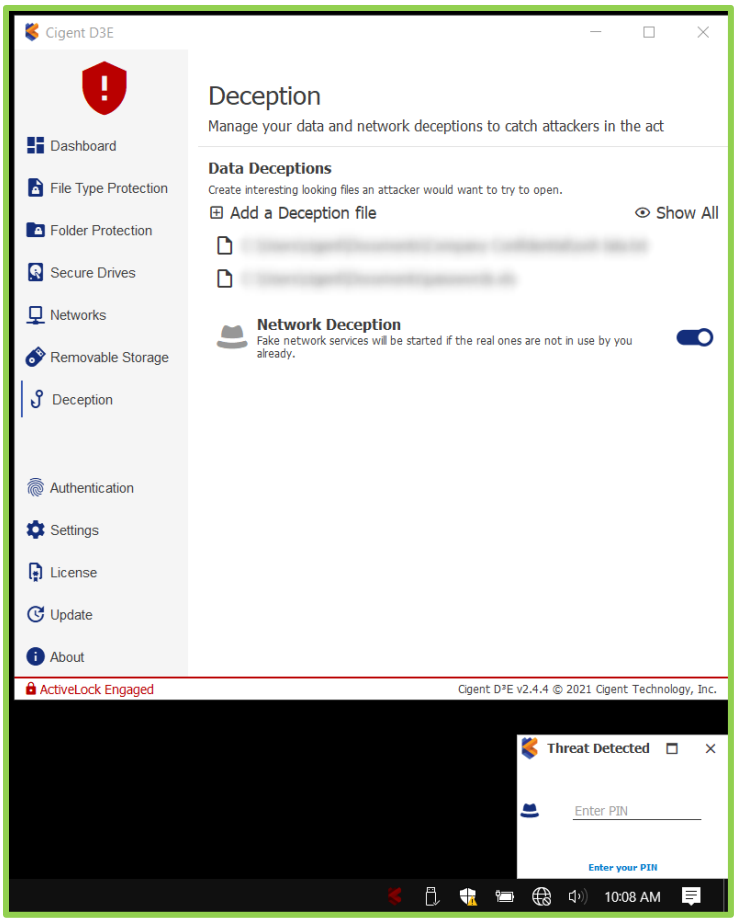


Figure A-49. D3E Reaction to Port Scan

- Enter the D3E PIN to clear the threat.

- *ActiveLock* is now disengaged, as shown in Figure A-50.

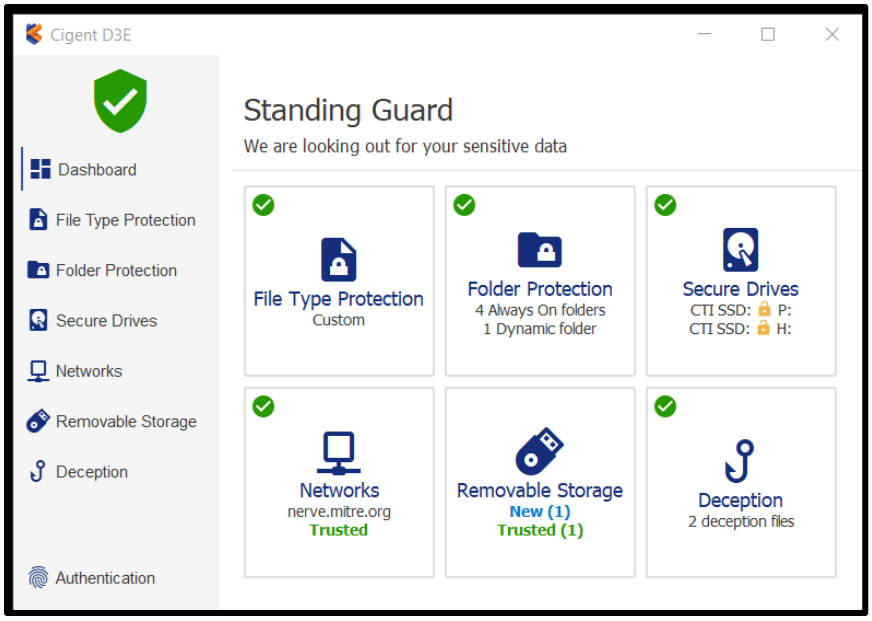


Figure A-50. *ActiveLock* Disengaged

A.1.5.3 Evaluation Results

D3E *Network Manager* functioned as advertised on the Cigent laptop equipped with Secure Drives.

A.2 Cigent Secure SSD Features

A.2.1 *Command Log Audit*

A.2.1.1 Evaluation Steps for *Command Log Audit*

Cigent Secure SSDs store every command sent to the drive automatically. The commands are kept in a tamperproof location in the SSD's memory. "Cigent D3E also periodically writes markers to the log to indicate the activity was performed with D3E 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[41] partition. … This command log can be used to audit drive activity to capture attempts to read information from the drive without D3E possibly indicating attempts to circumvent file protection. Further, the command log can be used to report on files accessed with or without D3E 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." [8].

[41] NTFS = New Technology File System

- Open ***Secure Drives*** at the D3E Desktop.
  - Select the top (…81) SSD drive.
  - Click on the *Advanced* icon, as indicated by the red arrow in Figure A-51.

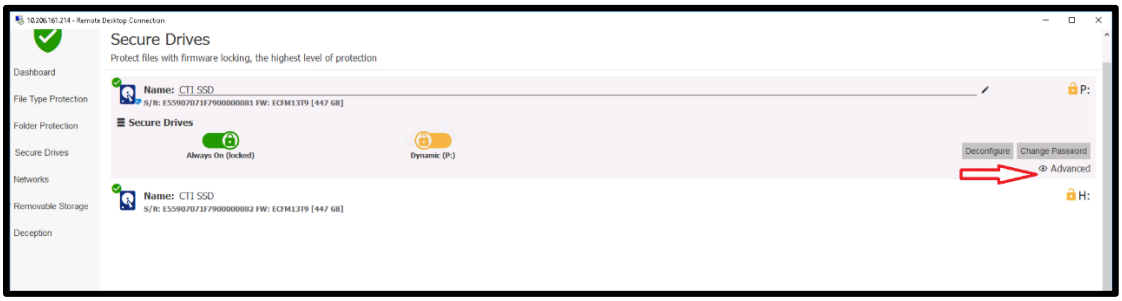


Figure A-51. Click "Advanced"

  - Click the Command Log Button. See Figure A-52. This will cause the *Command Log Audit* page (shown in Figure A-53) to be displayed.

Figure A-52. Click "Command Log"

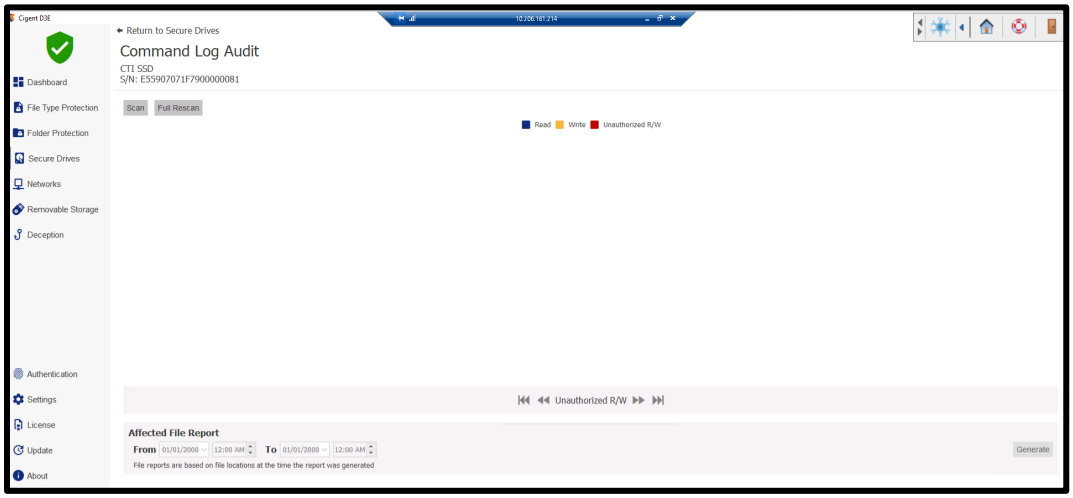


Figure A-53. *Command Log Audit* Page

- When we ran the *Command Log Audit* evaluation, the SSD had not yet been scanned, so it was necessary to scan the drive.
  - Click the **Scan** button. (Our initial scan took about 15 minutes.)

- The log provides start and end times to indicate the time window covered by the scan, i.e., the time elapsed from the previous scan to the current scan.
- The log shows the volume of authorized reads and authorized writes, as well as the combined unauthorized reads and writes (indicated below the x-axis in red on the bar chart).

Figure A-54. SSD Scan Results

- Note that our sample report covers approximately the 10 days leading up to the scan.
- Note also that scan results can be saved to comma-separated values (CSV) files. Refer to Figure A-55.
  - Two csv files, of type *csv_files* and *csv_ranges*, can be generated per scan. See Figure A-56 below. The csv files can be opened in Excel or in a text editor.
    - To generate csv reports:
      - Click **Generate**.
      - **Save** the file to the desired location.
      - Enter the prescribed authentication code (PIN).
  - Csv_files identify scan Time, Monitored status, Volumes, Letters, File IDs, Parent File IDs, and File Names.
  - Csv_ranges identify scan Time, Monitored status, Reads, Writes, and Ranges within memory.
- Administrators can drill down into specific scan timeframes by clicking on individual bars within the chart. Figure A-57 displays bar-chart data for a 48-minute span on 4/20/21. *Csv_file* and *csv_range* reports can be generated for these ranges, as well.

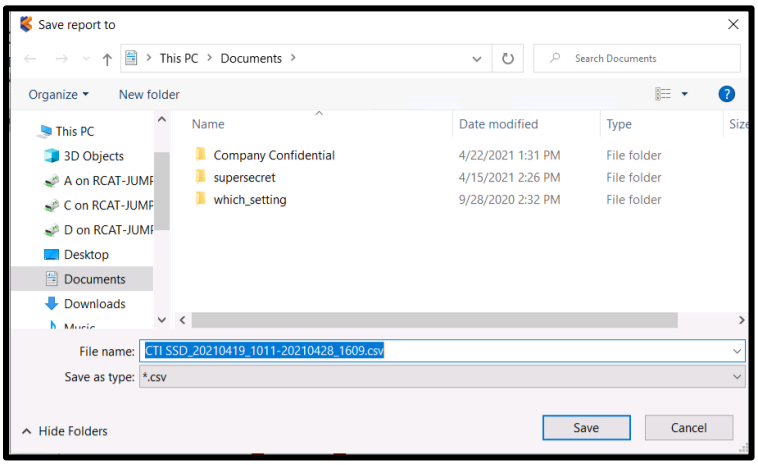


Figure A-55. Saving Scan Results to a CSV File

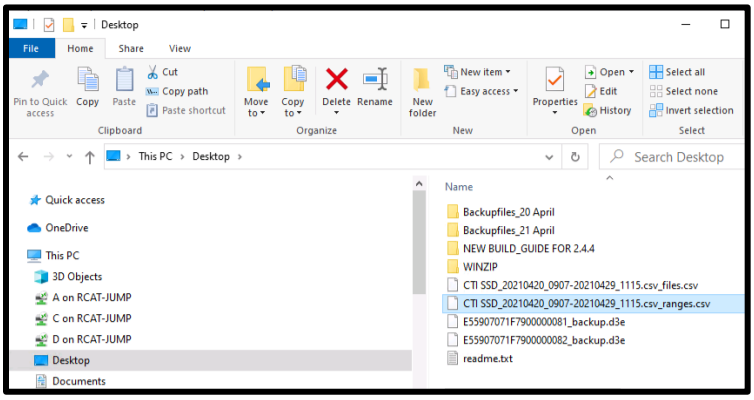


Figure A-56. Two CSV Files Generated

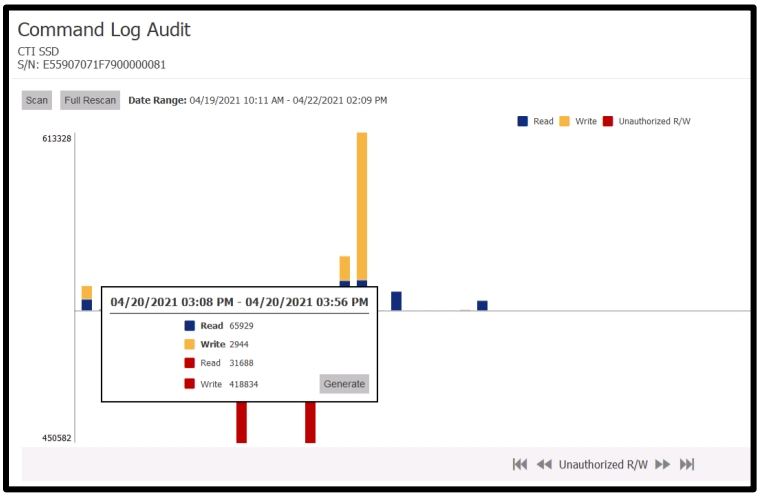


Figure A-57. Drill Down for Audit Data for Shorter Time Span

- After the initial scan completes, clicking the **Scan** button again simply (and promptly) retrieves the existing scan log. To obtain a fresh scan after some time has passed, press the **Full Rescan** button.

- Using Command Logs:
  - Cigent points out that the values in the csv_files of greatest importance are found in the *Time*, *Monitored*, and *File Name* columns.
    - Permissible values for *Monitored* are *Yes* and *No*. A *Monitored* value of *Yes* indicates that the file access was authorized (because the administrator entered the correct authentication code before the access attempt), while a value of *No* means that the file access was unauthorized.
    - Knowing the names of sensitive files can be beneficial when scanning audit logs. Recall that the file *Confidential.txt* resides on drive L and has *Always On* protection. Figure A-58 below shows that an unauthorized attempt was made to access the file on 20 April at 19:29:43 UTC, or ~3:30 PM local time.

Figure A-58. Command Log Showing Unauthorized Access to File

A.2.1.2 Evaluation Results

D3E *Command Log Audit* functioned as advertised on the Cigent laptop equipped with Secure Drives.

A.2.2 *True Erase*

Secure, verifiable data erasure from hard drives helps prevent unauthorized access to sensitive or classified information. Cigent SSDs provide a *True Erase* feature that supports "extended erasure verification commands to check each and every mapped and unmapped block to verify the data has been removed" [8]. The ***Erase Verify Secure Drive*** commands described below will result in **Failure** if any blocks in memory show un-erased data.

A.2.2.1 *True Erase* Evaluation Steps

- Select the detached SSD (S/N …82) to check whether there are un-erased data blocks on the drive. Since we're using the internal SSD (S/N …81) to conduct our *True Erase* evaluation, we know in advance that our SSD has not been erased. If it had been, D3E

wouldn't be installed and we couldn't conduct the evaluation. We can, however, check the detached drive.

- Open ***Secure Drives*** at the D3E Desktop.
  - Select the detached (…82) SSD drive.
  - Click on the *Advanced* icon.
  - Then click on the **Erase Verify** button. Refer to Figure A-59.

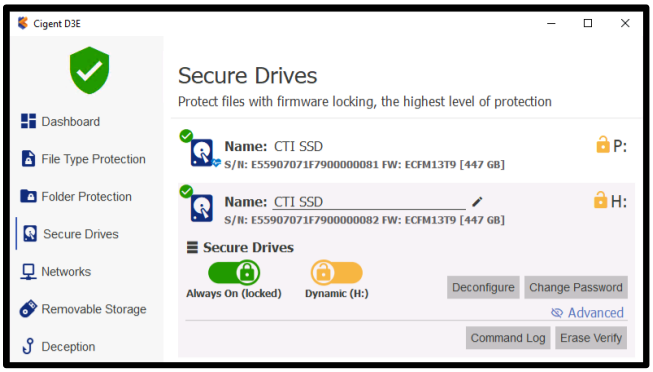


Figure A-59. Execute the Erase Verify Procedure

  - The results of the *Erase Verify* procedure are shown in Figure A-60. Because the detached SSD has not been erased, the *Erase Verify* action appropriately reports ***Device Not Erased***. The Erasure Verification Analysis shows that no blocks on the drive have been erased.

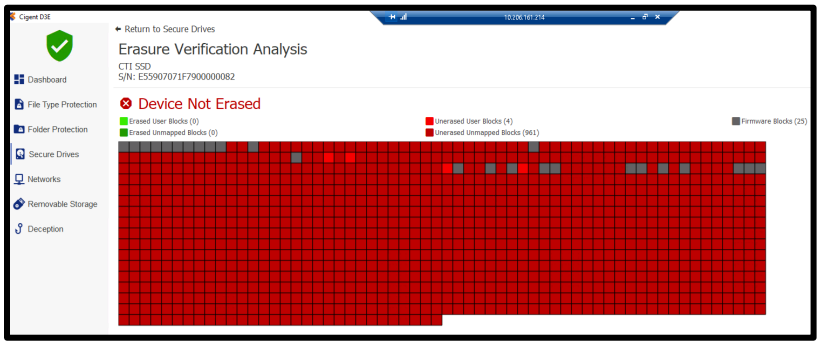


Figure A-60. Erase Verification Analysis

A.2.2.2 Evaluation Results

The D3E *True Erase* feature functioned as advertised on the Cigent laptop equipped with Secure Drives.

A.2.3 *KeepAlive* (Tethering)

The *KeepAlive* feature binds Cigent Secure SSDs to the D3E software running on them by means of a non-replayable heartbeat between the drive and D3E. When the feature is activated, Secure SSDs will enact *ActiveLock* and prevent file access if the drive fails to receive the heartbeat

signal in time. The feature prevents attackers from stopping D3E protection on unlocked Secure Drives.

If *KeepAlive* tethering has been provisioned for an SSD, there will be a small blue heart next to the drive icon in the Dashboard's ***Secure Drive*** panel. Figure A-61 indicates that the internal (…81) SSD has been provisioned with the *KeepAlive* feature, while the external (…82) drive has not.

Figure A-61. *KeepAlive* Provisioned on One Drive

A.2.3.1 *KeepAlive* Evaluation Steps

- Make sure both the *Always On* and *Dynamic* partitions on the internal SSD are unlocked.
- Enter "services" in the Windows search box.

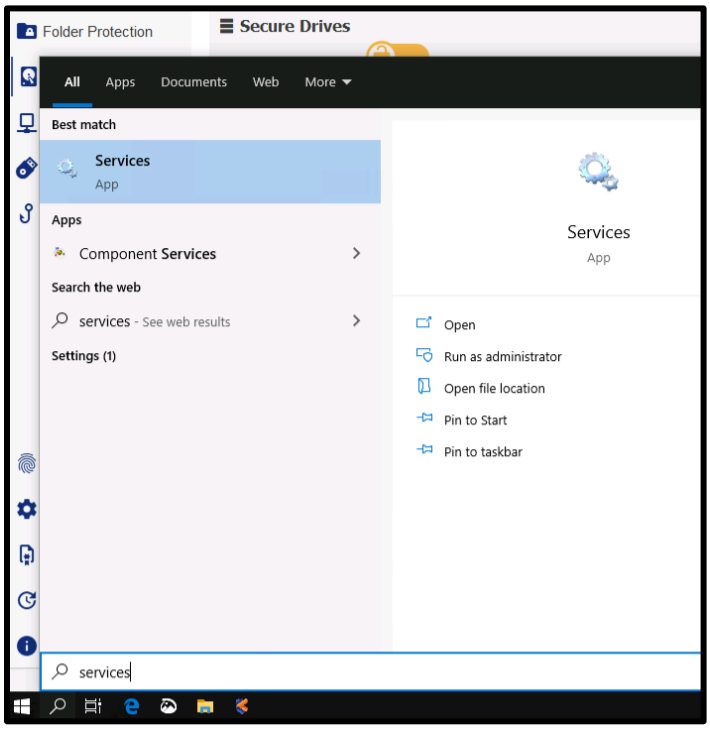


Figure A-62. Tethering Evaluation – Step 1

- Open the **Services** application and find the Cigent D3E Service.
- Right-click on the CigentD3E row and click *Properties*.

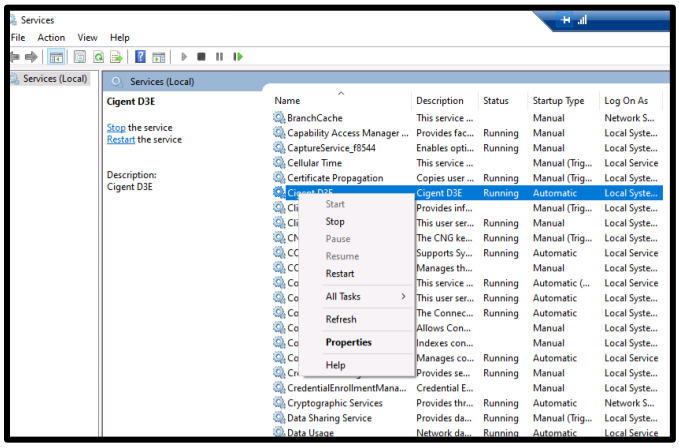


Figure A-63. Tethering Evaluation – Step 2

- At the *Recovery* tab, change all failure options to **Take No Action** and then click **OK**. See Figure A-64.

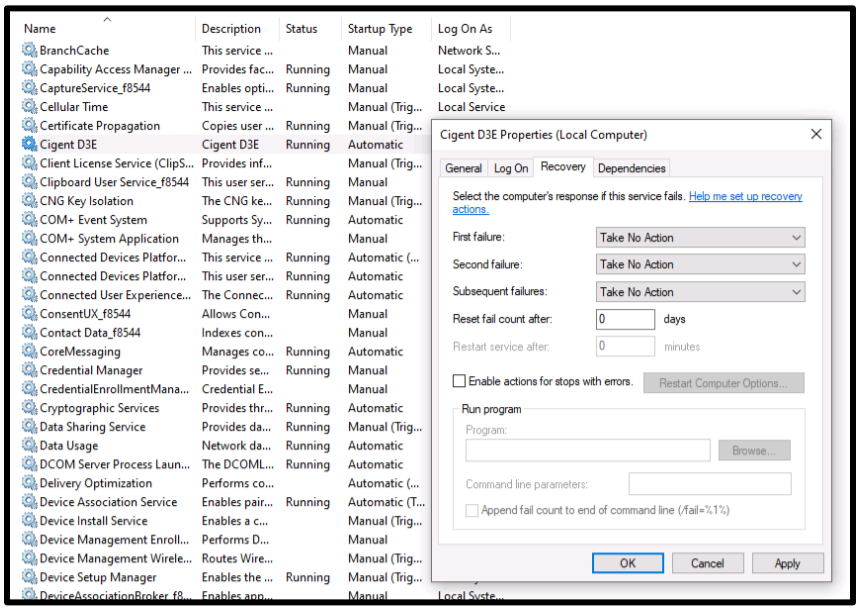


Figure A-64. Tethering Evaluation – Step 3

- Create a batch file called *keepalivetest.bat*, with contents as shown in Figure A-65 below. Note: Make sure that the drive letter in the "copy test" line matches that of the *Dynamic* partition on the Secure Drive.

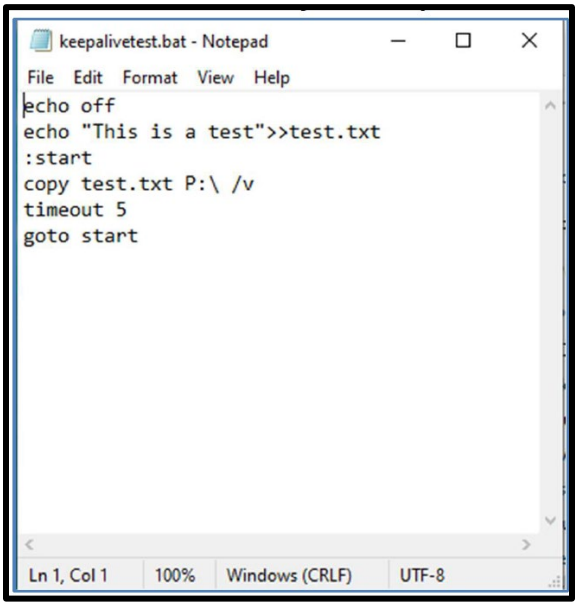


Figure A-65. Tethering Evaluation – Step 4

- Save the batch file to the ***Documents*** folder on the C:\ drive[42], as shown in Figure A-66.

[42] We saved the file to the user's ***Documents*** directory on the C:\ drive.

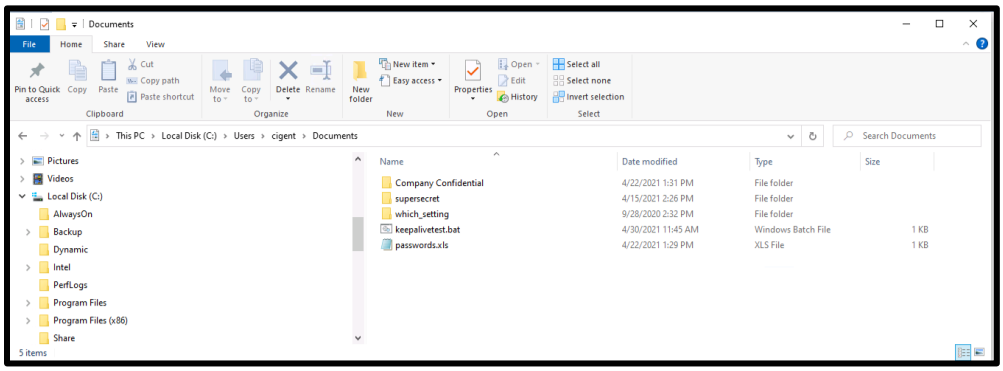


Figure A-66. Tethering Evaluation – Step 5

- Run the batch file, as described below and shown in Figure A-67:
  - Open a command-prompt window.
  - Navigate to the ***Documents*** directory.
  - Start the batch file (type "*keepalivetest.bat*").
  - Leave the batch file running.

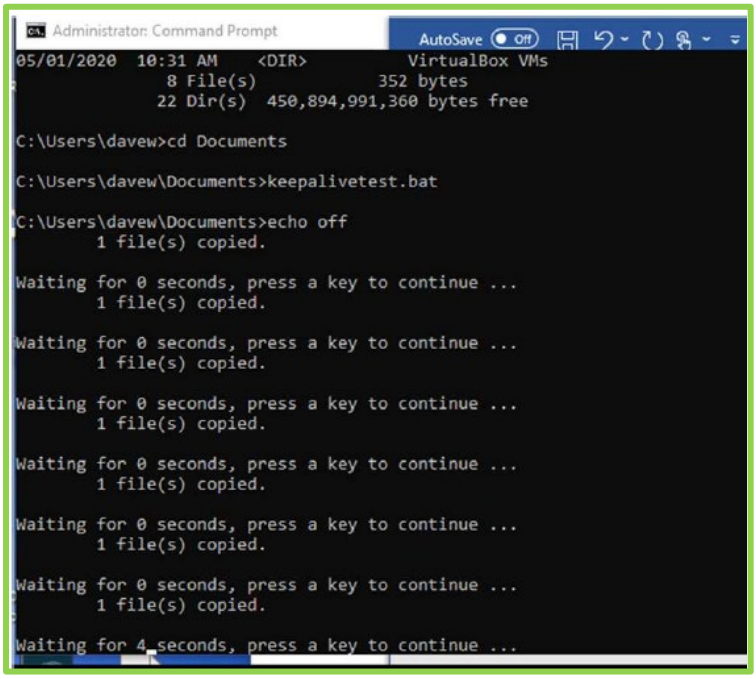


Figure A-67. Tethering Evaluation – Step 6 [8]

- Open a command prompt and navigate to C:\.
  - Run as administrator the command: "taskkill /IM cigentservice.exe /F"; this will shut down the Cigent Service. See Figure A-68.

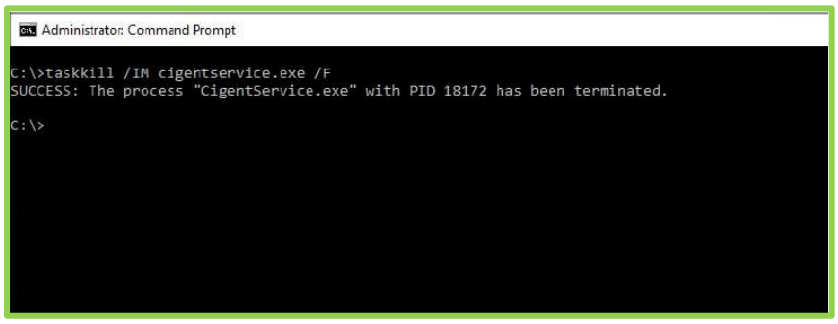


Figure A-68. Tethering Evaluation – Step 7 [8]

- Within 30 seconds the script output from the batch job will display an **ERROR Verify** message.
    - Press Ctrl-C to terminate the batch job.

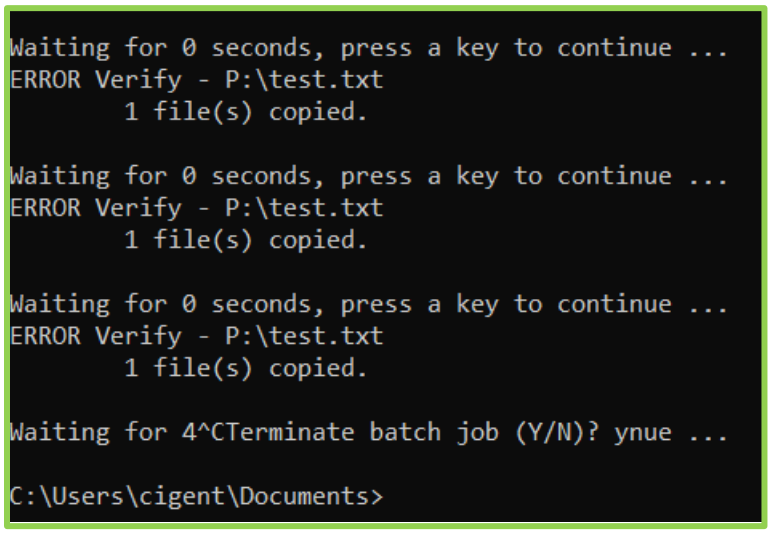


Figure A-69. Tethering Evaluation – Step 8 [8]

- Open Windows Explorer and Navigate to the L *Always On* drive.
    - Killing the D3E process severs the *KeepAlive* tether between D3E and the SSD. The drive's firmware locks the drive when no D3E heartbeat is detected.
        - The D3E Dashboard informs you that the service has been disabled. See Figure A-70.

Figure A-70. D3E Has Been Disabled

- Verify that it is impossible to open files or copy files to the drive. See Figure A-71.

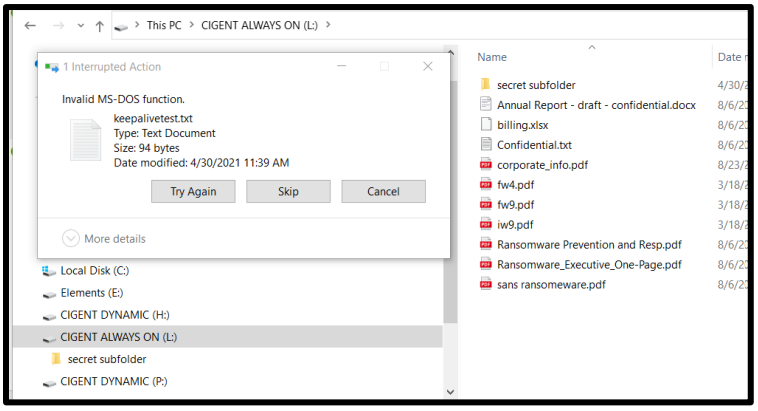


Figure A-71. Cannot Copy Files to the Always On Drive

- Return to normal operating mode by doing the following:
  - Turn the Cigent Service back on.
  - Return to the Cigent *Services Properties* page shown in Figure A-64 and change failure options at the *Recovery* tab back to **Restart the Service**.

A.2.3.2 Evaluation Results

The *KeepAlive* SSD feature performed as advertised. When the heartbeat tether between the SSD and D3E was severed, firmware in the drive locked the *Always On* drive, so that it was not possible to open files or write to that drive. In other words, when the heartbeat stopped, the *Always On* drive was protected, even though the D3E service had stopped. It was possible to open the *Dynamic* Drive and write to it, but that was expected.

We did notice an anomaly in the Cigent documentation. Reference [8] states that "In less than 30 seconds, the script output will start indicating 0 files copied and you will receive a Windows error indicating Write Protect Error. Press Ctrl-C to terminate the script." In fact, Windows gave the ***ERROR Verify*** message shown in Figure A-69.

A.3 D3E *Software Locking* Mode

The evaluation procedures below are described in reference [8] as pertaining to D3E software on Windows computers without SSD Secure Drives. Each of the procedures was run on our two Win7 test laptops. In a few instances, we supplemented earlier testing on the Cigent SSD-equipped Win10 laptop and ran D.3 software-locking tests on that machine, as well.

A.3.1 *Folder Protection*

Folder Protection for Cigent Secure SSD Drives was tested in Section A.1.2. The steps below demonstrate D3E *Folder Protection* for Windows PCs that are not equipped with Secure SSD Drives. For our evaluation, the two MITRE Win7 laptops were used to validate this Cigent capability.

A.3.1.1 Establish Secure Data Locations on Win7 Laptops

- At **both Win7 laptops**, perform the following steps. (The *CompanyInternal* and *HighlyConfidential* zipped files can be found in the desktop folder named EvaluationKitAuxFiles.)
    - Create a directory C:\Cigent.
    - Unzip *CompanyInternal* into C:\Cigent.
    - Unzip *HighlyConfidential* into C:\Cigent.
    - Select ***Folder Protection*** at the D3E Dashboard.
        - Click **Add a Dynamic Protection Folder**.

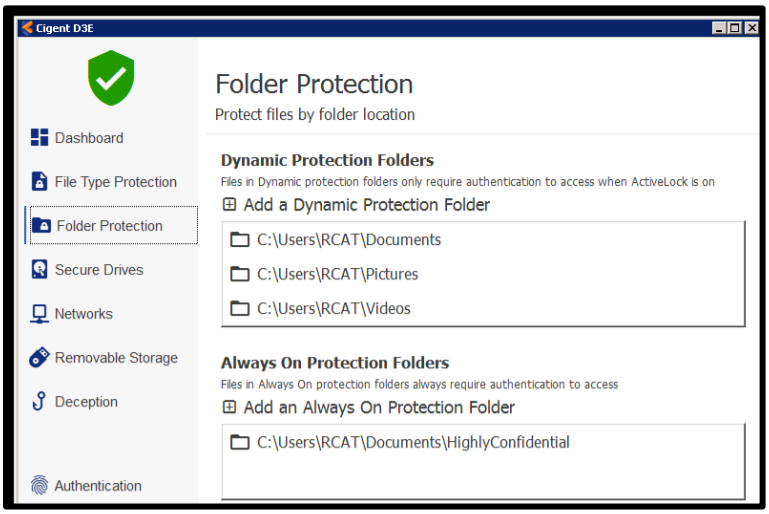


Figure A-72. Folder Protection – Setup Step 1

- Browse to C:\Cigent\CompanyInternal and click the **Select Folder** button.

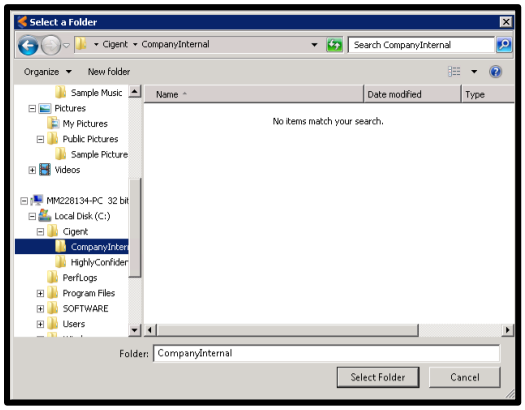


Figure A-73. Folder Protection – Setup Step 2

- Enter your PIN at the D3E prompt.

- Click **Add an Always On Protection Folder**.
  - Browse to C:\Cigent\HighlyConfidential and click the **Select Folder** button.
  - Enter your PIN at the D3E prompt.

- Results of these setup procedures are seen in Figure A-74.

Figure A-74. New *Dynamic* and *Always On* Folders Added

A.3.1.2 Remove *Always On* and *Dynamic* Protection Folders

- To remove an *Always On* or *Dynamic* protection folder, simply click on one of the displayed folders, and then click the **Remove** button and use the appropriate authentication method (PIN).

Figure A-75. Removing *Always On* and *Dynamic* Protection Folders

A.3.1.3 Assign both *Dynamic* and *Always On* Protection to a Folder

- Any attempt to assign both *Dynamic* and *Always On* protection to the same folder simultaneously should fail.
- Try to assign *Always On* protection to the C:\Cigent\CompanyInternal folder. (Note that the folder already has been assigned *Dynamic* protection.)
- Repeat the procedure described in Section A.3.1.2 for assigning *Always On* protection, browse to the C:\Cigent\CompanyInternal directory, and click **Select Folder**.

- The attempted double-assignment fails, as expected and desired.

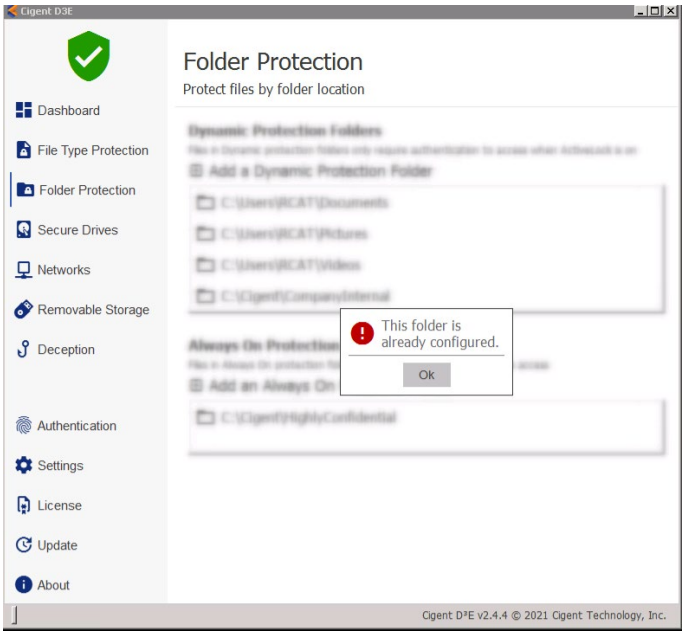


Figure A-76. Cannot Assign Dual Protection Configurations to a Folder

A.3.1.4 Win10 64-Bit Evaluation

(Verify Add & Delete Folder Protection for Secure SSD Drives)

- *Always On* and *Dynamic* protection features for Cigent Secure SSD Drives were covered as part of *Firmware Locking* in Section A.1.2 above, but the **Adding and Deleting Folder Protection** capability was omitted from that evaluation, because that functionality is considered software-only protection. Therefore, we revisited our earlier testing and tried to add and delete folder protection for the Cigent Win10 SSD-equipped machine. The D3E folder-protection feature met expectations, segregating important information into *Always On* and *Dynamic* folders to protect sensitive data.

A.3.1.5 Win7 32-Bit Evaluation

- Folder protection performed well and as expected for the MITRE Win7 32-bit laptop.

A.3.1.6 Win7 64-Bit Evaluation

- Folder protection performed well and as expected for the MITRE Win7 64-bit laptop.

A.3.2 *Dynamic* and *Always On* Protection

A.3.2.1 Accessing *Always On* Files

Perform the following steps at **both Win7 laptops**.

- Browse to C:\Cigent\HighlyConfidential in Windows Explorer.

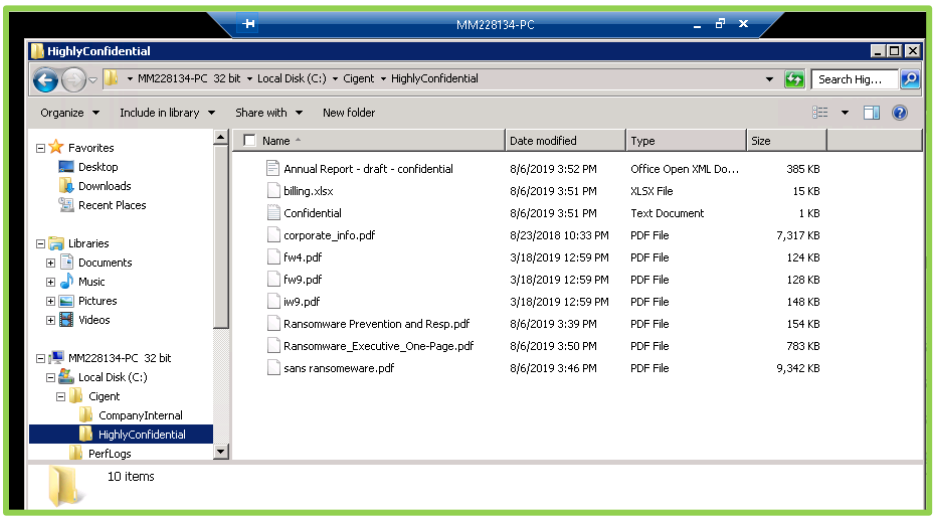


Figure A-77. Browse to HighlyConfidential Folder

- Double-click on the *Confidential.txt* to open the file. Regardless of the *ActiveLock* state, it will be necessary to use an approved authentication method to open the file, because the folder has *Always On* protection. See Figure A-78. After the correct PIN has been entered, opening/editing the file is possible.

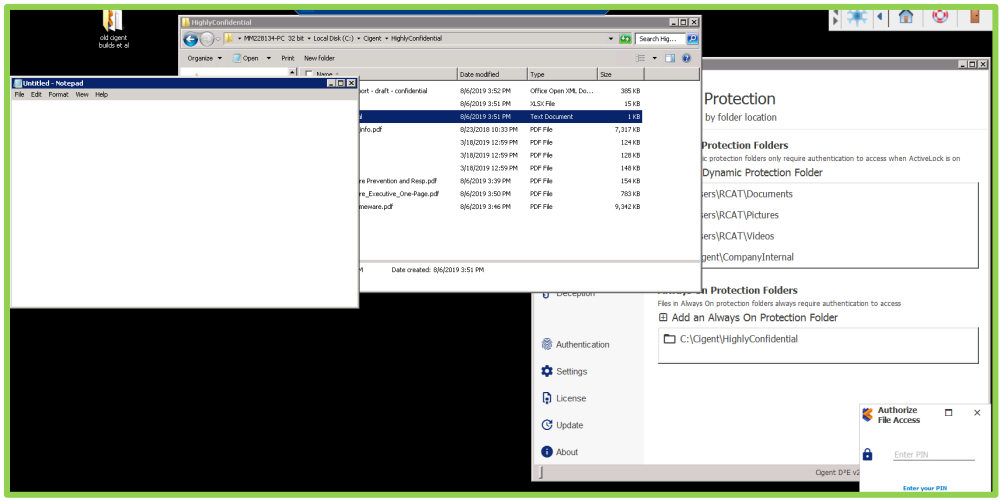


Figure A-78. Authentication Required to Unlock *Always On* Protection

A.3.2.2 Accessing *Dynamic* Files

Perform the following steps at **both Win7 laptops**.

- Make sure *ActiveLock* is not engaged. The shield at the D3E Desktop should be green.

- Browse to C:\Cigent\CompanyInternal in Windows Explorer.

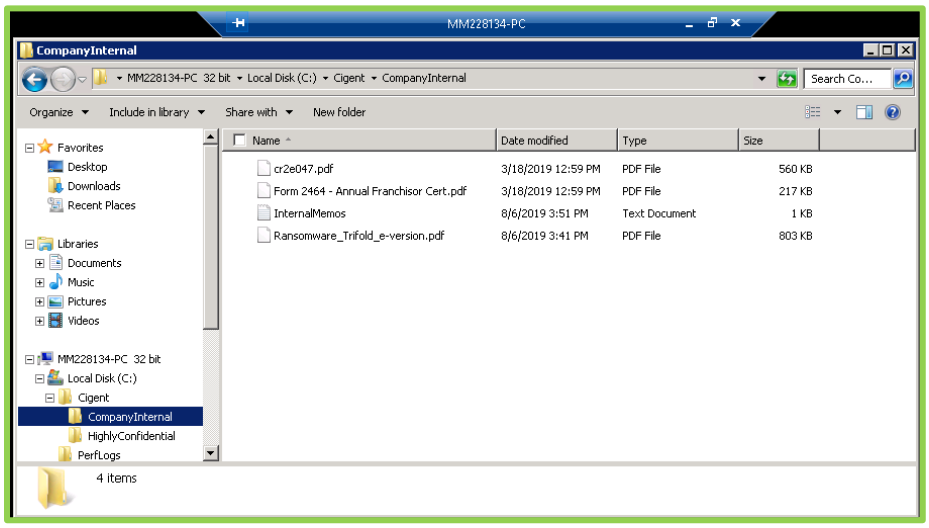


Figure A-79. Browse to CompanyInternal Folder

- Double-click on *InternalMemos* to open the text file. Because *ActiveLock* is not engaged, the file will open without the need for authentication.

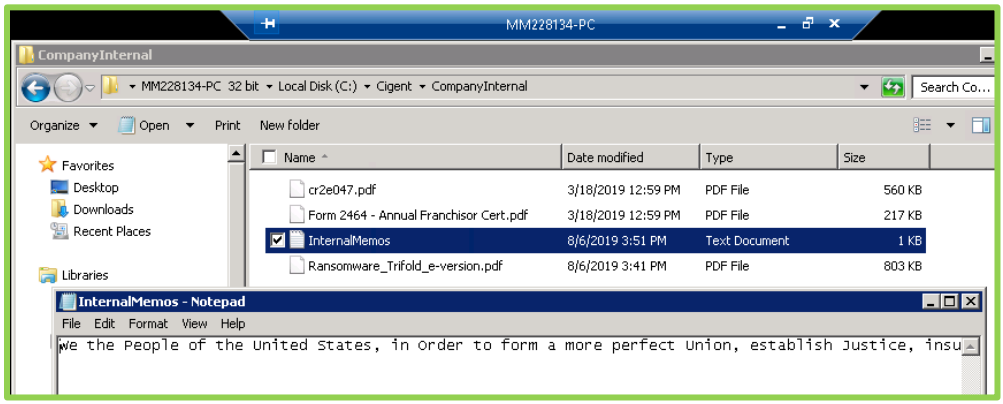


Figure A-80. *Dynamic* Files Open when *ActiveLock* not Engaged

- To demonstrate that D3E locks access to *Dynamic* files when *ActiveLock* is engaged, we will jump ahead and show that attempting to open a *Deception* file triggers *ActiveLock*, which, in turn, blocks access to *Dynamic* files and requires authentication to unlock. The topic of *Deception* Files is covered in greater detail in Section A.3.3 below.
    - Navigate to the *passwords.xls Deception* file in the ***Documents*** folder. See Figure A-81.

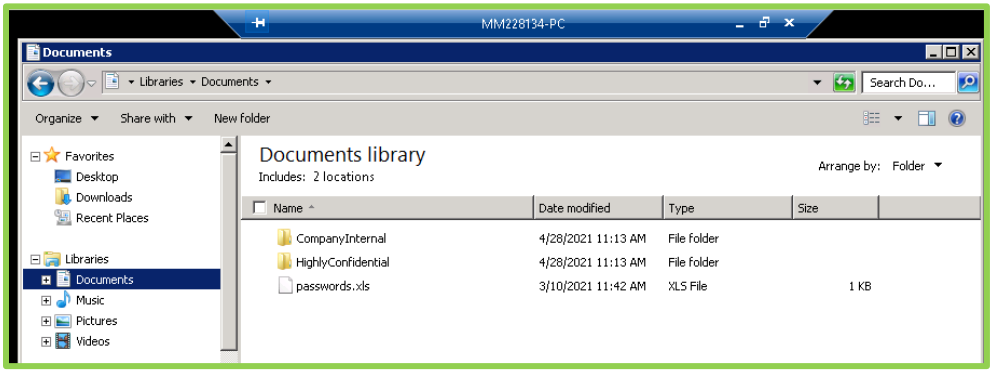


Figure A-81. Locate the Default *Deception* File

- Double-click on the file and attempt to open it. Note that trying to open the honeypot file triggers *ActiveLock* and access to the file is denied.

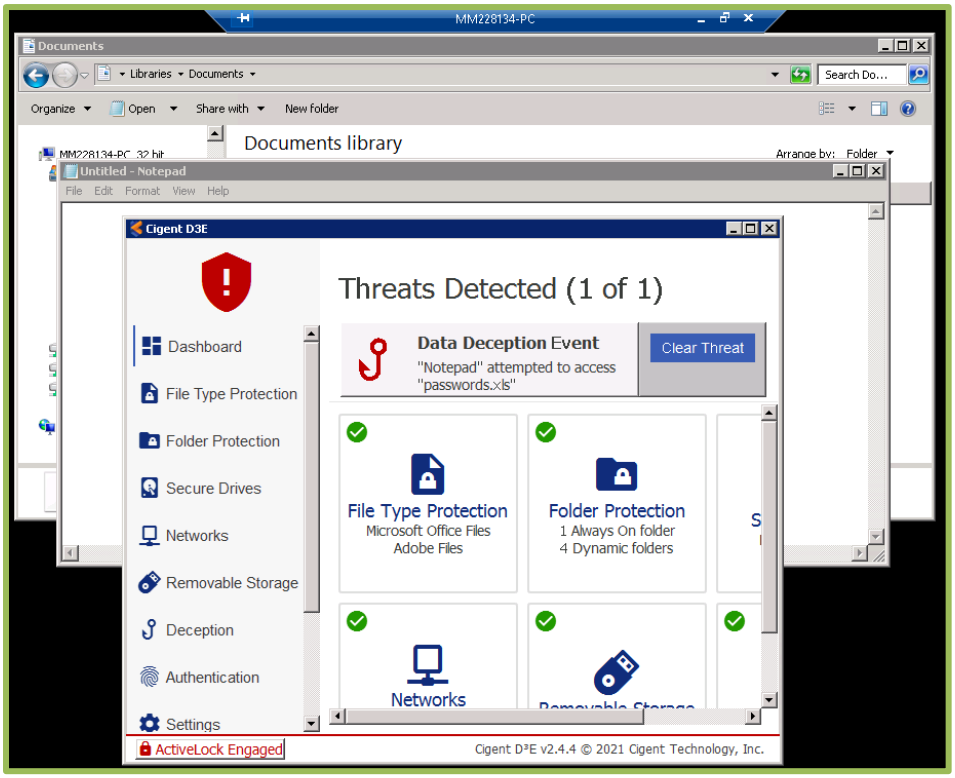


Figure A-82. D3E Locks Engages *ActiveLock* when Threats Are Sensed

- Ignore the *Data Deception Event* for now.
- Attempt to open *InternalMemos.txt* before clearing the alarm. Note that the D3E administrator must use authentication before the *Dynamic* file can be opened. See Figure A-83 and Figure A-84.

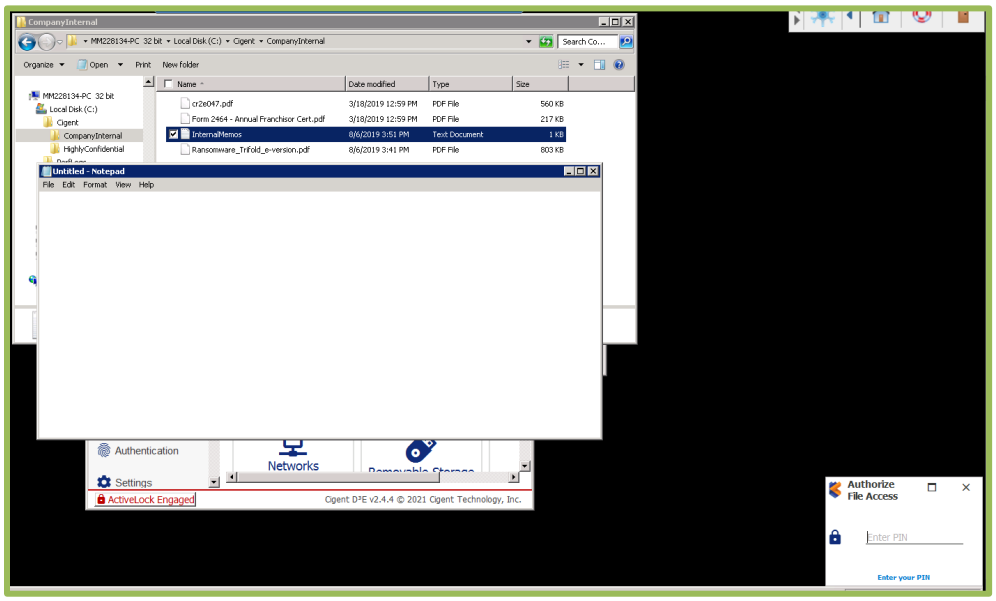


Figure A-83. *ActiveLock* Must Be Cleared before Opening *Dynamic* Files

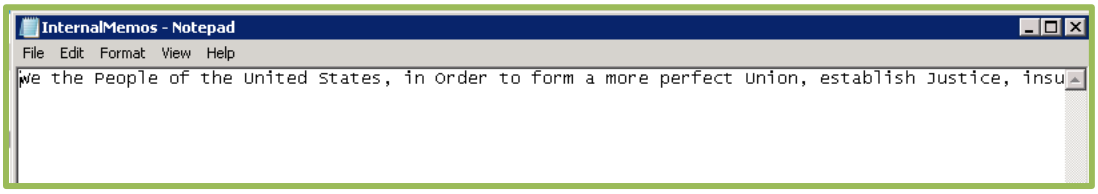


Figure A-84. *Dynamic* File Opens After *ActiveLock* Has Been Cleared

- Return to the D3E Dashboard to clear the *Data Deception Event* by using the prescribed authentication.

A.3.2.3 Win7 32-Bit Evaluation

- The evaluation of D3E *Dynamic* and *Always On* file protection on the MITRE Win7 32-bit laptop went as expected. All advertised features were demonstrated successfully.

A.3.2.4 Win7 64-Bit Evaluation

- The evaluation of D3E *Dynamic* and *Always On* file protection on the MITRE Win7 64-bit laptop went well and as expected.

A.3.3 *Deception* Files

The evaluation steps below were performed on the two MITRE Win7 laptops. They echo those conducted in Section A.1.3 for the Cigent SSD-equipped laptop and demonstrate D3E's response to attempts to access default and user-created honeypot *Deception* files.

A.3.3.1 Attempt to Access the Default passwords.xls *Deception* File

- Find the location of the D3E default *Deception* file, *passwords.xls*.
  - Click Deception at the D3E Dashboard.
  - Then click Show All at the *Deception* panel and enter appropriate authentication (PIN). Figure A-85 shows the results of these actions.

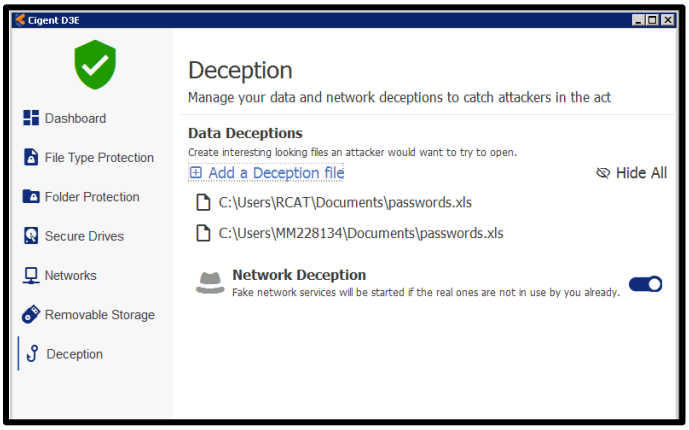


Figure A-85. Location of Default *Deception* File for This Laptop

- In Windows Explorer, browse to the location of the *passwords.xls* default *Deception* file (C:\Users\RCAT\Documents\passwords.xls).
- Try to open the honeypot file by double-clicking on *passwords.xls* in Windows Explorer.

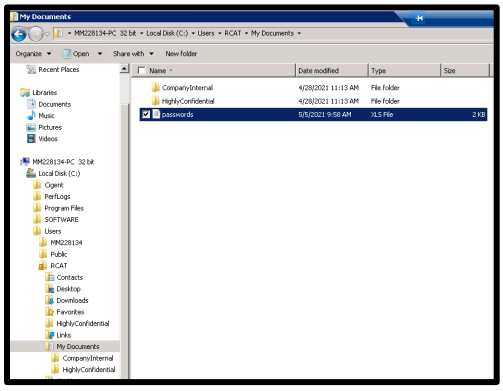


Figure A-86. Honeypot File in Explorer

- The attempt to open the honeypot file triggers *ActiveLock* and the alarms shown in Figure A-87.

Figure A-87. D3E Reaction to File *Deception* Event

- When *ActiveLock* is engaged, it is not possible to open files with *Dynamic* protection unless the administrator uses an appropriate authentication method to clear the alert. Try to open *InternalMemos.txt*. See Figure A-88.

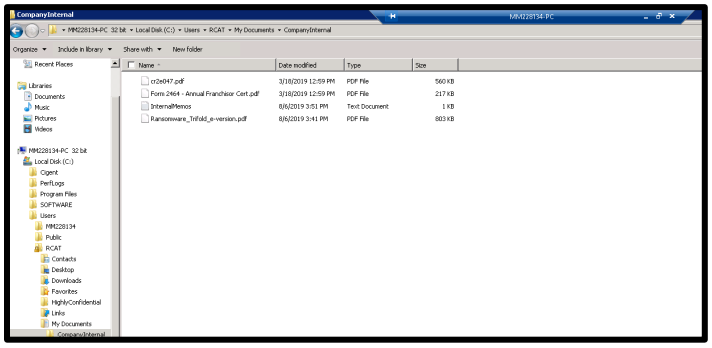


Figure A-88. Attempt to Open File with *Dynamic* Protection

- Note that D3E prompts the administrator to use authentication. See Figure A-89. Entering the correct PIN allows access to the file and clears the *ActiveLock* status.

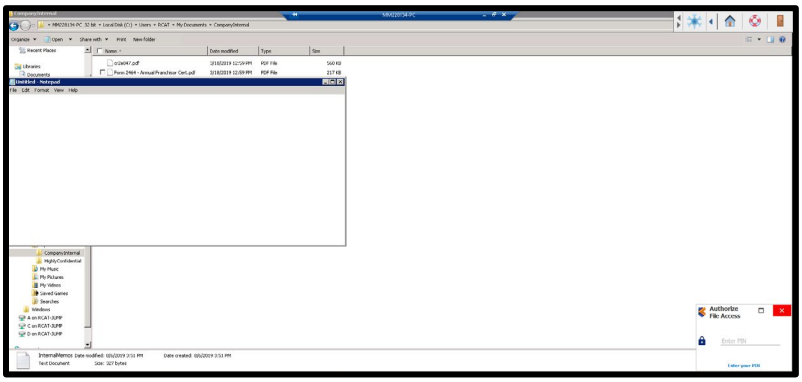


Figure A-89. Access Blocked to File with Dynamic Protection

A.3.3.2 Win7 32-Bit Evaluation

- D3E's *Deception Files* feature performed as advertised on MITRE's Win7 32-bit laptop. We did, however, notice some anomalous behavior[43]. Cigent is investigating the anomalous *Deception*-file behavior.
    - Although attempts to open user-created *Deception* files triggered the appropriate response, it was possible to delete those files from within Windows Explorer. The files also could be moved to another location and subsequently opened and edited.
    - While it was not possible to permanently delete the system-generated *passwords.xls* file, that file also could be moved and subsequently opened/edited. We moved the system-generated *Deception* file from the ***Documents*** folder to the Desktop prior to opening. We then edited the file and copied it back to its original honeypot location. See Figure A-90, which displays the new contents of the system-generated *passwords.xls* file.

[43] The anomalies cited here also were encountered on the SSD-equipped Cigent Win10 64-bit laptop and on the MITRE Win7 64-bit laptop.

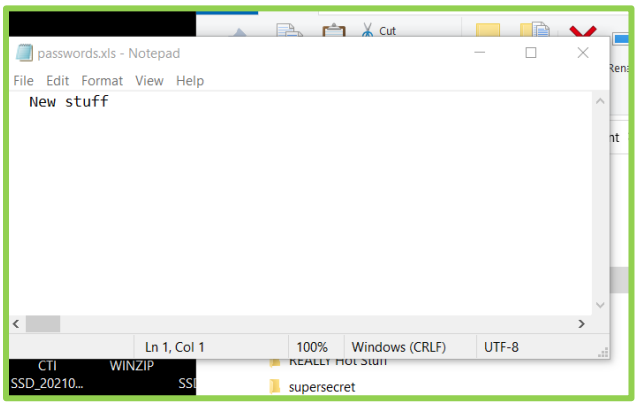


Figure A-90. Default Honeypot File after Editing and Return to Original Location

A.3.3.3 Win7 64-Bit Evaluation

- D3E's *Deception Files* feature performed as advertised on MITRE's Win7 64-bit laptop. The anomalies cited above were seen on this machine, as well.

A.3.4 Windows Defender Integration

The evaluation steps below were performed on the two MITRE Win7 laptops. They mirror the steps conducted in Section A.1.4 for the Cigent SSD-equipped laptop.

The subsections below evaluate D3E's integration with Windows' AV protection.

A.3.4.1 Evaluation Steps for Antivirus Integration

- At the D3E Dashboard Settings screen, make sure that *Trigger Active Lock if your Antivirus becomes disabled* is turned on. If it's not enabled, push the slider to the right and enter the appropriate authentication. (See Figure A-31.)
- As soon as this feature was enabled at the MITRE Win7 32-bit and 64-bit laptops, D3E triggered *ActiveLock*. See Figure A-91. There was no need to disable the host's AV software, because that software had not been installed. See Figure A-92. (To display the screen shown in Figure A-92, type "antivirus" at the search window and select "*Review your computer's status and resolve issues*." See Figure A-93.)

Figure A-91. Lack of AV Protection Triggers *ActiveLock*

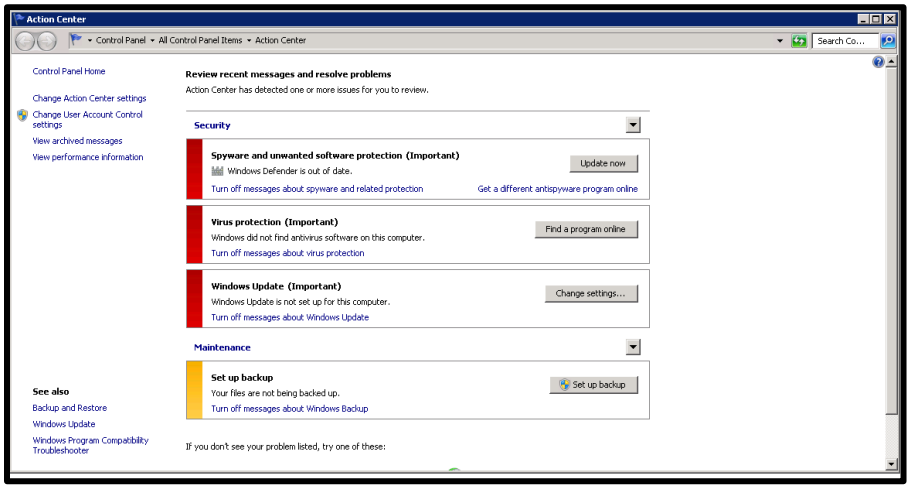


Figure A-92. AV Protection Missing from Win7 Host

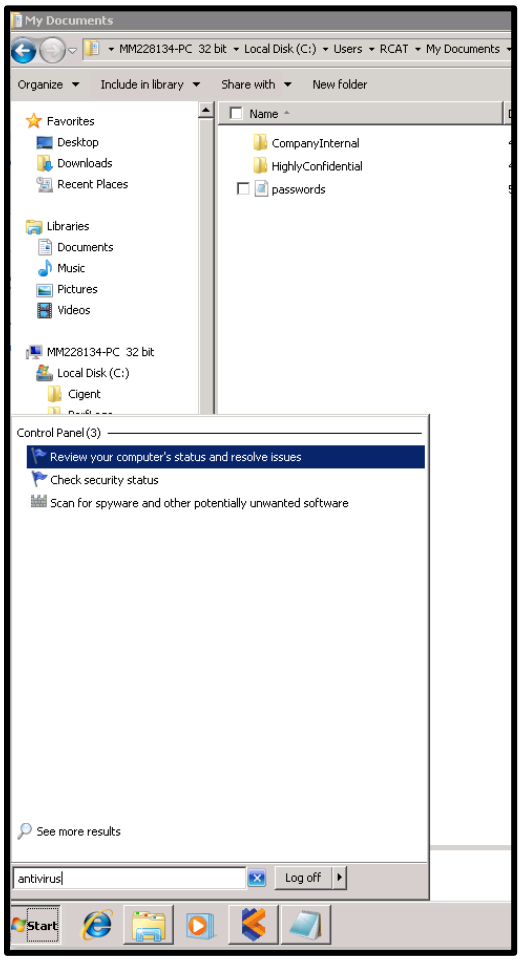


Figure A-93. Review the PC's Security Status

- The lack of AV protection on the host triggered *ActiveLock*. Ensure that it's not possible to access files with *Dynamic* protection when *ActiveLock* is engaged.
    - Repeat steps from the *Deception* Files evaluation and try to access the *InternalMemos.txt* file. Ensure that D3E yields results identical to those encountered in the *Deception* test. See Figure A-94.

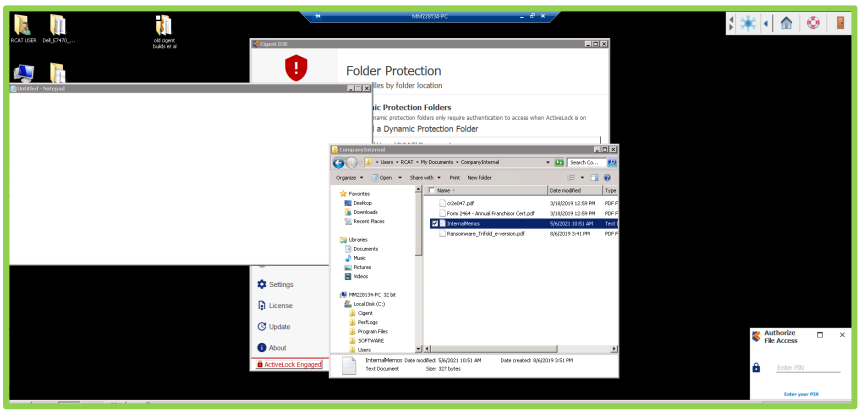


Figure A-94. Cannot Access File with *Dynamic* Protection in *ActiveLock* State

- Return D3E settings to their original status and turn off the *ActiveLock* condition.
    - Go to the D3E Dashboard's ***Settings*** menu and deactivate the *Trigger Active Lock if your Antivirus becomes disabled* setting. Push the slider to the left and use the appropriate authentication.

A.3.4.2 Win7 32-Bit Evaluation

- D3E's *Windows Defender Integration* feature performed as advertised on MITRE's Win7 32-bit laptop.

A.3.4.3 Win7 64-Bit Evaluation

- D3E's *Windows Defender Integration* feature performed as advertised on MITRE's Win7 64-bit laptop.

A.3.5 *Network Manager*

The evaluation steps below were performed on the two MITRE Win7 laptops. They repeat those executed in Section A.1.5 for the Cigent SSD-equipped laptop and demonstrate D3E's response to attempts by unauthorized devices to access the D3E-protected host.

A.3.5.1 D3E Response to Untrusted Network Connections

- Untrust the current network to simulate the effects of connecting the D3E-protected host to an untrusted network.
    - Select *Networks* at the D3 Dashboard.
    - Click on a trusted network.
    - Click the **Untrust** button. Refer to Figure A-95.

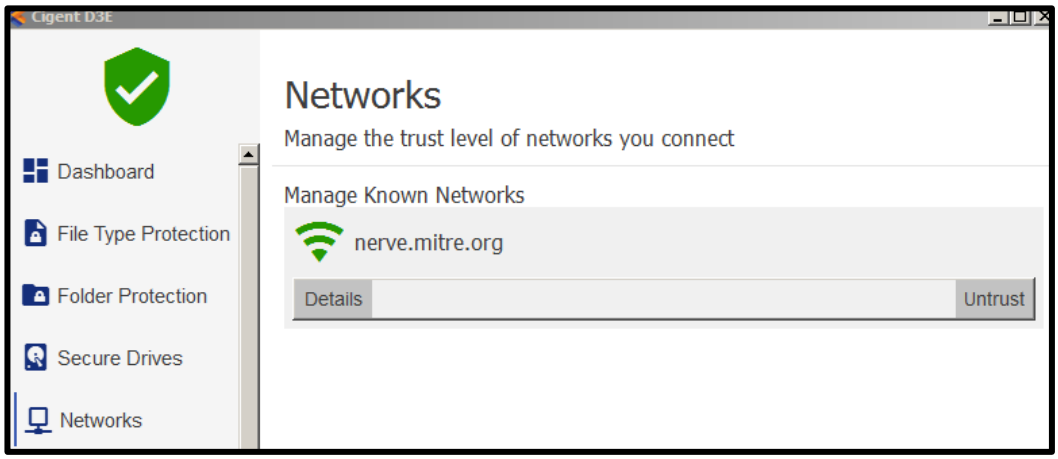


Figure A-95. Untrust the Current Host Network

- *ActiveLock* is engaged. Refer to Figure A-96.

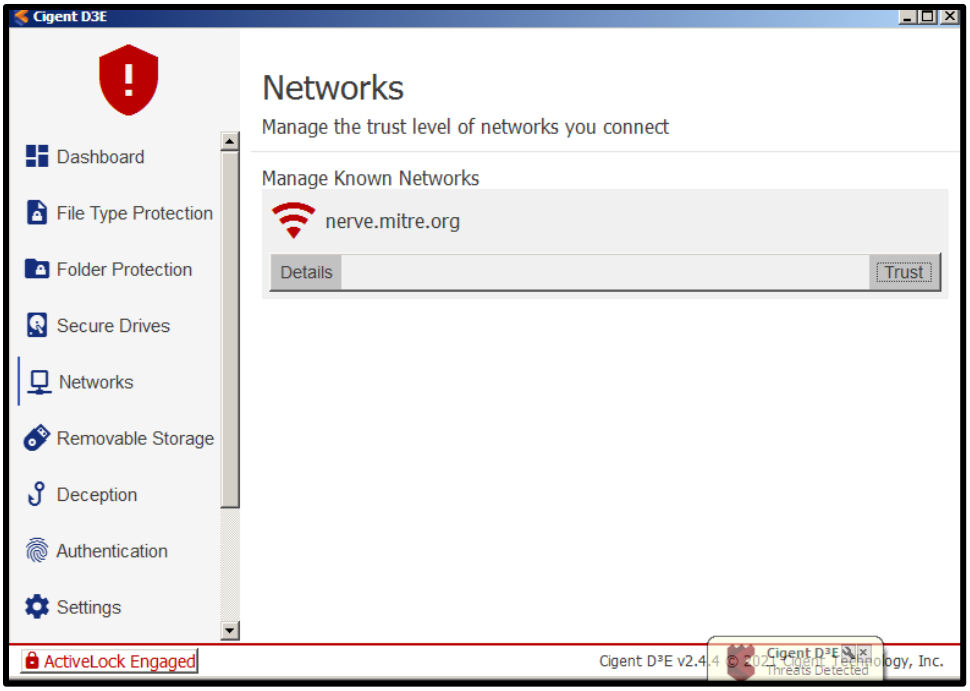


Figure A-96. Untrusted Network Connection Triggers *ActiveLock*

- Show that files with *Dynamic* protection cannot be opened under *ActiveLock* condition.
  - Attempt to open *InternalMemos.txt* while D3E is in *ActiveLock*. See Figure A-97.

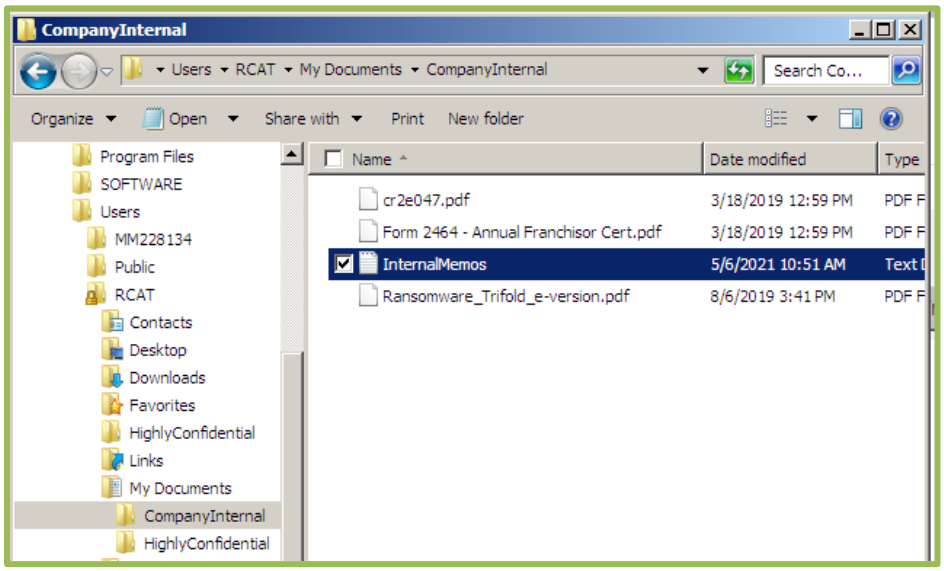


Figure A-97. Attempt to Open File with *Dynamic* Protection

- D3E Requires Authentication to Open file, as shown in Figure A-98 and Figure A-99.

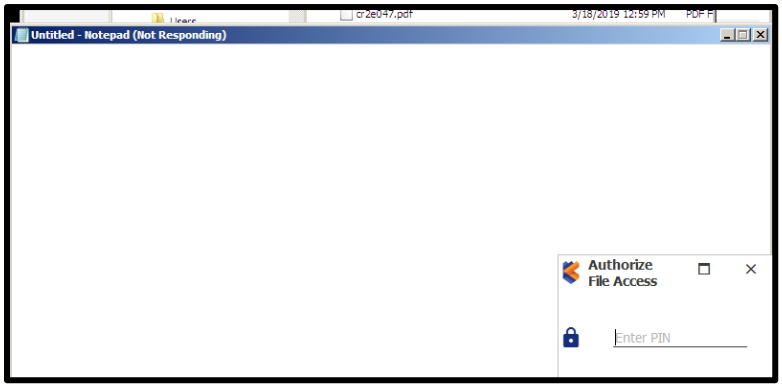


Figure A-98. Enter Authentication to Open Protected File

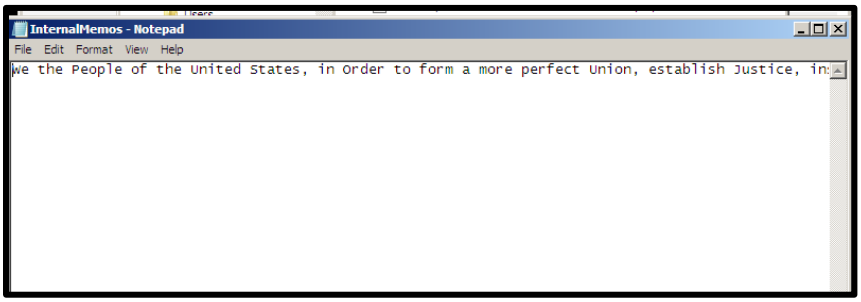


Figure A-99. File Opens with Authentication

- Clicking **Untrust** also causes the network connection to drop. To clear the *ActiveLock* condition and restore the network connection, return to the *Networks*

page at the D3E Dashboard, click **Trust** for the network you previously untrusted, and use the prescribed authentication method. Refer to Figure A-100 and Figure A-101.

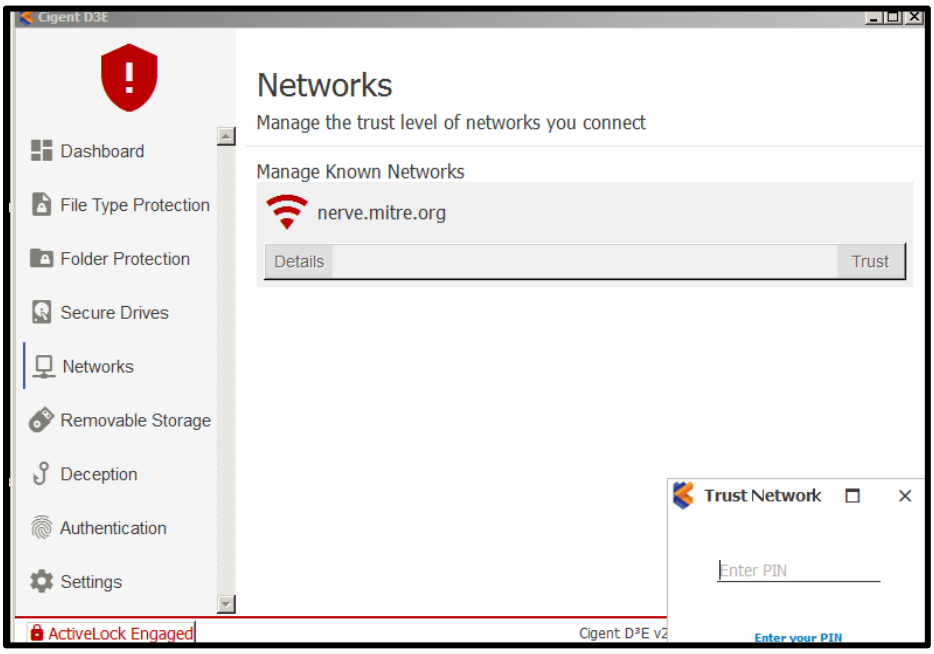


Figure A-100. Return to Original Network Trust Status

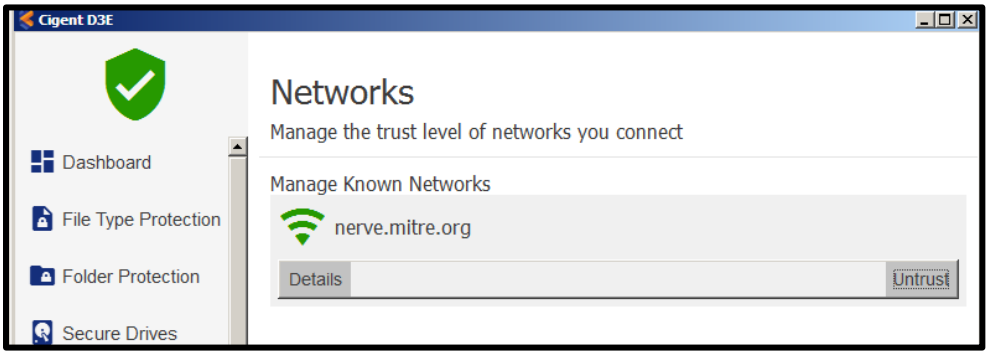


Figure A-101. In Network We Trust

A.3.5.2 D3E Response to Port-Scanning Attempts

- Before starting the network-scanning evaluation, go to the D3E *Deception* menu and make sure *Network Deception* is turned on.

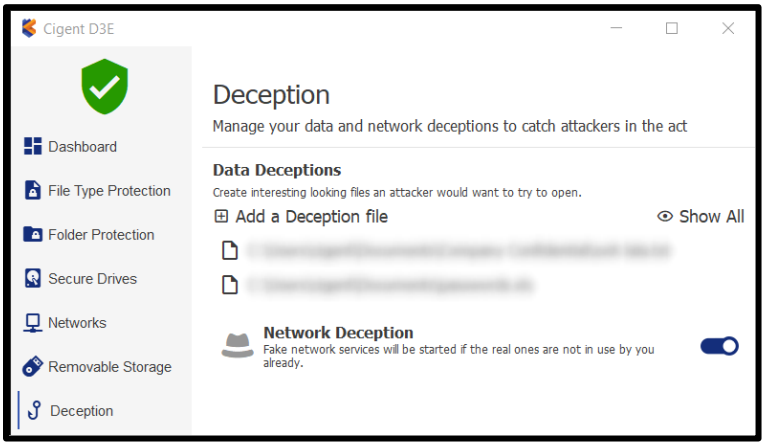


Figure A-102. Make Sure *Network Deception* is Active

Note that separate scanning applications were used for the 32-bit and 64-bit Win7 laptops.

- To perform the network-scanning evaluation, we used a port-scanning program provided by Cigent. That file is included on the laptop, as described below and shown in Figure A-103.
    - The desktop of the evaluation laptop contains a folder called **NEW BUILD_GUIDE FOR 2.4.4.** Open the folder.
    - Next, open the folder called ***16 April Cigent Stuff for hard drive and laptops***.
        - **For the Win7 64-bit laptop**, click on the ***EvaluationKitAuxFiles.zip*** folder, within which you'll see *network_recon_local_only.zip*. Unzip that file. We will use *network_recon_local_only.exe* to scan network ports of the 64-bit laptop.
            - **For the Win7 32-bit laptop,** use the *local-netscan-32.exe* file contained within the ***16 April Cigent Stuff for hard drive and laptops*** folder.

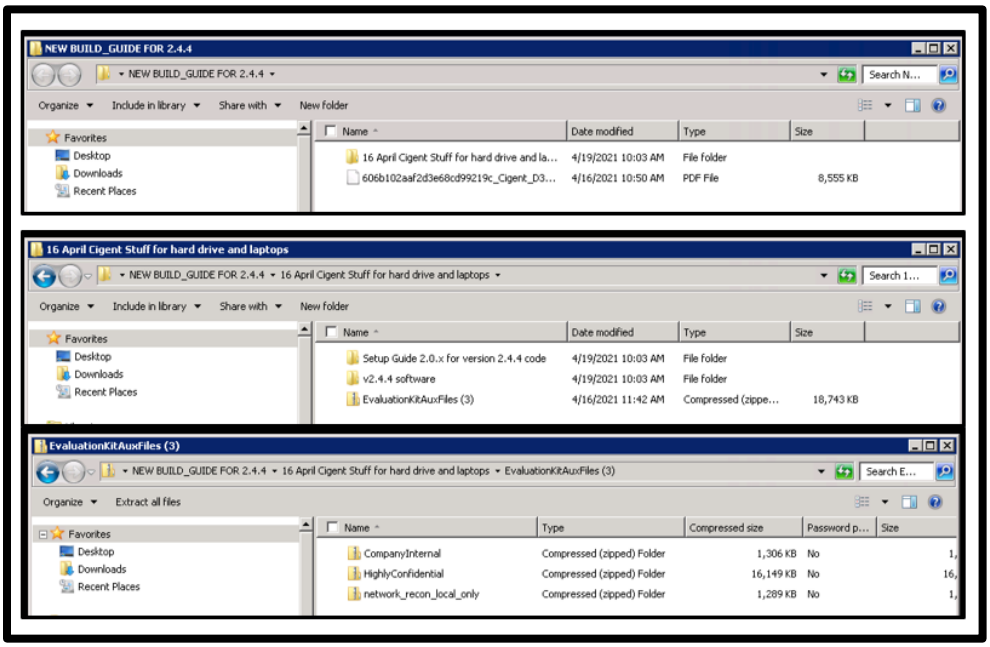


Figure A-103. Locate the Port-Scanning File on the Desktop

- Copy *network_recon_local_only.exe* (or *local-netscan-32.exe* for the 32-bit machine) to C:\ directory. (The file can be run from anywhere; we chose that location arbitrarily.)
- Open a command prompt; set the current directory to C:\; then run the attack script. Refer to Figure A-104 and Figure A-105.
    - Note that the script attacks ports 21, 3389, 445, 139, and 135. These ports are used for File Transfer Protocol (FTP), Remote Desktop Protocol (RDP), Transmission Control Protocol (TCP), Server Message Block (SMB), and Remote Procedure Call (RPC), respectively.

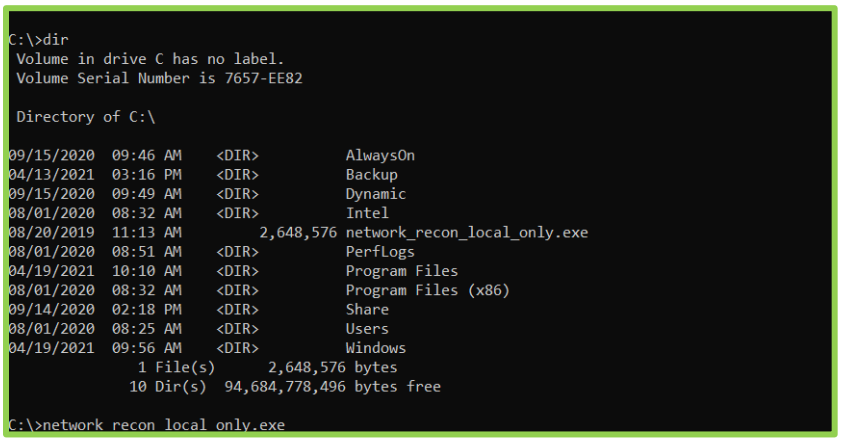


Figure A-104. Run the Attack Script

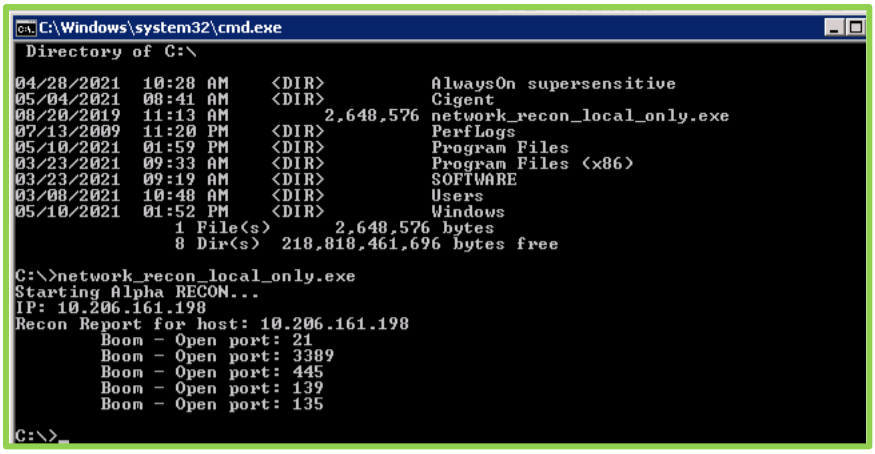


Figure A-105. Execution of Port-Scan Attack Script

- D3E's reaction to the *Network Deception* is shown in Figure A-106.
  - *ActiveLock* is engaged.
  - The D3E icon turns red.

- You are prompted to enter authentication to clear the threat.

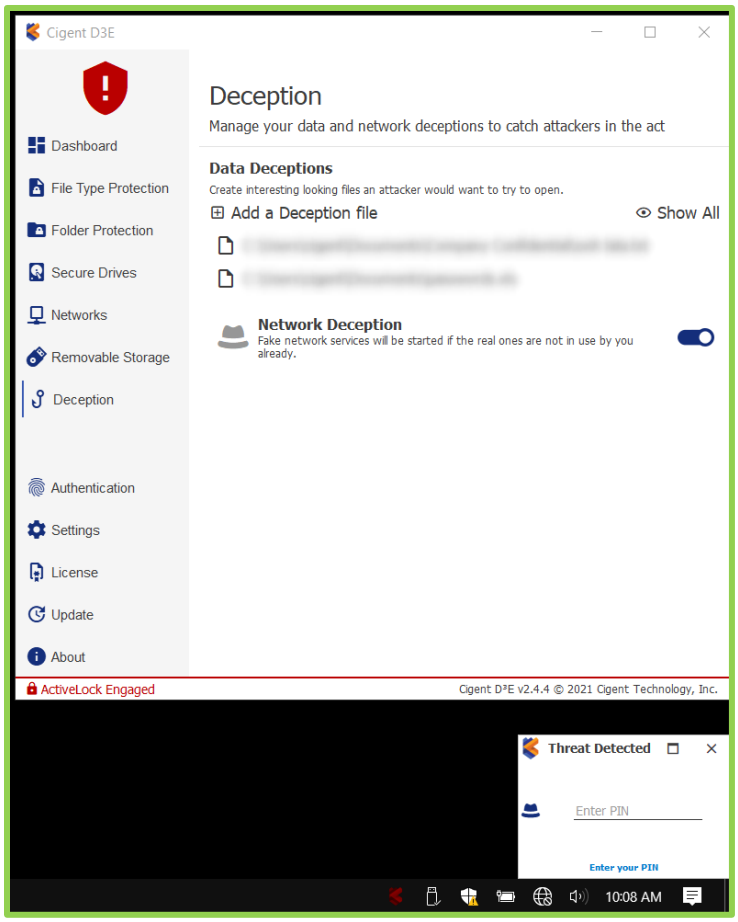


Figure A-106. D3E Reaction to Port Scan

- For completeness, after initiating port scanning, we attempted to open a file that had been assigned *Dynamic* protection. D3E appropriately protected the file and prompted the administrator to enter authentication. See Figure A-107.

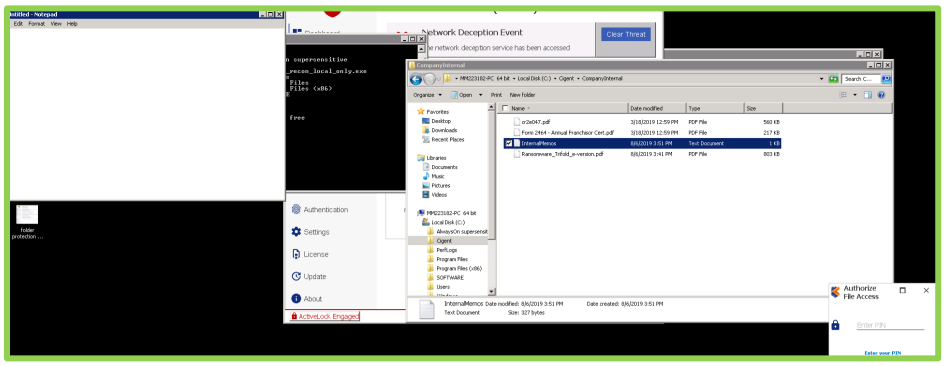


Figure A-107. PIN Needed to Open *Dynamic* File after Port Scan

- Go to the Security Status tab and enter a PIN to clear the test threat.
  - *ActiveLock* is now disengaged, as shown in Figure A-108.

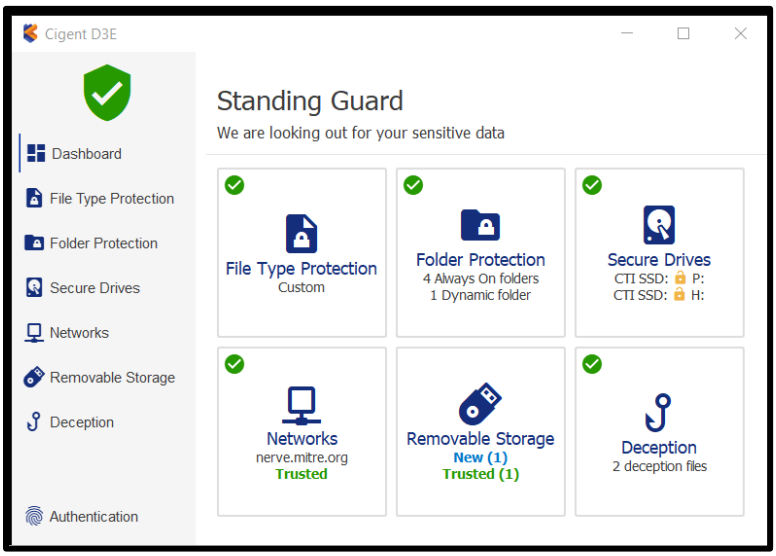


Figure A-108. ActiveLock Disengaged

A.3.5.3 Win7 32-Bit Evaluation

- The "untrust" portion of the *Network Manager* evaluation performed well and as expected on the MITRE Win7 32-bit laptop.
- Results of the network-scanning evaluation on the MITRE Win7 32-bit laptop went well.

A.3.5.4 Win7 64-Bit Evaluation

- The "untrust" portion of the *Network Manager* evaluation performed well and as expected on the MITRE Win7 64-bit laptop.
- The network-scanning evaluation went well and as expected on the MITRE Win7 64-bit machine.

A.3.6 *File Extension Protection*

In addition to the drive/partition and folder protection documented earlier, D3E also lets administrators assign *Always On* and *Dynamic* protection to files based on the files' extension. This feature was added to D3E to spare administrators from having to reorganize files into designated protection folders. Instead, global protection is given to files with the designated extension(s), regardless of their location within the PC's directories. Cigent cautions that, because this protection-assignment method is global, it could have unintended consequences. Cigent advises users to "implement File Extension protection on files that are used only for a particular application, for example, PDF" [8]. Section A.3.6.2 examines in more detail the potential for conflict between *Folder Protection* and *File Extension Protection*.

The *File Extension Protection* demonstration was conducted on all three evaluation laptops. Following reference [8], we opted to assign *Always On* protection to files with *.pdf* extension and *Dynamic* protection to files with *.txt* extensions. Prior to starting the exercise, we removed existing folder protections, so that the effects of *File Extension Protection* would not be masked.

A.3.6.1 Evaluation Steps for *File Extension Protection*

Execute the following steps on all three evaluation laptops.

- Remove *Folder Protection*.
  - Click the *Folder Protection* menu at the D3E Dashboard.

Figure A-109. *Folder Protection* Menu [8]

  - Remove *Folder Protection* by selecting the folder and then clicking the **Remove** button. Use the prescribed authentication method to enact the removal. Repeat this step for each *Dynamic* and *Always On* folder. Refer to Figure A-110.

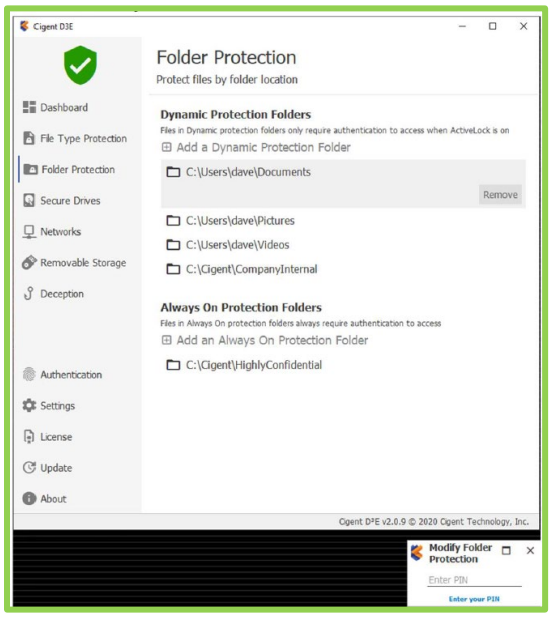


Figure A-110. Remove *Folder Protection* [8]

- At the conclusion of the previous step, the *Folder Protection* menu should look like Figure A-111 below. In other words, no *Folder Protection* should be assigned.

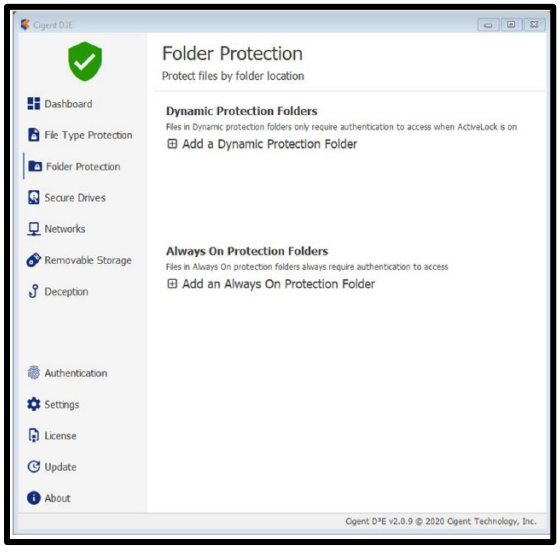


Figure A-111. No *Folder Protection* Assigned [8]

- Assign *File Extension Protection*

  Full *Always On* or *Dynamic* protection may be assigned to Microsoft Office files, as well as to Adobe files. In addition, D3E lets administrators customize the *File Extension Protection* feature by designating other file extensions for protection.

  In this exercise, we assign *Always On* protection to files with a .pdf extension, and *Dynamic* protection to files with .txt extension.

- Select the *File Type Protection* menu at the D3E Dashboard.

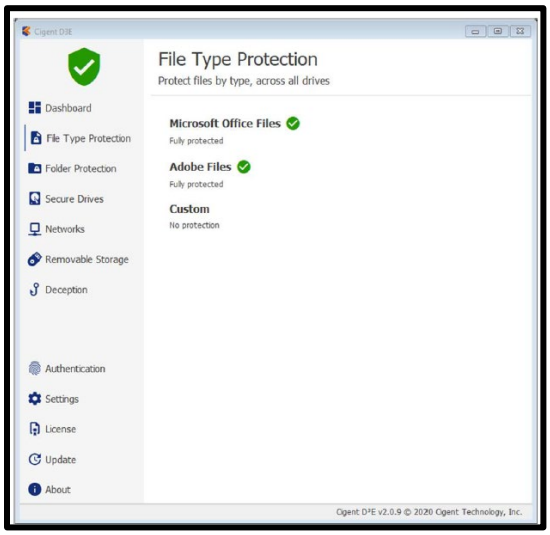


Figure A-112. *File Type Protection* Menu [8]

- Click ***Adobe Files.***
  - It may be necessary to enable the *Allow Always On File Extension* feature at the Dashboard's ***Settings*** screen. If the message **"Enable 'Allow Always On File Extension' option to add Always On extensions"** appears at the top of the Adobe Files screen (as shown in Figure A-113), simply enable the feature at the ***Settings*** screen.
    - Move the slider to the right and use the prescribed authentication. See Figure A-114.

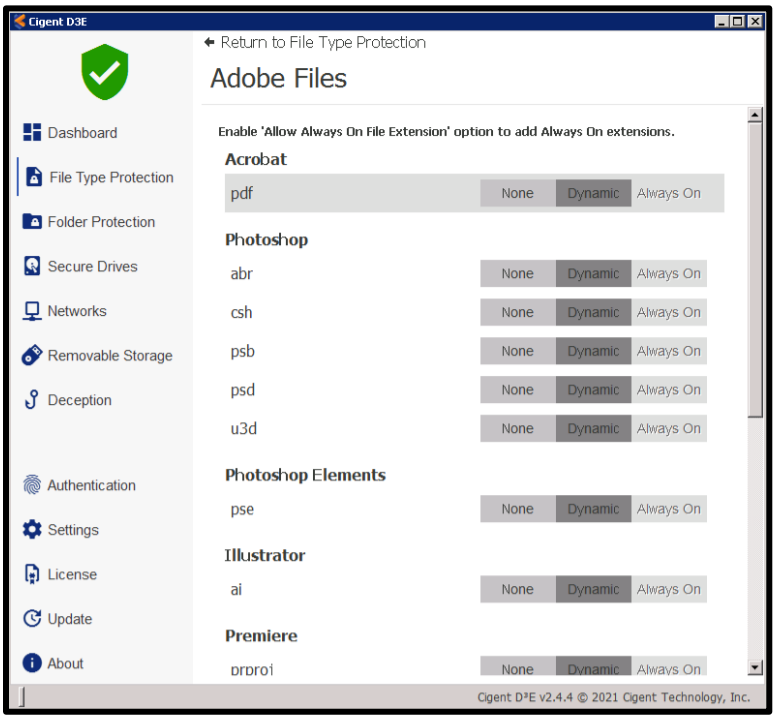


Figure A-113. *Allow Always On File Extension* Must Be Enabled

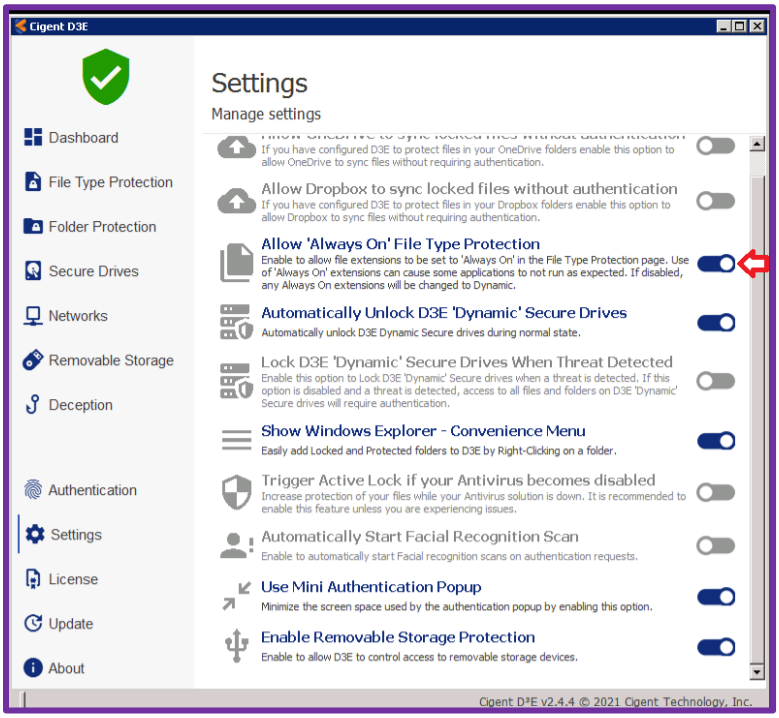


Figure A-114. Enabling *Always On* File Protection

- After *Always On File Protection* has been enabled, clicking ***Adobe Files*** will display the screen shown in Figure A-115 below.

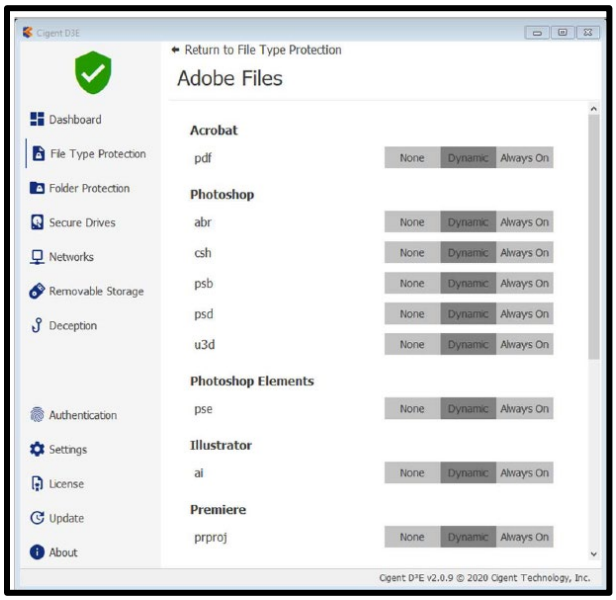


Figure A-115. Setup Screen for Adobe File Protection

- Note that multiple Adobe file-extension types may be assigned D3E protection. For this exercise, select *Always On* protection for PDF files, as shown in Figure A-116.
  - Click the **Save** button.
  - Then use the prescribed authentication method to enact your selection.

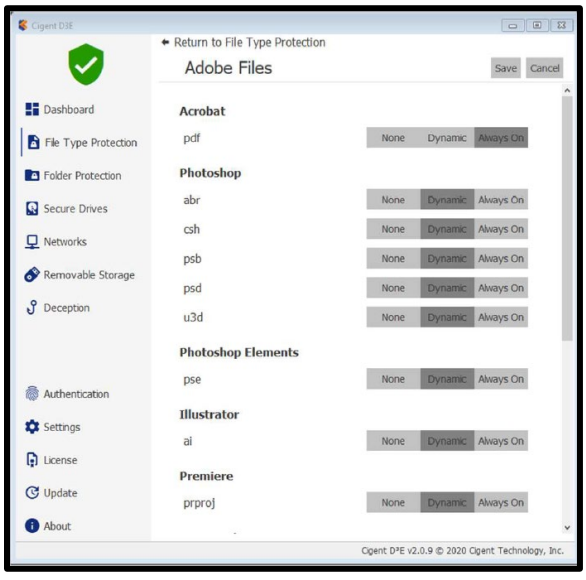


Figure A-116. Choose Protection Type for PDF Files

- Click on ← Return to File Type Protection at the top of the screen to display the screen below.

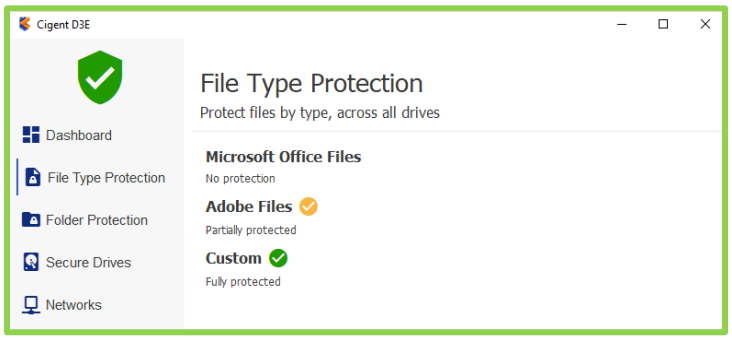


Figure A-117. Adobe Files Partially Protected

- Note that Adobe Files are marked "Partially protected." This reflects the fact that PDF files have been given D3E protection, but other Adobe file types have not been assigned protection.

- Click ***Custom*** to display the screen shown in Figure A-118 below.

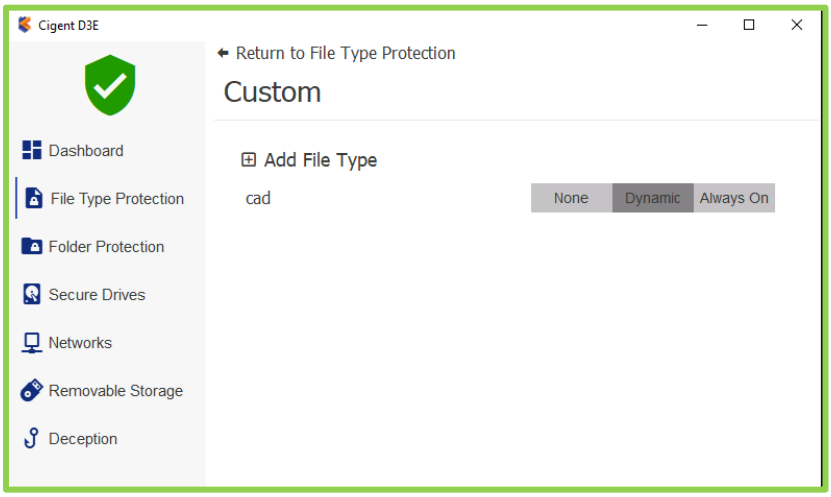


Figure A-118. Custom File Type Protection

- Note that, if text files are not listed in the Custom File Extension list, we'll have to add the .txt extension.
  - Click **Add File Type** to display the screen shown in Figure A-119
    - Type ***txt*** in the space provided.
    - Make sure *Dynamic* protection is assigned.
    - Click **Save**.
    - Use the prescribed authentication method.
    - Click on Return to File Type Protection at the top of the screen.

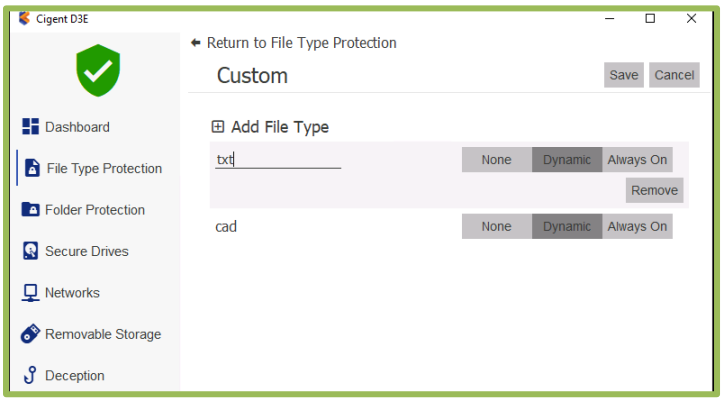


Figure A-119. Add Dynamic Protection for txt Files

- Test *File Extension Protection* for PDF extensions.

  Files with pdf extensions have just been given *Always On* protection, so authentication should be required to access the information in the file, regardless of the *ActiveLock* status.

  - Browse to C:\Cigent\HighlyConfidential. (Actually, any path to a pdf file will work.)
  - Click on *fw4.pdf* (or any other pdf file on the laptop) to open the file.
  - Note that authentication is required to open this file. See Figure A-120.

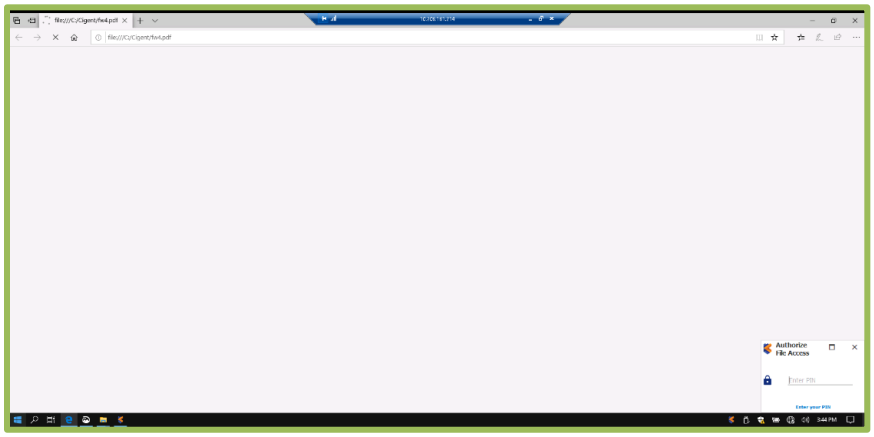
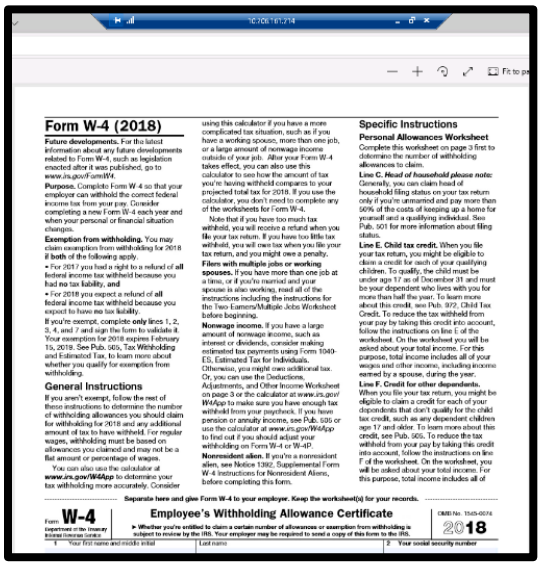


Figure A-120. Authentication Required to Open File with *Always On* Protection

  - The contents of the file can be accessed after the appropriate authentication has been used. See Figure A-121.



Form W-4 (2018)

Future developments. For the latest information about any future developments related to Form W-4, such as legislation enacted after it was published, go to www.irs.gov/FormW4.

Purpose. Complete Form W-4 so that your employer can withhold the correct federal income tax from your pay. Consider completing a new Form W-4 each year and when your personal or financial situation changes.

Exemption from withholding. You may claim exemption from withholding for 2018 if **both** of the following apply.

- For 2017 you had a right to a refund of **all** federal income tax withheld because you had **no** tax liability, **and**
- For 2018 you expect a refund of **all** federal income tax withheld because you expect to have **no** tax liability.

If you're exempt, complete **only** lines 1, 2, 3, 4, and 7 and sign the form to validate it. Your exemption for 2018 expires February 15, 2019. See Pub. 505, Tax Withholding and Estimated Tax, to learn more about whether you qualify for exemption from withholding.

General Instructions

If you aren't exempt, follow the rest of these instructions to determine the number of withholding allowances you should claim for withholding for 2018 and any additional amount of tax to have withheld. For regular wages, withholding must be based on allowances you claimed and may not be a flat amount or percentage of wages.

You can also use the calculator at **www.irs.gov/W4App** to determine your tax withholding more accurately. Consider using this calculator if you have a more complicated tax situation, such as if you have a working spouse, more than one job, or a large amount of nonwage income outside of your job. After your Form W-4 takes effect, you can also use this calculator to see how the amount of tax you're having withheld compares to your projected total tax for 2018. If you use the calculator, you don't need to complete any of the worksheets for Form W-4.

Note that if you have too much tax withheld, you will receive a refund when you file your tax return. If you have too little tax withheld, you will owe tax when you file your tax return, and you might owe a penalty.

Filers with multiple jobs or working spouses. If you have more than one job at a time, or if you're married and your spouse is also working, read all of the instructions including the instructions for the Two-Earners/Multiple Jobs Worksheet before beginning.

Nonwage income. If you have a large amount of nonwage income, such as interest or dividends, consider making estimated tax payments using Form 1040-ES, Estimated Tax for Individuals. Otherwise, you might owe additional tax. Or, you can use the Deductions, Adjustments, and Other Income Worksheet on page 3 or the calculator at www.irs.gov/W4App to make sure you have enough tax withheld from your paycheck. If you have pension or annuity income, see Pub. 505 or use the calculator at www.irs.gov/W4App to find out if you should adjust your withholding on Form W-4 or W-4P.

Nonresident alien. If you're a nonresident alien, see Notice 1392, Supplemental Form W-4 Instructions for Nonresident Aliens, before completing this form.

Specific Instructions

Personal Allowances Worksheet

Complete this worksheet on page 3 first to determine the number of withholding allowances to claim.

Line C. *Head of household please note:* Generally, you can claim head of household filing status on your tax return only if you're unmarried and pay more than 50% of the costs of keeping up a home for yourself and a qualifying individual. See Pub. 501 for more information about filing status.

Line E. Child tax credit. When you file your tax return, you might be eligible to claim a credit for each of your qualifying children. To qualify, the child must be under age 17 as of December 31 and must be your dependent who lives with you for more than half the year. To learn more about this credit, see Pub. 972, Child Tax Credit. To reduce the tax withheld from your pay by taking this credit into account, follow the instructions on line E of the worksheet. On the worksheet you will be asked about your total income. For this purpose, total income includes all of your wages and other income, including income earned by a spouse, during the year.

Line F. Credit for other dependents. When you file your tax return, you might be eligible to claim a credit for each of your dependents that don't qualify for the child tax credit, such as any dependent children age 17 and older. To learn more about this credit, see Pub. 505. To reduce the tax withheld from your pay by taking this credit into account, follow the instructions on line F of the worksheet. On the worksheet, you will be asked about your total income. For this purpose, total income includes all of

Separate here and give Form W-4 to your employer. Keep the worksheet(s) for your records.

Form **W-4** Employee's Withholding Allowance Certificate OMB No. 1545-0074 2018

▶ Whether you're entitled to claim a certain number of allowances or exemption from withholding is subject to review by the IRS. Your employer may be required to send a copy of this form to the IRS.

1 Your first name and middle initial | Last name | 2 Your social security number

Figure A-121. File Displayed After Authentication

- Test File Extension Protection for txt extensions.

  Files with txt extensions have just been assigned *Dynamic* protection. Authentication should be required to access such files only when *ActiveLock* is engaged.

  - Browse to C:\Cigent*Confidential.txt*. Figure A-122 demonstrates that, when *ActiveLock* is not engaged, it is not necessary to use authentication to access the file.
  - Demonstrate that authentication is required to access .txt files when *ActiveLock* is engaged.
    - Trigger ActiveLock by attempting to access *passwords.xls*. Ignore D3E warnings for now.
    - Try to open C:\Cigent*Confidential.txt*. Note that the file will not open until authentication has been employed. See Figure A-123 and Figure A-124.
    - At the D3E Dashboard, enter authentication to clear the *Data Deception Event* threat.
      - After clearing the threat, note that the *Confidential.txt* file opens without authentication.

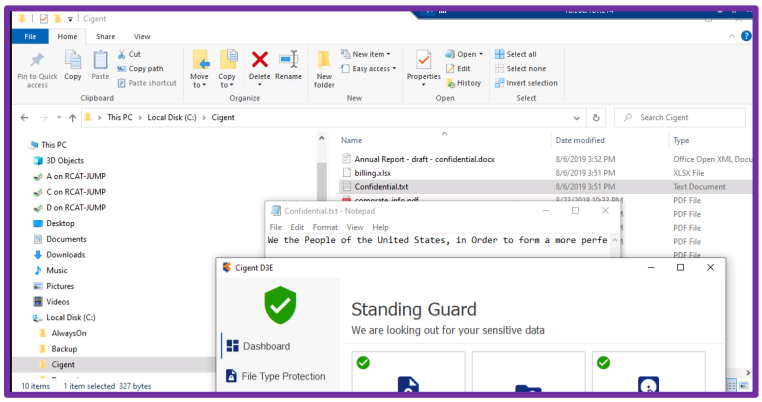


Figure A-122. Authentication Not Needed if *ActiveLock* Not Engaged

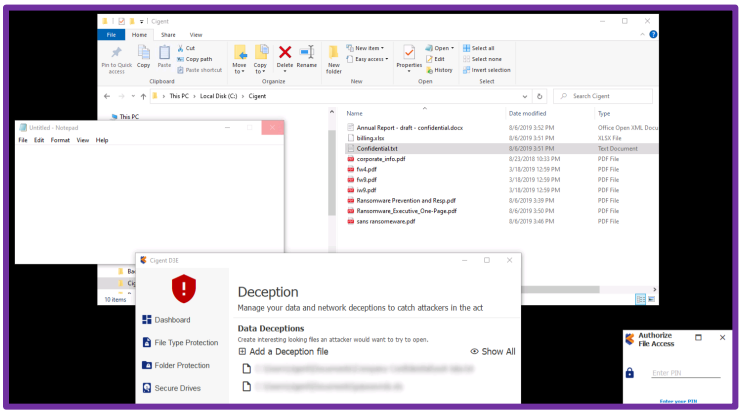


Figure A-123. Under *ActiveLock* Text File Won't Open without Authentication

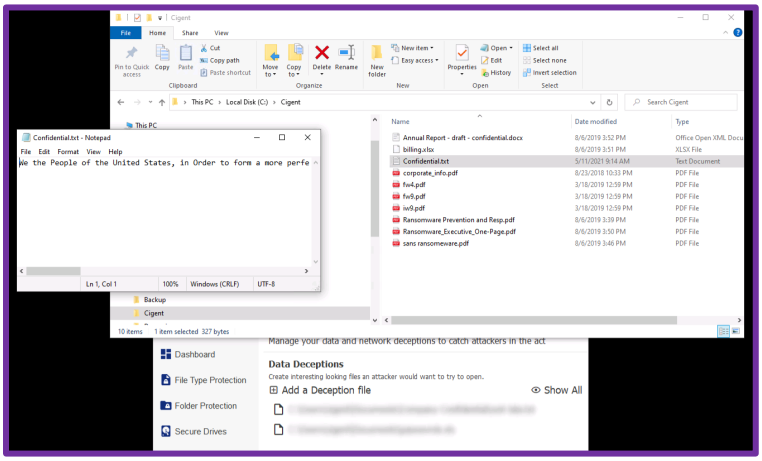


Figure A-124. Text File is Accessible after Authentication

- At the conclusion of this evaluation, clear *ActiveLock*, remove *File Extension Protection* for TXT files and mark PDF files for *Dynamic* protection.

A.3.6.2 Conflicts between Folder Protection and File Extension Protection

- Before we ran the *File Extension Protection* evaluation described above, we removed *Folder Protection*, so that the latter's effects would not mask the D3E's *File Extension Protection* performance. After our baseline checkout of the feature, we wanted to go back and see whether the simultaneous use of *File Extension* and *Folder* protections could lead to conflicts. (The following test was conducted only on the Win10 64-bit laptop.)
    - We marked a folder for *Dynamic* protection and made sure that the folder contained a PDF file.
    - We then assigned *Always On* protection to files with the PDF extension.
    - Finally, we tried to access the *fw4.pdf* file:
        - (1) when *ActiveLock* was engaged and
        - (2) when *ActiveLock* was not engaged.
- Evaluation steps are depicted below in Figure A-125 through Figure A-127.

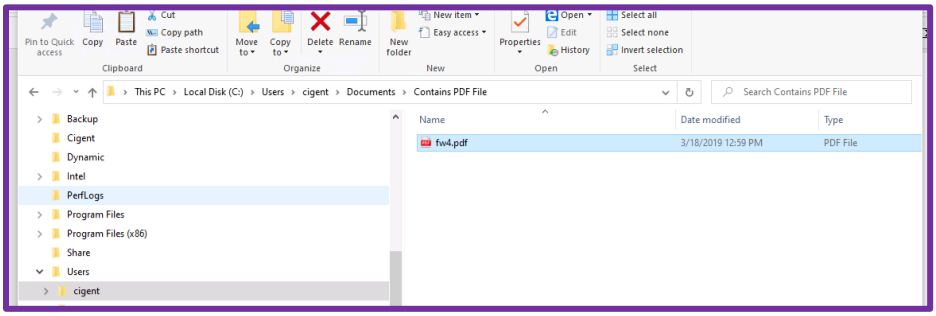


Figure A-125. Folder with PDF File

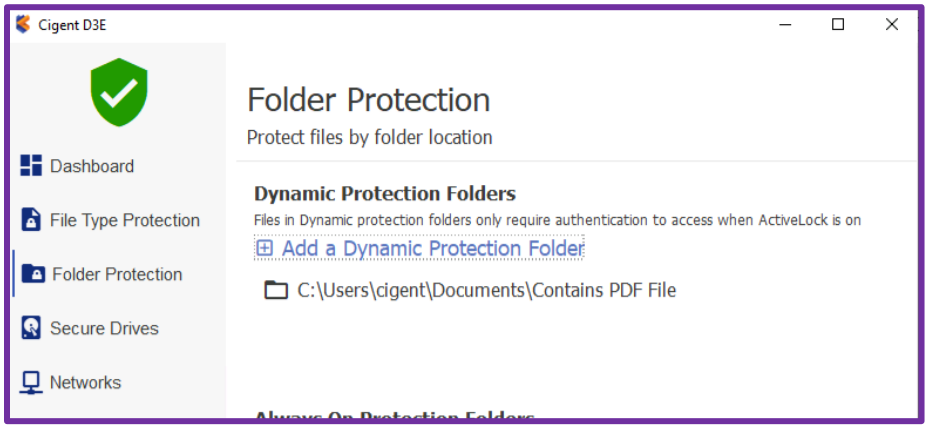


Figure A-126. Mark Folder for *Dynamic* Protection

- Before turning on *File Extension Protection*, we verified (again) that *Dynamic Folder Protection* behaved appropriately under *ActiveLock* and non-*ActiveLock* conditions.

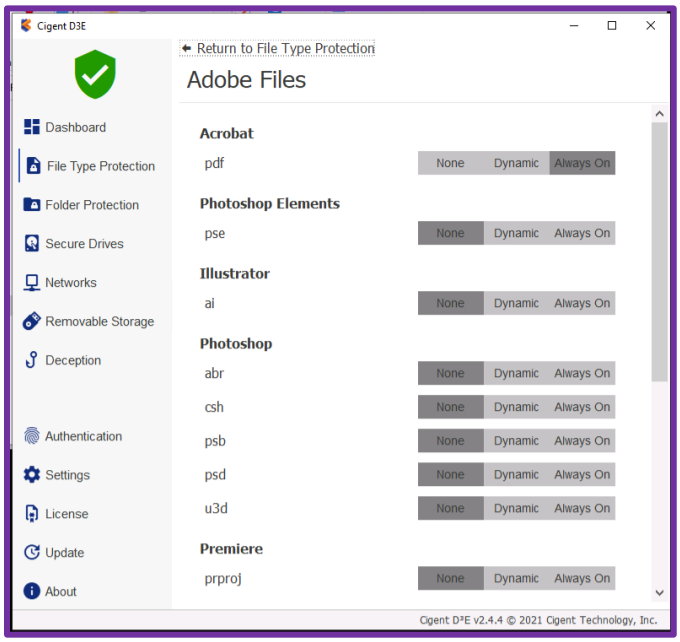


Figure A-127. *Always On* Protection Assigned to PDF Files

- With *ActiveLock* not engaged, we tried to access the PDF file in the folder marked for *Dynamic* protection. When we tried to access the *fw4.pdf* file, we saw that the *Always On* protection assigned to the PDF file extension had precedence over the protection level assigned to the folder. This behavior does not constitute a problem, but it could be confusing to users encountering *Always On* treatment for a file in a folder marked explicitly for *Dynamic* protection. Recall Cigent's caution that "because this protection-assignment method is global, it could have unintended consequences unless care is taken" [8].
- To bolster our conclusion, we reran the test, assigning *Always On* Protection to the folder, and *Dynamic* protection to PDF files. As expected, behavior followed *Always On* rules when we tried to access the PDF file. This behavior echoes what we saw through our earlier *Always On/Dynamic* tests.

Key Takeaway: If a dual assignment of *Folder Protection* and *File Extension Protection* causes a file to be assigned both *Always On* and *Dynamic* protection, *Always On* treatment will prevail.

- **Recommendations**:
  1. For common file extensions, such as *docx*, *pdf*, *xlsx*, and *txt*, it is preferable to segregate files needing *Always On* or *Dynamic* protection into folders marked explicitly for the desired treatment and to use D3E's *Folder Protection* feature. Use *File Extension Protection* only for less common file-extension types, and only if needed. The extra administrative steps required to collect sensitive information into separate files may be cumbersome, but it will avoid the potential confusion that could result from the *Folder/File Extension* conflict described above.

2. When moving sensitive information into folders for *Dynamic* or *Always On* protection, make sure that residual copies or variants of the information do not exist in unprotected folders.
3. MITRE believes that the addition of a new *File Name Protection* feature, supplementing *Folder* and *File Extension Protection*, would enhance the D3E product. D3E administrators should be able to build an alphabetized list of files that receive either *Always On* or *Dynamic* protection. Such an implementation would avoid the *Folder/File Extension* conflict and confusion described above.

   E.g.,
   - Sensitive personnel data.docx — *Dynamic Protection*
   - Attack plans 2021.pdf — *Always On Protection*

   - Use of wild-card characters would help to ensure that outdated or other variants of sensitive files receive appropriate protection.

     E.g.,
     - Sensitive personnel*.* — *Dynamic Protection*
     - Attack plans 20**.* — *Always On Protection*

A.3.6.3 Win10 Evaluation

- File Extension protection worked well on the Win10 64-bit laptop equipped with Cigent Secure SSD Drives. The feature performed as advertised.

A.3.6.4 Win7 32-Bit Evaluation

- File Extension protection worked well and as advertised on the MITRE Win7 32-bit laptop.

A.3.6.5 Win7 64-Bit Evaluation

- File Extension protection worked well and as advertised on the MITRE Win7 64-bit laptop.

A.4 *Removable Storage Protection*

- To evaluate D3E's *Removable Storage Protection* feature, we connected a **WD Elements** hard drive via USB cable to the three evaluation laptops sequentially, tested the drive under *Trusted* and *Untrusted* conditions, and documented how D3E protected file access.

A.4.1 *Removable Storage Protection* – Evaluation Steps

- The removable drive had previously been connected to the evaluation laptops and trusted. Therefore, to test storage protection, it was necessary first to untrust the device before proceeding with the test. Refer to Figure A-128 and Figure A-129.

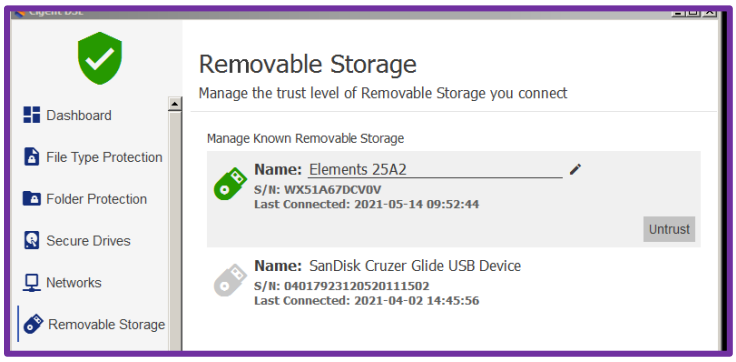


Figure A-128. Untrust Removable Storage – Non-SSD Laptop

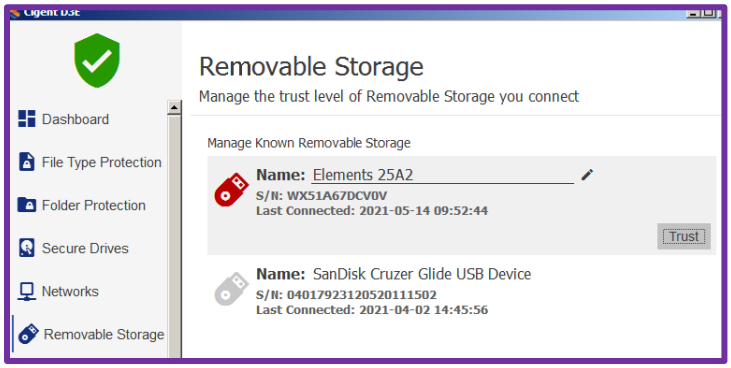


Figure A-129. Post Untrust of Removable Storage – Non-SSD Laptop

- After untrusting the USB drive, our attempt to access a file on the drive failed. See Figure A-130. Similarly, an attempt to copy a file to the drive failed while the drive was untrusted.

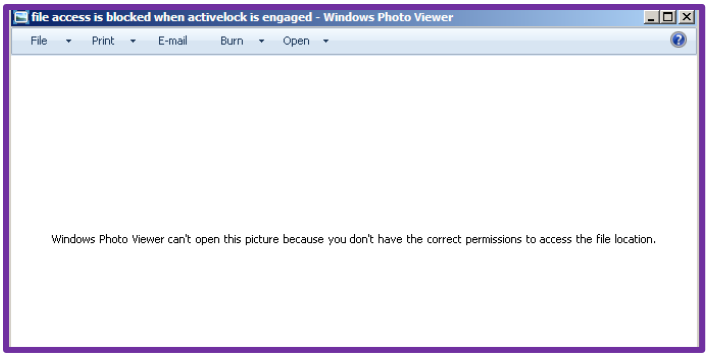


Figure A-130. Cannot Access File on Untrusted Removable Drive

- As expected, untrusting the removable device did not trigger *ActiveLock* at the laptop, and it was possible to access files not on the USB. In summary, it was possible to access files on the storage device only when the device was trusted in D3E. This behavior is entirely appropriate.

- We noticed slightly different behavior when evaluating *Removable Storage Protection* on the SSD-equipped Cigent Win10 laptop. Compare Figure A-131 below with Figure A-129 above. Note that the SSD-equipped laptop provides the option to "forget" a removable storage device after it has been untrusted. The status of the "Forgotten" USB drive is shown in Figure A-132. The next time the storage device is connected to the laptop, the user must make an explicit choice to trust the device.

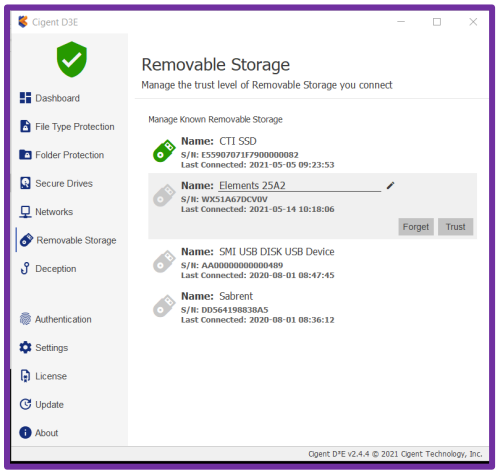


Figure A-131. "Forget" Removable Device on Cigent SSD Laptop

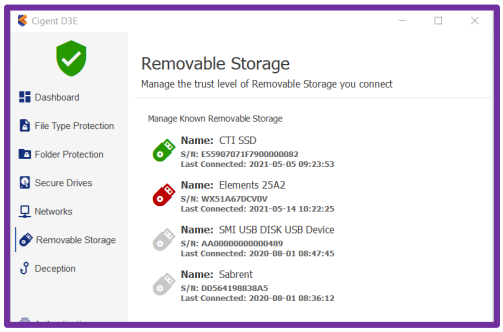


Figure A-132. Forgotten Storage Device – SSD-Equipped Laptop

A.4.1.1 Win10 Evaluation

- *Removable Storage Protection* performed as expected on the Cigent SSD-equipped Win10 64-bit laptop, preventing access to files on an untrusted removable-storage device without affecting access to files on the laptop itself.

A.4.1.2 Win7 32-Bit Evaluation

- *Removable Storage Protection* performed appropriately on the MITRE Win7 32-bit laptop.

A.4.1.3 Win 7 64-Bit Evaluation

- *Removable Storage Protection* performed appropriately on the MITRE Win7 64-bit laptop.

Appendix B Anomalies

As we noted elsewhere in this report, our impression of the data-protection features of Cigent's Dynamic Data Defense Engine (D3E) software is favorable. Cigent's dual firmware- and software-protection approaches combine to form a strong defense against tampering and theft of sensitive data.

The D3E suite of tools is simple to use, and D3E would be particularly effective and easy to manage in a networked deployment with a centralized management console.

As is to be expected in software still under development, however, we did encounter a few instances of anomalous D3E behavior. None of these instances constitutes a "show stopper," and some may be attributable to the underlying computing environment, rather than to D3E. The perceived idiosyncrasies are catalogued here to enable the vendor to consider, explain, or fix them.

B.1 Password Reuse is Allowed

As part of the procedure for de-configuring (Section A.1.1.2) and re-configuring (Section A.1.1.3) a Cigent Secure Solid-State Drive (SSD), we were required to enter a provisioning password. D3E let us reuse the old provisioning password when we re-configured the SSD. This was convenient for the purpose of our evaluation, but DoD and other government agencies recommend more stringent practices regarding passwords and identity management.

Recommendation: We recommend that D3E consult NIST Special Publication 800-63-3 [10] and other entities, government and civilian, for guidance on constructing robust digital identities.[44] The following is a non-comprehensive list of recommended practices.

- Enforce a strict (high) *Password history* parameter value to discourage password reuse.
- Make users change passwords at frequent intervals, e.g., 90 days or less.
- Prevent passwords from being changed immediately; i.e., enforce a minimum wait time to change passwords (enforce *minimum password age*).
- At a minimum, prompt users/administrators to follows DoD guidance when creating passwords.
- Ideally, creation of login credentials should be under the oversight of a Central Administrator Console, and local users/administrators should not be able to weaken the assigned password policy.

Similar guidance should apply to creation of D3E authentication PINs, as well.

[44] Cigent response: "Cigent will add the ability for password policy enforcement for both the Secure SSD password and authentication PIN in the upcoming release. It is also worth noting that that file authentication via CAC/PIV will be supported in a near term release."

B.2 Honeypot Files Can Be Moved, Changed, and Deleted

D3E provides a system-generated *passwords.xls* honeypot (*Deception*) file to ensnare malefactors. If any user or attacker attempts to open the file in its assigned *Deception* location, D3E triggers an *ActiveLock* condition and locks all sensitive file types and folders. Under *ActiveLock*, Secure SSD drives also are locked and unmounted; i.e., they become "invisible." D3E allows the administrator to create additional *Deception* folders; when the contents of a *Deception* folder are opened, D3E triggers *ActiveLock* to protect sensitive data elsewhere on the machine. Refer to Section A.1.3 for details.

D3E satisfies its advertised *Deception* functionality, in that it detects an attacker (or any user) clicking on a honeypot file and appropriately takes action to keep designated drives, folders, and file types safe. We discovered some aspects of the feature, however, that likely are outside the scope of Cigent's intended *Deception*-file behavior.

B.2.1 Manipulation of User-Generated Honeypot Files

Although attempts to open user-created *Deception* files triggered the appropriate D3E responses, it was possible to delete those files from within Windows Explorer. The files also could be moved to another location and subsequently opened, edited, and copied back to the original *Deception* folder. Refer to Section A.3.3 for details.

B.2.2 Manipulation of *passwords.xls* File

While it was not possible to delete the system-generated *passwords.xls* file, that file could be moved, opened, examined, edited, and copied back to the original *Deception* location.

B.2.3 Impact of Unintended *Deception* Feature Behavior

While the *Deception* file is merely a honeypot, and the ability to delete, copy/move, open, or edit it with impunity perhaps may not immediately harm the host, such behavior provides an attacker with a means of analyzing and eventually circumventing D3E defenses.

Also, failure to prevent hackers from manipulating honeypot files could have embarrassing consequences, if original file contents were replaced by threatening, mocking, or otherwise inappropriate text or images.

B.2.4 Issue Resolution

At present, D3E appropriately triggers *ActiveLock* whenever someone "double-clicks" on a honeypot file in an attempt to open it. It should be fairly straightforward to tweak D3E software so that it reacts to attempts to "right-click" on the file/folder to manipulate (i.e., copy, move, modify, or delete) the data. Cigent has identified a fix for this issue.[45]

[45] Cigent response: "Deception files should not be able to be opened, edited or overwritten. This behavior is a bug inadvertently introduced in the latest version of D3E and will be fixed in the next release."

B.3 Windows Service Host Process Tries to Access *passwords.xls*

During the Version 2.4.4. D3E evaluation at the Win7 64-bit laptop, something in the host process for Windows Service kept trying to access the *passwords.xls* file, triggering *ActiveLock*. This happened periodically while D3E was running. See Figure B-1.[46]

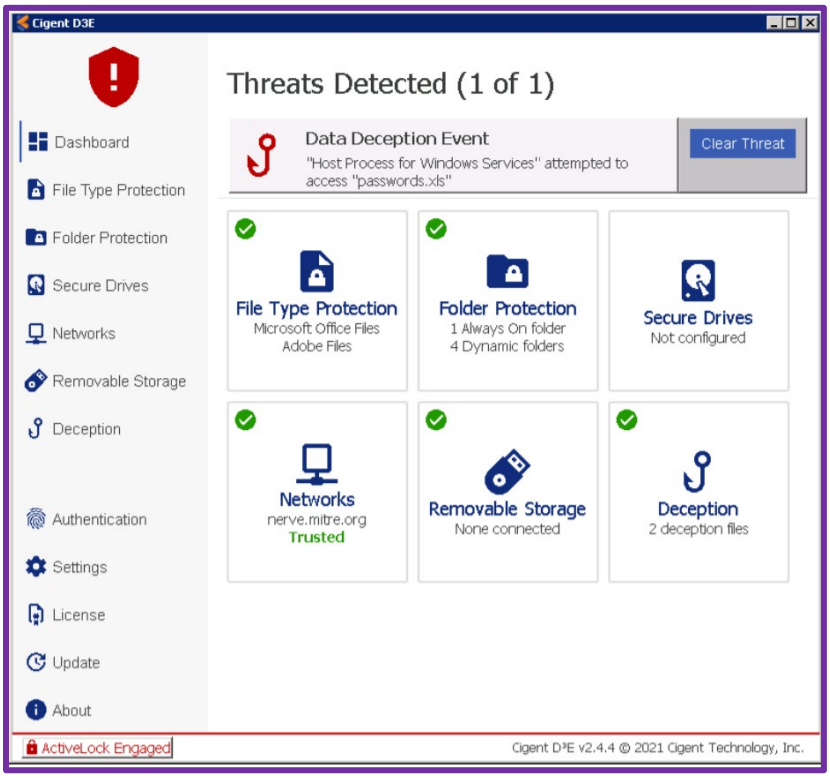


Figure B-1. Host Process Triggers D3E *Deception* Event

Recovery from the problem is straightforward: simply use the prescribed authentication method to clear the threat. The condition's persistence, however, even after reboot, makes it a good candidate for further investigation. Our observation indicated that D3E consistently and repeatedly generated the *Data Deception Event* message shown in Figure B-1 seven minutes after the administrator cleared the threat.

MITRE is working with Cigent to determine which process is attempting to access the *Deception* file. If the application is deemed legitimate, it could be designated a "Safe App." This would put a stop to the unwanted *Data Deception Event* alarms. Note that the Safe App feature requires a special license from Cigent, available to premium customers upon request.

[46] Cigent response: "Most Windows processes and all registered AV programs are allowed to access the deception file. When connected to the Cigent Management console, additional details regarding the offending application (including PATH) are collected and reported. Should the application be determined to be authorized (backup, EDR, etc.) administrators can add the application as a Safe App to a D3E policy."

B.4 APPCRASH Condition at Win7 64-Bit Laptop

On a few occasions during testing at the Win7 64-bit laptop, the D3E Dashboard stopped working due to an "APPCRASH" condition. Like the *Deception* issue cited in Section B.3, this problem deserves further investigation.[47]

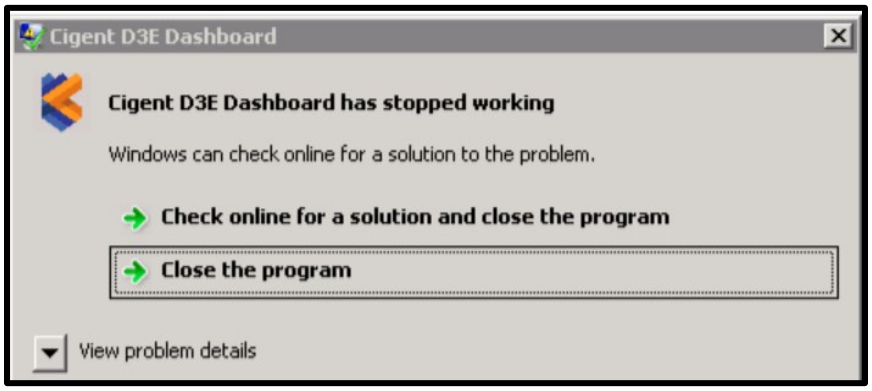


Figure B-2. D3E Dashboard APPCRASH

[47] Cigent response: "Cigent would be very interested in further investigating the cause of this crash condition as we have been unable to reproduce in-house."

Appendix C D3E Central Management Console

MITRE did not evaluate D3E central-management capabilities. We did, however, receive a Cigent briefing [12] on the subject on 26 May 2021 to familiarize ourselves with the capability and to buttress our belief that centralized D3E management would be a safer, more efficient means of deploying D3E than per-device configuration and management.

The following paragraphs contain a very high-level summary of D3E Central Management capabilities.

C.1 Overview

D3E can be deployed with a central management console capable of monitoring and managing data security throughout a network and responding (activating *ActiveLock*) either manually or automatically.[48] Cigent's centralized D3E-management feature can run either in the cloud or locally on-prem.

With centralized management, D3E software running on each end-user machine can be controlled remotely. Management policies can be created and applied for user groups and/or for individual devices. The Central Management Console administrator can make D3E software-protection changes at any of the managed machines, but a user/administrator at the local computer also can change settings, as long as those changes do not lower the assigned security profile. Both the central and local administrators may respond to *ActiveLock* security alerts.

Figure C-1 shows the Central Management Console Dashboard.

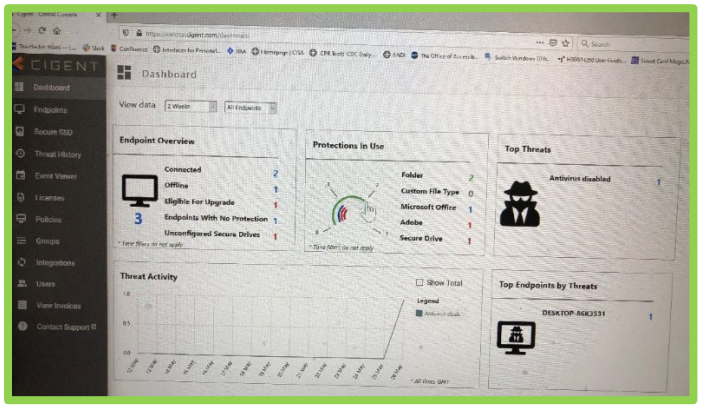


Figure C-1. Central Management Console Dashboard

- The central manager creates default or specialized security policy for computers or for groups of computers.
    - Users/administrators at the end devices may increase the security level of their devices, but they may not lower security below the assigned default level.

[48] Presently D3E Central Management & Configuration applies only to D3E software; however, the ability to extend this centralized management capability to secure Solid State Drives is on the Cigent roadmap.

- D3E at each end device responds autonomously to security events, protecting data (engaging *ActiveLock*) in accordance with the security profile for the device or the group of which the device is a member.
- End devices reach out automatically at configurable intervals to provide security-status updates to the central manager and to download changes.
    - An overview of the security status of specific devices can be displayed at the Central Management Console, as shown in Figure C-2.

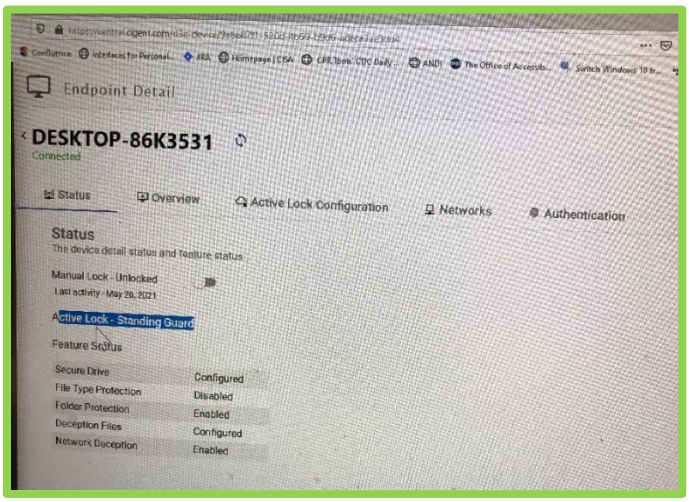


Figure C-2. Device Security Status

    - The Central Console administrator also can view the threat history for each of the managed devices. See Figure C-3.

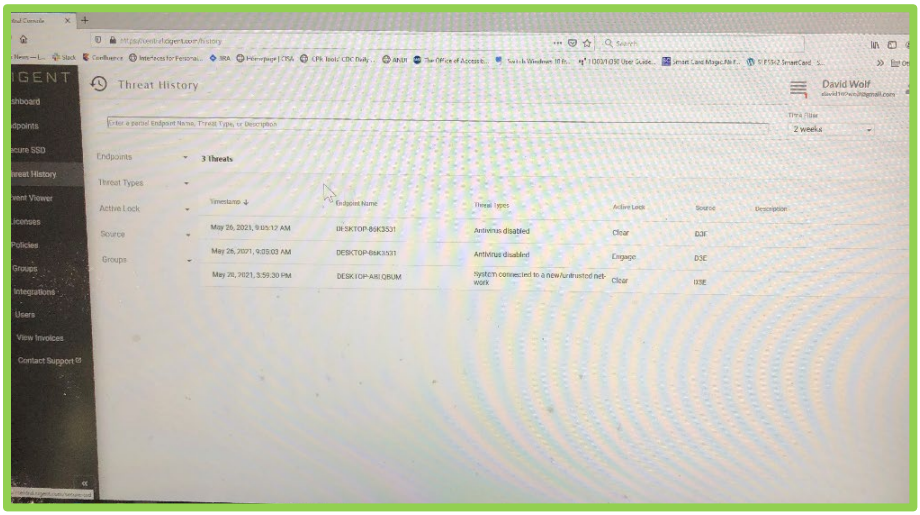


Figure C-3. Threat History for Managed Devices

- Presently D3E Central Management applies only to D3E software. Cigent plans to extend the feature to firmware protection and Secure Solid-State Drives (SSDs).

C.2 Notifications

The Central Management Console administrator chooses how notifications will be sent from managed devices. Note that both email and in-app notifications may be made, and the option is configurable for each of many possible security events. Refer to Figure C-4 below.

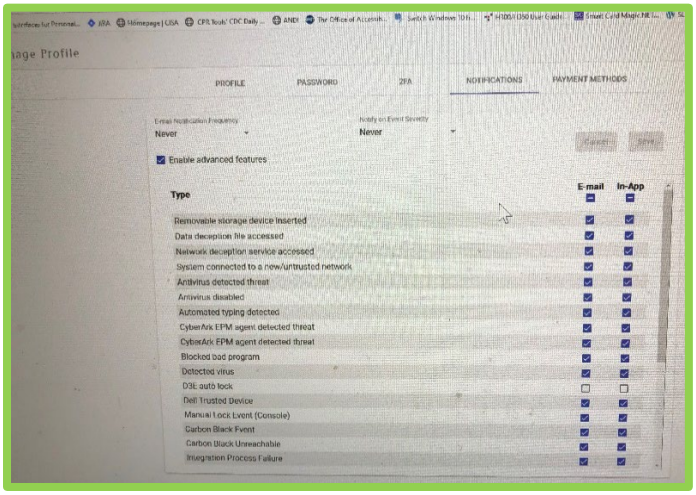


Figure C-4. Security-Event Notifications

C.3 Security Policies

The Central Console administrator sets D3E policies for various computer work groups. As the note in Figure C-5 states, if a device falls outside a group ("device-set") policy, the default policy will be assigned to the device.

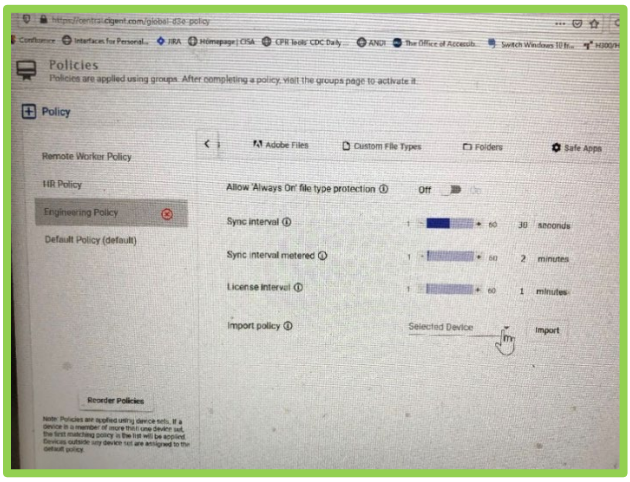


Figure C-5. Central Manager Policy Screen

C.3.1 Set the Synchronization Interval

The Central Management Console administrator sets the sync interval – the frequency at which managed devices reach out to provide security-status updates to the central terminal – at the

Policy screen. Refer to Figure C-5 above. Note that a unique sync interval may be established for each policy. The interval should be fairly tight, to ensure that important status information is sent to the central administrator on a near-real-time basis.

C.3.2 Safe Applications

Occasionally applications at a device will need access to sensitive files for legitimate and safe reasons, and it will be impracticable to cope with large numbers of *ActiveLock* alerts generated for accesses that are harmless. For example, backup software requires access to all files on a device, including sensitive files. Cigent allows selected programs to access protected files without end-user authorization. Such programs can be designated as "Safe Apps" at the policy screen shown in Figure C-6 below.

For security, PKI[49] certificates should be used for Safe Apps, and the path or filename for the application should be identified.

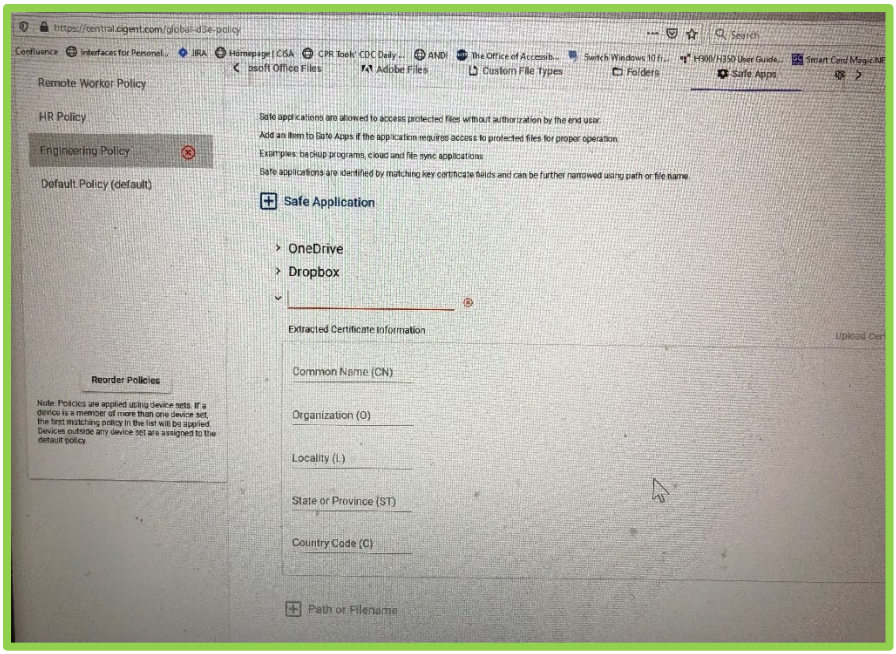


Figure C-6. Policy – Safe Applications

C.4 Third-Party Security Integration

D3E can work with 3rd-party Antivirus (AV) and Identity and Access Management (IDAM) products to provide enhanced endpoint protection and authentication. Figure C-7 shows the vendors with which Cigent has partnered thus far.

At this time, the Cisco and CyberArk products can provide security notifications to the D3E administrator, but they are not yet fully integrated with D3E. Sophos and Carbon Black are

[49] PKI = Public Key Infrastructure

sufficiently tightly integrated with D3E that suspicious behavior detected in their software can trigger security alerts in D3E.

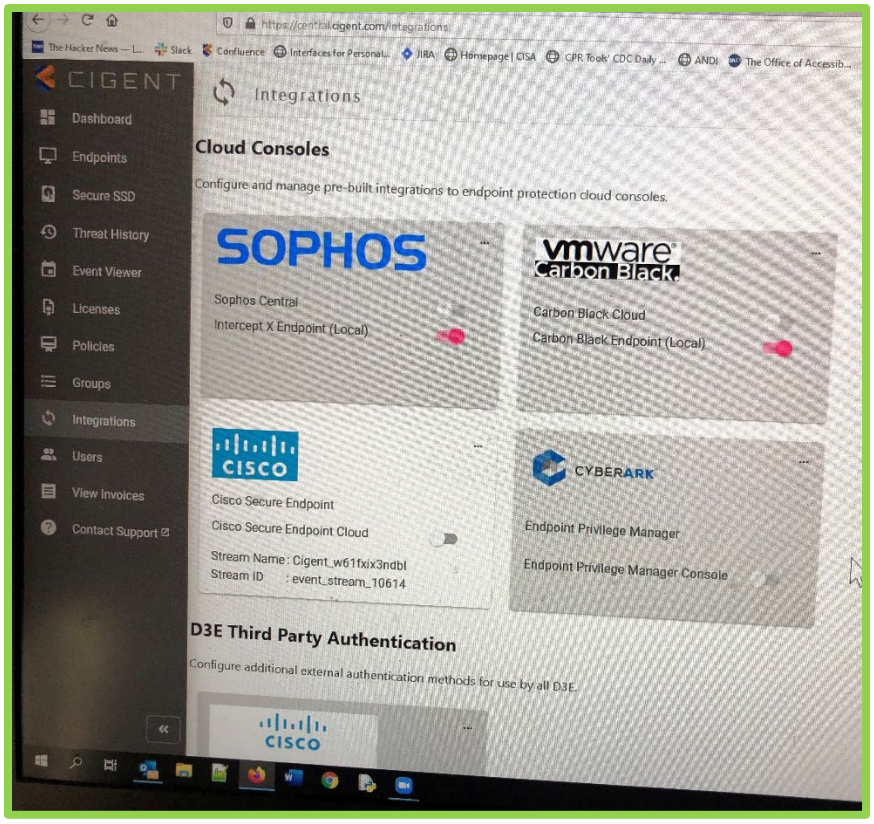


Figure C-7. Third-Party Integration for User Authentication

Appendix D Abbreviations and Acronyms

AF	Air Force
AI	Artificial Intelligence
API	Application Programming Interface
AV	Antivirus
CAC	Common Access Card
CROWS	Cyber Resiliency Office for Weapons Systems
CSV	Comma Separated Values
CTI	Cigent Technology, Inc.
CUI	Controlled Unclassified Information
D3E	Dynamic Data Defense Engine
DCO	Defensive Cyber Operations
DoD	Department of Defense
EDR	Endpoint Detection and Response
FIPS	Federal Information Processing Standard(s)
FOUO	For Official Use Only
FTP	File Transfer Protocol
GB	Gigabyte
HDD	Hard Disk Drive
IDAM	Identity and Access Management
I/O	Input/Output
IP	Internet Protocol
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
ML	Machine Learning
NERVE	Networked Experimentation, Research, & Virtualization Environment
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
NVMe	Non-Volatile Memory Express

OPAL	Storage specification for self-encrypting drives (not an acronym)
OS	Operating System
PC	Personal Computer
PCIe	Peripheral Component Interconnect Express
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PW	Password
RCAT	Reconfigurable Cockpit Avionics Testbed
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
SATA	Serial Advanced Technology Attachment
SED	Self-Encrypting Drive
SIEM	Security Information and Event Management system
SMB	Server Message Block
S/N	Serial Number
SOC	Security Operations Center
SP	Special Publication
SSD	Solid-State Drive
TB	Terabyte
TCP	Transmission Control Protocol
TCG	Trusted Computing Group
Telnet	Terminal Network
UBA	User Behavior Analytics
USAF	United States Air Force
USB	Universal Serial Bus
Win7	Windows 7 Operation System

Distribution

Government

NAWROCKI, JOHN P NH-04 USAF AFMC AFLCMC/CROWS john.nawrocki@us.af.mil;
HOPKINS, LYLE L GS-13 USAF AFMC AFLCMC/CROWS lyle.hopkins.2@us.af.mil;
MARTIN, LLOYD H NH-04 USAF AFMC AFLCMC/CROWS lloyd.martin@us.af.mil;
BEARD, ROGER A NH-04 USAF AFMC AFLCMC/CROWS roger.beard.1@us.af.mil;
LEHMANN, ZACHARY M Lt Col USAF AFMC AFLCMC/CROWS
zachary.lehmann@us.af.mil

MITRE

Christian Fiore
Jeffrey Higginson
John Mulrey
Donna Rondeau (Project File)
Sven Skoog
Justin Yeager