Opal Lock
User Guide

TABLE OF CONTENTS

1. INTRODUCTION AND OVERVIEW

Opal Lock is a drive security management application for self-encrypting drives (SEDs) which have 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 drive can be set up by setting up the preboot image, which is the environment used for preboot authentication. To lock a drive after it has been set up with Opal Lock, the system must be powered down completely. Once the drive has been locked, the drive's data will be encrypted and inaccessible until it is unlocked. The next time the system is powered up, it will boot into the preboot environment for preboot authentication. After successful authentication, the drive can be accessed by rebooting the system.

2. SYSTEM REQUIREMENTS

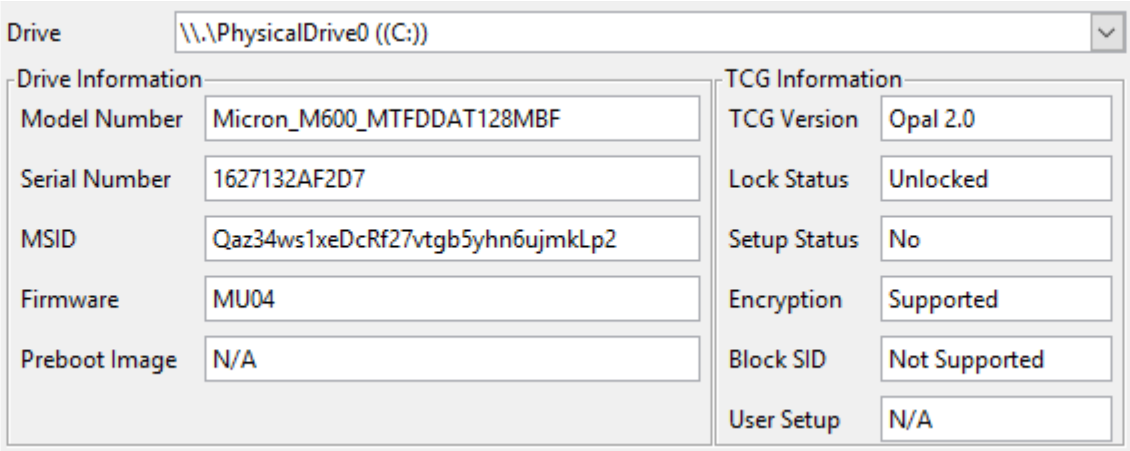
Before getting started, you will need:

- Windows 10, Windows 8.1, or Windows Server 2012 R2 or 2016
- SATA or NVMe (Windows 10 or Server 2016 only) Opal SED drive
- MyFidelity1.exe installation file and license key
- Internet connection for license validation
- A spare USB flash drive

Other system requirements:

- CPU: Hyper-threading CPU; Core 2 processor and above is recommended
- RAM: 1GB or above; 2GB is recommended for Windows 8.1 and above
- Video Card: 32MB; 64MB and above is recommended
- System Drive: minimum 500MB free space
- BIOS: Secure Boot must be off/disabled

3. GETTING STARTED



Drive	\\.\PhysicalDrive0 ((C:))

Drive Information

Model Number	Micron_M600_MTFDDAT128MBF
Serial Number	1627132AF2D7
MSID	Qaz34ws1xeDcRf27vtgb5yhn6ujmkLp2
Firmware	MU04
Preboot Image	N/A

TCG Information

TCG Version	Opal 2.0
Lock Status	Unlocked
Setup Status	No
Encryption	Supported
Block SID	Not Supported
User Setup	N/A

Opal Lock displays information about the drives detected on the system. This display is for showing drive status and also for selecting the drive for operations.

Each drive is listed by their drive name according to the system. On Windows, drives are listed as physical drives (e.g. \\.\PhysicalDrive0). If a drive partition (e.g. C:) is associated with a physical drive, the partition will be listed alongside the physical drive list for easier identification. TCG drives are listed up to the drive limit determined by the version being used.

The drive's **model number** and **serial number** are displayed along with the drive manufacturer. The drive's **firmware** version is manufacturer specific and is displayed for informational purposes. The **MSID (manufacturer secure ID)** is the default password of the drive. This is the drive's authentication key before it is set up. If the previously set up password is reset, then the password will also be reset to the MSID.

The **Preboot Image** field displays the preboot image version written to the drive's shadow MBR. If the field displays "Not Supported", then the drive does not support MBR shadowing, and the preboot image cannot be written to the drive. If the field displays "N/A", and the selected drive is a TCG drive, then the preboot image has not been written to the drive.

The **TCG Version** field displays the TCG specification version that the drive supports. If the drive is not a TCG drive, then this field and the following fields will display "N/A".

Lock Status indicates whether the drive is locked. **Setup Status** indicates whether the drive has been set up using Opal Lock. If the drive has been set up without using Opal Lock, Setup Status will display "No".

The **Encryption** field indicates whether the selected drive supports full-disk encryption. Most versions of TCG support full-disk encryption, with the exception of Pyrite, which does not require encryption.

Block SID is a feature present in some TCG drives which if enabled, blocks any attempt to change the authentication key. If Block SID is enabled, Opal Lock is not able to set up a password for the drive. Therefore, Block SID needs to be disabled before the drive can be set up using Opal Lock. Block SID can be disabled in the BIOS on startup before the Block SID command is executed.

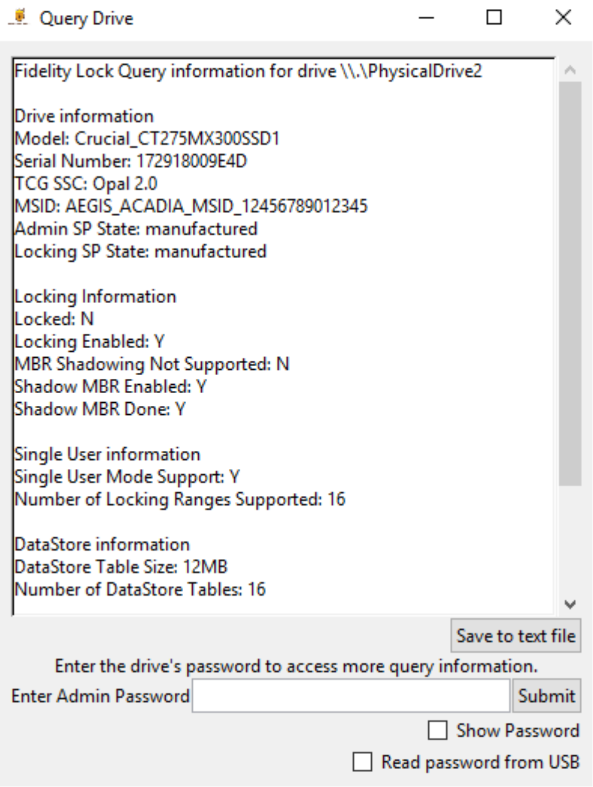
4. FEATURES

4.1 Drive

This section covers features which pertain to viewing and updating information on TCG drives. The easiest way to know whether a drive is a TCG drive is to check whether the drive has a PSID (physical secure ID). All TCG drives have their PSID included on their label. All TCG drives are compatible with Opal Lock, but certain TCG versions such as Pyrite and Enterprise do not support certain operations.

4.1.1 Query Drive

Query brings up a window displaying information about the drive. The window also has the option of entering the drive's Admin password to access additional, password-protected information. There is an option to save the Query information to a text file. Refer to Appendix A for a sample Query save file, and Appendix B for a sample of the password-protected information.



```
Fidelity Lock Query information for drive \\.\PhysicalDrive2

Drive information
Model: Crucial_CT275MX300SSD1
Serial Number: 172918009E4D
TCG SSC: Opal 2.0
MSID: AEGIS_ACADIA_MSID_12456789012345
Admin SP State: manufactured
Locking SP State: manufactured

Locking Information
Locked: N
Locking Enabled: Y
MBR Shadowing Not Supported: N
Shadow MBR Enabled: Y
Shadow MBR Done: Y

Single User information
Single User Mode Support: Y
Number of Locking Ranges Supported: 16

DataStore information
DataStore Table Size: 12MB
Number of DataStore Tables: 16
```

Save to text file

Enter the drive's password to access more query information.

Enter Admin Password [ ] Submit

□ Show Password

□ Read password from USB

4.1.2 Audit Log

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. The Audit Log can be accessed via View Audit Log using the drive's password. Refer to Appendix C for a list of events that are logged. The Audit Log can be saved as a CSV file, refer to Appendix D for a sample of the contents.

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.

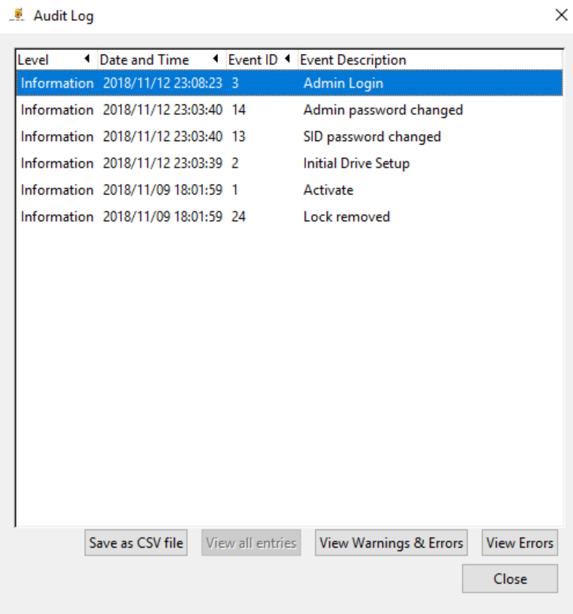
NOTE: Audit Log requires that the drive supports Datastore. Some TCG versions like Enterprise do not support Datastore.

4.1.3 Rescan drives

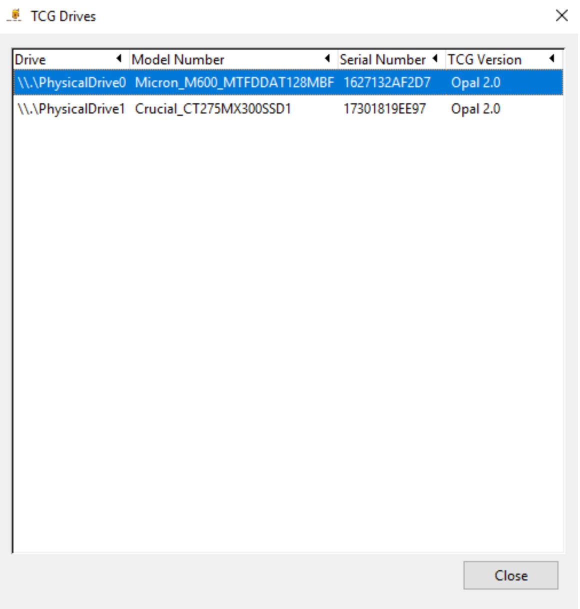
Rescan Drives makes the system rescan the drives that are mounted, and then queries the drives to acquire updated status information to display on the application. In the case that the total number of detected TCG drives exceeds the drive limit, any drives that were previously listed and are still present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

4.1.4 View TCG Drives

View TCG drives brings up a window displaying a list of all TCG drives detected on the system, plus their model and serial numbers and their TCG version.



Level	Date and Time	Event ID	Event Description
Information	2018/11/12 23:08:23	3	Admin Login
Information	2018/11/12 23:03:40	14	Admin password changed
Information	2018/11/12 23:03:40	13	SID password changed
Information	2018/11/12 23:03:39	2	Initial Drive Setup
Information	2018/11/09 18:01:59	1	Activate
Information	2018/11/09 18:01:59	24	Lock removed



Drive	Model Number	Serial Number	TCG Version
\\.\PhysicalDrive0	Micron_M600_MTFDDAT128MBF	1627132AF2D7	Opal 2.0
\\.\PhysicalDrive1	Crucial_CT275MX300SSD1	17301819EE97	Opal 2.0

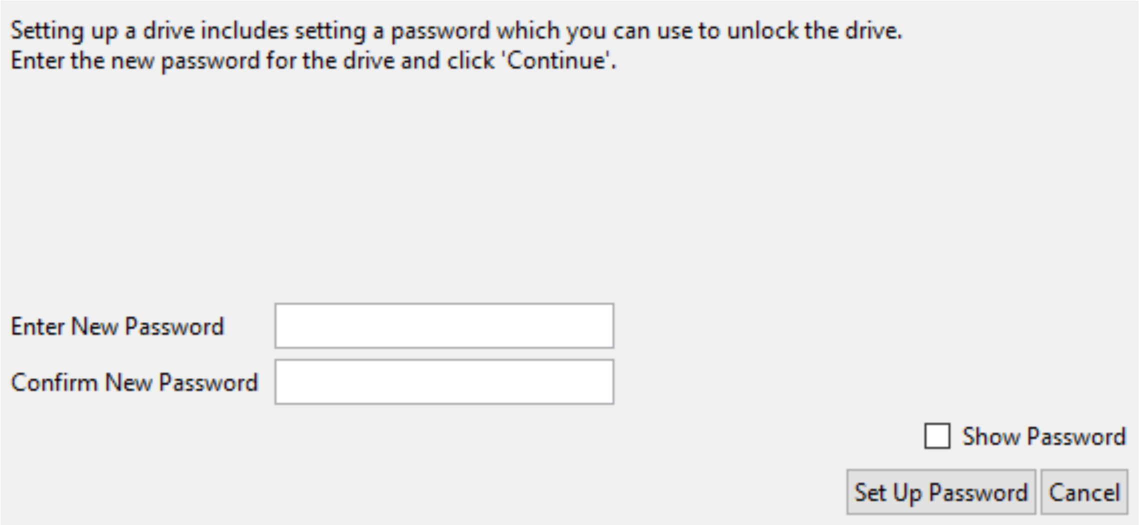
4.2 Setup

The following sections introduce features for setting up the password and locking/unlocking mechanisms for the drives.

4.2.1 Setting up the password

The first step to setting up a drive is to set a password for the drive. This password is to be used for all Opal Lock operations on the drive, such as unlocking the drive. This password is different from the password you normally enter on your operating system's startup screen. For security purposes, the password must be at least 8 characters long. For verification purposes, the new password must be entered and confirmed twice.

WARNING: If the drive's password is lost/forgotten, the only course for recovery is to revert setup using the drive's PSID, which reverts the drive to manufacturer settings and erases all of the drive's data without any way of recovering it. Therefore, it is of utmost importance that users remember the password that they set.



Setting up a drive includes setting a password which you can use to unlock the drive.
Enter the new password for the drive and click 'Continue'.

4.2.2 Setting up and updating the preboot image

The second step of setting up a drive is to set up the preboot image. The preboot image is a small operating system image with Opal Lock embedded in it that can be written onto a drive's shadow MBR. When a drive is locked, the contents of the drive are encrypted and inaccessible, except for its shadow MBR. When booting into a locked drive with the preboot image written, the system will boot into preboot image. Upon booting into the preboot image, the embedded Opal Lock application will load and can be used to unlock the drive. After unlocking the drive, the drive's contents can be accessed by rebooting the system.

If Opal Lock is being used to manage multiple drives, the preboot image does not necessarily need to be written to every drive. When booting up to unlock the drives, at least one drive that has the preboot image written to it must be mounted on the system in order to be able to access the preboot environment and use it to unlock all of the drives. If each drive will be managed individually rather than as a group, then every drive will need to have the preboot image written to its shadow MBR.

WARNING: Writing the preboot image to a drive can take up to 15 minutes. Do not power down the system while the preboot image is being written, otherwise the image will not be written, and the drive will be locked with no way of unlocking itself internally.

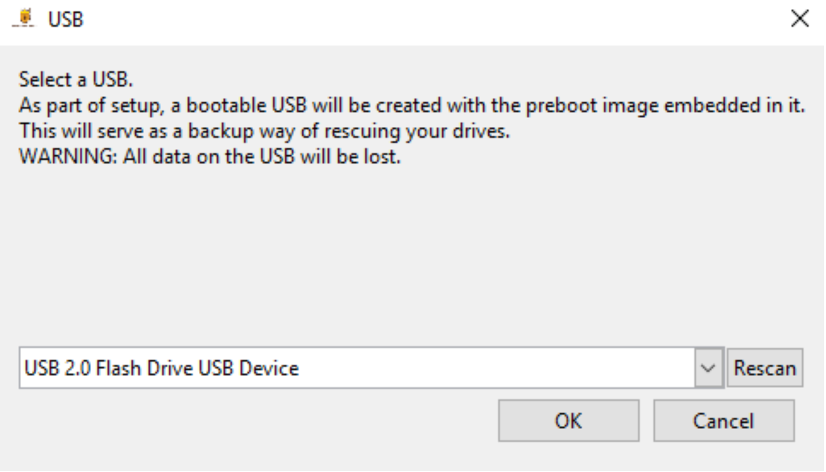
WARNING: Some TCG versions do not support the shadow MBR. If your drive does not support MBR shadowing, then it is not possible for the preboot image to be set up on the drive. The only ways to unlock a drive without a shadow MBR are either using Opal Lock installed on another drive to unlock it, or setting up the preboot environment on a bootable USB. (see section 4.2.3)

WARNING: It is essential that a way to unlock the drive is set up immediately. If a drive is locked without any way for unlocking it, then the drive will be in an unusable state and all of its data will be lost if the drive becomes locked.

4.2.3 Setup Bootable USB

The preboot image can also be set up on a USB, creating a bootable USB drive that can be an alternative to writing the preboot image to a drive's shadow MBR. This is included as part of initial setup, and is also a separate menu option. Select the drive you want the USB to be set up to unlock and proceed with setting up the USB. To unlock the drive with the bootable USB, boot into the USB on startup, and proceed with unlocking drives just like if the preboot image is on the shadow MBR. The drive that was selected when setting up the USB must be present in the system when booting into the USB in order for the bootable USB to be verified and usable.

NOTE: For premium versions, passwords can also be saved on the bootable USB. This is automatically done in initial setup and is also an option for the standalone operation.

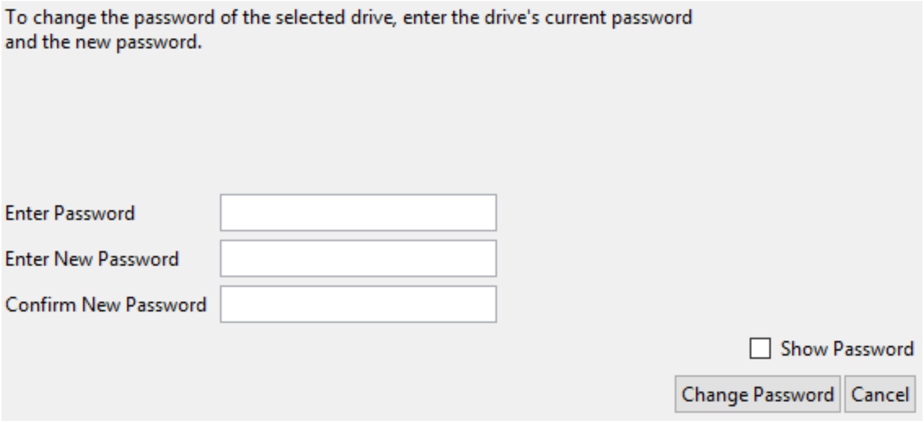


Select a USB.
As part of setup, a bootable USB will be created with the preboot image embedded in it.
This will serve as a backup way of rescuing your drives.
WARNING: All data on the USB will be lost.

USB 2.0 Flash Drive USB Device

4.2.4 Changing the password

Opal Lock comes with the option of changing the password set up on a drive. Simply enter the current password, the new password, and confirm the new password.
For Premium versions, Change Password can be used to change either the Admin password or the User password. For more information about the User password and how to set up or remove it, please refer to section 5.3.4.



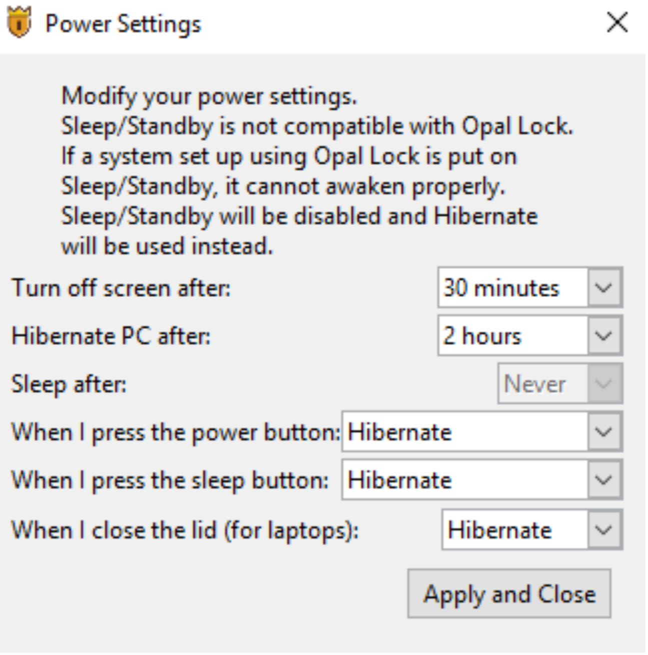
To change the password of the selected drive, enter the drive's current password and the new password.

4.2.5 Power Settings

After setting up the drive(s), it is recommended that the system power settings be adjusted. At the end of setup, if the power settings do not match the recommended settings, you will be prompted to adjust the settings.

Drives only lock when they are powered down completely. This happens when you either Shut Down or Hibernate the system. However, this does not happen properly when the system is put on Standby/Sleep. To work around this, Standby/Sleep will be disabled when changing power settings with Opal Lock, and users can use the Power Settings window in Opal Lock to set when to turn off the screen and when to Hibernate the system. In addition, other buttons and actions that typically are used to put the system to Sleep such as closing the lid on a laptop or pressing the Sleep button will need to be set to options other than Sleep. Finally, the Sleep option will be hidden in the Start menu and replaced by the Hibernate option.

WARNING: If the power settings are not changed to disable Standby/Sleep, and the drive goes into Standby/Sleep mode, then there will be problems when trying to awake the system that will force the user to power down the system completely, which will then fully lock the drive.



Power Settings

Modify your power settings.
Sleep/Standby is not compatible with Opal Lock.
If a system set up using Opal Lock is put on
Sleep/Standby, it cannot awaken properly.
Sleep/Standby will be disabled and Hibernate
will be used instead.

Turn off screen after: 30 minutes

Hibernate PC after: 2 hours

Sleep after: Never

When I press the power button: Hibernate

When I press the sleep button: Hibernate

When I close the lid (for laptops): Hibernate

4.3 Lock/Unlock

Once a drive has been set up, then the drive will lock itself upon shutdown, encrypting all of its data and rendering it inaccessible until it is unlocked.

4.3.1 Locking a drive

To lock a drive, the system must be powered down completely. Shut Down and Hibernate are the only two options that completely shut off power to the system. Restarting the system does not power cycle the drive, and therefore does not lock the drive.

4.3.2 Unlocking a drive

If the preboot image is written to the drive's shadow MBR or if the bootable USB is attached to the system, on startup the system will boot into the preboot environment. Upon booting up, Opal Lock will open and load the prompt for unlocking drives. To unlock drives, enter the drive(s) password. Once the drive has been unlocked, complete the process by restarting the system. Shutting down the system will re-lock any drives that had been unlocked.

4.4 Revert Setup

Revert Setup 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.

NOTE: Some TCG versions (e.g. Pyrite) may only support keeping data or erasing data and not both options.

4.4.1 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.

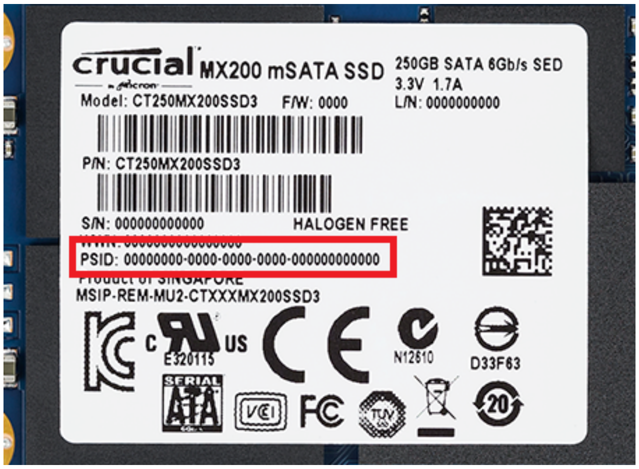
4.4.2 Revert Setup and Erase Data with Password

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 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.

4.4.3 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.



5. VERSION-SPECIFIC INFORMATION

All of the basic features mentioned in Section 4 are available in the Standard version. This section covers information about the other versions available.

5.1 Demo

The Demo version is the free version meant to provide users with an understanding of the features of Opal Lock. This version comes with all Setup Drive and Drive Management features disabled.

5.2 Preboot

This version is embedded in the Preboot Image that can be written into a drive's shadow MBR or the bootable USB. The Preboot version includes most of the regular features except for the Setup menu. The limit on the number of drives matches the version used to write the preboot image. In the case that the total number of detected drives exceeds the drive limit, the locked drives are prioritized over other drives to be listed in the drive selection menu.

5.3 Standard

The Standard version contains all of the features mentioned above, with support for a maximum of five drives.

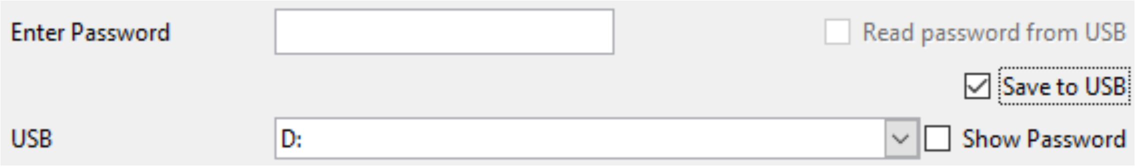
5.4 Premium

The Premium versions of Opal Lock has additional features not included in the Standard version. The following features are only available on the Premium version.

5.4.1 Save password to USB and Read password from USB

Premium users have the option to save their drive password(s) on a password file that is stored on a USB. This can be done when setting up the drive's password, or anytime the password is being used. To save the password to USB, select the "Save to USB" checkbox and proceed with the operation as usual. Afterwards, the USB can be used for authenticating any operations for the drive. If the password is read from the USB for changing the password, the new password will automatically replace the old password on the USB drive. If the USB is used to authenticate for Revert Setup, then the password file will be automatically erased if Revert Setup is successful.

NOTE: It is required that you use a USB drive that has been formatted using FAT. This requirement is necessary because the preboot environment is not able to read passwords from drive that are formatted differently.



Enter Password

□ Read password from USB

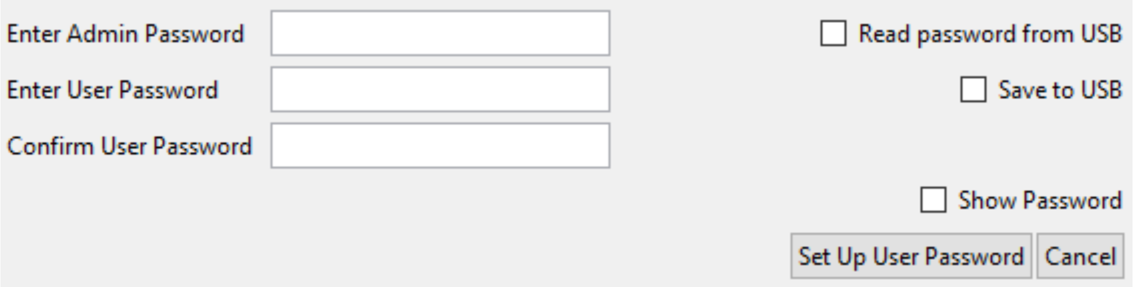
☑ Save to USB

USB D:

□ Show Password

5.4.2 User setup and removal

With the Premium versions, a second password can be set that has limited authority. The main password is referred to as the Admin password, while this second password is called the User password. The User has the authority to unlock the drive, access the drive's Audit Log and to change its own password. Setting up and removing the User password requires the Admin password.



Enter Admin Password

Enter User Password

Confirm User Password

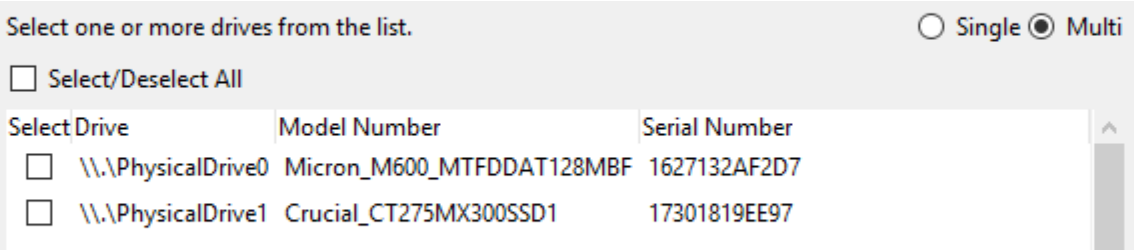
□ Read password from USB

□ Save to USB

□ Show Password

5.4.3 Multi-drive operations

With a Premium version, users can manage multiple drives simultaneously with one click. This applies to setting up drives, changing the password on drives, unlocking drives, and removing lock on drives. To switch between Single and Multi mode on an operation that supports multi-drive operations, select the "Multi" or "Single" radio button. All the drives recognized by Opal Lock are listed, and drives that are eligible for the operation are selectable with checkboxes.



Select one or more drives from the list.

○ Single ● Multi

□ Select/Deselect All

Select	Drive	Model Number	Serial Number
□	\\.\PhysicalDrive0	Micron_M600_MTFDDAT128MBF	1627132AF2D7
□	\\.\PhysicalDrive1	Crucial_CT275MX300SSD1	17301819EE97

5.4.4 Preboot auto-unlock and reboot

As an added benefit to saving passwords to a drive, on startup in the preboot environment, Opal Lock scans for password files stored on USBs. If any are found, Opal Lock will notify the user that it will proceed to attempt unlocking all locked drives after 5 seconds unless the user cancels it. If allowed to proceed, Opal Lock will automatically attempt to unlock all drives using detected password files. If all locked drives are unlocked, then the system will reboot automatically.

6. 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 sub-items Radio buttons - Change selection Dropdown Menus - Up and Down cycles through options

7. 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 bootable 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.

Bootable USB

Q: What is a bootable USB?
A: A bootable 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.

8. GLOSSARY

Manufacturer secure ID (MSID): The default password for the drive. After Revert Setup, the password will be reset to the MSID.

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.

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 bootable USB (Premium 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.

9. APPENDIX

Appendix A: Query Save File

```
Opal Lock Query information for drive \\.\PhysicalDrive1

Drive information
Model: Crucial_CT275MX300SSD1
Serial Number: 17301819EE97
TCG SSC: Opal 2.0
MSID: AEGIS_ACADIA_MSID_12456789012345
Admin SP State: manufactured
Locking SP State: manufactured

Locking Information
Locked: N
Locking Enabled: Y
MBR Shadowing Not Supported: N
Shadow MBR Enabled: Y
Shadow MBR Done: Y
Single User information
Single User Mode Support: Y
Number of Locking Ranges Supported: 16
DataStore information
DataStore Table Size: 12MB
Number of DataStore Tables: 16
Opal information
Number of Admins: 4
Number of Users: 16
Base comID: 0x1000
Initial PIN: 0x0
```

Appendix B: Query Additional Information

```
Shadow MBR size 0x8000000
MandatoryWriteGranularity 0x1
RecommendedAccessGranularity 0x1000
User1 enabled = 0
User2 enabled = 0
User3 enabled = 0
User4 enabled = 0
User5 enabled = 0
User6 enabled = 0
User7 enabled = 0
User8 enabled = 0
User9 enabled = 0
User10 enabled = 0
User11 enabled = 0
User12 enabled = 0
User13 enabled = 0
User14 enabled = 0
User15 enabled = 0
User16 enabled = 1
Admin1 enabled = 1
Admin2 enabled = 0
Admin3 enabled = 0
Admin4 enabled = 0
```

```
Admin1 TryLimit = 5 : Tries = 0
Admin2 TryLimit = 5 : Tries = 0
Admin3 TryLimit = 5 : Tries = 0
Admin4 TryLimit = 5 : Tries = 0
User1 TryLimit = 5 : Tries = 0
User2 TryLimit = 5 : Tries = 0
User3 TryLimit = 5 : Tries = 0
User4 TryLimit = 5 : Tries = 0
User5 TryLimit = 5 : Tries = 0
User6 TryLimit = 5 : Tries = 0
User7 TryLimit = 5 : Tries = 0
User8 TryLimit = 5 : Tries = 0
User9 TryLimit = 5 : Tries = 0
User10 TryLimit = 5 : Tries = 0
User11 TryLimit = 5 : Tries = 0
User12 TryLimit = 5 : Tries = 0
User13 TryLimit = 5 : Tries = 0
User14 TryLimit = 5 : Tries = 0
User15 TryLimit = 5 : Tries = 0
User16 TryLimit = 5 : Tries = 0
SID TryLimit = 5 : Tries = 0
Preboot Image Version: demo.1.16-5-gd04b6ef
Audit Log Version: 1.0
```

Appendix C: 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 D: Sample Audit Log CSV file

```
Drive,\\.\PhysicalDrive1
Model,Crucial_CT275MX300SSD1
Serial Number,17301819EE97
Time,2018/11/19 15:16:53
Level,Date/Time,Event ID,Event Description
Information,2018/11/19 14:52:07,3,Admin Login
Information,2018/11/19 14:51:54,16,Drive unlocked
Information,2018/11/19 14:51:54,3,Admin Login
Information,2018/11/19 14:51:12,3,Admin Login
Error,2018/11/19 14:51:05,4,Failed Admin Login
Information,2018/11/16 16:15:53,3,Admin Login
Information,2018/11/16 16:15:41,14,Admin password changed
Information,2018/11/16 16:15:40,13,SID password changed
Information,2018/11/16 16:15:39,19,Password saved to USB
Information,2018/11/16 16:15:38,20,Password read from USB
Information,2018/11/16 16:02:00,3,Admin Login
Information,2018/11/16 16:02:00,20,Password read from USB
Information,2018/11/16 15:25:06,19,Password saved to USB
Information,2018/11/16 15:24:43,14,Admin password changed
Information,2018/11/16 15:24:42,13,SID password changed
Information,2018/11/16 15:24:42,2,Initial Drive Setup
Information,2018/11/14 01:05:12,1,Activate
Information,2018/11/14 01:05:12,24,Lock removed
```

10. 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