



Copyright © 2024 Fidelity Height LLC. All rights reserved.

User Guide

Revision History:

Version 1.3.0 (February 2022): Initial Release

Version 1.3.1 (March 2024): Added new features, and improved user interface

Version 1.3.2 (April 2024): Added new product_Opal Lock Lite

Version 1.3.3 (May 2024): Added new fixes and reformatting of User Guide

Contents

1. INTRODUCTION AND OVERVIEW	5
2. SYSTEM REQUIREMENTS	6
3. GLOSSARY	7
4. INSTALLATION.	8
4.1 Download and Run Application:	8
4.2 Allow Permissions:	8
4.3 Setup Wizard:	8
4.4 License Agreement:.	9
4.5 Ready to Install:.	10
4.6 Installation Complete:.	11
5. OPAL LOCK LITE ACTIVATION	14
6. REGULAR LICENSE ACTIVATION.	15
6.1 Activate Online:	16
6.2 Activate Offline:	18
7. LICENSE DEACTIVATION	20
8. OPAL LOCK REGULAR VERSION USE CASE: ENABLING DRIVE LOCKING	24
9. REGULAR VERSION TYPES AND USE CASES.	25
9.1 USB License	25
9.2 Standard License	25
9.3 Premium License	26
10. PREMIUM VERSION GUIDE	27
10.1 Opal Lock Premium Version Home screen Display and Drive Detection.	27
10.2 DETAILS	29
10.2.1 Drive Information	29
10.2.2 TCG Information.	30
10.3 DRIVE	30
10.3.1 Query Drive	31

10.3.2 Audit Log	33
10.4 Setup.	35
10.4.1 Set up Drive	36
10.4.2 Password Authentication Guide.	42
10.4.3 UPDATE PRE-BOOT IMAGE	44
10.4.4 SETUP RECOVERY USB	45
10.4.5 CHANGE DRIVE PASSWORD	47
10.4.6 MANAGE PASSWORD	48
10.4.7 USER SETUP AND REMOVAL	49
10.5 Locking and Unlocking Drives.	51
10.5.1 Locking Drives.	51
10.5.2 System Drive Locking by UI.	52
10.5.3 Unlocking Drives.	52
10.6 MULTI DRIVE OPERATIONS	54
10.6.1 Multi-Drive Setup	54
10.6.2 Multi-Drive Lock	56
10.6.3 Multi-Drive Unlock.	56
10.7 Revert Setup/Erase User Guide.	57
10.7.1 Revert Setup and Keep Data	59
10.7.2 Revert Setup and Erase Data with Password.	59
10.7.3 Revert Setup and Erase Data with PSID	59
10.7.4 Instant Erase.	60
10.7.5 Certificate of Sanitization	61
11. STANDARD VERSION GUIDE	62
12. USB VERSION GUIDE	63
13. OPAL LOCK LITE USE CASE: DATA ACCESS ON ANOTHER SYSTEM	64
14. OPAL LOCK LITE FUNCTIONALITY	65

14.1 Opal Lock Home Screen Display and Drive Detection	65
14.2 Drive Unlocking	66
14.3 Authentication	67
14.4 Access Granted	67
14.5 Data Utilization:	67
14.6 Limitations:.	68
14.7 Completion:	68
15. PREBOOT AUTHENTICATION (PBA) VERSION USE CASE.	69
16. PBA VERSION FUNCTIONALITIES	71
16.1 Opal Lock PBA Screen Display and Drive Detection	71
16.2 Drive	72
16.2.1 Query Drive	73
16.2.2 Audit Log	74
16.2.3 Rescan drives	76
16.2.4 View Opal Drives	77
16.3 Unlock	78
16.3.1 Preboot Manual Unlock	79
16.3.2 Preboot Auto-Unlock and Reboot	79
16.4 Revert Setup.	80
16.4.1 Remove Lock and Keep Data.	81
16.4.2 Remove Lock and Erase Data with Password	82
16.4.3 Remove Lock and Erase Data with PSID	83
17. KEYBOARD NAVIGATION	85
18. FREQUENTLY ASKED QUESTIONS	86
19. APPENDIX	90
20. ACKNOWLEDGEMENTS.	95

GETTING STARTED

1. INTRODUCTION AND OVERVIEW

Opal Lock is a drive security management application for self-encrypting drives (SEDs) with built-in full-disk encryption. Self-encrypting drives use specifications developed by the Trusting Computing Group (TCG), and we will refer to these drives as TCG drives. Using Opal Lock, users can utilize full-disk encryption to protect the data on their TCG drives.

When setting up a drive using Opal Lock, a password for the drive is set and locking is enabled. After setting the password, the mode of unlocking the System drive can be set up by setting up the preboot image, which is the environment used for pre-boot authentication.

Opal Lock offers two primary methods for locking the drive after it has been set up with Opal Lock: locking by power cycle and locking via the user interface (UI).

Locking by Power Cycle- Locking the drives post-Opal Lock setup can be achieved by power cycling the drive.

For Internal Drives, Users accomplish this by complete shutdown of the system, system reboot and setting the system in hibernate mode . Once the system is powered down, the drive automatically locks, encrypting its data. Upon the next system startup, the preboot environment prompts pre-boot authentication. Successful authentication grants access to the drive after the system is rebooted.

For USB Drives, Users accomplish this by physically disconnecting the USB drive from the system and then reconnecting it. This action triggers the drive to lock, ensuring the security of its data until it's unlocked through the appropriate authentication process.

Locking via User Interface (UI)- Opal Lock provides a streamlined method for users to lock their drives through the UI. By simply clicking on the designated lock icon within the Opal Lock application interface, users can swiftly initiate the locking process. This method prioritizes convenience, allowing users to secure their drives seamlessly while working within the application.

These locking methods cater to different user preferences and scenarios, providing flexibility and robust security measures for drives managed with Opal Lock. Whether users prioritize ease of use or stringent security protocols, Opal Lock offers suitable options to meet their needs.

2. SYSTEM REQUIREMENTS

Before beginning the installation process, ensure you have the following:

Operating System:

- ✓ Windows 10, Windows 11, or Windows Server 2019/2022

Drive Compatibility:

- ✓ SATA or NVMe drive (compatible with Windows 10, Windows 11, or Server 2019/2022)

Installation Files:

- ✓ Opal Lock Setup_x86 installation file
- ✓ License key

Internet Connection:

- ✓ Required for online license validation

System Requirements:

- ✓ CPU: Hyper-threading CPU; a Core 2 processor or above is recommended
- ✓ RAM: At least 1GB; 2GB is recommended for Windows 10 and above
- ✓ Video Card: At least 32MB; 64MB or above is recommended
- ✓ System Drive: Minimum 500MB free space
- ✓ BIOS: Secure Boot must be off/disabled

Ensure you have all these prerequisites in place before proceeding with the installation process.

3. GLOSSARY

Manufacturer secure ID (MSID): The default password for the drive. After setting up a drive with the Opal lock application, the default Security Identifier (SID) is usually replaced by the password set by the user, which serves as the authentication credential for accessing the drive. However, in the event of a revert setup action, the password will be reset to the Manufacturer Secure ID (MSID), which is the default password for the drive.

Physical secure ID (PSID): The PSID is a backup option if the password has been forgotten. It can only be used to revert setup and erase data and reset the drive to manufacturer settings.

Drive Manufacturer Settings: Manufacturer settings of Self Encrypting Drives (SEDs) refer to the default configurations and parameters established by the drive's manufacturer for encryption, key management, and security features.

Shadow MBR: A small "hidden" portion of a drive (not all drives) that becomes visible when locked. When a drive is locked, the only portion of the drive that can be booted into is the shadow MBR. The preboot image is written into the shadow MBR so that booting into the locked drive will lead to booting into the shadow MBR.

Preboot Image: A mini-operating system image that is written onto a drive's shadow MBR or recovery USB (Premium and Standard version only). The Preboot version of Opal Lock is embedded into the image and set to automatically run on startup when booting into the preboot environment. The user can then use Opal Lock to unlock the drive.

Block SID: This feature, if enabled in some TCG drives, prevents changing the authentication key. If Block SID is enabled, Opal Lock can't set up a password for the drive. It needs to be disabled in the BIOS before executing the Block SID command.

Opal Lock Lite: This tool is designed to facilitate the unlocking of USB drives that adhere to the Opal standard for hardware-based encryption. It provides users with a convenient way to unlock compatible external USB drives without the need for a Regular license.

System Drive: The system drive typically refers to the primary hard drive or storage device in a computer system where the operating system (OS) is installed. It contains all the necessary files, libraries, and configurations needed for the operating system to function properly. On Windows systems, the system drive is usually labeled as "C:."

4. INSTALLATION

After purchasing the license, the license key and Opal Lock application executable (exe) will be sent to your email and available on the E-Commerce account section.

4.1 Download and Run Application:

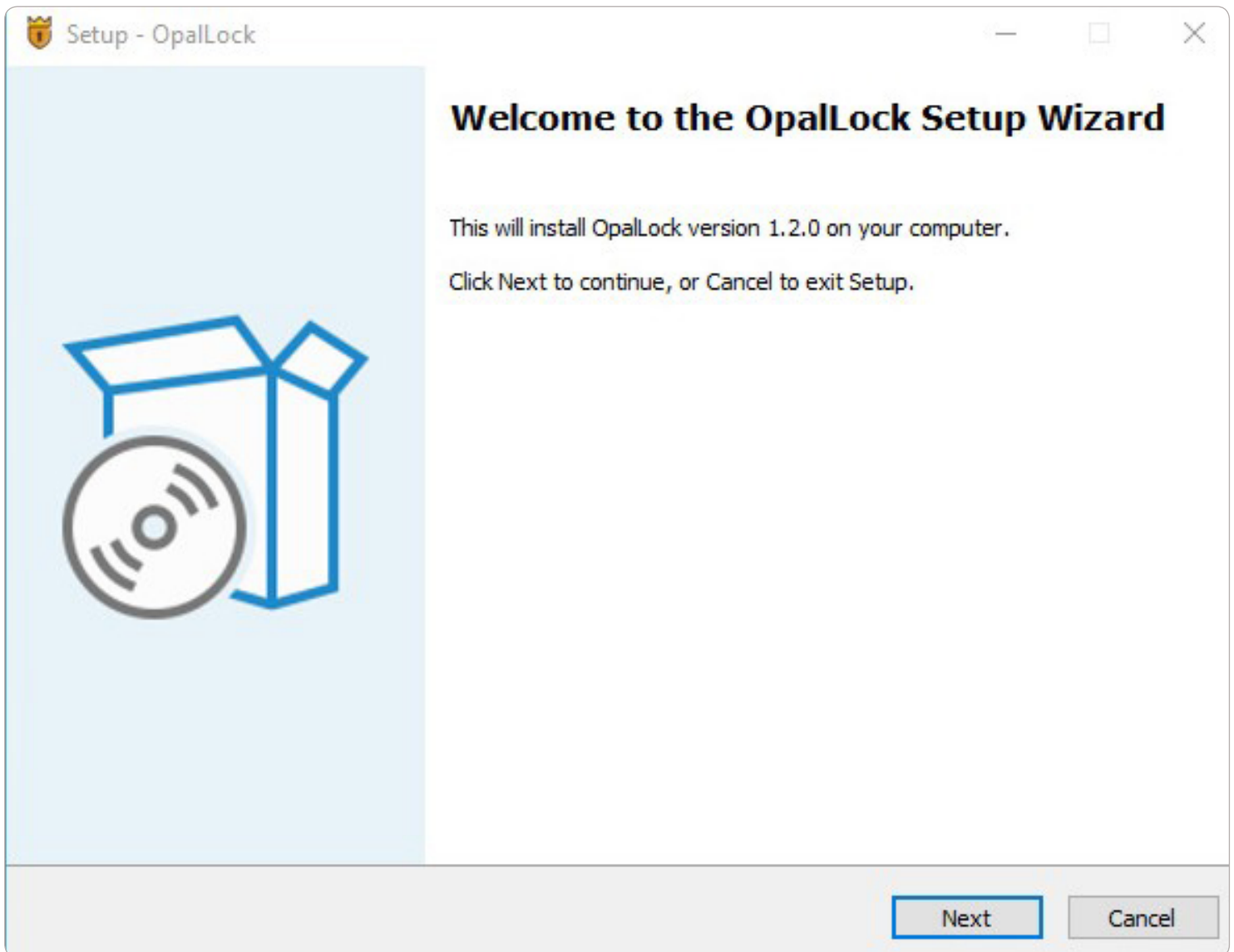
- Download the application file (exe) from the provided link or account section.
- Double click on the downloaded exe icon to initiate the installation process.

4.2 Allow Permissions:

- Upon running the application, you may be prompted to allow permissions for the application to make changes in the system for smoother operations.
- Click on the “Allow” button to grant these permissions.

4.3 Setup Wizard:

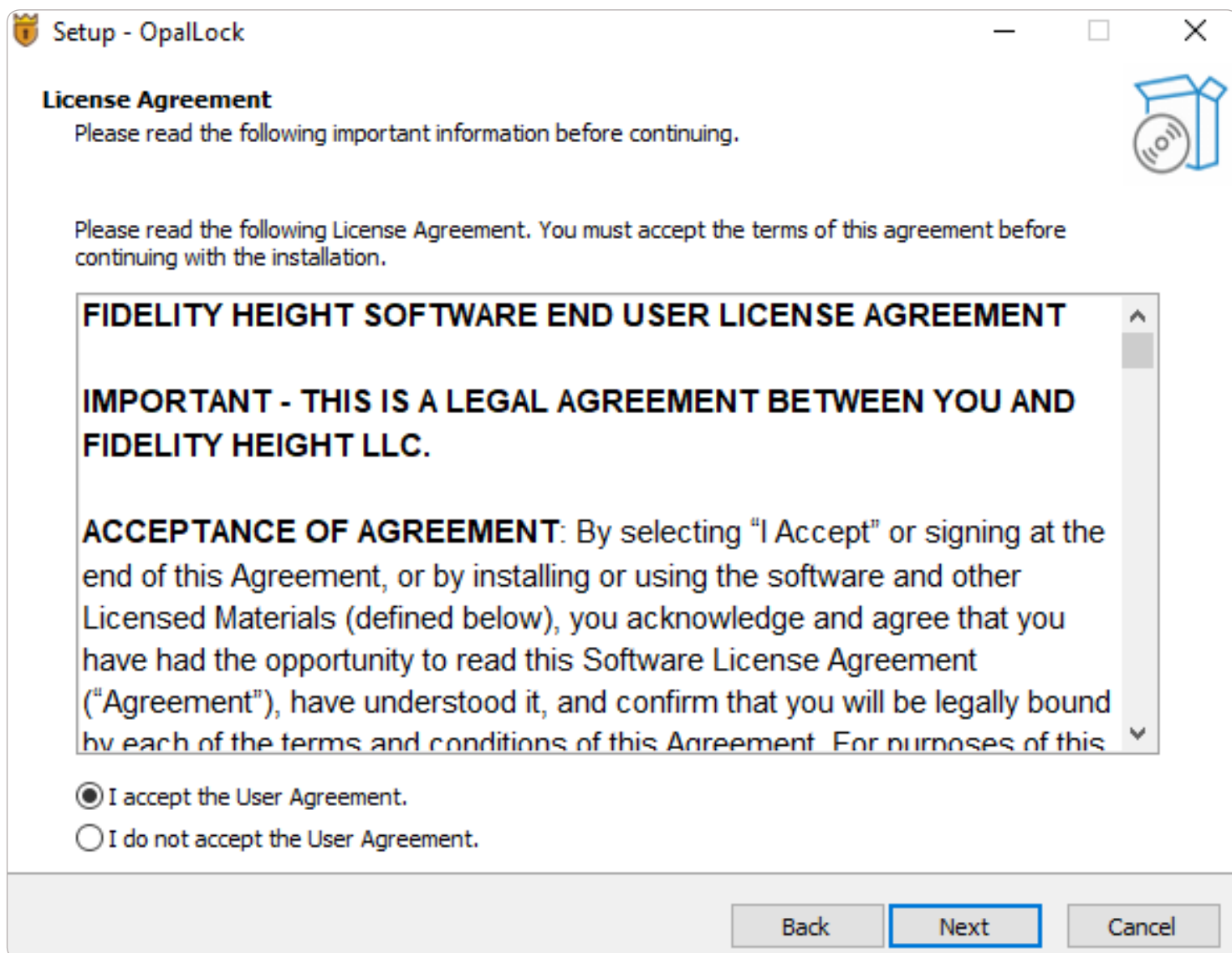
- The Setup Wizard will open after granting permissions.
- Click on the “Next” button to proceed with the installation.



Installation welcome screen.

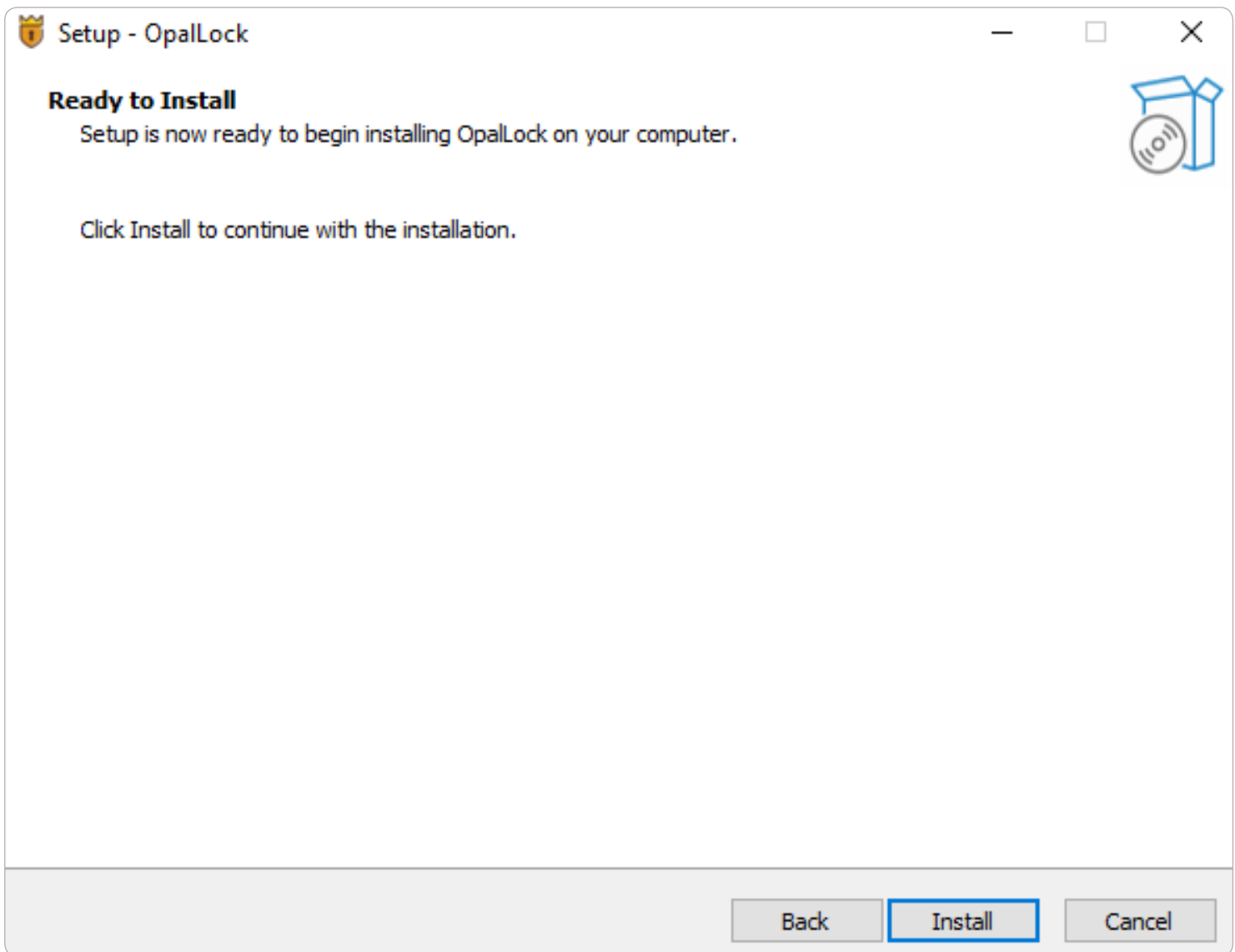
4.4 License Agreement:

- On the License Agreement screen, review the User Agreement.
- If you agree to the terms, select the "I accept the User Agreement" radio button.
- Click the "Next" button to continue. If you do not agree, select the "I do not accept the User Agreement" radio button and exit the installer.

*License Agreement*

4.5 Ready to Install:

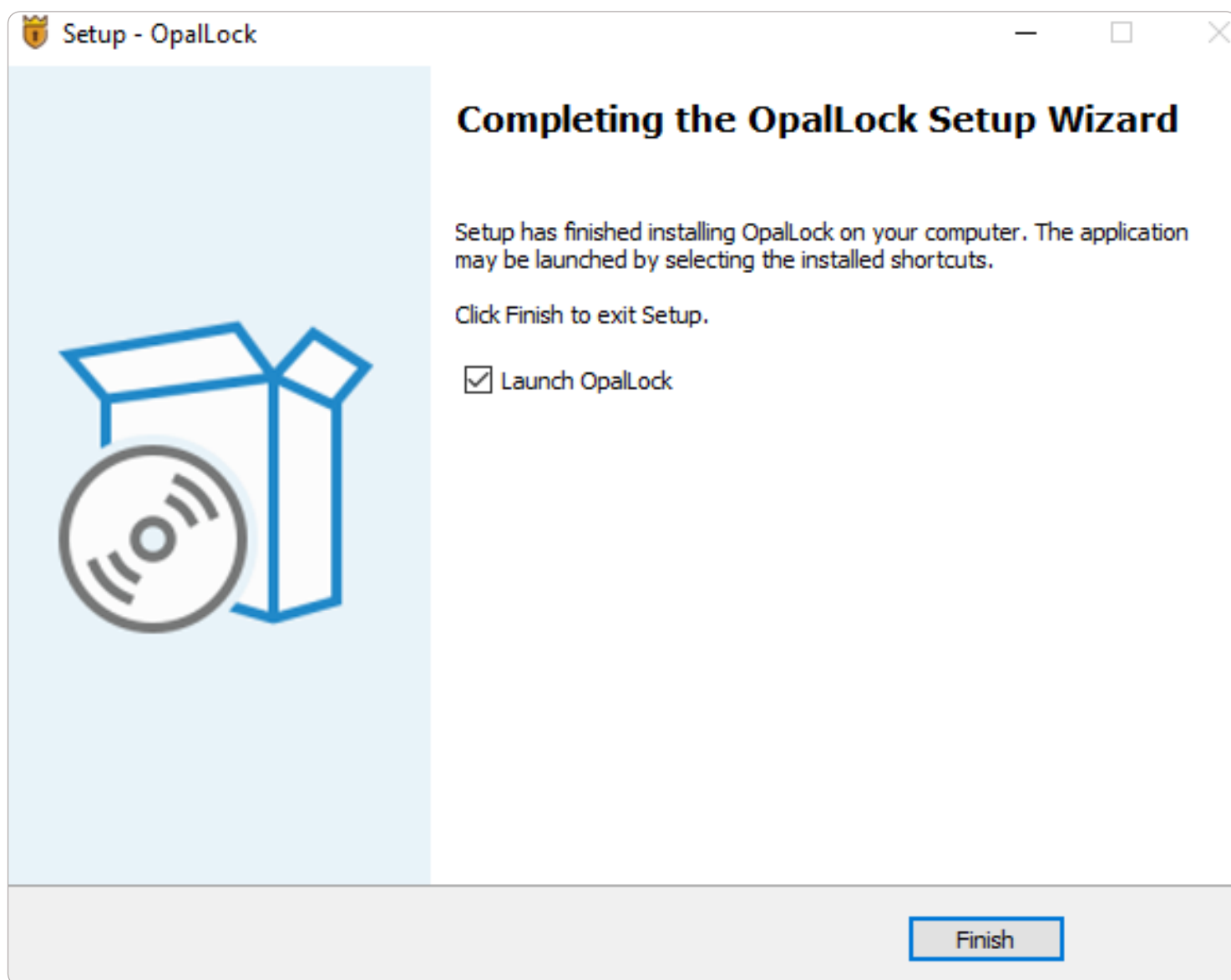
On the "Ready to Install" screen, click on the "Install" button to start the installation process.



Ready to Install

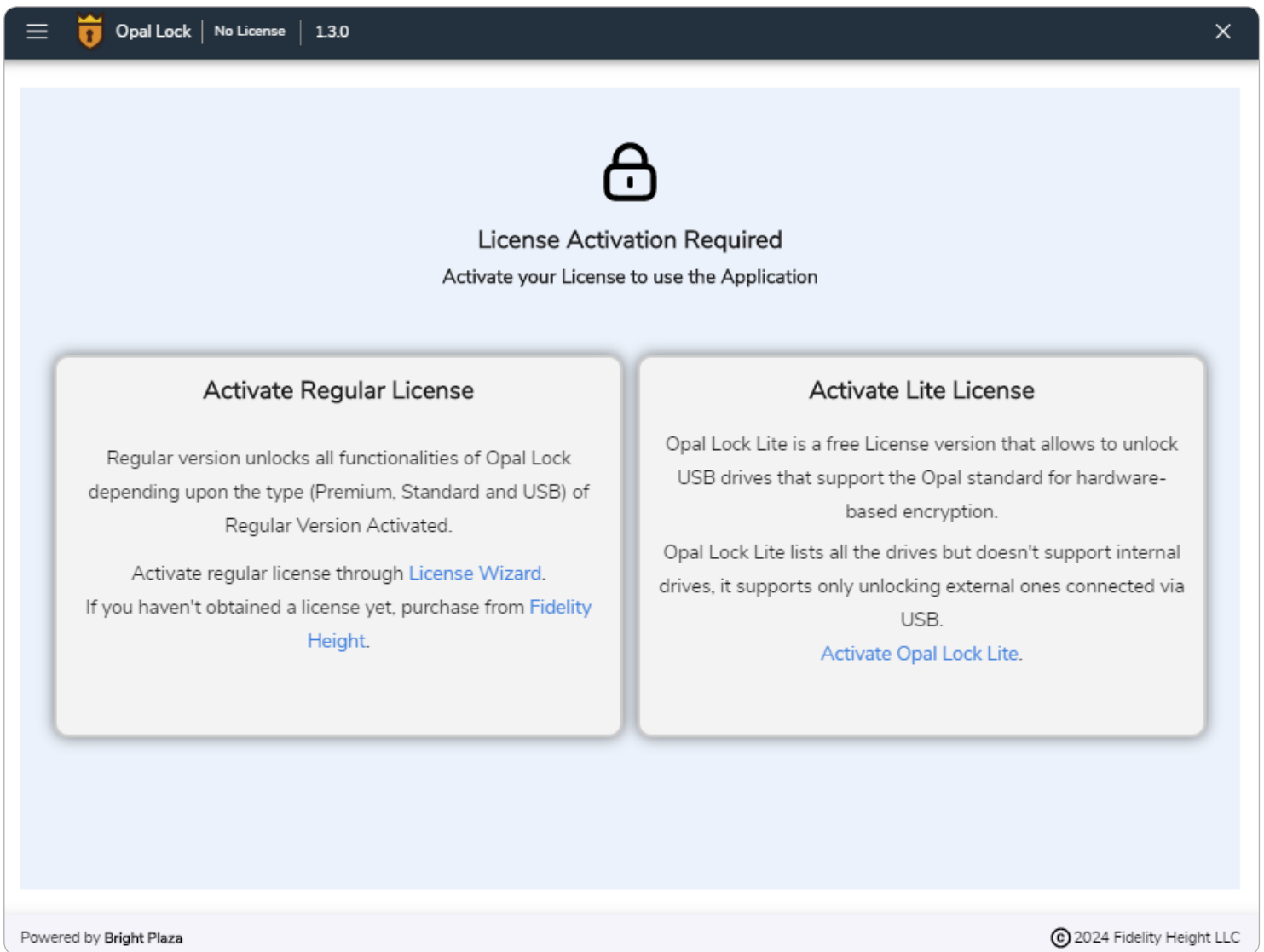
4.6 Installation Complete:

- Once the installation is complete, you will see a message indicating that the setup has been completed successfully.
- Optionally, you can check the “Launch OpalLock” checkbox if you want to launch the application immediately upon clicking the “Finish” button.



Installation Completed. Exit Installation Wizard

- Following these steps will ensure a smooth installation of Opal Lock on your system, allowing you to efficiently manage the security of your self-encrypting drives.
- After the installation is completed and you click the “Finish” button, the Opal Lock application will be launched successfully. Upon launching, you will be prompted to activate either a Regular License or Opal Lock Lite. This step is crucial for accessing the functionality of the application and ensuring that you have the appropriate licensing for your needs.

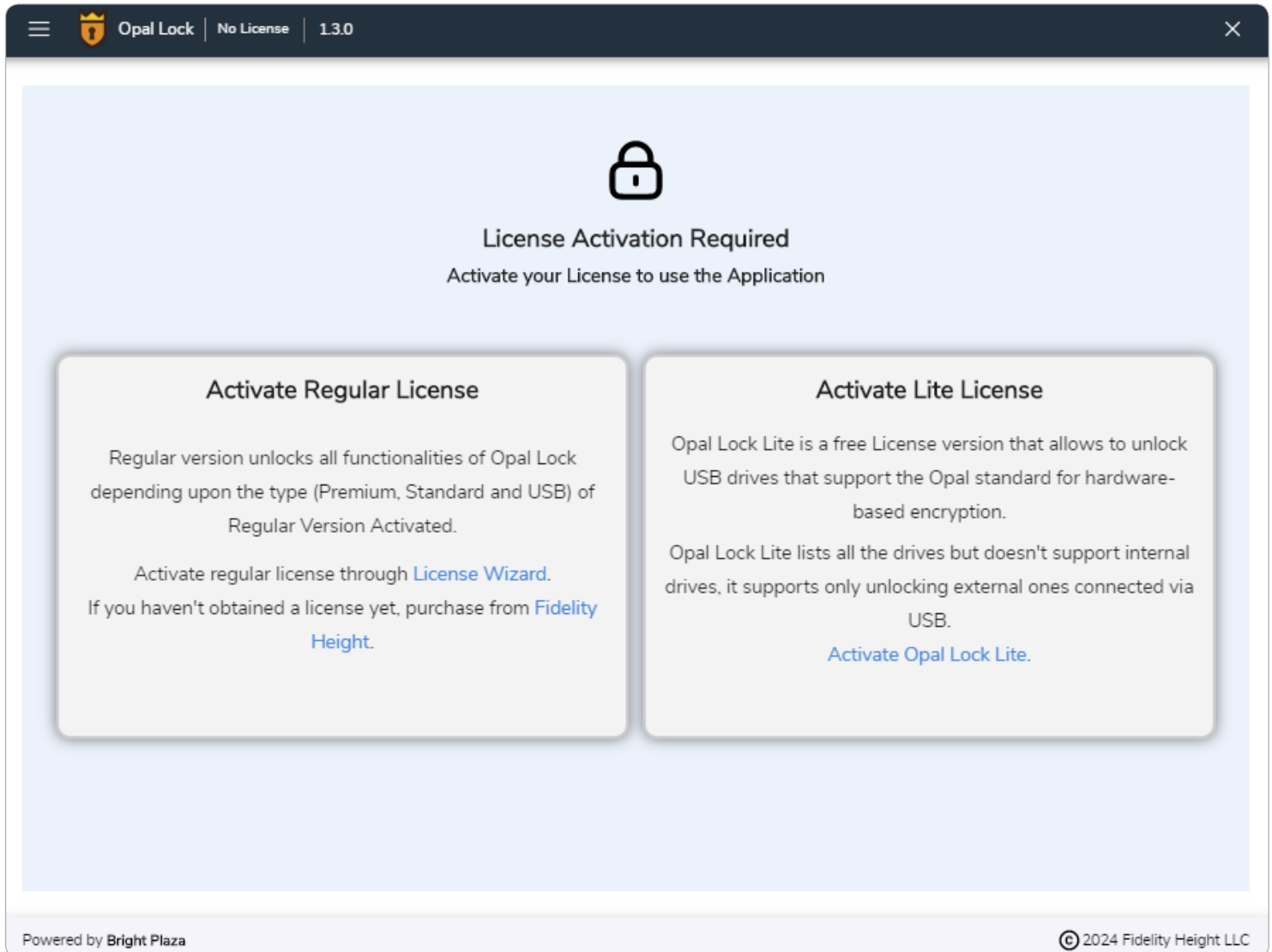


No License Activated

- Depending on your requirements and the type of license you've purchased, you can select either the Regular License option or the Opal Lock Lite option. This activation process ensures that you can fully utilize the features and capabilities of Opal Lock according to the terms of your license type.
- Once you've selected the desired activation option and completed the activation process, you'll be ready to utilize Opal Lock to manage the security of your self-encrypting drives effectively. This includes tasks such as setting up drive encryption, and ensuring data protection in accordance with Trusting Computing Group (TCG) standards.

5. OPAL LOCK LITE ACTIVATION

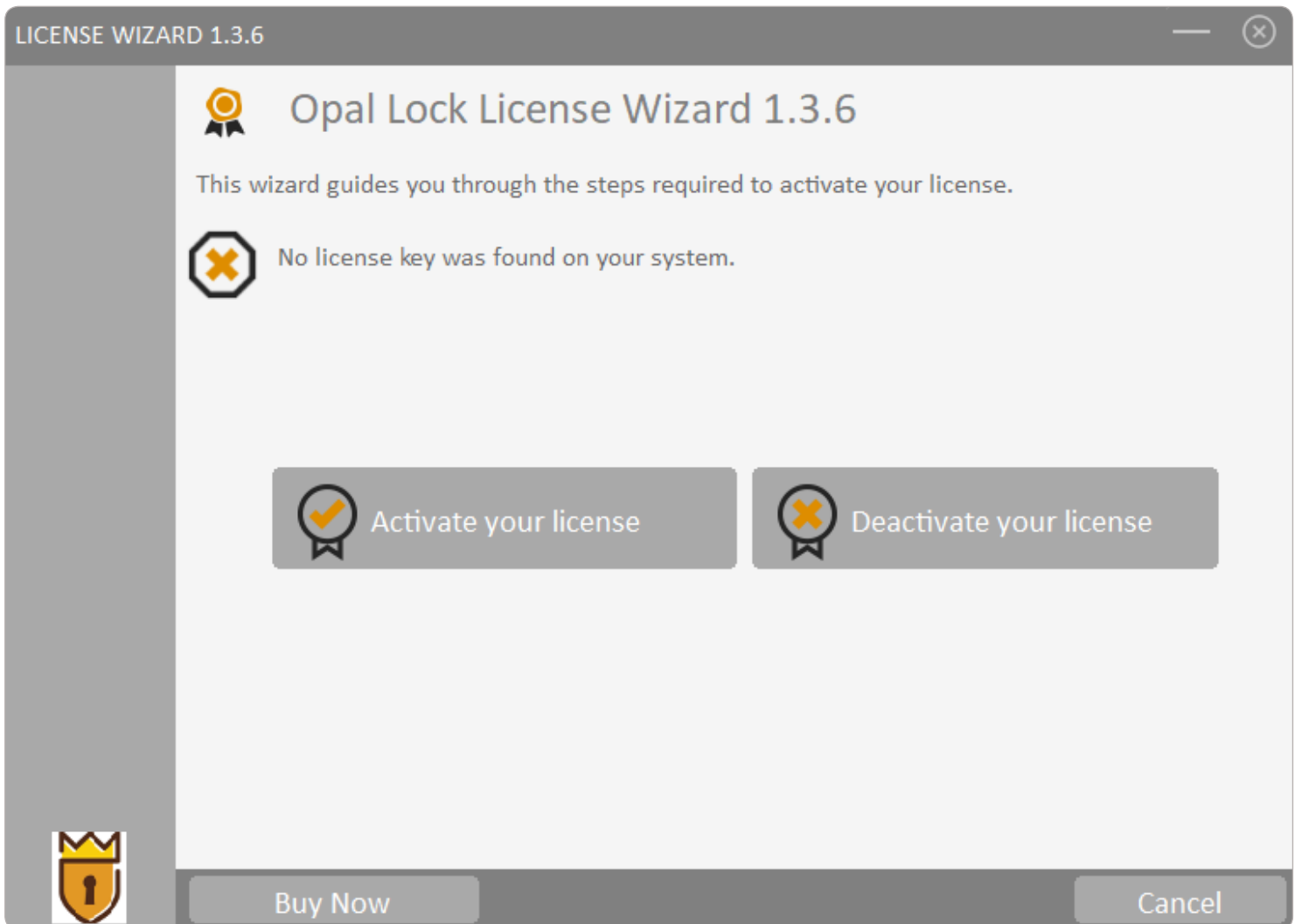
- Click the “Activate Opal Lock Lite” option to activate Lite mode.



No License Activated

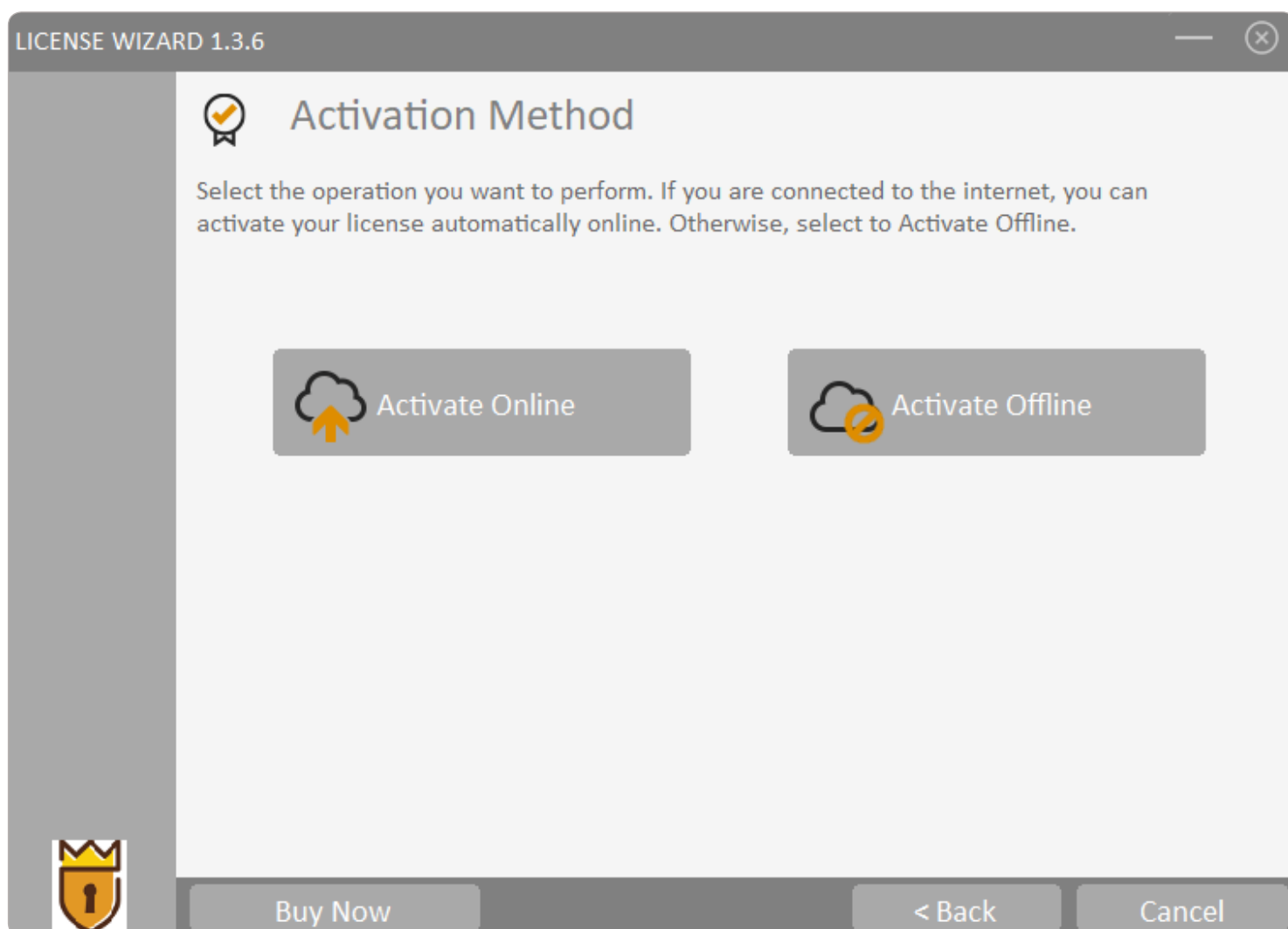
6. REGULAR LICENSE ACTIVATION

- **Launch License Wizard:** Click on the “License Wizard” option. It will open the License Wizard 1.3.6.



License Wizard

- **Choose Activation Method:** On the Activation Method screen, choose whether to Activate Online or Offline



Select your activation method

6.1 Activate Online:

- If the internet is connected, click on Activate Online and enter the License key received in the email on completing the License Purchase.

LICENSE WIZARD 1.3.6

Activate Online

Enter your Activation Key below and click Activate. The License Wizard will then connect to the License Server to activate your license. If you do not know your Activation Key, enter your email address instead.

Activation Key

[Proxy Settings](#) [Activate](#)

 [Buy Now](#) [< Back](#) [Cancel](#)

Enter your activation key

- Click on the Activate button to activate the License

LICENSE WIZARD 1.3.6

Activate Online

Enter your Activation Key below and click Activate. The License Wizard will then connect to the License Server to activate your license. If you do not know your Activation Key, enter your email address instead.

Activation Key



 Your license is activated.



< Back Finish

Your license is activated

6.2 Activate Offline:

- Enter the Activation Key and Computer key in respective fields. Computer Identifier will come pre-filled.
- Click on the Activate button.

LICENSE WIZARD 1.3.6



Activate Offline

To activate your license offline, enter your Activation Key and Computer Key then click Activate. If you have a smartphone with internet access, you can get your Computer Key by clicking the scan QR code below.

Activation Key

Computer Identifier

Computer Key

[How to get your Computer Key](#)

[Scan QR Code](#)

Activate

 Your license is activated.



< Back

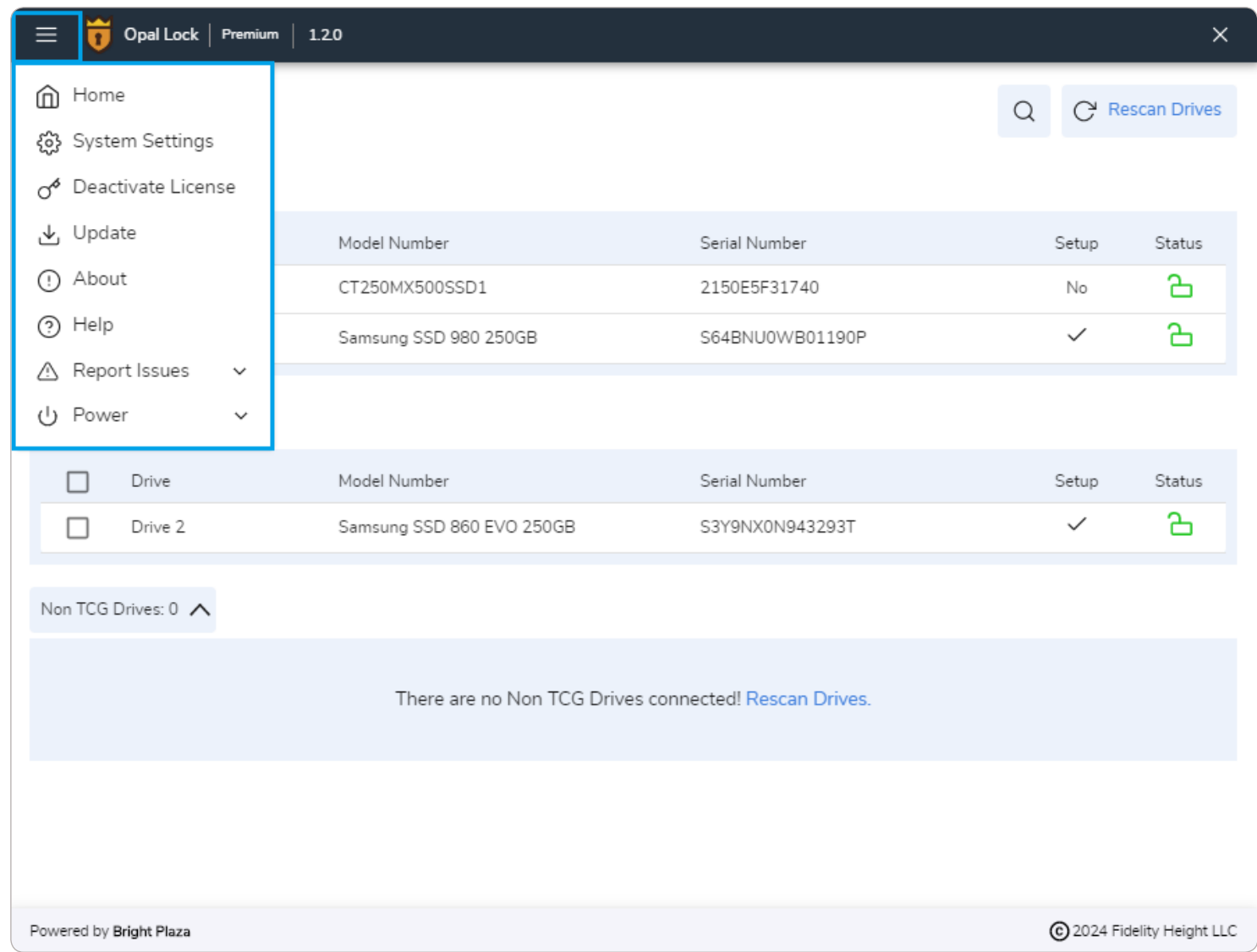
Finish

Activate your license offline

7. LICENSE DEACTIVATION

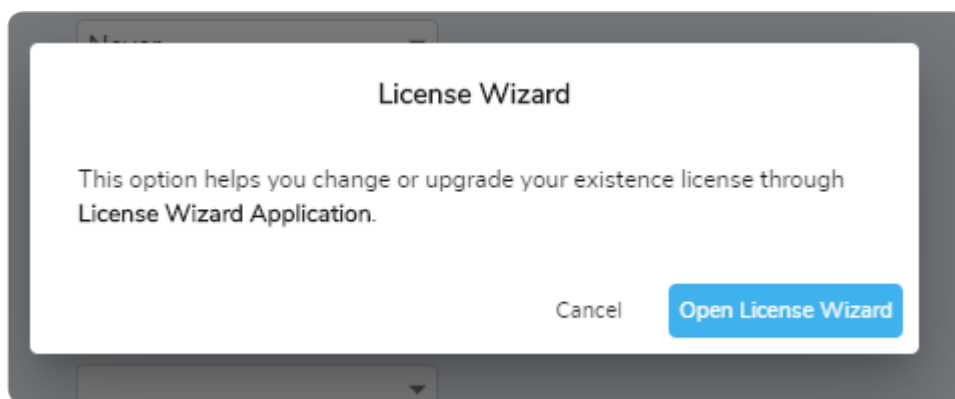
To deactivate your license, follow these steps:

- Click on the Hamburger icon to open the Menu.
- Select the “Deactivate License” option.



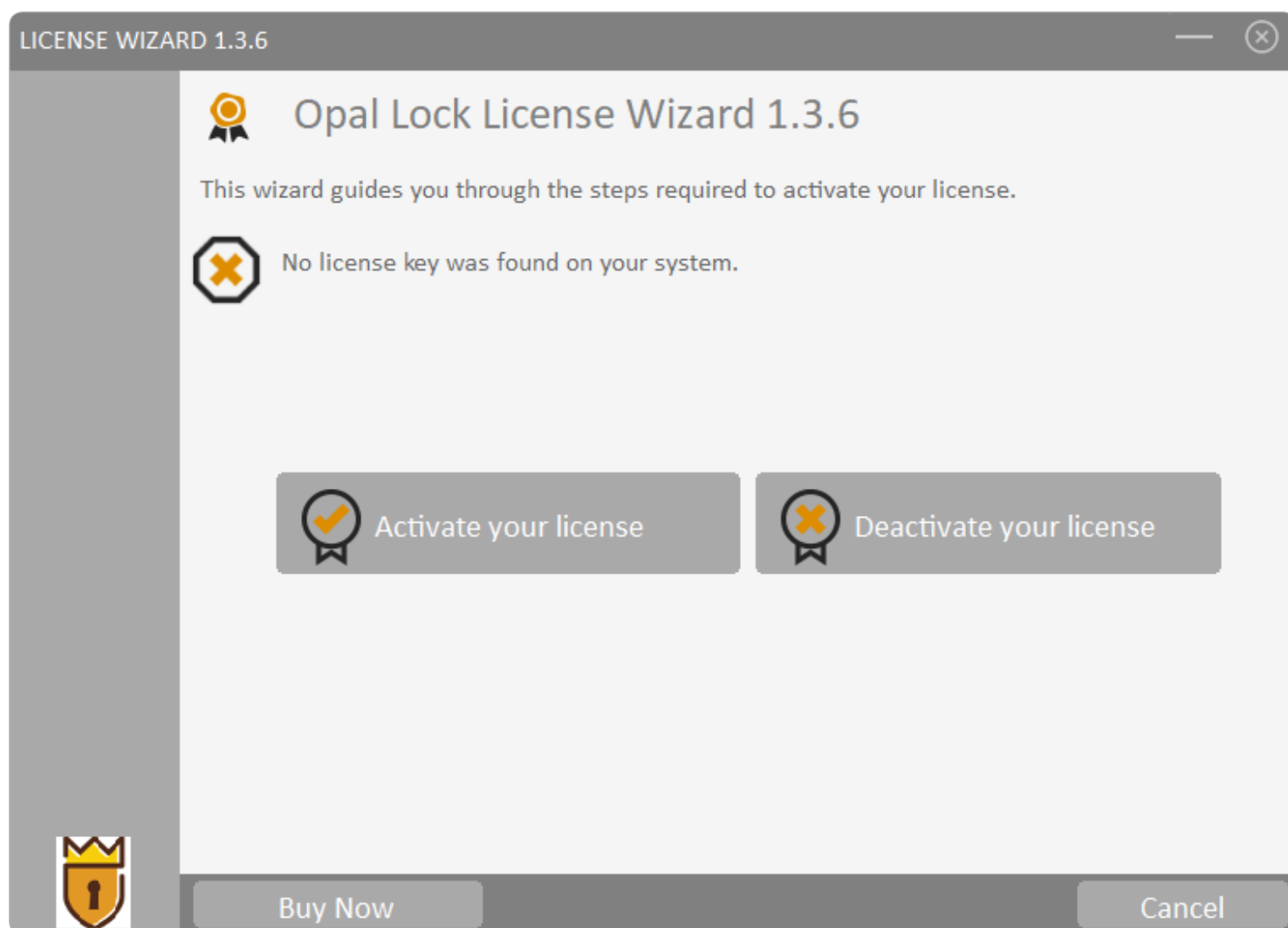
Hamburger Icon > Deactivate License option

- This will prompt the License Wizard window to pop up.



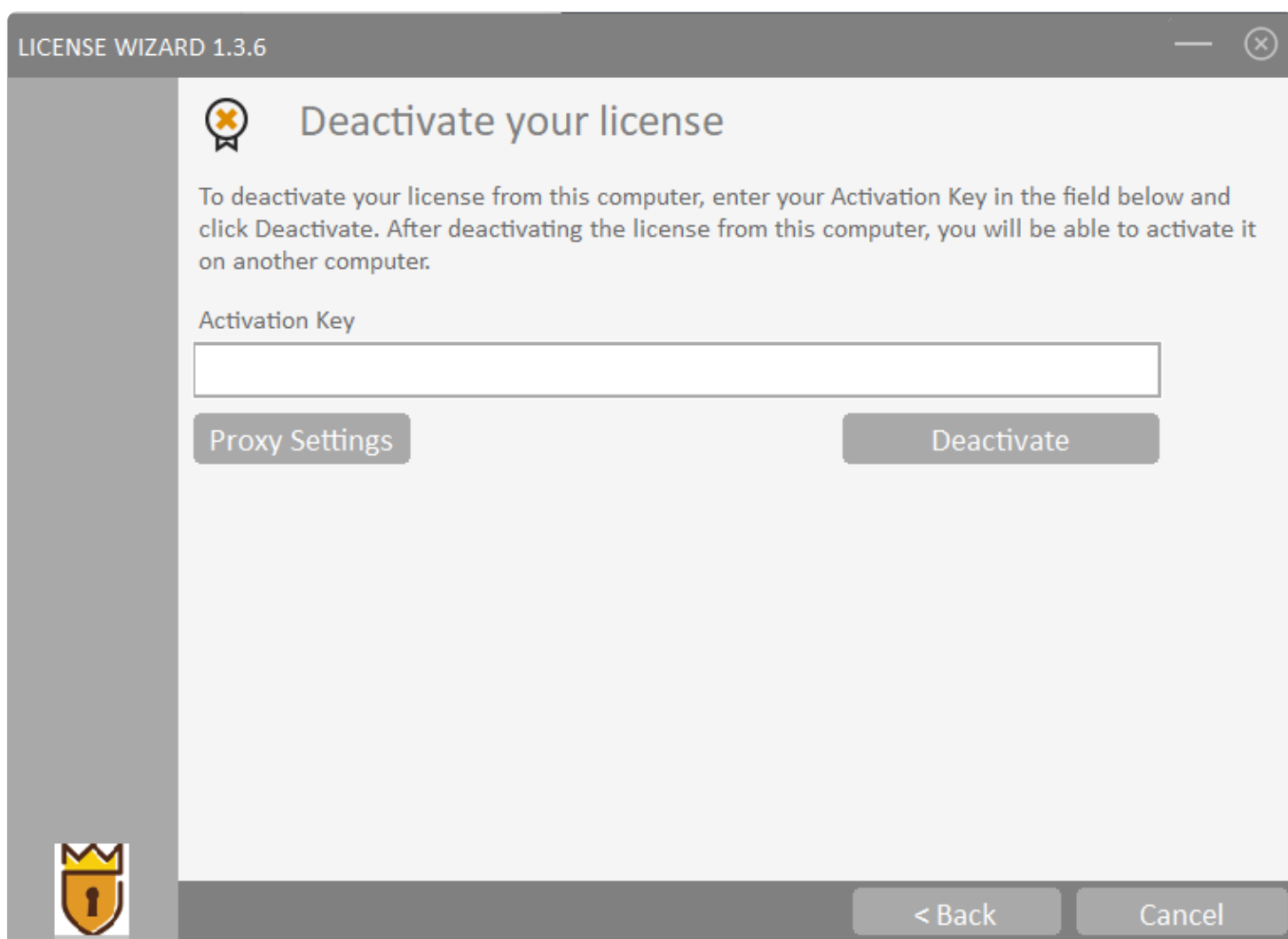
License Wizard

- Click on the "Open License Wizard" button. This action will open the "License Wizard" application.
- Click on the "Deactivate Your License" button.



License Wizard

- Click on the “Deactivate Your License” button. This will open the “Deactivate your License” window.



The screenshot shows a window titled "LICENSE WIZARD 1.3.6" with a close button in the top right corner. The main content area has a light gray background. At the top left of this area is a yellow speech bubble icon with a black 'X' inside. To its right is the title "Deactivate your license" in a large, dark gray font. Below the title is a paragraph of text: "To deactivate your license from this computer, enter your Activation Key in the field below and click Deactivate. After deactivating the license from this computer, you will be able to activate it on another computer." Below this text is a label "Activation Key" followed by a white text input field with a thin gray border. Below the input field are two buttons: "Proxy Settings" on the left and "Deactivate" on the right, both with a dark gray background and white text. At the bottom left of the window is a small icon of a shield with a crown on top and a keyhole in the center. At the bottom right are two buttons: "< Back" and "Cancel", both with a dark gray background and white text.

LICENSE WIZARD 1.3.6

Deactivate your license

To deactivate your license from this computer, enter your Activation Key in the field below and click Deactivate. After deactivating the license from this computer, you will be able to activate it on another computer.

Activation Key

Proxy Settings Deactivate

< Back Cancel

Deactivate your license

- Click on the Deactivate button to confirm and deactivate the License.

8. OPAL LOCK REGULAR VERSION USE CASE: ENABLING DRIVE LOCKING

- ◆ **Scenario:** Securing Drives with Opal Lock Regular Version
- ◆ **User Situation:** The user has the Opal Lock Software installed and Regular License activated on their system.
- ◆ **Need for access:** The Regular version of Opal Lock offers enhanced functionalities and capabilities, making it suitable for users with more advanced security needs or those requiring additional features. Organizations with stringent security requirements, such as government agencies, financial institutions, or healthcare providers, often need advanced security features to protect sensitive data effectively. Users who deal with highly sensitive or confidential data, such as intellectual property, customer records, or trade secrets, need advanced security features to safeguard their information from unauthorized access or data breaches. The Regular version provides additional security controls and features that help mitigate risks associated with data loss, unauthorized access, or cyber threats.

9. REGULAR VERSION TYPES AND USE CASES

Here's an overview of the types of Regular versions of Opal Lock and their respective use cases:

9.1 USB License

Use Case: The USB License version is designed for users who primarily work with USB-mounted Opal Drives and require basic drive security functionalities.

Features:

- Supports basic functionalities of Opal Lock for up to five External USB-mounted Opal Drives.
- Includes features such as setting up drive encryption, password protection, unlocking drives, changing passwords, and reverting setup.
- Supports Data Erasure and user can view the “Certificate of Sanitization”
- Supports automatic unlocking using passwords saved in the System drive or password stored on USB

Target Users: Individuals or small businesses with a limited number of USB-mounted Opal Drives who need essential drive security features.

9.2 Standard License

Use Case: The Standard License version caters to users who require drive security functionalities for both internal and external drives, including setting up a pre-boot OS environment for unlocking drives.

Features:

- Supports basic functionalities of Opal Lock for up to five Opal Drives, including internal drives.
- Includes features such as setting up drive encryption, password protection, unlocking drives, changing passwords, and reverting setup.
- Supports Data Erasure and user can view and download the “Certificate of Sanitization”
- Includes setting up a pre-boot OS environment for unlocking drives when the boot drive is locked.

- Setting up drive encryption includes configuring the pre-boot OS environment on a bootable USB drive.
- Supports automatic unlocking using passwords saved in the System drive or password stored on USB
- Supports automatic unlocking of drives in the pre-boot OS environment using passwords stored on USB.

Target Users: Businesses or individuals needing drive security features for a mix of internal and external drives, with a focus on seamless unlocking mechanisms.

9.3 Premium License

Use Case: The Premium License version is suited for users managing multiple drives and requiring advanced management capabilities, such as automatic unlocking and multiple password support.

Features:

- Allows easy setup and management of multiple drives with a single click.
- Includes features such as setting up drive encryption, password protection, unlocking drives, changing passwords, and reverting setup.
- Supports Data Erasure and user can view and download the “Certificate of Sanitization”
- Enables the creation of a second password with limited authority.
- Supports basic functionalities of Opal Lock for up to five Opal Drives, including internal drives.
- Includes setting up a pre-boot OS environment for unlocking drives when the boot drive is locked.
- Setting up drive encryption includes configuring the pre-boot OS environment on a bootable USB drive.
- Supports automatic unlocking using passwords saved in the System drive or password stored on USB
- Supports automatic unlocking of drives in the pre-boot OS environment using passwords stored on USB.

Target Users: Enterprises or organizations managing multiple drives across various systems, where efficient management and advanced security features are paramount.

10. PREMIUM VERSION GUIDE

10.1 Opal Lock Premium Version Home screen Display and Drive Detection

The Opal Lock Home screen provides users with clear and concise information about detected drives, including their setup status, lock status, model number, and serial number. Users can easily identify and manage drive security settings and configurations based on the displayed information. Additionally, the option to rescan drives ensures that users have access to real-time drive status updates as needed.

The screenshot displays the Opal Lock Premium Home screen interface. At the top, a dark header bar contains the Opal Lock logo, the text 'Opal Lock | Premium | 1.2.0', and a close button. Below the header, the main content area shows 'Drives: 3' with a search icon and a 'Rescan Drives' button. The drives are categorized into three sections: Internal TCG Drives (1), External TCG Drives (2), and Non TCG Drives (0). Each section contains a table of drive information.

Drive	Model Number	Serial Number	Setup	Status
Drive 0	CT250MX500SSD1	2150E5F31740	✓	🔒
Drive 1	Samsung SSD 980 250GB	S64BNU0WB01190P	✓	🔒
Drive 2	Samsung SSD 860 EVO 250GB	S3Y9NX0N943293T	No	🔒

Below the tables, a message states: 'There are no Non TCG Drives connected! [Rescan Drives.](#)'

At the bottom, the footer indicates 'Powered by Bright Plaza' and '© 2024 Fidelity Height LLC'.

Premium Home screen

Here's a breakdown of the displayed information and functionalities:

Drive Setup Status: The Home screen displays the setup status of each detected drive. If a drive is set up with Opal Lock encryption and security features, a check mark symbol (✓) will appear under the Setup column for that drive. If the drive is not set up, the column will display “No” to indicate the status.

Lock Status: A visual indicator is provided to denote the lock status of each drive. A red lock icon indicates that the drive is set up and currently locked. Conversely, a green unlock icon with Setup “No” indicates the drive is unlocked and not setup and a green unlock icon with Setup “✓” indicates drive is unlocked and setup is created

Drive Model Number and Serial Number: The Home screen lists the model number and serial number of each detected drive. This information helps users identify and differentiate between drives, especially in environments with multiple drives connected to the system.

Drive Name: Drives are listed by their drive names according to the system's naming convention. On Windows, drives will be listed as physical drives (e.g., Drive1). TCG (Trusted Computing Group) drives are listed based on the drive limit determined by the Opal Lock version being used.

Rescan Drives Button: The Home screen features a “Rescan Drives” button, which allows users to manually trigger a rescan of mounted drives. This action updates the drive status information displayed on the application by querying the drives for updated status information.

Drive Prioritization: In cases where the total number of detected TCG drives exceeds the drive limit determined by the Opal Lock version, the Home screen prioritizes listing previously detected drives that are still present ahead of other drives. This ensures that important drive information is displayed promptly and clearly to users.

10.2 DETAILS

Upon clicking on a specific drive from the Opal Lock interface, users can access detailed information about that drive

Opal Lock | Premium | 1.2.0

Drive / Drive 2 CT250MX500SSD1 ...

Setup : No ●

Details Drive Setup Revert Setup/Erase Lock/Unlock

Drive Information

Model Number CT250MX500SSD1	Serial Number 2150E5F31740	Preboot Image Not Available
MSID crucial_bymicron	Manufacturer Name MICRON TECHNOLOGY, INC.	Firmware M3CR043

TCG Information

TCG Version Opal 2.0	Encryption Supported	Block SID Disabled
Setup Status No	Lock Status Unlocked	User Setup No

Powered by Bright Plaza © 2023 Fidelity Height LLC

Details Screen

Here's a breakdown of the Drive Information section:

10.2.1 Drive Information

- **Model Number and Serial Number:** These fields display the model number and serial number of the selected drive, allowing users to identify the drive uniquely.

- **Manufacturer:** The manufacturer of the drive is provided for reference, indicating the company that produced the drive.
- **Firmware Version:** This field shows the firmware version of the drive, which is manufacturer-specific. It provides information about the installed firmware for diagnostic and compatibility purposes.
- **MSID (Manufacturer Secure ID):** The MSID serves as the default password of the drive before it's set up with Opal Lock. If the previously set up password is reset, it reverts to the MSID. This field helps users understand the initial authentication key of the drive.
- **Preboot Image:** This field indicates the version of the preboot image written to the drive's shadow Master Boot Record (MBR). If the drive doesn't support MBR shadowing, or if the preboot image hasn't been written to the drive (for TCG drives), appropriate messages such as "Not Supported" or "Not Available" are displayed.

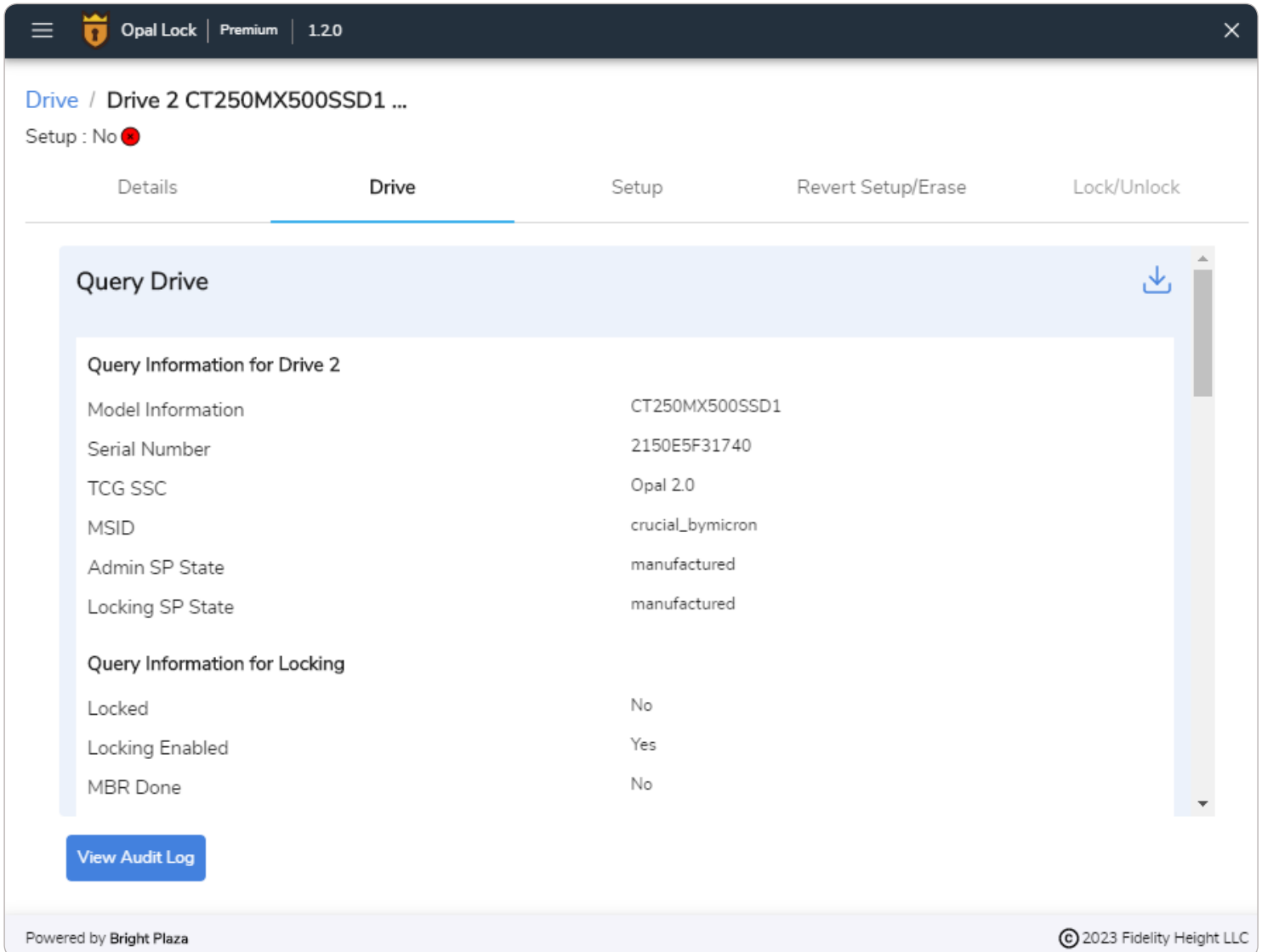
10.2.2 TCG Information

- **TCG Version:** This field displays the version of the TCG (Trusted Computing Group) specification that the drive supports.
- **Setup Status:** Indicates whether the drive has been set up using Opal Lock. If not set up, it will display "No." and if setup, it will display "Completed"
- **Lock Status:** Displays whether the drive is currently locked or unlocked. If locked, it will show "Locked"; otherwise, it will display "Unlocked."
- **Encryption:** Indicates whether the selected drive supports full-disk encryption. Most TCG versions support full-disk encryption, except for certain exceptions like Pyrite, which doesn't support the encryption.
- **Block SID:** This feature, if enabled in some TCG drives, prevents changing the authentication key. If Block SID is enabled, Opal Lock can't set up a password for the drive. It needs to be disabled in the BIOS before executing the Block SID command.

10.3 DRIVE

This section covers features related to viewing on TCG drives. To determine whether a drive is a TCG drive, users can check if it has a PSID (physical secure ID), typically included on the drive's label. All TCG drives are compatible with Opal Lock, but certain TCG versions such as Pyrite and Enterprise may not support specific operations.

10.3.1 Query Drive



The screenshot shows the Opal Lock Premium 1.2.0 application window. The top navigation bar includes a menu icon, the Opal Lock logo, the version 'Premium 1.2.0', and a close button. Below the navigation bar, the breadcrumb 'Drive / Drive 2 CT250MX500SSD1 ...' is displayed, followed by 'Setup : No' with a red status indicator. A horizontal tab bar contains 'Details', 'Drive' (selected), 'Setup', 'Revert Setup/Erase', and 'Lock/Unlock'. The main content area is titled 'Query Drive' and features a download icon. It contains two sections: 'Query Information for Drive 2' and 'Query Information for Locking'. The first section lists various drive attributes and their values. The second section shows the current locking status.

Query Information for Drive 2	
Model Information	CT250MX500SSD1
Serial Number	2150E5F31740
TCG SSC	Opal 2.0
MSID	crucial_bymicron
Admin SP State	manufactured
Locking SP State	manufactured

Query Information for Locking	
Locked	No
Locking Enabled	Yes
MBR Done	No

Below the tables is a blue button labeled 'View Audit Log'.

At the bottom of the window, it says 'Powered by Bright Plaza' on the left and '© 2023 Fidelity Height LLC' on the right.

Query Drive

- Query Information: Opens a window displaying detailed information about the drive. Users can save this information as a CSV file for reference.

Opal Lock | Premium | 1.2.0

Drive / Drive 2 CT250MX500SSD1 ...

Setup : No

Details	Drive	Setup	Revert Setup/Erase	Lock/Unlock
Mechanism: Overwrite Data Erase		N/A		
Mechanism: Erase		N/A		
Mechanism: Crypto Erase		N/A		
Mechanism: Unmap		N/A		
Mechanism: Reset Rewrite Pointers		N/A		
Mechanism: Vendor Specific Erase		N/A		
Data Removal Time: Overwrite Data Erase		N/A		
Data Removal Time: Block Erase		N/A		
Data Removal Time: Crypto Erase		N/A		
Data Removal Time: Unmap		N/A		
Data Removal Time: Reset Write Pointers		N/A		
Data Removal Time: Vendor Specific Erase		N/A		

[View Additional Information](#)

[View Audit Log](#)

Powered by Bright Plaza

© 2023 Fidelity Height LLC

View Additional Information

- **Additional Password-Protected Information:** Users can enter the drive's Admin password to access additional, password-protected information. Clicking on the "View Additional Information" option opens a window where this information can be accessed with a valid Admin password. When the drive is not set up, the application automatically reads the **default password (MSID)** to view additional query information.
- **Save Query Information:** Users have the option to save the query information to a text file for future reference.

10.3.2 Audit Log

- **Audit Log:** Opal Lock stores an event log embedded within each drive, known as the Audit Log, which records operations performed on the drive such as setting up the password and authentication attempts.
- **View Audit Log:** The application provides a “View Audit Log” button to fetch the Audit Logs. Clicking on this button opens a window where audit log information can be accessed with a valid Admin password.

Drive / Drive 2 CT250MX500SSD1 ... / Audit Log [Download as CSV](#)

Type	Date & Time	Event ID	Description
Information	2023/12/04 17:10:52	22	Audit Log accessed
Information	2023/12/04 17:10:52	3	Admin Authenticated
Information	2023/12/04 17:10:33	21	Query information accessed
Information	2023/12/04 17:10:33	3	Admin Authenticated
Information	2023/12/04 17:01:26	1	Drive Activated

Rows per page: 5 1-5 of 207

Audit Log successfully retrieved.

Powered by Bright Plaza

Audit Logs

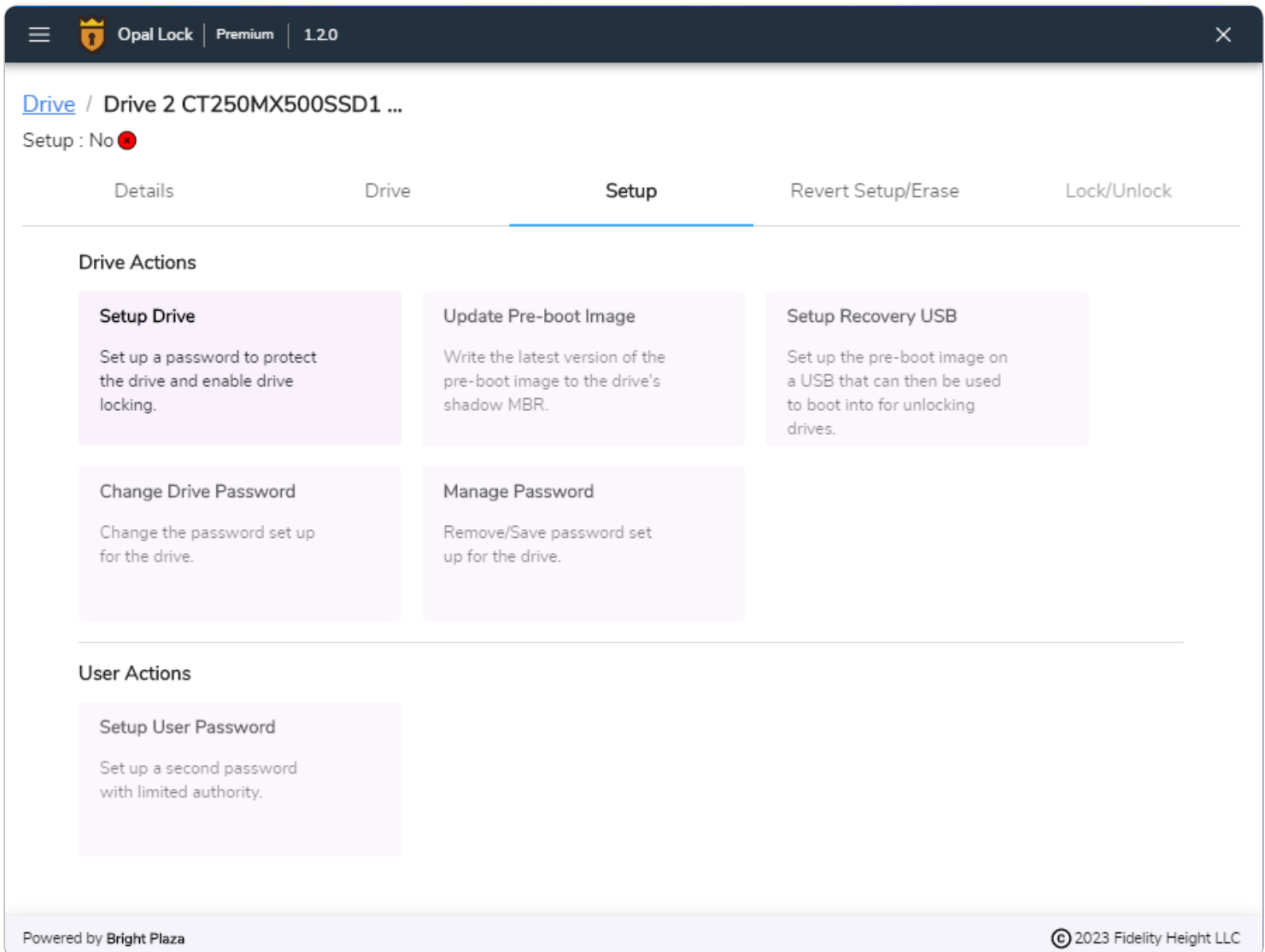
- Saving Audit Log: The Audit Log can be saved as a CSV file. Refer to the provided appendix A for a sample of the contents.

Notes:

- ▶ When the drive is not set up, the application automatically reads the default password (MSID) to view the Audit Logs.
- ▶ During drive setup, Opal Lock also establishes an audit user, a separate internal password that writes events to the audit log.
- ▶ The Audit Log requires that the drive supports Datastore. Some TCG versions like Enterprise may not support Datastore.

10.4 Setup

This section introduces the following features:



Setup screen

- **Setup Drive:** This feature enables users to set up the password and locking/unlocking mechanisms for the drives.
- **Update Pre-boot Image:** Users can utilize this feature to write the latest version of the pre-boot image to the drive's shadow Master Boot Record (MBR).
- **Setup Recovery USB:** This feature allows users to set up the pre-boot image on a USB flash drive, which can then be used to boot into for unlocking drives.

- **Change Drive Password:** Users can change the password that is set up for the drive using this feature.
- **Manage Password:** This feature enables users to save and remove the password files from the System drive and USB flash drives.
- **Setup User Password:** Users can use this feature to set up a second password with limited authority.

Note

- ▶ The features, Update Pre-boot Image, Setup Recovery USB, Change Drive Password, Manage Password, and Setup User Password can be accessed only if a password for the drive has been set up previously.

10.4.1 Set up Drive

Set up Password: The first step in setting up a drive is to establish a password for the drive. This password will be utilized for all Opal Lock operations on the drive, including unlocking the drive. It's important to note that this password is distinct from the one typically entered on the operating system's startup screen. To ensure security, the password must be a minimum of 8 characters long. For verification purposes, the new password must be entered and confirmed twice.

[Drive](#) / [Drive 2 CT250MX500SSD1 ...](#) / **Setup Drive**
Cancel

1 Create Admin Password
 2 Select USB
 3 Setup Drive

Create Admin Password

Enter the current password for the drive and click on 'Next'

Enter Password
 Confirm Password

Enter password with minimum eight characters, at least one uppercase letter, one lowercase letter, one number and one special character (ex = !"#\$%&'()*+,-./:;<=>?@[!^_{}~)

☒ Save password
 ?

Next

Powered by **Bright Plaza**
© 2023 Fidelity Height LLC

Create Admin Password

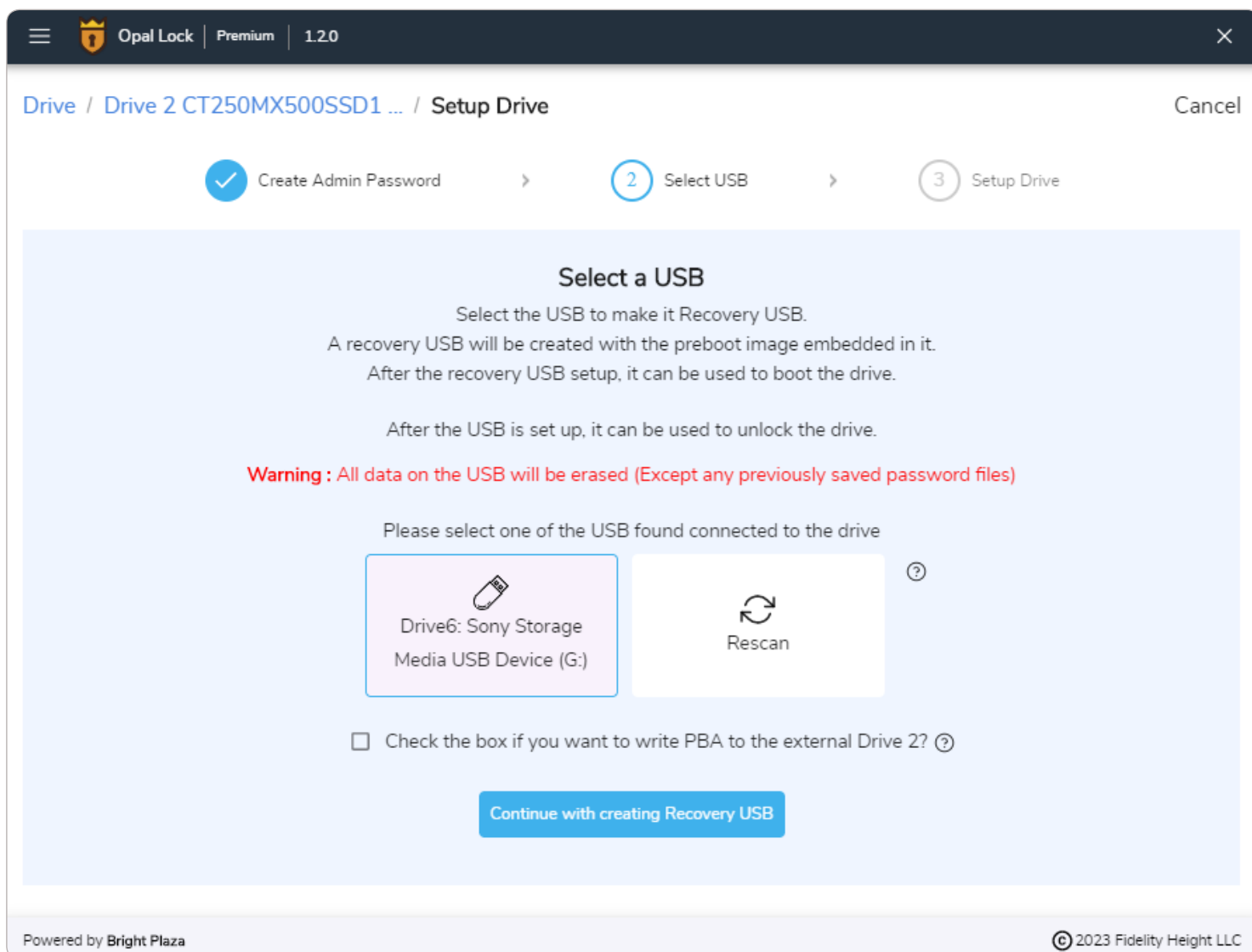
Note

- ▶ The “Save Password” checkbox will be automatically checked and disabled by default. We highly recommend saving the password to a USB flash drive. However, users still have the option to uncheck the checkbox on the “Save Password” pop-up that appears during the final step of the drive setup process.

WARNING

- If the drive's password is lost or forgotten, the only recourse for recovery is to revert setup using the drive's PSID (physical secure ID). This action resets the drive to its manufacturer settings and erases all of the drive's data, with no means of recovery. Therefore, it is imperative that users remember the password they set.

Select a USB: A Recovery USB flash drive will be created with the pre-boot image embedded in it. This USB can then be used to unlock the drive. Additionally, a pre-boot image will be written on the Opal drive's Shadow MBR.



Select a USB

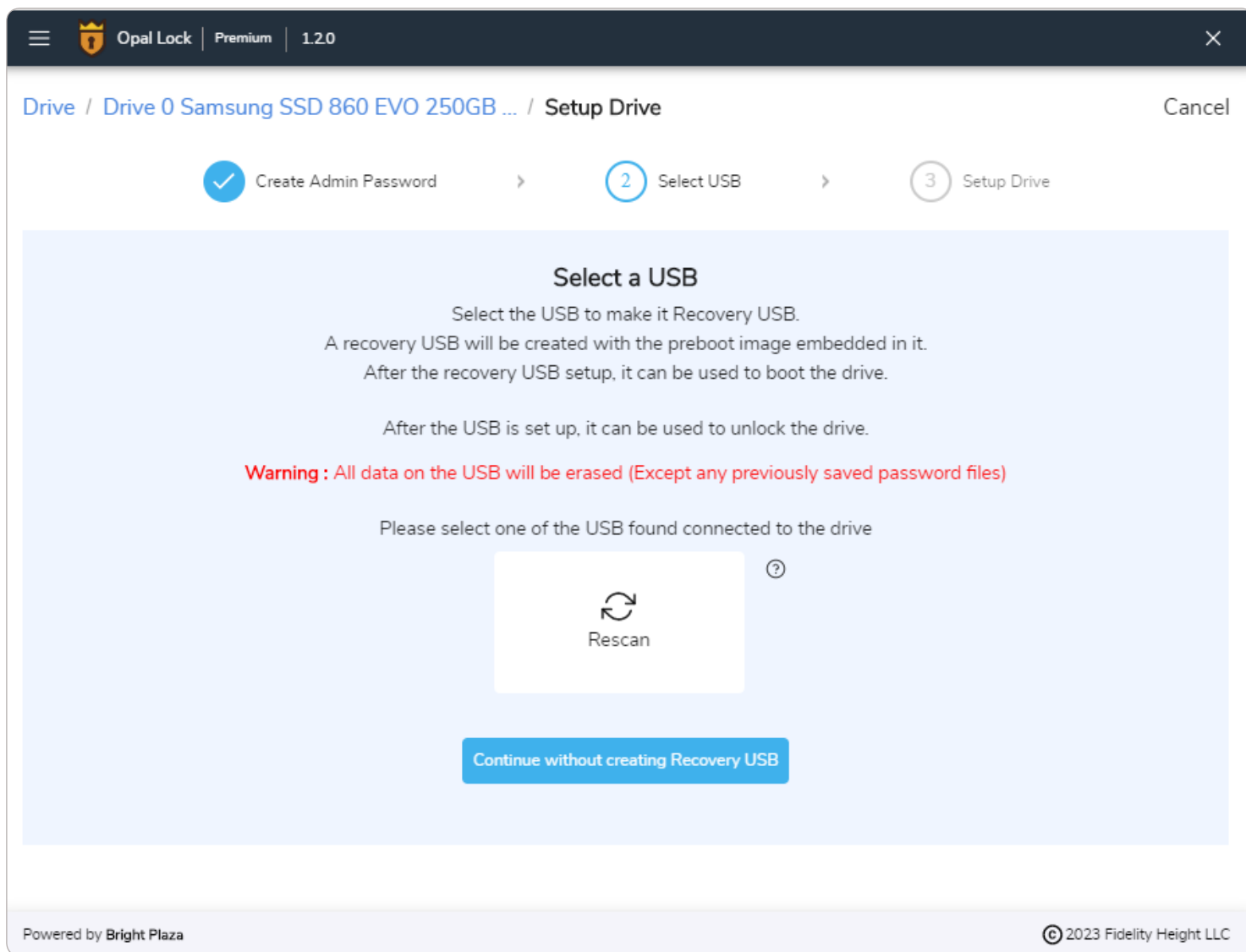
To select the USB flash drive, attach the USB flash drive to the system, and click on the “Rescan” option. Then, click on the USB flash drive to select it.

The pre-boot image is a small operating system image with Opal Lock embedded in it, which can be written onto a drive’s Shadow MBR. When a drive is locked, its contents are encrypted and inaccessible, except for its Shadow MBR. Booting into a locked drive with the pre-boot image written allows the system to boot into the pre-boot image. From there, the embedded Opal Lock application loads and can be used to unlock the drive. After unlocking the drive, its contents can be accessed by rebooting the system.

If Opal Lock is used to manage multiple drives, the pre-boot image doesn’t necessarily need to be written to every drive. However, at least one drive with the pre-boot image must be mounted on the system to access the pre-boot environment and unlock all drives. If each drive will be managed individually, then every drive needs to have the pre-boot image written to its Shadow MBR.

Note

- For Internal Opal Drive, Writing the pre-boot image on the Opal drive’s Shadow MBR is compulsory because Internal drives can be used for boot purposes. Therefore there is no way to skip the Preboot writing while setting up the Internal drive



Select a USB(Internal Drives)

For External Opal Drive, Writing the pre-boot image on the Shadow MBR is optional. To do so, the user must check the checkbox provided.

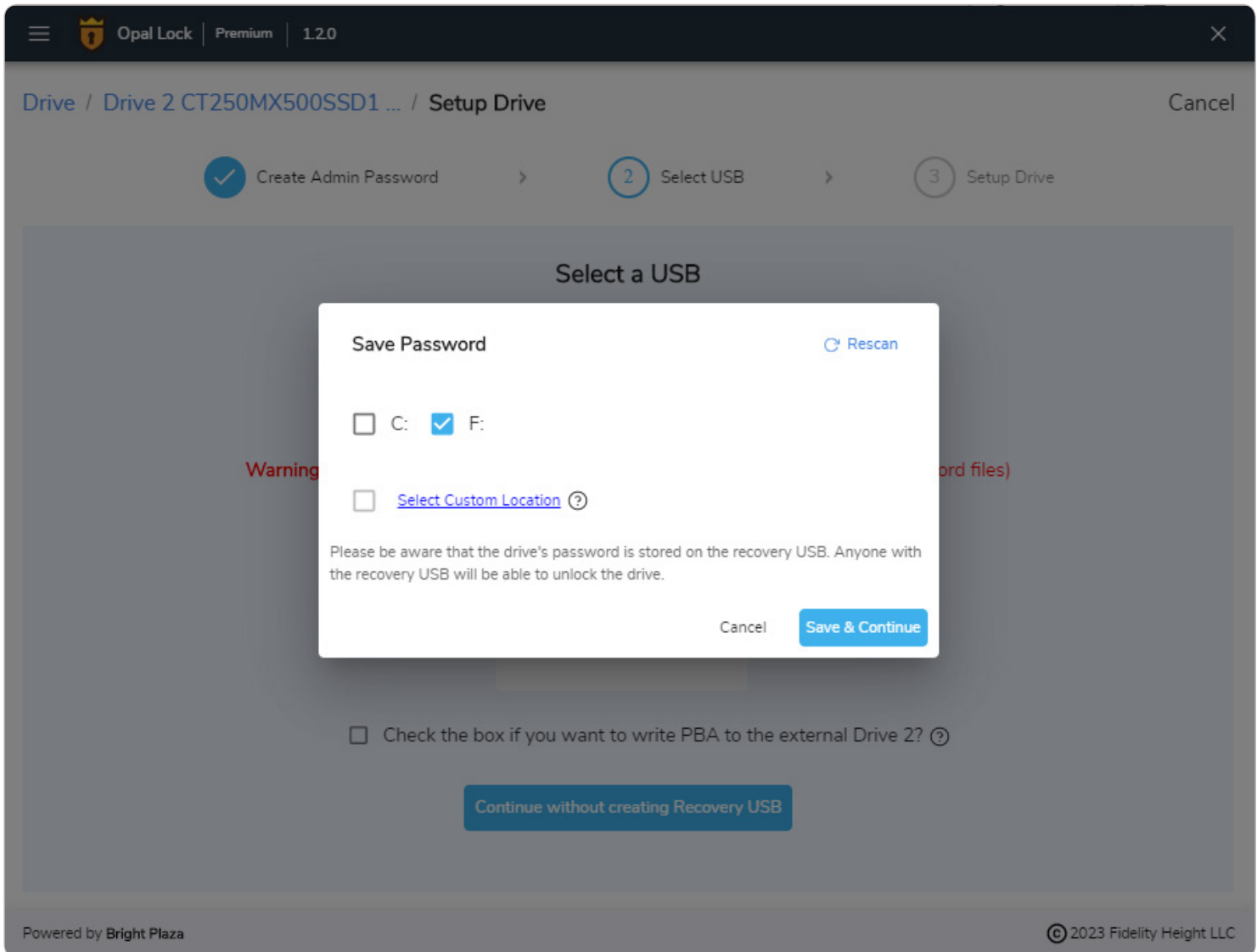
WARNING

- Writing the pre-boot image to a drive can take up to 15 minutes. Do not power down the system during this process, or the image will not be written, and the drive will be locked with no means of unlocking itself internally.

Some TCG versions do not support Shadow MBR. If your drive doesn't support MBR shadowing, then it's not possible to set up the pre-boot image on

the drive. In such cases, alternative methods for unlocking the drive need to be employed, refer section 10.4.4

Save Password: Passwords can be saved in various locations for convenience and security purposes.



Save Password pop up

Save Password to System Drive: On Windows systems, the system drive is typically labeled as “C:”. Check the “C:” checkbox to save the password in the system drive. This saved password can be further used by utilizing the “Read Password” feature for password authentication.

Save Password to USB Flash Drive: This involves saving password informa-

tion onto a USB flash drive. The USB flash drive can then be carried with you and accessed when needed to read the password from it.

Save Password to Custom Location: Custom locations refer to alternative storage locations outside of the default ones provided by the application, such as system drives and USB flash drives. Users may choose to save passwords in encrypted files stored on their local computer or external storage devices. Additionally, passwords can be stored in encrypted files on cloud storage services such as Dropbox, Google Drive, or iCloud.

Note

- ▶ Opal Lock ensures that the files are adequately encrypted and that strong security measures are in place to protect them. However, the application cannot directly read passwords saved in the custom location. Users can copy the password file from the custom location and save it onto a USB flash drive. The USB flash drive can then be used for password authentication when needed.

10.4.2 Password Authentication Guide

User has to authenticate the drive by submitting the set Password to use any feature of the Opal Lock Software once the drive is set up.

Enter Admin Password

Enter the admin password to view the audit log of the drive

SSD

✓ Admin

☐ Read password ?

OR

Enter Password

☐ Save Password ?

Submit

Enter Admin Password screen

Manual Authentication: Enter Password- Type the password associated with the encrypted drive into the designated text field within the Opal Lock Enter Admin Password interface.

Manual Authentication :Read Password Option- Read Password Checkbox: Check the “Read Password” checkbox within the Opal Lock Lite interface.

Auto Unlock- If the password is saved on a designated USB flash drive, Opal Lock can automatically unlock the encrypted USB drive when the designated USB flash drive is inserted into the computer.

Note

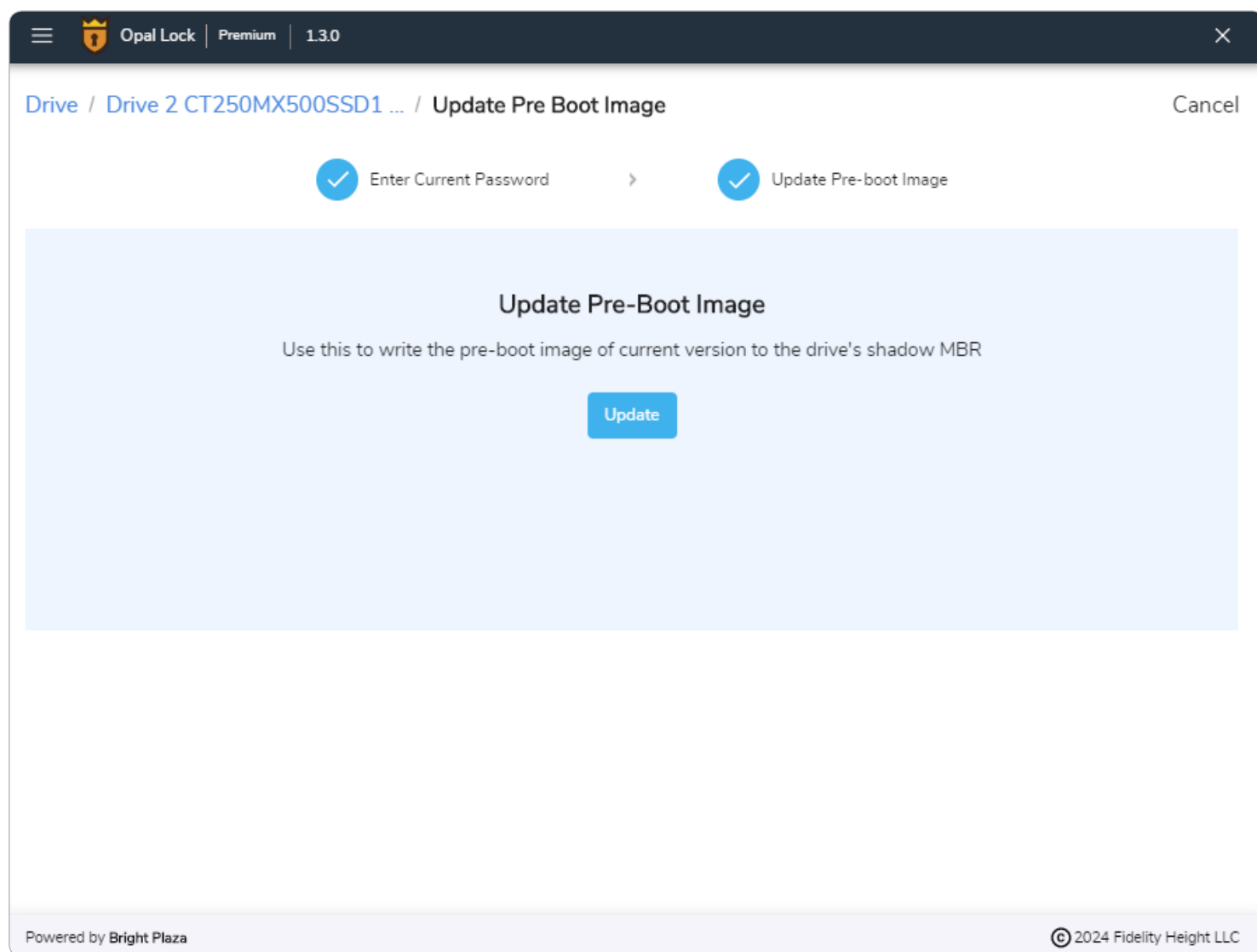
- This Automatic reading of the password implies only to Unlock the drive.

10.4.3 UPDATE PRE-BOOT IMAGE

This feature allows users to write the latest version of the pre-boot image to the drive's shadow MBR, provided that a password has already been set up for the drive.

Password Authentication: Authenticate the drive by submitting the set Password. Refer section 10.4.2

Click on the “Update” button to proceed with updating the pre-boot image.



Update Preboot Image screen

WARNING:

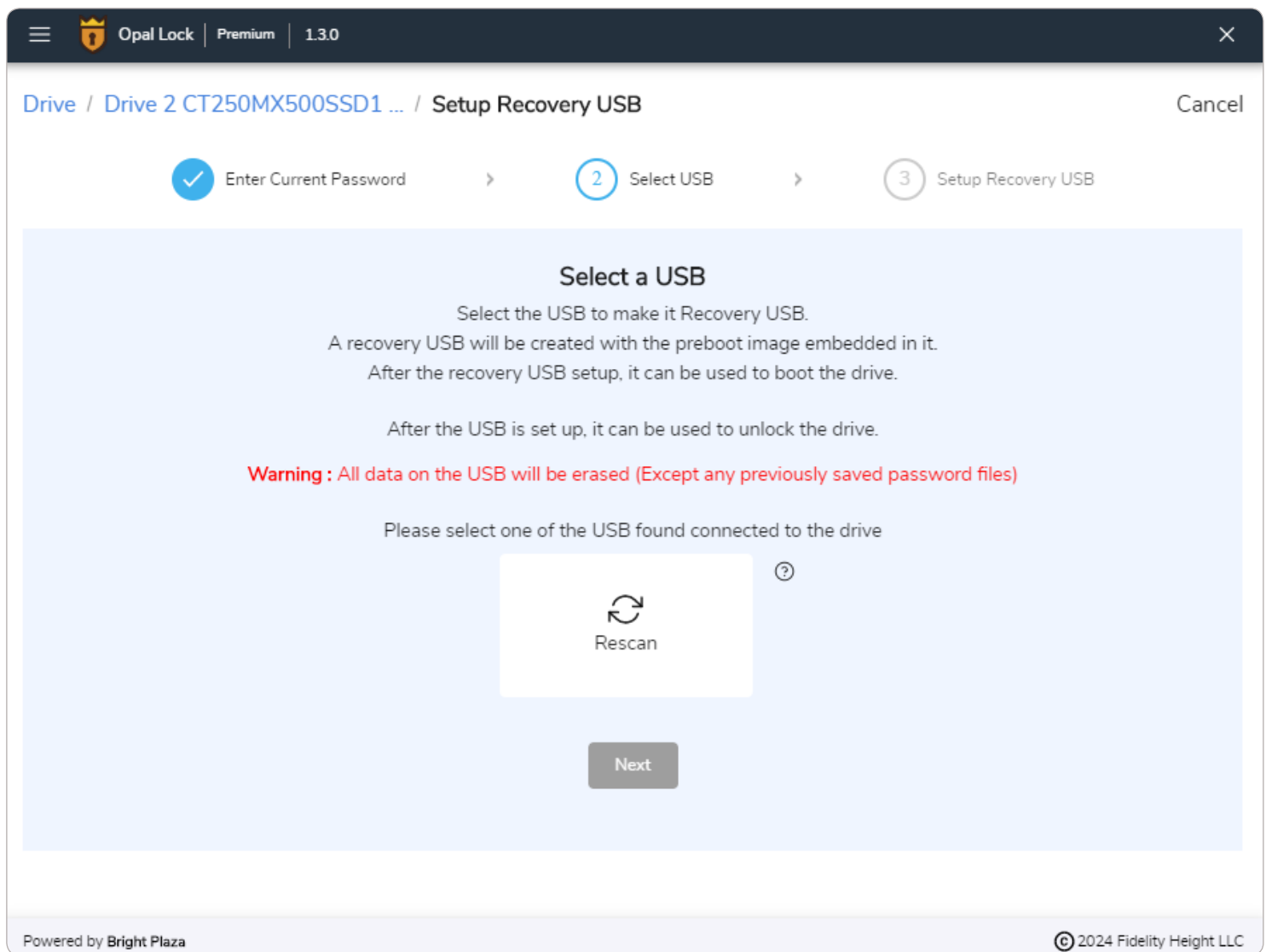
- It is crucial to ensure that a way to unlock the System drive is set up immediately after updating the pre-boot image. If a System drive becomes locked without any means of unlocking it, the drive will be rendered unusable, and all of its data will be lost.

10.4.4 SETUP RECOVERY USB

The Setup Recovery USB feature enables users to create a Recovery USB drive with the preboot image embedded on a USB flash drive. This serves as an alternative to writing the preboot image directly to a drive's shadow MBR.

Password Authentication: Authenticate the drive by submitting the set Password. Refer section 10.4.2

- Select the USB flash drive
- Proceed with setting up the USB flash drive as Recovery USB drive.



Select a USB screen_Recovery USB

Usage:

To unlock the drive using the bootable USB:

- Boot into the USB during system startup.
- Follow the prompts to unlock drives, similar to unlocking with the preboot image on the shadow MBR.

Note

- ▶ The drive selected during USB setup must be present in the system when booting into the USB for verification and usability.
- ▶ Setting up a Recovery USB does not remove any already saved passwords in the USB flash drive used to create the Recovery USB.

10.4.5 CHANGE DRIVE PASSWORD

Opal Lock provides the option to change the password set up on a drive. Follow these steps to change the drive password:

Password Authentication: Authenticate the drive by submitting the set Password. Refer section 10.4.2

Opal Lock | Premium | 1.3.0

Drive / [Drive 2 CT250MX500SSD1...](#) / Change Drive Password Cancel

Change Drive Password

Enter the current password for the drive and then enter a new password



☐ Read password ?

OR

Enter Current Password

Enter New Password

Confirm Password

Enter password with minimum eight characters, at least one uppercase letter, one lowercase letter, one number and one special character (ex = !"#\$%&'()*+,-./:;<=>?@[!^_{}~)

Change password

Powered by Bright Plaza © 2024 Fidelity Height LLC

Change Drive Password screen

- Enter the current password.
- Enter the new password.
- Confirm the new password.

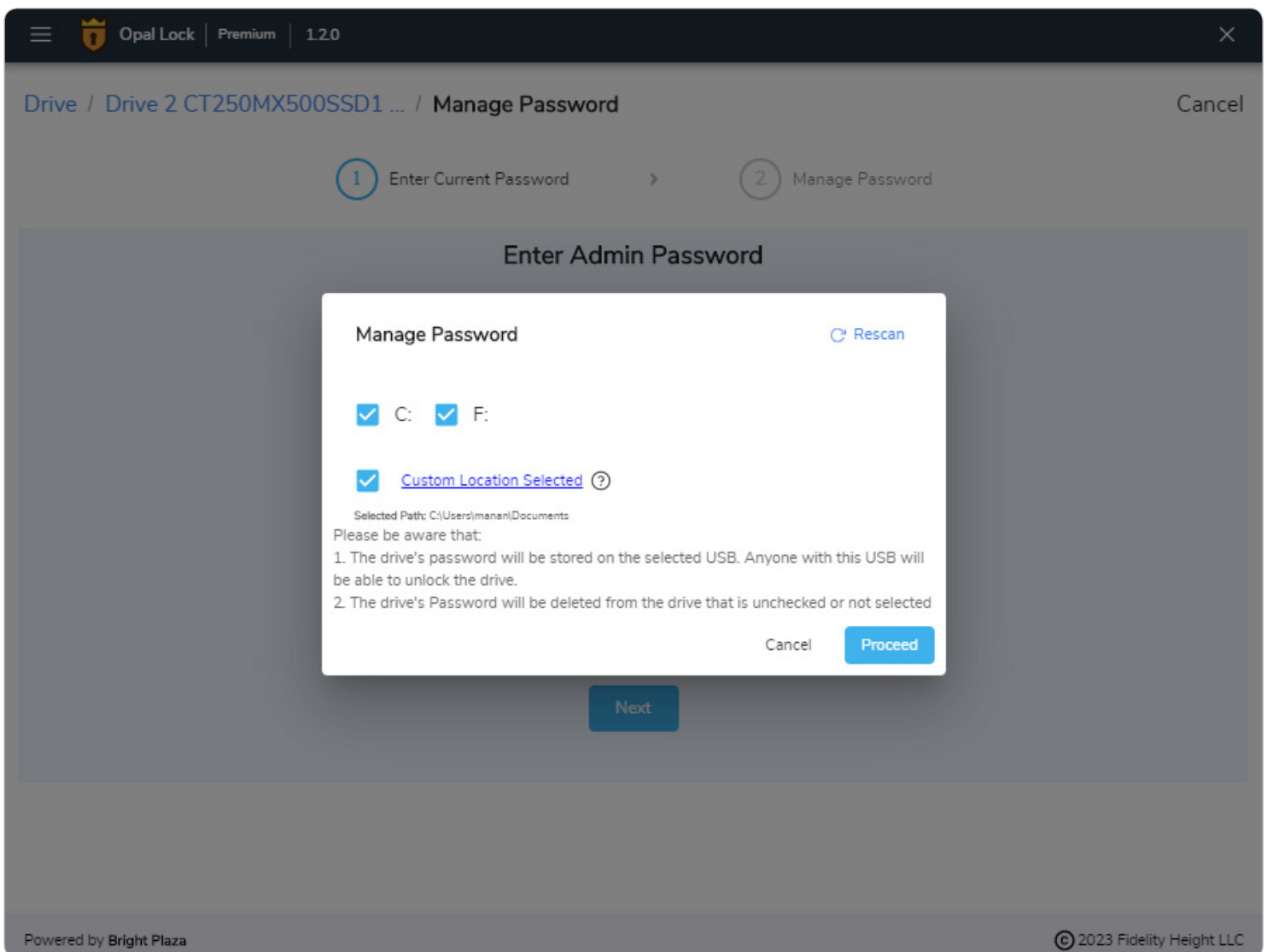
10.4.6 MANAGE PASSWORD

The Manage Password feature allows you to save and remove the Admin Password from USB flash drives and the system drive. Here's how you can manage passwords:

Password Authentication: Authenticate the drive by submitting the set Password. Refer section 10.4.2

Password Management:

- To save the Admin Password: Check the checkbox corresponding to the location where you want to save the password (USB flash drive or system drive).
- To remove the Admin Password: Uncheck the checkbox corresponding to the location from which you want to remove the password.



Manage Password pop up

Note

- This feature can be used to Manage the Admin Password but not User Password

10.4.7 USER SETUP AND REMOVAL

USER PASSWORD SETUP :

With Premium versions of Opal Lock, you can set up a second password with limited authority, known as the User password. Here's how it works:

Authority of User Password:

- The User password has limited authority compared to the Admin password.
- Users with the User password can unlock the drive, access the drive's Audit Log, and change their own password.

Admin Password Requirement:

- Setting up and removing the User password requires the Admin password. Authenticate the drive by submitting the set Password. Refer section 10.4.2

Drive / Drive 2 CT250MX500SSD1 ... / Setup User Password Cancel

Setup User Password

Setting up a user password creates a second password with limited authority

User password can be used to unlock the drive and view audit log



☐ Read password ?

OR

Enter Admin Password

Enter User Password

Confirm User Password

Enter password with minimum eight characters, at least one uppercase letter, one lowercase letter, one number and one special character (ex = !"#\$%&'()*+,-./:;<=>?@[]^_{}~)

Setup User Password

Powered by Bright Plaza © 2024 Fidelity Height LLC

Setup User Password screen

10.5 Locking and Unlocking Drives

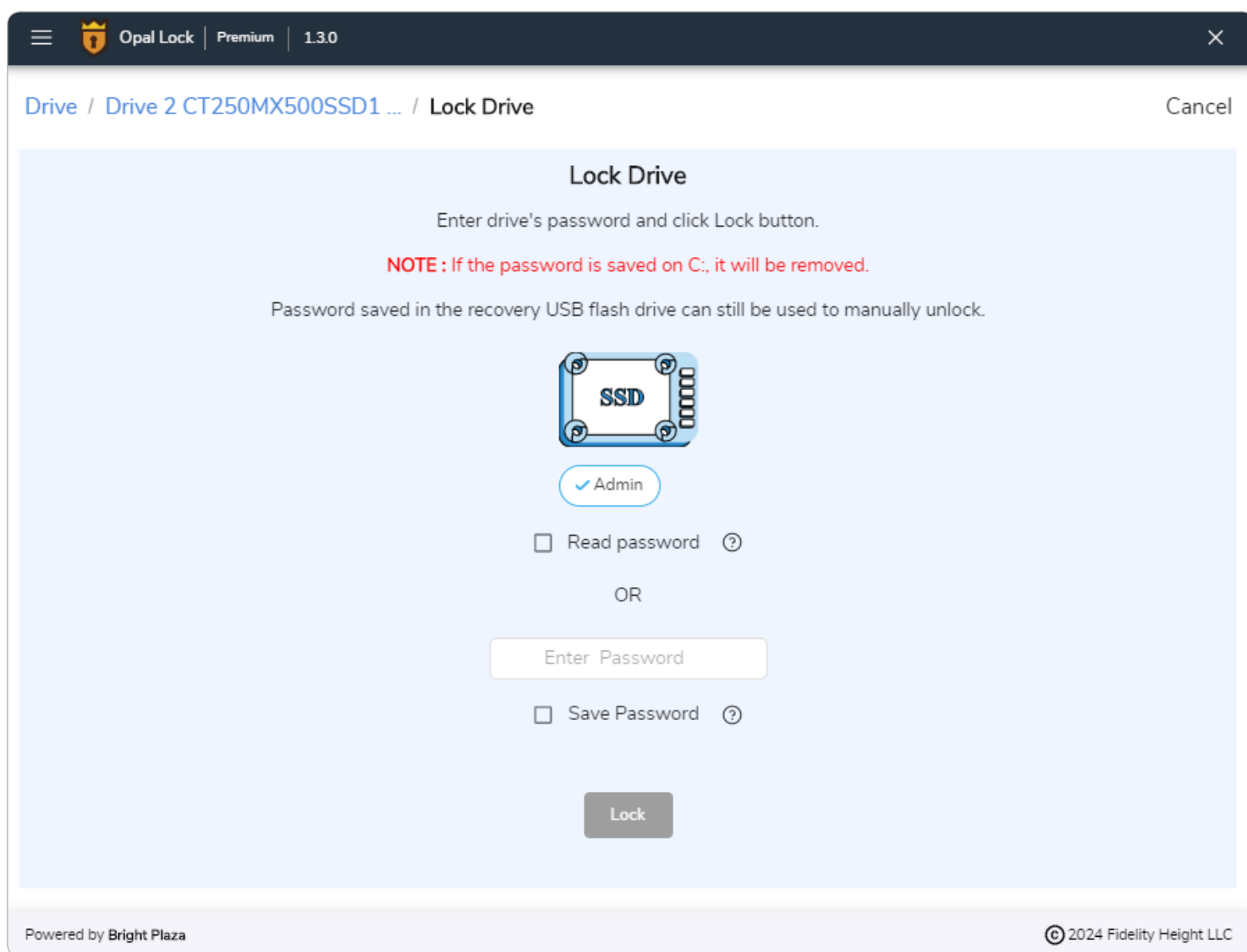
10.5.1 Locking Drives

Lock by Power Cycling:

- Internal Drive: Complete shutdown (power cycling) of the system is necessary.
- External Drive: Detach and reattach the drive to the system to initiate locking.

Lock by UI (User Interface):

- Submit the password on the lock screen to lock the drive without shutting down or power cycling. Authenticate the drive by submitting the set Password. Refer section 10.4.2



Lock Drive screen

10.5.2 System Drive Locking by UI

- Locking the system drive will crash the Windows OS, ensuring a high level of security.

10.5.3 Unlocking Drives

System Drive (Primary Internal Drive): Using Preboot Environment:

- A preboot environment with the preboot image written to the drive's Shadow MBR is employed.

- During system startup, the preboot environment automatically boots up.
- Users are prompted to submit the password to unlock the system drive, ensuring secure access. Refer section 16.3 for detailed information.

External/USB and Secondary Internal Drives:

- Users submit the password on the lock screen. Authenticate the drive by submitting the set Password. Refer section 10.4.2
- The password is automatically read if it's saved in the system drive or attached USB flash drive, streamlining the unlocking process.

Drive / Drive 2 CT250MX500SSD1 ... / Unlock Drive Cancel

Unlock Drive

Enter drive's password and click Unlock button.



☒ Admin

☐ Read password ?

OR

☐ Save Password ?

Powered by Bright Plaza © 2024 Fidelity Height LLC

Unlock Drive screen

10.6 MULTI DRIVE OPERATIONS

This setup allows users to manage multiple drives efficiently by applying actions such as locking, unlocking, changing passwords, and updating preboot images across all selected drives simultaneously.

10.6.1 Multi-Drive Setup

- With the Opal Lock application, users can set up multiple drives together.
- The admin password for all the drives will be the same.
- To set up multiple drives:
 - Check the checkboxes of the SSDs listed on the Home screen.
 - Click on the “Setup” option displayed at the bottom to create the setup for all the selected TCG drives.

Opal Lock | Premium | 1.2.0
×

Drives: 3
🔍
↻ Rescan Drives

Internal TCG Drives: 1

☒	Drive	Model Number	Serial Number	Setup	Status
☒	Drive 0	CT250MX500SSD1	2150E5F31740	No	

External TCG Drives: 2

☒	Drive	Model Number	Serial Number	Setup	Status
☒	Drive 1	Samsung SSD 980 250GB	S64BNU0WB01190P	No	
☒	Drive 2	Samsung SSD 860 EVO 250GB	S3Y9NX0N943293T	No	

Non TCG Drives: 0

There are no Non TCG Drives connected! [Rescan Drives.](#)

3 Drives Selected

Setup Drive

Powered by Bright Plaza
© 2024 Fidelity Height LLC

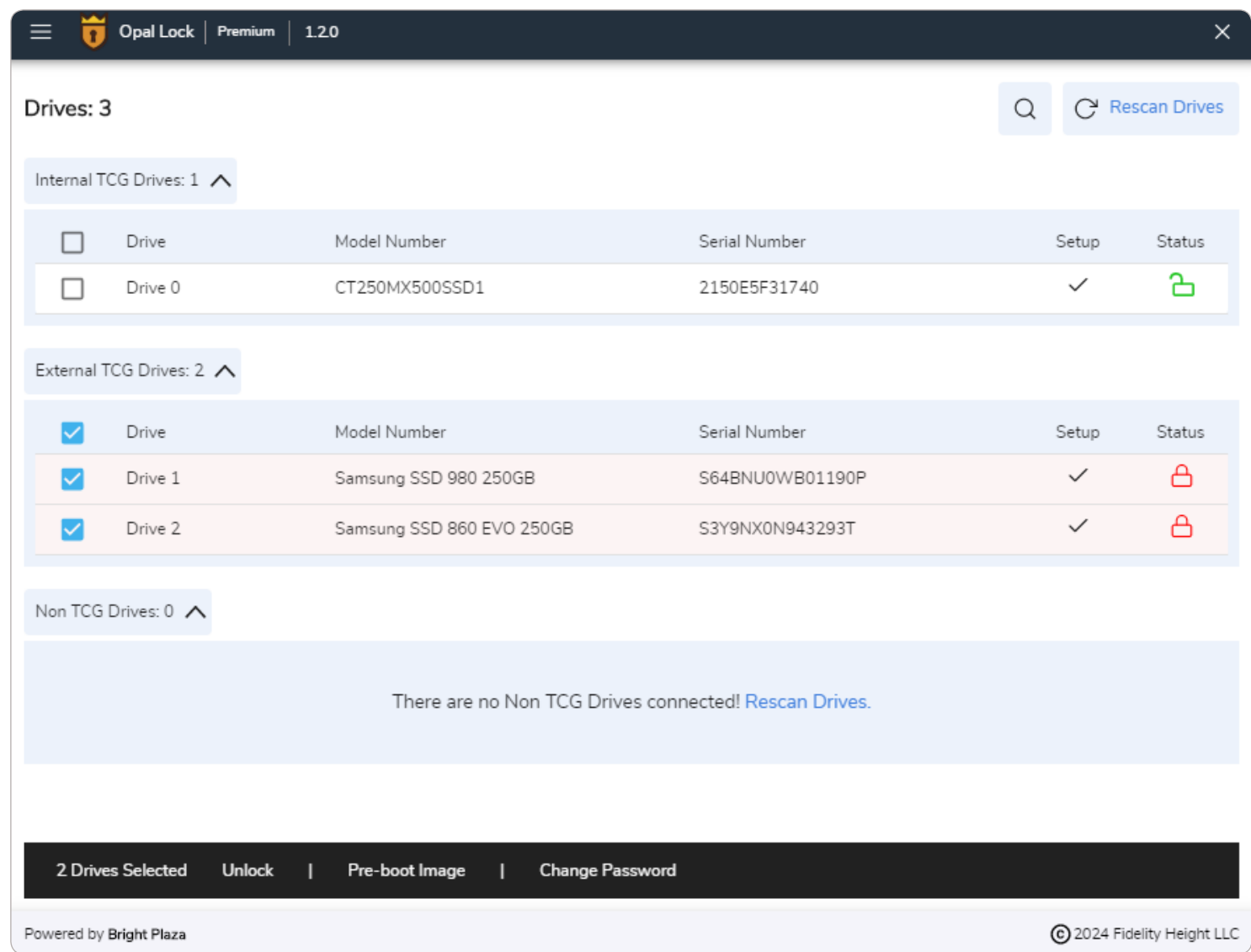
Home screen Multidrive Setup

Once the setup is created and the password for all drives is the same, users can perform the following actions on the multiple drives:

- Lock Drives
- Unlock Drives
- Change Password
- Update Preboot Image

10.6.2 Multi-Drive Lock

- Users can lock multiple drives simultaneously using the multi-drive lock feature.



Home screen Multidrive Operations

10.6.3 Multi-Drive Unlock

- Users can unlock multiple drives simultaneously using the multi-drive unlock feature.

Opal Lock | Premium | 1.2.0
✕

Drives: 3
🔍
🔄 Rescan Drives

Internal TCG Drives: 1

☒	Drive	Model Number	Serial Number	Setup	Status
☒	Drive 0	CT250MX500SSD1	2150E5F31740	✓	

External TCG Drives: 2

☒	Drive	Model Number	Serial Number	Setup	Status
☒	Drive 1	Samsung SSD 980 250GB	S64BNU0WB01190P	✓	
☒	Drive 2	Samsung SSD 860 EVO 250GB	S3Y9NX0N943293T	✓	

Non TCG Drives: 0

There are no Non TCG Drives connected! [Rescan Drives.](#)

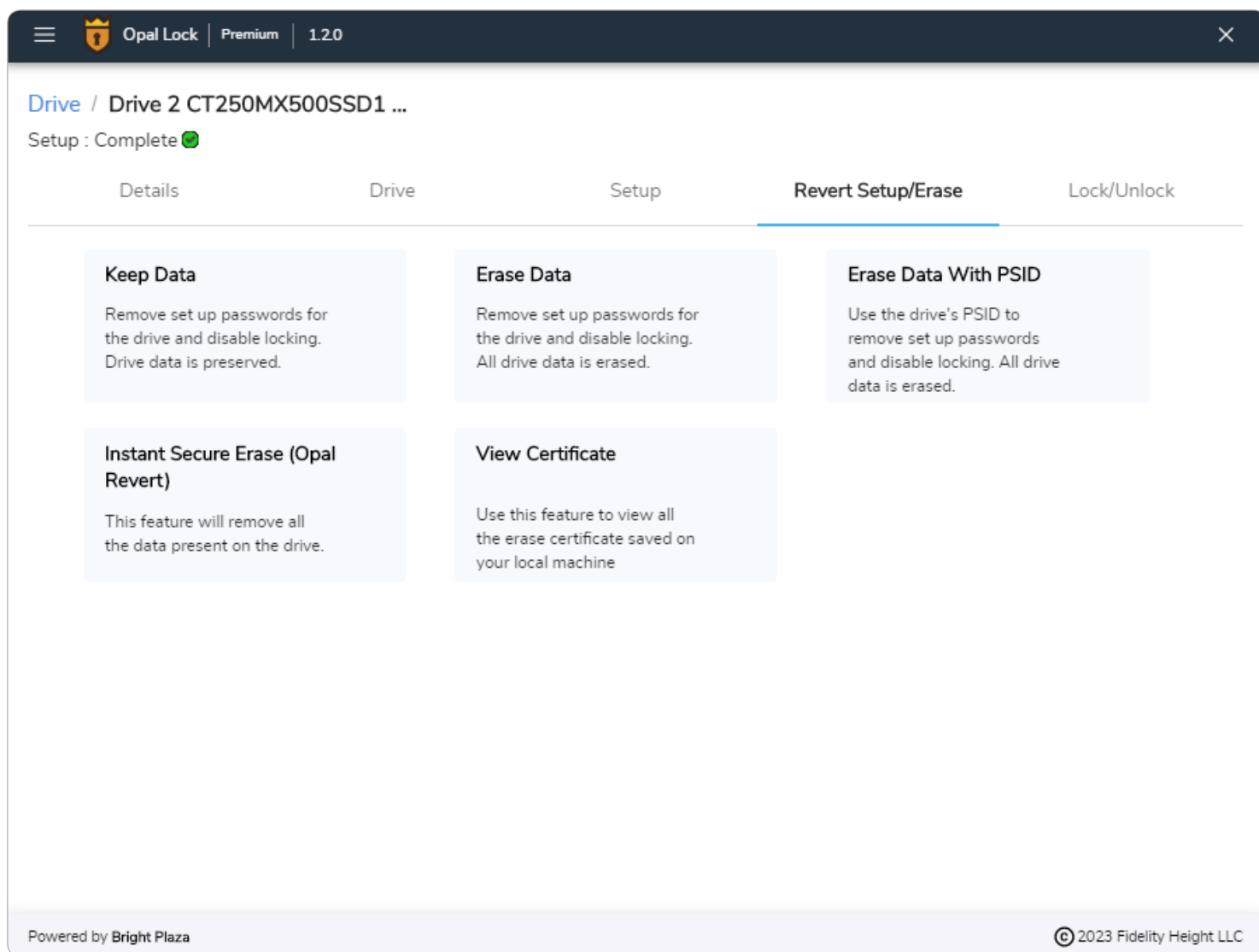
3 Drives Selected | Lock | Pre-boot Image | Change Password

Powered by Bright Plaza
© 2024 Fidelity Height LLC

Home screen_Multidrive Unlocking

10.7 Revert Setup/Erase User Guide

The Revert Setup function is designed to disable the locking mechanism and reset the password to the Manufacturer Storage Identifier (MSID). Once this process is completed, the drive will no longer lock when power cycled, eliminating the need for unlocking on startup. It's important to note that after any of the following options are executed (except for the "View Certificate" option), the drive can be set up again. There are four options available for removing the lock, each serving different purposes and levels of data protection.



Revert Setup Erase screen

IMPORTANT NOTE I: Data Management Options:

- ▶ After setting up the password for the drive, both “Keep Data” and “Erase Data” options will be enabled. These features require Admin Password authentication for execution.
- ▶ **Password Authentication:** Authenticate the drive by submitting the set Password. Refer section 10.4.2
- ▶ It's noted that certain TCG versions, like Pyrite, may support only keeping data and not erasing data

IMPORTANT NOTE II: View Certificate Option:

- ▶ The “View Certificate” option allows users to view all the certificates generated till date.
- ▶ It’s important to note that all these certificates will be removed from the system when the Opal Lock application is uninstalled.

10.7.1 Revert Setup and Keep Data

With this option, the drive’s data will not be touched. The locking mechanism will be disabled and the password will be reset to the MSID. After this has been executed, the drive will not be locked when powered down, all data on the drive will become accessible, and for boot drives, booting into the drive will result in booting into the installed operating system normally.

10.7.2 Revert Setup and Erase Data with Password

Proceeding with this option resets the password and also has the effect of resetting the drive to manufacturer settings, which will cryptographically erase all data on the drive.

WARNING

- ▶ Removing the lock with erasing data will reset the entire drive to manufacturer settings. All existing data on the drive will be deleted with no way to recover it. Do not use Revert Setup & Erase Data if the drive’s data is still needed.

10.7.3 Revert Setup and Erase Data with PSID

The PSID can be used to revert the drive to manufacturer settings if the password has been forgotten or lost. The drive’s PSID can be found on the drive label.



PSID

10.7.4 Instant Erase

- Instant Secure Erase is the process of completely removing all data from a TCG Storage device.
- Opal Lock uses the TCG Opal crypto erase method, ensuring that your data is instantly and securely wiped in a matter of seconds.
- Unlike traditional methods that might take hours, Opal Lock completes the process in a few seconds, providing both speed and efficiency.

(I) Instant Erase when Drive is not Setup

- Password Authentication- Password Authentication is not required as the drive is not set up.
- Enter “Yes” key word in the text field and click on “Erase” button

(II) Instant Erase when Drive is Setup

- Admin Password radio button will come selected by default.
- Select PSID radio button if Admin Password is not known.
- Enter Admin Password in the text field if the “Admin Password” radio button is selected OR Enter PSID in the text field if “PSID” radio button is selected.
- Click on the Instant Erase button.
- Type “Yes” keyword in the text field to confirm and click on Erase button

10.7.5 Certificate of Sanitization

Opal Lock introduces the Certificate of Sanitization—a feature that generates a verified certificate post-data erasure. This certificate offers you peace of mind by providing concrete proof of the data eradication process and compliance, bolstering trust in your data management practices.

Certificate of Sanitization can be downloaded to the system for future use and users can view these certificates in future as well.

Note

- These certificates will be removed from the system when the app is uninstalled.

11. STANDARD VERSION GUIDE

The Standard License version of Opal Lock offers comprehensive features with the support for both External and Internal drives. Below are the key features and guidelines:

Standard Version Inclusions(Supported Functionalities):

- ◆ **Drive Setup (Drive Encryption Enablement):** Users have the option to enable locking of the drives using the “Setup Drive” feature, ensuring data security.
- ◆ **Drive Locking:** Users can activate the locking mechanism for their drives either by authenticating the password through the app’s user interface or by power cycling the drive.
- ◆ **Drive Unlocking:** Encrypted drives can be unlocked by users to access their stored data.
- ◆ **Password Modification and Management:** Users can modify drive passwords using the “Change Password” feature and manage passwords stored in various locations through the “Manage Password” feature.
- ◆ **Revert Setup (Disabling Locking Mechanisms)/Data Erasure:** If necessary, users can revert drive setups to disable the locking mechanism and users can also erase the drive data. These actions reset the password to the default admin password, which is the Manufacturer Storage Identifier (MSID).
- ◆ **Shadow MBR Writing:** Users can write preboot images onto Opal drives’ Shadow MBR, thereby enhancing security and boot functionalities.

Device Support:

The Standard version supports both Internal and External Opal Drives, offering versatility in drive compatibility.

Standard Version Exclusions(Unsupported Functionalities):

- ◆ **Second/User Password:** Users cannot set a second password (User Password) with limited authority in the Standard version.
- ◆ **Multidrive Operations:** Multiple drives cannot be set up together with a single click in the Standard version, necessitating individual setup procedures for each drive.

Understanding these features and limitations will enable users to effectively manage their Opal Drives using the Standard License version of Opal Lock.

12. USB VERSION GUIDE

The USB version of Opal Lock provides essential functionalities for managing up to five USB-mounted Opal Drives.

USB Version Inclusions(Supported Functionalities):

1. **Drive Setup (Drive Encryption Enablement):** Users have the option to enable locking of the drives using the “Setup Drive” feature, ensuring data security.
2. **Drive Locking:** Users can activate the locking mechanism for their drives either by authenticating the password through the app’s user interface or by power cycling the drive.
3. **Drive Unlocking:** Encrypted drives can be unlocked by users to access their stored data.
4. **Password Modification and Management:** Users can modify drive passwords using the “Change Password” feature and manage passwords stored in various locations through the “Manage Password” feature.
5. **Revert Setup (Disabling Locking Mechanisms)/Data Erasure:** If necessary, users can revert drive setups to disable the locking mechanism and users can also erase the drive data. These actions reset the password to the default admin password, which is the Manufacturer Storage Identifier (MSID).

USB Version Exclusions(Unsupported Functionalities):

1. **Limited Device Support:** Only USB Opal drives are supported; other drive types are not compatible.
2. **Shadow MBR Writing:** The USB version does not support writing preboot images on Opal drive’s Shadow MBR.
3. **Second Password:** Users cannot set a second password (User Password) with limited authority.
4. **Multidrive Setup:** Multiple drives cannot be set up simultaneously with a single click, requiring individual setup procedures for each drive.

Understanding these limitations ensures users can effectively utilize Opal Lock according to its capabilities.

13. OPAL LOCK LITE USE CASE: DATA ACCESS ON ANOTHER SYSTEM

- ◆ **Scenario:** Accessing Data from a USB Drive Protected with Opal Lock Regular License on Another System
- ◆ **User Situation:** The user possesses a USB drive that has been secured with Opal Lock using a Regular License on their primary system.
- ◆ **Need for Access:** The user needs to access the data stored on this USB drive on another system, which does not have the Opal Lock Regular License installed.
- ◆ **Utilizing Opal Lock Lite:** Instead of acquiring a Regular License for the new system, the user opts to use Opal Lock Lite, a free version of Opal Lock, to unlock the secured USB drive.

14. OPAL LOCK LITE FUNCTIONALITY

14.1 Opal Lock Home Screen Display and Drive Detection

- The Opal Lock home screen provides information about the drives detected on the system. This display includes details such as drive setup status, lock status, model number, and serial number.
- If a drive is set up, a tick (✓) will be displayed under the “Setup” column for that drive. If the drive is not set up, “No” will be displayed under the “Setup” column.
- A red lock icon indicates that the drive is set up and locked, while a green unlock icon indicates that the drive is set up and unlocked.
- Each drive is listed by its drive name according to the system. On Windows, drives are listed as physical drives (e.g., Drive1). TCG drives are listed up to the drive limit determined by the version being used.
- The “Rescan Drives” button allows the system to rescan the drives and query the drives to acquire updated status information for display on the application. If the total number of detected TCG drives exceeds the drive limit, any drives that were previously listed and are still present will be prioritized for listing ahead of other drives.
- The user connects the Opal-locked USB drive to the new system.
- Opal Lock Lite automatically detects the connected external USB drive that adheres to the Opal standard.

The screenshot displays the Opal Lock Lite Home screen. At the top, a dark blue header bar contains a menu icon, the text 'Opal Lock | Lite | 1.3.1', and a close icon. Below the header, the main content area is titled 'Drives: 3' on the left and features a search icon and a 'Rescan Drives' button on the right. The drives are categorized into two sections: 'Internal TCG Drives: 1' and 'External TCG Drives: 2'. Each section contains a table with columns for Drive, Model Number, Serial Number, Setup, and Status.

Drive	Model Number	Serial Number	Setup	Status
Drive 0	Samsung SSD 860 EVO 250GB	S3Y9NX0N943293T	No	

Drive	Model Number	Serial Number	Setup	Status
Drive 1	Samsung SSD 980 250GB	S64BNU0WB01190P	✓	
Drive 2	CT250MX500SSD1	2150E5F31740	✓	

At the bottom of the screen, a light blue footer bar contains the text 'Powered by Bright Plaza' on the left and '© 2024 Fidelity Height LLC' on the right.

Opal Lock Lite Home screen

14.2 Drive Unlocking

- The user selects the detected USB drive from within the Opal Lock Lite interface.
- By clicking on the red Lock icon, Opal Lock Lite opens the Unlock screen for the respective drive

Drive 2 CT250MX500SSD1 ... / Unlock Drive

Unlock Drive

Enter drive's password and click Unlock button.



☐ Read password ?

OR



Opal Lock Lite Unlock Drive screen

14.3 Authentication

- The user authenticates the drive by entering the correct password associated with the Opal-locked USB drive or by reading the password from the System drive or attached USB flash drive. Refer section 10.4.2

14.4 Access Granted

- Upon successful authentication, Opal Lock Lite unlocks the USB drive, allowing the user to access its contents on the new system.

14.5 Data Utilization:

- With the USB drive unlocked, the user can freely view, modify, or transfer files stored on the drive as needed.

14.6 Limitations:

- Opal Lock Lite exclusively supports unlocking external TCG drives connected via USB ports.
- It does not offer functionality for managing or unlocking internal drives.

14.7 Completion:

- Once the user has finished accessing the data on the USB drive, they can safely eject the drive and disconnect it from the system.

In this scenario, Opal Lock Lite serves as a convenient and cost-effective solution for users needing to access data from Opal-secured USB drives on systems without the Regular License installed, providing essential drive unlocking capabilities without the need for additional licensing.

15. PREBOOT AUTHENTICATION (PBA) VERSION USE CASE

The Opal Lock PBA version serves as a vital component in the drive encryption and security ecosystem, providing users with a reliable means of unlocking locked system drives and accessing their data. By leveraging the preboot image and authentication interface, users can seamlessly regain control of their systems while ensuring data integrity and security.

Opal Lock PBA version serves as a mini-operating system designed primarily for unlocking locked primary internal/system drives. This use case is especially useful when a user has locked their system drive using Opal Lock encryption technology and needs to regain access to their system.

User Situation:

1. **Locked System Drive:** The user has encrypted and locked their primary internal/system drive using Opal Lock encryption.
2. **Preboot Image Written:** The preboot image required for Opal Lock PBA version is written on the drive's shadow MBR, allowing the system to access it during boot-up.
3. **Recovery USB Setup:** Alternatively, the user may have set up a recovery USB containing the Opal Lock PBA version, providing an external means of accessing the drive.

Need for Access: Opal Lock PBA version provides a critical pathway for unlocking system drives, enabling the user to boot into the Windows operating system and access their data.

Process:

1. **Preboot Image Access:** If the preboot image is written on the system drive's shadow MBR, the system accesses it during the boot process. System reads the preboot image from the visible Shadow MBR of the locked drive and boot the Opal Lock PBA version.
2. **Opal Lock PBA Interface:** The Opal Lock PBA version interface is presented to the user, prompting them to authenticate with the drive's password for unlocking.
3. **Password Authentication:** The user inputs the required password through the interface to authenticate and unlock the drive.
4. **Drive Unlocking:** Upon successful authentication, Opal Lock PBA unlocks

the encrypted system drive, allowing the system to proceed with booting into the Windows operating system.

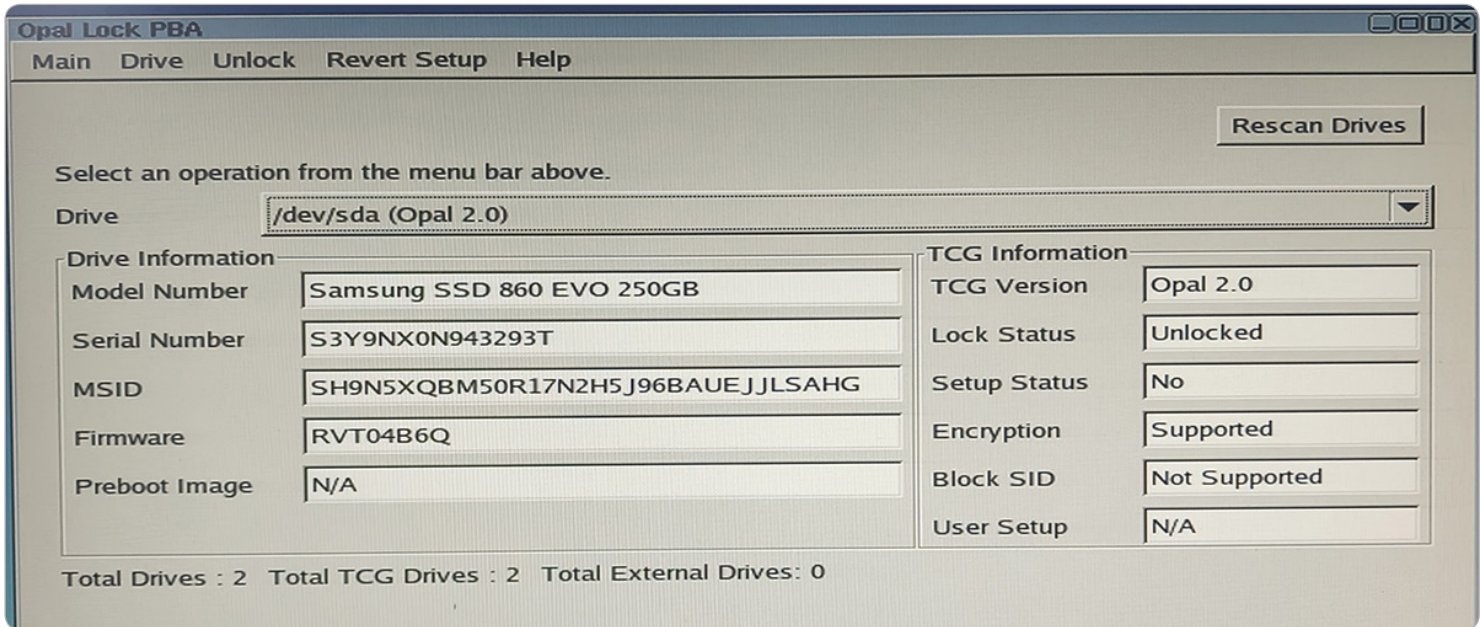
5. **Windows Access:** With the drive successfully unlocked, the system proceeds to boot into Windows, granting the user access to their data and system resources.

Benefits:

1. **Data Security:** Opal Lock encryption ensures robust security for the system drive, protecting sensitive data from unauthorized access.
2. **Ease of Use:** Opal Lock PBA version provides a user-friendly interface for drive unlocking, simplifying the process for end-users.
3. **Recovery Options:** The availability of Opal Lock PBA via the system drive's shadow MBR or a recovery USB offers flexibility in accessing locked drives, even in the event of system failures or password issues.

16. PBA VERSION FUNCTIONALITIES

16.1 Opal Lock PBA Screen Display and Drive Detection



PBA Dashboard screen

The Opal Lock PBA version home screen provides following information about the drives detected on the system :

Drive Identification:

- Displayed by their drive names according to the system, including physical drives

Drive Information:

- Model number, serial number, manufacturer, and firmware version are displayed for each drive.

MSID (Manufacturer Secure ID):

- Default password or authentication key of the drive before it's set up. Resetting the drive's password restores it to the MSID.

Preboot Image:

- Displays the version of the preboot image written to the drive's shadow

MBR. It indicates if the drive supports MBR shadowing, and whether the preboot image has been written.

TCG Version:

- Indicates the TCG (Trusted Computing Group) specification version supported by the drive.

Lock Status:

- Indicates whether the drive is currently locked or unlocked.

Setup Status:

- Indicates whether the drive has been set up using Opal Lock. If not, it displays “No” and if drive is setup, it displays “Yes”

Encryption:

- Indicates whether the selected drive supports full-disk encryption. Pyrite is an exception that doesn’t require encryption.

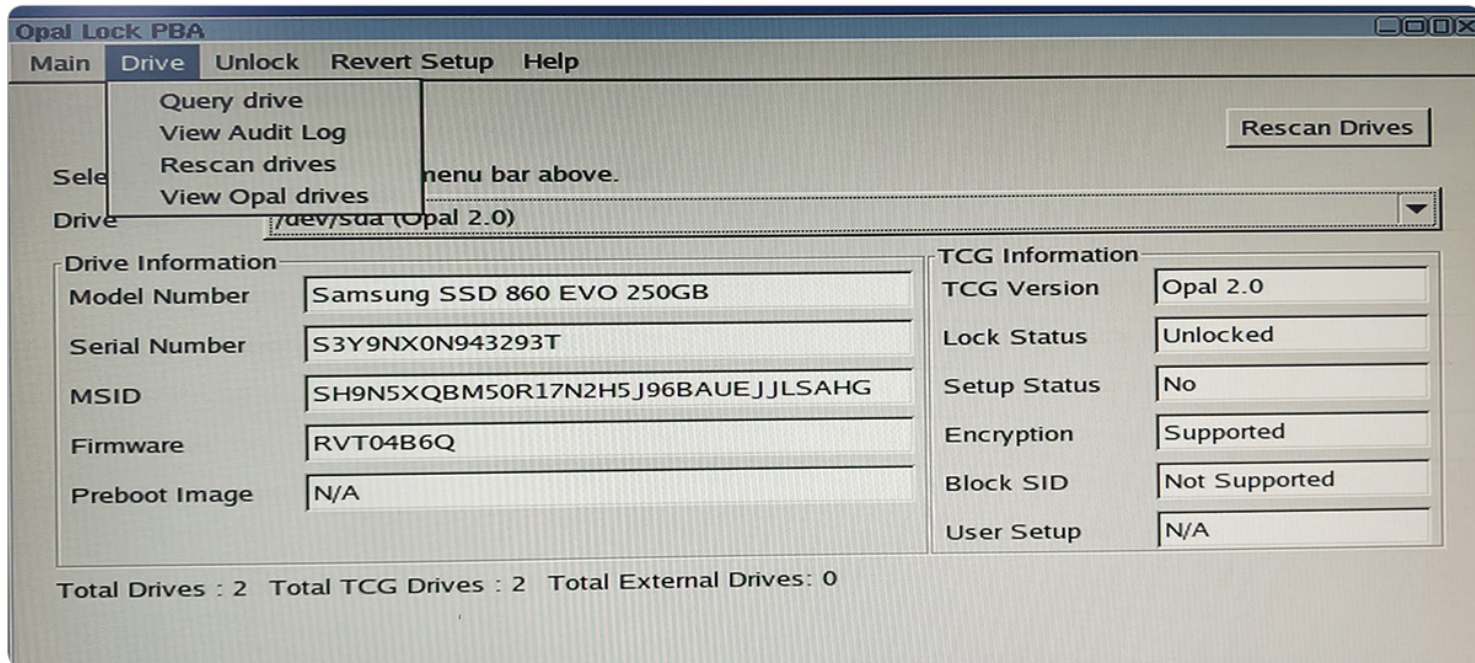
Block SID:

- A feature in some TCG drives that blocks attempts to change the authentication key. It needs to be disabled for setting up the drive using Opal Lock. This can be done in the BIOS before executing the Block SID command.

16.2 Drive

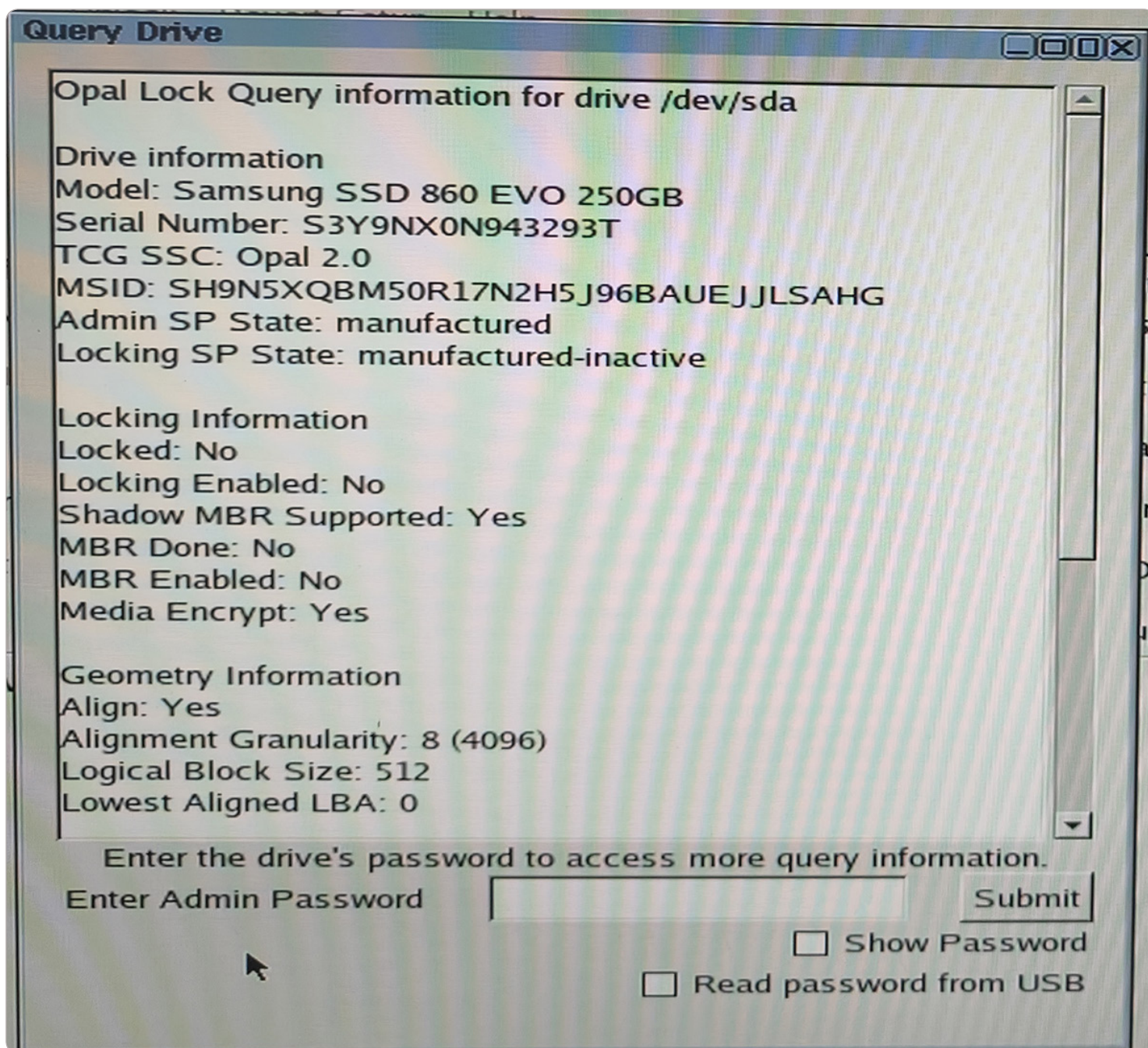
This segment provides insights into the features relevant to managing data on TCG (Trusted Computing Group) drives. Determining the TCG compliance of a drive is simplified by checking for a PSID (Physical Secure ID) displayed on the drive’s label. It’s important to acknowledge that Opal Lock functionality is standard across all TCG drives. However, it’s prudent to acknowledge that certain TCG versions, such as Pyrite and Enterprise, may restrict certain operations.

16.2.1 Query Drive



PBA Drive menu

- Click on the Query drive option from the “Drive” menu. Refer to the above screenshot.
- The “Query Drive” function initiates a window presenting comprehensive information regarding the drive. Within this window, users have the option to input the drive’s Admin password, granting access to additional, password-protected details.



PBA Query Drive screen

16.2.2 Audit Log

- Click on the View Audit Log option from the “Drive” menu.
- The Audit Log can be accessed via the View Audit Log button using the drive’s password.

Drive: /dev/sdb (Opal 2.0)

Drive Information		TCG Information	
Model Number	Crucial_CT128M550SSD1	TCG Version	Opal 2.0
Serial Number	14270C8A6F17	Lock Status	Locked
MSID	micron	Setup Status	Yes
Firmware	MU01	Encryption	Supported
Preboot Image	N	Block SID	Not Supported
		User Setup	No

Total Drives : 2 Total TCG Drives : 2 Total External Drives: 0

A drive's audit log stores a log of actions done on the drive by this application.
Enter the drive's password to access its audit log.

Enter Password:

☐ Read password from USB
☐ Save to USB
☐ Show Password

[View Audit Log](#) [Cancel](#)

PBA Audit Log screen

- Opal Lock stores an event log embedded within each drive called the Audit Log which logs operations done on the drive such as setting up the password, authentication attempts, etc.

Level	Date and Time	Event ID	Event Description
Information	2024/06/05 16:26:29	22	Audit Log accessed
Information	2024/06/05 16:26:29	3	Admin Authenticated
Error	2024/06/05 16:26:19	40	Audit Log Access Failed
Error	2024/06/05 16:26:19	4	Invalid Admin Password
Information	2024/06/05 16:23:54	21	Query information accessed
Information	2024/06/05 16:23:54	3	Admin Authenticated
Information	2024/06/03 19:43:39	15	Drive unlocked
Information	2024/06/03 19:43:39	3	Admin Authenticated
Information	2024/06/03 19:43:39	25	Admin Password read from USB
Error	2024/06/03 19:01:47	33	Drive unlock failed
Error	2024/06/03 19:01:47	4	Invalid Admin Password
Error	2024/06/03 16:38:33	40	Audit Log Access Failed
Error	2024/06/03 16:38:33	4	Invalid Admin Password
Error	2024/06/03 15:58:20	40	Audit Log Access Failed
Error	2024/06/03 15:58:20	4	Invalid Admin Password
Information	2024/06/03 15:57:02	22	Audit Log accessed

[View all entries](#)
[View Warnings & Errors](#)
[View Errors](#)
[Close](#)

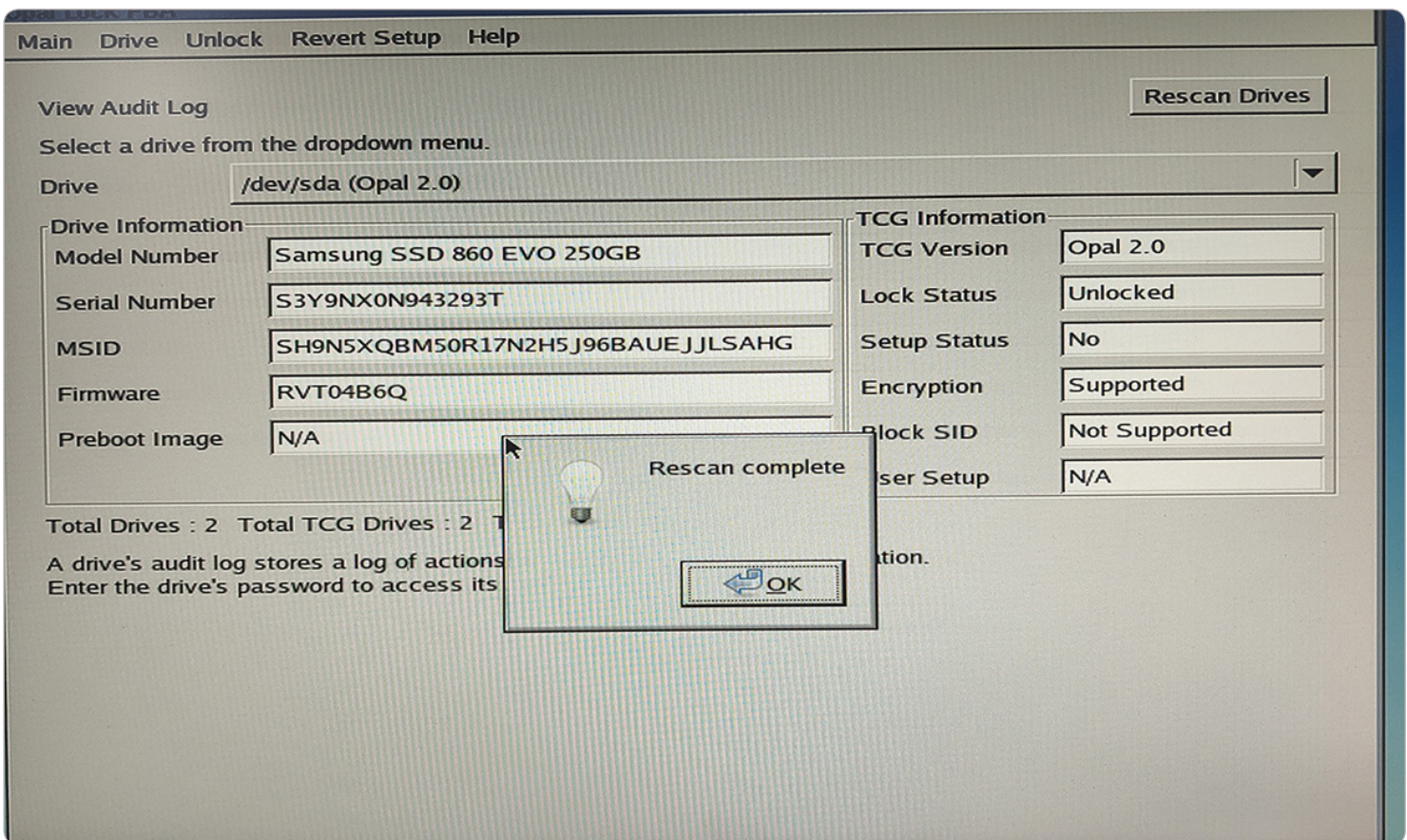
PBA Audit Log events

Note

- ▶ When setting up a drive, Opal Lock also sets up an audit user, which is a separate, internal password that writes events to the audit log.
- ▶ Audit Log requires that the drive supports Datastore. Some TCG versions like Enterprise do not support Datastore.

16.2.3 Rescan drives

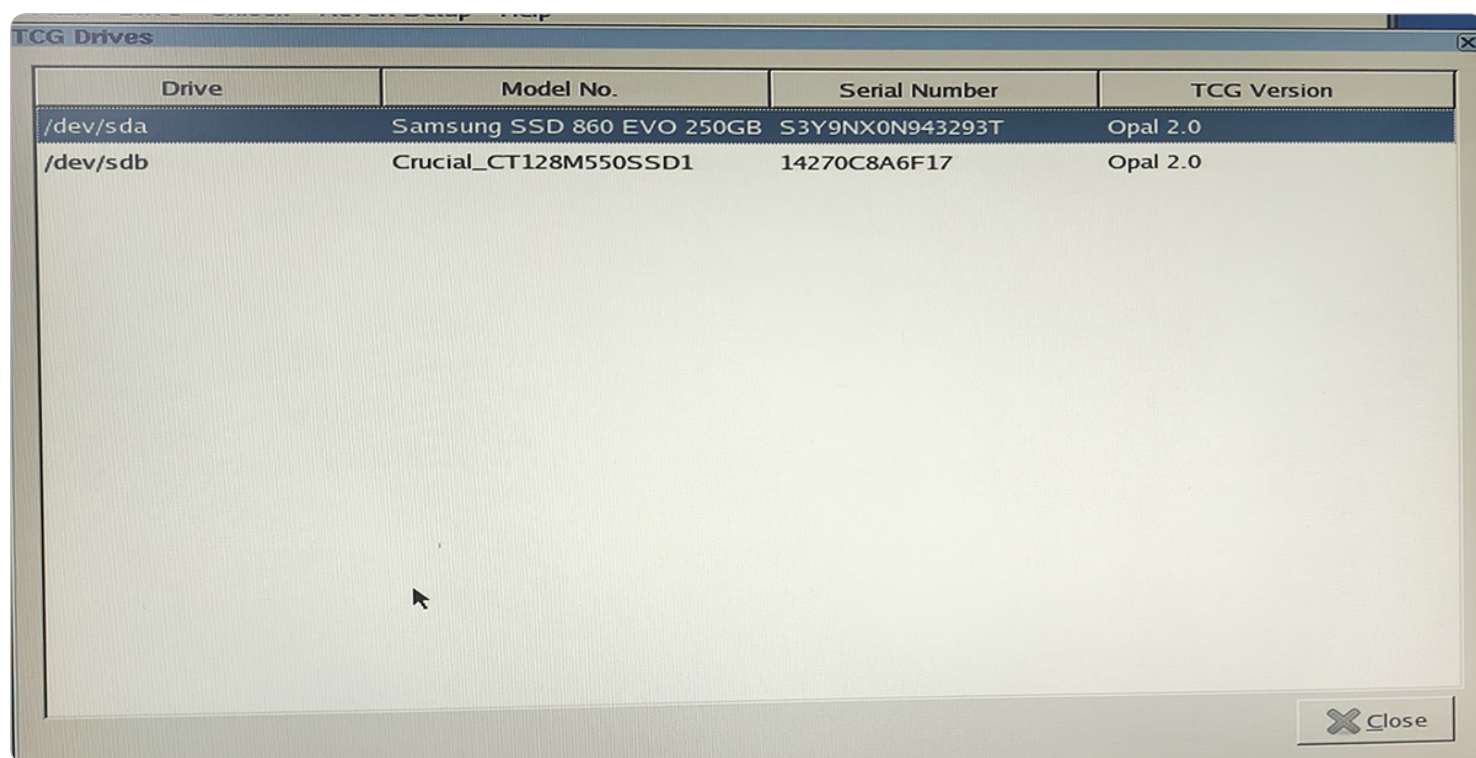
Rescan Drives makes the system rescan the drives that are mounted, and then queries the drives to acquire updated status information to display on the application. In the case that the total number of detected TCG drives exceeds the drive limit, any drives that were previously listed and are still present will be prioritized for listing ahead of other drives.



PBA Rescan

16.2.4 View Opal Drives

The “View TCG Drives” function prompts a window to appear, presenting a comprehensive list of all TCG drives detected within the system. This list includes pertinent details such as the drive’s model and serial numbers, alongside their corresponding TCG version.



Drive	Model No.	Serial Number	TCG Version
/dev/sda	Samsung SSD 860 EVO 250GB	S3Y9NX0N943293T	Opal 2.0
/dev/sdb	Crucial_CT128M550SSD1	14270C8A6F17	Opal 2.0

PBA View Opal Drives screen

16.3 Unlock

These sections detail the process of manually unlocking drives in the preboot environment and the option for auto-unlocking drives with stored passwords. These sections also provide a clear explanation of how users can manually unlock drives and how Opal Lock can automatically unlock them using stored password files, enhancing user convenience and system accessibility.

Drive: /dev/sdb (Opal 2.0)

Drive Information		TCG Information	
Model Number	Crucial_CT128M550SSD1	TCG Version	Opal 2.0
Serial Number	14270C8A6F17	Lock Status	Locked
MSID	micron	Setup Status	Yes
Firmware	MU01	Encryption	Supported
Preboot Image	FL.1.3.9	Block SID	Not Supported
		User Setup	No

Total Drives : 2 Total TCG Drives : 2 Total External Drives: 0

Preboot Unlock unlocks a drive for bootup.
Enter the drive's password and press 'Preboot Unlock'
Afterwards, reboot into the unlocked drive.

Enter Password:

☐ Read password from USB
☐ Save to USB
☐ Show Password

PBA Unlock

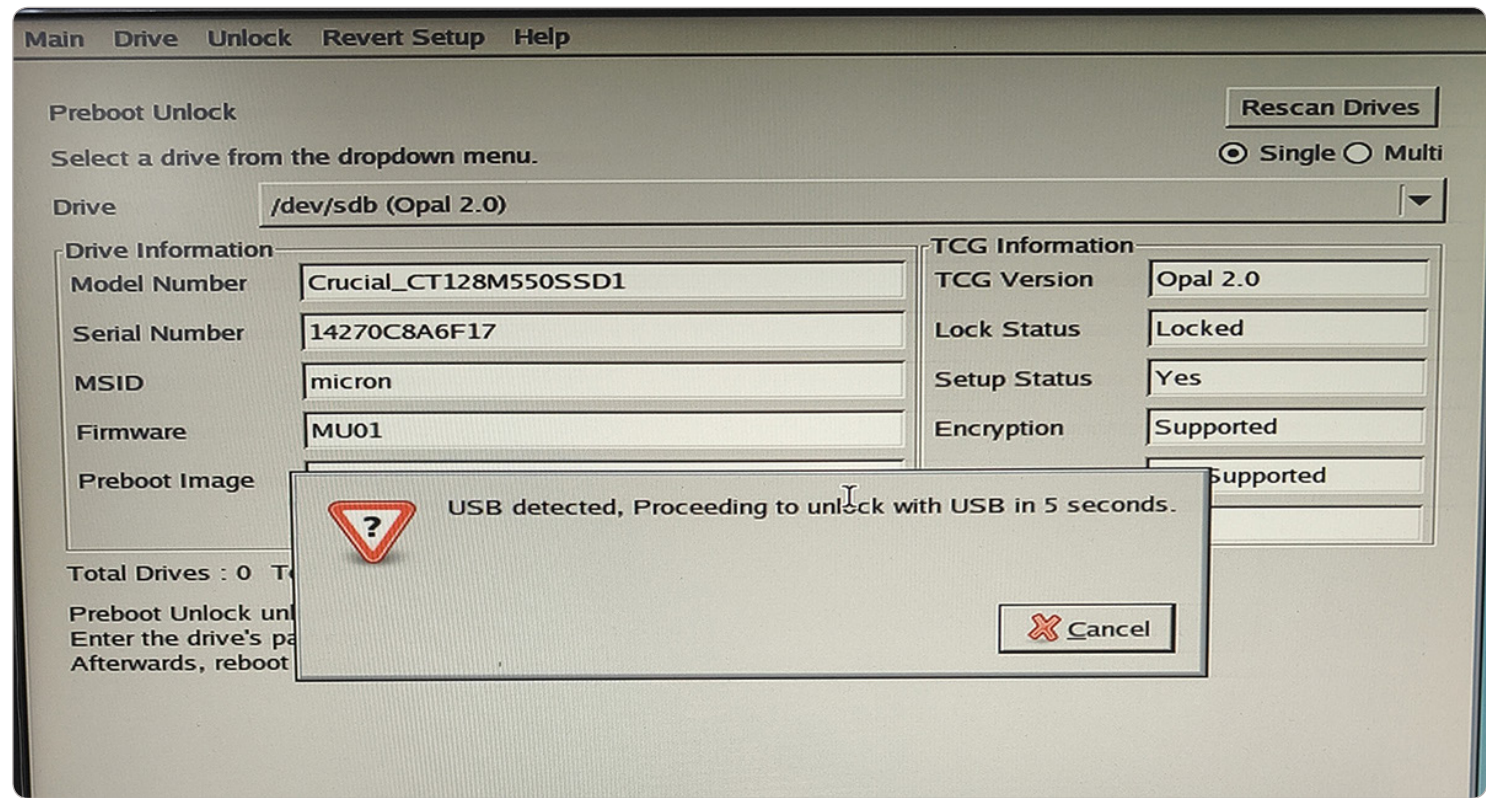
16.3.1 Preboot Manual Unlock

When the system drive is locked and the system is rebooted, it fails to access the OS from the locked drive. Instead, it reads the preboot image from the visible Shadow MBR or from a bootable USB if attached. This initiates the Preboot Authentication (PBA) version. In this environment, Opal Lock prompts for drive unlocking. Users can manually enter the drive password or use a USB flash drive with the password saved. Once unlocked, the system can be restarted, and shutting down will re-lock any previously unlocked drives.

16.3.2 Preboot Auto-Unlock and Reboot

Opal Lock provides the option to auto-unlock drives by scanning for password files on attached USB drives during startup in the preboot environment. If found, Opal Lock notifies the user and initiates a 5-second countdown before attempting to unlock all drives using the detected password files. If successful,

the system reboots automatically. Users have the option to cancel this process if desired.



PBA Auto Unlock

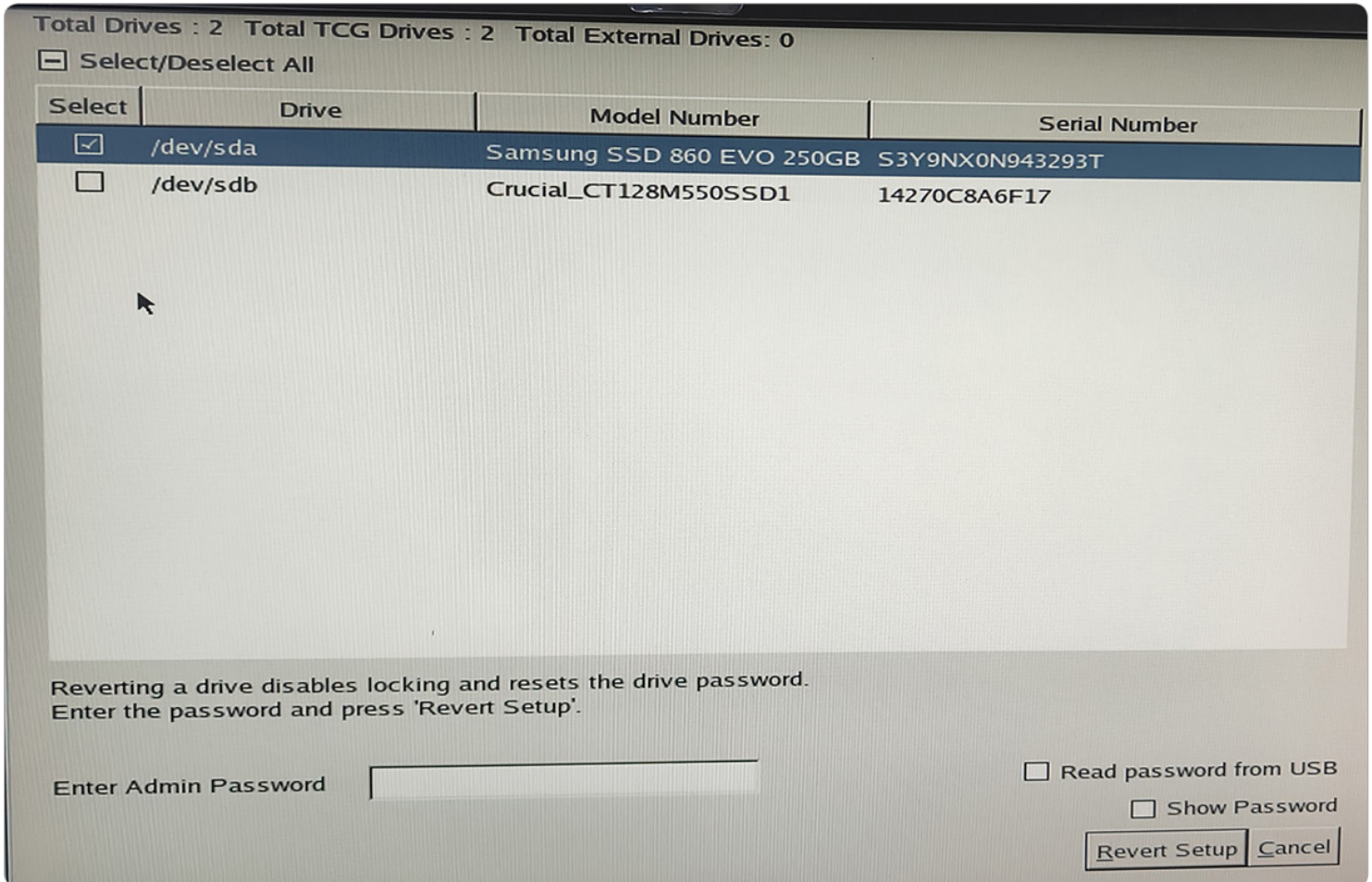
16.4 Revert Setup

Remove Lock disables locking and resets the password to the MSID. Once the lock has been removed from a drive, the drive will no longer lock when power cycled and thus will not need to be unlocked on startup. After any of the following options are used, the drive can be set up again.

There are three different options for removing the lock. These options provide users with flexibility in managing locked drives, allowing them to choose the most suitable option based on their requirements and circumstances.

IMPORTANT NOTES

- ▶ Users should exercise caution, especially when selecting options that involve data erasure, as the action is irreversible and may lead to permanent data loss.
- ▶ Some TCG versions (e.g. Pyrite) may only support keeping data or erasing data and not both options.

*PBA Revert and Keep Data*

16.4.1 Remove Lock and Keep Data

This option disables the locking mechanism and resets the password to the MSID without altering the drive's data. After execution, the drive remains unlocked when powered down, allowing immediate access to all data. For boot ives, the system boots into the installed operating system normally.

16.4.2 Remove Lock and Erase Data with Password

Total Drives : 2 Total TCG Drives : 2 Total External Drives: 0

☐ Select/Deselect All

Select	Drive	Model Number	Serial Number
☒	/dev/sda	Samsung SSD 860 EVO 250GB	S3Y9NX0N943293T
☐	/dev/sdb	Crucial_CT128M550SSD1	14270C8A6F17

Revert with Password reverts the drive's LockingSP.
This resets the drive's password and disables locking.
Enter the drive's password and choose whether or not to erase all data.

Enter Admin Password

Type 'I agree'

☐ Read password from USB

☐ Show Password

PBA Revert and Remove data

Choosing this option not only resets the password but also resets the drive to manufacturer settings, effectively erasing all data stored on the drive. It's crucial to note that this action is irreversible, and all existing data will be permanently lost. Therefore, it's advised not to use this option if the data on the drive is still required.

Drive: /dev/sdb (Opal 2.0)

Drive Information		TCG Information	
Model Number	Crucial_CT128M550SSD1	TCG Version	Opal 2.0
Serial Number	14270C8A6F17	Lock Status	Unlocked
MSID	micron	Setup Status	Yes
Firmware	MU01	Encryption	Supported
Preboot Image	FL.1.3.9	Block SID	Not Supported
		User Setup	No

Total Drives : 2 Total TCG Drives : 2 Total External Drives: 0

Reverting with PSID reverts the drive to manufacturer settings and erases all data.
Enter the drive's PSID and press 'Revert Setup with PSID'.

You can find the PSID on the label of the drive

Enter PSID (omit dashes)

Type 'I agree'

[Revert Setup and Erase with PSID](#) [Cancel](#)

PBA Erase Data with PSID

16.4.3 Remove Lock and Erase Data with PSID

This option leverages the PSID (Physical Security ID) to revert the drive to manufacturer settings. It's particularly useful if the drive's password has been forgotten or lost. Users can find the drive's PSID on its label. Similar to the previous option, using this method will erase all data on the drive.



PSID

17. KEYBOARD NAVIGATION

If there are problems with the mouse in the preboot environment, all operations can be done using the keyboard. The standard keyboard shortcuts apply for navigating the user interface.

Key(s)	Description
F10	Access the Menu Bar
SPACE	Toggle checkboxes
Tab	Switch focus to the next GUI feature
Enter	Dropdown menus - Open and close menu Buttons - Same as pressing the button
Arrow Keys	Menu Bar - Navigate around the menus and subitems Radio buttons - Change selection Dropdown Menus - Up and Down cycles through options

18. FREQUENTLY ASKED QUESTIONS

Compatibility

Q: What drives are compatible with Opal Lock?

A: TCG drives are compatible with Opal Lock. TCG versions other than Opal may not support all of the features offered by Opal Lock.

Q: How do I know whether my drive is a TCG drive?

A: All TCG drives have a PSID that can be found on the drive's label.

Setup

Q: Why do I need a USB for setup?

A: USB is needed to create a Recovery USB, which acts as a way to unlock or erase your drives if your drive does not support the shadow MBR or if the preboot image somehow becomes inaccessible and you don't have any other way to access Opal Lock.

Preboot Image

Q: How do I know whether or not my drive supports shadow MBR?

A: If your TCG drive does not support shadow MBR, the Preboot Image field in the Drive Information section will display "Not Supported".

Q: My drive does not support the preboot image. Can I still use Opal Lock to set up the drive?

A: The initial setup process includes writing the preboot image onto a newly created bootable USB drive, which you can use as a substitute to having the preboot image on your drive.

Q: When would I need to use Update Preboot Image?

A: Update Preboot Image is primarily meant to be used whenever a new version of Opal Lock is released.

Recovery USB

Q: What is a Recovery USB?

A: A Recovery USB set up with Opal Lock has the preboot image written into it. When booting up your system, you can boot into the USB and use the preboot image to manage your drives.

Lock/Unlock

Q: I finished setting up my drive. How do I lock my drive?

A: Once the drive has been set up, the drive will be locked when the system is power cycled. This happens when the system is shut down or put into hibernate, and not when the system is rebooted. External drives can also be power cycled by removing the drive from the system.

Q: My drive is locked. How do I unlock my drive?

A: If unlocking via preboot image on the drive's shadow MBR: When booting into the drive, the system will boot into the drive's preboot image written into the shadow MBR. Once bootup is complete, the Opal Lock application will run, displaying the unlock prompt to enter the password. Once successfully authenticated, you can reboot the system which will then boot into the unlocked drive.

If unlocking via preboot image on bootable USB: Similar to unlocking via shadow MBR, except you boot into the USB instead of the locked drive.

Password

Q: I lost/forgot my password. What should I do?

A: If the password is lost/forgotten, there is no way to recover the password. Once the drive is locked, all data will be inaccessible. The only way to unlock the drive without the password is to use the drive's PSID to revert setup, which resets the drive to manufacturer settings and erases all data on the drive.

Q: Where can I find my drive's MSID?

A: If your drive is an Opal drive, then the MSID is displayed in the MSID field in the Drive Information section.

Q: How do I reset the retry counter? What should I do if Opal Lock says I'm locked out?

A: Anytime that there is a successful authentication, the corresponding retry counter (Admin, User, or PSID) is reset. All retry counters are reset if the system is power cycled.

Opal Lock Lite

Q: What is Opal Lock Lite?

A: Opal Lock Lite is a user-friendly solution tailored for individuals and businesses seeking a convenient way to unlock their external USB drives. Built upon the Opal standard, Opal ILock Lite ensures robust encryption while simplifying the unlocking process.

Q: How to Activate Opal Lock Lite?

A: Start by downloading Opal Lock exe from our official website. Follow the installation instructions to set up the tool on your system. Once installation is completed, launch the application and click on "Activate Opal Lock Lite" option.

Block SID

Q: What is Block SID?

A: Block SID, or Block Security Identifier, is a unique identifier associated with individual blocks or units of data within a storage device, particularly in the context of self-encrypting drives (SEDs). Block SIDs are used to enforce granular access control and encryption at the block level, providing enhanced security measures.

Q: What if the Block SID of the drive is Enable?

A: When Block SID is enabled on a self-encrypting drive, it restricts certain operations on the drive at the block level. This means that access to specific blocks of data can be controlled more precisely, enhancing security by allowing encryption and access control to be managed at a finer granularity than traditional methods.

Q: How to set up a drive that has Block SID Enable ?

A: To set up such drives using Opal Lock, you'll need to disable the Block SID feature in the BIOS settings. This option is typically found under the Security or Advanced Settings section of the BIOS.

Once Block SID is disabled, retry the operation with Opal Lock. With Block SID turned off, Opal Lock should be able to perform the desired operation on Drive without encountering compatibility issues.

Note- It's important to note that the Block SID feature status will revert to its original value upon system reboot. This means that if you disable Block SID in the BIOS settings to perform the desired operation with Opal Lock, the feature will be re-enabled automatically when the system restarts.

19. APPENDIX

Appendix A: Audit Event List

Event ID	Level	Description
1	Information	Drive Activated
2	Information	Initial Drive Setup
3	Information	Admin Authenticated
4	Error	Admin Incorrect Password
5	Warning	Admin Locked Out
6	Information	User Authenticated (Premium)
7	Error	User Incorrect Password (Premium)
8	Warning	User Locked Out (Premium)
9	Warning	Potential Intrusion Attempt Detected
10	Information	Preboot Image written to MBR
11	Information	User Setup (Premium)
12	Information	User Removed (Premium)
13	Information	SID and Admin Password Changed
14	Information	User Password Changed (Premium)
15	Information	Drive Unlocked
16	Information	Preboot Unlock from MBR
17	Information	Preboot Unlock from USB (Premium)
18	Information	Lock Removed
19	Information	Lock Removed and Data Erased using Password
20	Information	Lock Removed and Data Erased using PSID
21	Information	Query Information Accessed
22	Information	Audit Log Accessed
23	Information	Admin password written to USB

24	Information	User password written to USB
25	Information	Admin password read from USB
26	Information	User password read from USB
27	Information	Cryptographic Erase
28	Error	Preboot image write to MBR Failed
29	Error	User Setup Failed
30	Error	User Removal Failed
31	Error	SID and Admin password change failed
32	Error	User password change failed
33	Error	Drive unlock failed
34	Error	Preboot unlock from MBR failed
35	Error	Preboot unlock from USB failed
36	Error	Revert Setup Failed
37	Error	Revert Setup and Erase Data with Password Failed
38	Error	Revert Setup and Erase Data with PSID Failed
39	Error	Query information access Failed
40	Error	Audit Log access Failed

Appendix B: SampleAudit Log CSV file

Type	Date&Time	Event ID	Description
Information	2024/05/20 16:08:25	22	Audit Log accessed
Information	2024/05/20 16:08:25	3	Admin Authenticated
Information	2024/05/15 19:13:09	10	Preboot Image written to MBR
Information	2024/05/15 19:13:08	23	Admin Password Saved
Information	2024/05/15 19:13:03	13	SID and Admin password changed
Information	2024/05/15 19:13:03	2	Initial Drive Setup
Information	2024/05/15 17:32:45	1	Drive Activated

Information	2024/05/15 17:32:45	27	Cryptographic Erase
Information	2024/05/15 17:32:45	20	Lock removed and data erased using PSID
Information	2024/05/15 17:31:57	1	Drive Activated
Information	2024/05/15 17:31:57	18	Lock removed
Information	2024/05/15 17:31:52	3	Admin Authenticated
Information	2024/05/10 14:42:18	15	Drive unlocked
Information	2024/05/10 14:42:18	3	Admin Authenticated
Information	2024/05/10 14:42:18	25	Admin Password Read
Information	2024/05/10 14:39:09	15	Drive unlocked
Information	2024/05/10 14:39:09	3	Admin Authenticated
Information	2024/05/10 14:39:09	25	Admin Password Read
Information	2024/05/10 13:52:47	10	Preboot Image written to MBR
Information	2024/05/10 13:52:47	3	Admin Authenticated
Information	2024/05/10 13:52:46	23	Admin Password Saved
Information	2024/05/10 13:52:45	25	Admin Password Read
Information	2024/05/10 13:21:23	10	Preboot Image written to MBR
Information	2024/05/10 13:21:23	3	Admin Authenticated
Information	2024/05/10 13:21:23	23	Admin Password Saved
Error	2024/05/10 13:18:14	28	Preboot Image write to MBR failed
Error	2024/05/10 13:18:14	4	Invalid Admin Password
Information	2024/05/10 13:04:07	10	Preboot Image written to MBR
Information	2024/05/10 13:04:03	13	SID and Admin password changed
Information	2024/05/10 13:04:03	2	Initial Drive Setup
Information	2024/05/10 12:59:49	1	Drive Activated
Information	2024/05/10 12:59:49	18	Lock removed
Information	2024/05/10 12:59:43	3	Admin Authenticated
Information	2024/05/10 12:50:17	15	Drive unlocked

Information	2024/05/10 12:50:17	3	Admin Authenticated
Information	2024/05/10 12:46:55	15	Drive unlocked
Information	2024/05/10 12:46:55	3	Admin Authenticated
Information	2024/05/10 12:42:16	15	Drive unlocked
Information	2024/05/10 12:42:16	3	Admin Authenticated
Information	2024/05/09 17:06:22	10	Preboot Image written to MBR
Information	2024/05/09 17:06:18	13	SID and Admin password changed
Information	2024/05/09 17:06:18	2	Initial Drive Setup
Information	2024/05/09 14:34:35	1	Drive Activated
Information	2024/05/09 14:34:35	18	Lock removed
Information	2024/05/09 14:34:29	3	Admin Authenticated
Error	2024/05/08 18:24:48	31	SID and Admin password change failed
Warning	2024/05/08 18:24:48	9	Potential Intrusion Attempt Detected
Warning	2024/05/08 18:24:48	5	Admin Locked Out
Information	2024/05/08 15:54:44	15	Drive unlocked
Information	2024/05/08 15:54:44	3	Admin Authenticated
Information	2024/05/08 15:50:10	15	Drive unlocked
Information	2024/05/08 15:50:10	3	Admin Authenticated
Information	2024/05/07 14:19:30	13	SID and Admin password changed
Information	2024/05/07 14:19:30	2	Initial Drive Setup
Information	2024/05/07 13:20:39	1	Drive Activated
Information	2024/05/07 13:20:39	18	Lock removed
Information	2024/05/07 13:20:31	3	Admin Authenticated
Information	2024/04/26 15:12:15	15	Drive unlocked
Information	2024/04/26 15:12:15	3	Admin Authenticated
Information	2024/04/26 12:16:30	15	Drive unlocked
Information	2024/04/26 12:16:30	3	Admin Authenticated

Information	2024/04/25 19:38:27	41	Drive locked
Information	2024/04/25 19:14:08	15	Drive unlocked
Information	2024/04/25 19:14:08	3	Admin Authenticated
Information	2024/04/25 14:55:16	41	Drive locked
Information	2024/04/25 14:06:00	15	Drive unlocked
Information	2024/04/25 14:06:00	3	Admin Authenticated
Information	2024/04/25 13:04:51	15	Drive unlocked
Information	2024/04/25 13:04:51	3	Admin Authenticated
Information	2024/04/25 12:31:51	41	Drive locked
Information	2024/04/25 12:00:36	15	Drive unlocked
Information	2024/04/25 12:00:36	3	Admin Authenticated
Error	2024/04/25 12:00:28	33	Drive unlock failed
Error	2024/04/25 12:00:28	4	Invalid Admin Password
Information	2024/04/24 12:23:59	13	SID and Admin password changed
Information	2024/04/24 12:23:59	2	Initial Drive Setup
Information	2024/04/24 12:23:28	1	Drive Activated
Information	2024/04/24 12:23:28	18	Lock removed
Information	2024/04/24 12:23:23	3	Admin Authenticated
Information	2024/04/23 18:27:29	10	Preboot Image written to MBR
Information	2024/04/23 18:27:29	3	Admin Authenticated
Information	2022/12/02 05:43:41	13	SID and Admin password changed
Information	2022/12/02 05:43:41	2	Initial Drive Setup

20. ACKNOWLEDGEMENTS

Fidelity Height acknowledges third parties whose open source code has been used in permissible form in Opal Lock.

Drive Trust Alliance Component: sedutil

Webpage: <https://github.com/Drive-Trust-Alliance/sedutil>

License: GNU General Public License

