Aegis **Fortress L3**

User Guide

Remember to save your PIN in a safe place and to back up important data in more than one secure place, e.g. a second Aegis Secure Drive.

Table of Contents

Revised Sept 2022

About the Aegis Fortress L3

For the ultimate protection of your most sensitive data in storage and transportation, the Aegis Fortress L3 is designed and built to meet NIST FIPS 140-2 Level-3 requirements for the entire device. This complete FIPS validation includes the encryption module, all electronics, the hard drive, and the enclosure itself within the certification boundary.

The Fortress L3's membrane-type polymer-coated keypad is resistant to wear from repetitive button presses, impervious to dust and grit, and with software-free setup and operation, enables you to access the drive simply and easily with your own unique PIN. And the super fast USB 3.0 / 3.1 / 3.2 cables allow you to connect to USB type A or type C ports.

Package contents

- Aegis Fortress L3 Drive
- USB 3.1 Type A Cable
- USB 3.1 Type C Cable
- Travel pouch
- Quick Start Guide

Aegis Fortress L3 Connections

1. Attach one of the included USB cables in the port at the top of the device and the other to any available USB port on your computer.

2. At least one of the LEDs should turn on, indicating that the device is receiving power. In the unlikely event that no LEDs illuminate, connect to your computer via a powered hub.

Attention: Use only the included cables with your Aegis Fortress L3. Using cables not provided with the unit may not function properly and may cause damage to the device.

When you first plug in the Fortress L3, the unit will do a self-test to verify all security components are working properly. The LEDs will go through 3 test stages **RED**, **GREEN**, and **BLUE**. This will be followed by three **GREEN** flashes on a successful test. Any test failure will leave the unit in an inoperable state indicated by a flashing **RED** LED. Should this occur, contact our Tech Support department.

Aegis Fortress Keypad Panel

1	🔓	**UNLOCK** button
2	🔒	**LOCK** button
3		**LED** Indicator lights

First Time Use

Before the Fortress can be used, the Admin PIN MUST be set. Both the **BLUE and GREEN** LEDs glowing constantly indicate that the Admin PIN has yet to be established.

To Set-up the Admin PIN:

Plug device into USB Port. Both the **BLUE** and **GREEN** LEDs will glow steadily.

Press 🔓 **+ 9** at the same time. The **BLUE** LED will glow steadily and the **GREEN** LED will blink.

1. Enter the series of numbers that you will use for the Admin PIN and press the 🔓 button.*

2. Re-enter that same PIN and press the 🔓 button again. The **GREEN** LED will illuminate for one second, then replaced by the **BLUE** LED glowing steadily.

3. The drive is now in Admin mode where Admin features can be set (e.g., adding a User.)

4. If no further user(s) or functions are to be added, you can exit the Admin mode by pressing the 🔒 button and the drive will return to the locked standby state. If no action is taken within 30 seconds, the drive will return to its locked sleep state.

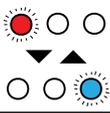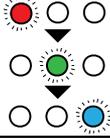   * *GREEN LED will blink if the PIN is accepted; If the PIN is NOT accepted, the RED LED will blink-- see PIN requirements below.*

   PINs must be a minimum length of 7 and a maximum of 16 digits. By default, minimum is set to 7, but can be programmed to be up to 16 for enhanced security.

   Cannot contain all consecutive numbers (2345678 or 9876543)

   Cannot contain all same number (1111111)

LED States and Their Meaning

LED	State	Meaning
○ ○ ○	No LEDs	Drive locked, power switch is off, device unplugged
● ○ ○ (blinking)	Blinking **RED**	Error / incorrect button entry; Mode Not Available; User PIN Change
● ○ ○	Solid **RED**	Locked / Standby state; Awaiting PIN entry
○ ● ○ (blinking)	Blinking **GREEN**	Button-entry accepted
○ ● ● (blinking green)	Solid **BLUE** / Blinking **GREEN**	Waiting for New User or Admin PIN to be established
○ ○ ●	Solid **BLUE**	Admin Mode
○ ● ○	Solid **GREEN**	Drive unlocked
○ ○ ● (slow blinking)	Slow Blinking **BLUE**	Drive unlocked in Lock-Override Mode
● ● ○ (slow blinking red)	Solid **GREEN** / Slow Blinking **RED**	Drive unlocked in Read-Only Mode
● ○ ○ ▼▲ ○ ○ ●	Alternating **RED** / **BLUE**	Indicates a mode has been entered that can result in the deletion of a User or the data on the drive (depending on the mode chosen.) Also used when setting Auto-lock feature
● ○ ○ ▼ ○ ● ○ ▼ ○ ○ ●	One second of **RED** followed by one second of **GREEN** followed by one second of **BLUE**	Self-test mode (automatically occurs during device startup) ensures all components are ready and working properly
● ● ○	Three Seconds of Solid **RED** / **GREEN**	During Reset Process, indicates successful resetting of cryptographic security parameters

Locking the Drive

To lock the drive, press the 🔒 button. When successfully locked, The **RED** LED will glow steadily, indicating that it's returned to its standby state.

If data is still being written to the drive, the Fortress will wait until all data has been written to the drive and then it will lock automatically.

Note: The Aegis Fortress will not be recognized by any operating system in its standby state.

Unlocking the Drive

Enter either a User PIN or Admin PIN and press the 🔓 button. If the PIN is accepted, the **GREEN** LED will blink three times, then will rapidly blink for a short time, followed by steady glowing, indicating that it's now unlocked and ready for use. If the PIN is incorrect, the **RED** LED will blink.

Admin Mode

To set up any of the drive's Admin functions and features, the Admin mode must first be entered. Once in the Admin mode, each of the drive's functions can be addressed with the appropriate button commands. Also note that while in the Admin mode, the actual data on the drive will not be accessible.

To return to the Admin mode for future setups, perform the following steps below.

1. Press and hold 🔓 **+ 0** for five seconds until the **RED** LED blinks.
    (This indicates that the drive is prepared to accept the correct Admin PIN.)
2. Enter the Admin PIN and press the 🔓 button.
3. Successfully entering the Admin Mode is indicated by a solid **BLUE** LED.
4. To exit the Admin Mode, either allow 30 seconds of inactivity or press the 🔒 button.

Changing the Admin PIN

Changes to the Admin PIN can only be made while the drive is in the Admin mode.

1. Enter the Admin mode. (Hold 🔓 **+ 0** for five seconds – with the **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will glow steadily.

2. Press 🔓 **+ 9**. The **BLUE** LED will glow steadily and the **GREEN** LED will blink.

3. Enter the new Admin PIN and press the 🔓 button. The **GREEN** LED will blink three times.

4. Re-enter the new Admin PIN and press the 🔓 button. The **GREEN** LED will glow steadily for two seconds and then return to the Admin mode, indicated by the **BLUE** LED glowing steadily.

Adding a New User PIN

If no additional User beyond the Admin will be permitted to access the Fortress's data, disregard the next two pages as they pertain to User PIN settings.

In addition to the Admin PIN, there can also be one User PIN allowed to access the drive as well. Adding a User PIN is the perfect way to securely share the Aegis Fortress or deploy it for use where the User does not require access to the device's Admin features. While Users have limited functionality and no Admin rights to the drive, they can still access its data, change their own PINs, and set the drive to *Read Only* or *Read / Write mode.*

There are two ways to establish a User PIN: Admin generated while in Admin Mode, or User generated while in User Forced Enrollment State.

A.)   ADMIN-GENERATED USER PIN

1.   Enter the Admin Mode by holding 🔓 **+ 0** for five seconds; With **RED** LED blinking, enter the Admin PIN and press the 🔓 button. The **BLUE** LED will glow steadily.

2.   Press the 🔓 **+ 1** buttons together until the **BLUE** LED glows steadily and the **GREEN LED** starts blinking.

3.   Enter the User PIN* and press 🔓. The **GREEN** LED will blink three times by itself, then the **BLUE** LED will glow steadily as the **GREEN** LED continues blinking.

4.   Enter that same User PIN again and press 🔓 to verify. The **GREEN** LED will glow steadily for three seconds verifying that the User PIN was successfully added, and then will be replaced by the **BLUE** LED glowing steadily, indicating that the drive has returned to the Admin mode.

B.)   USER-GENERATED USER PIN *(USER FORCED ENROLLMENT)*

Note: User Forced Enrollment state can only be implemented where there is no Admin-generated User PINs set up as described in the process above.

User Forced Enrollment Security Warning:
When a drive is in the User Forced Enrollment state, it is essentially unlocked until a User PIN is established. Therefore, DO NOT load sensitive data onto the drive if User Forced Enrollment is to be implemented.

1.   Enter the Admin Mode by holding 🔓 **+ 0** for five seconds; With **RED** LED blinking, enter the Admin PIN and press the 🔓 button. The **BLUE** LED will glow solidly.

2.   Press **0 + 1** and the **GREEN** LED will blink three times, then will be replaced by **BLUE** LED glowing solidly. Press the 🔒 button to return the device to its locked state. The device is now in *User Forced Enrollment State*, allowing a User to establish a unique User PIN.

CREATING USER-GENERATED USER PIN IN FORCED ENROLLMENT STATE

1.   Press 🔓 and ensure that the **BLUE** and the **GREEN** LEDs are glowing steadily.

2.   Press 🔓 **+ 1** and ensure that the **BLUE** LED is glowing solidly with the **GREEN** LED blinking.

3.   Enter the new User PIN and press the 🔓 button. The **GREEN** LED will blink three times by itself and then will be joined by the **BLUE** LED glowing solidly.

4.   Within 30 seconds, enter that same User PIN once more, and press the 🔓 button again. This time, the **GREEN** LED will glow solidly for a few seconds, then the drive will return to its locked state, indicated by the **RED** LED glowing solidly. The device's data can now be accessed using either the User PIN or the Admin PIN.

*   **Note: Default setting for minimum PIN length is 7 characters, and a maximum of 16.**

9

Deleting a User PIN

1. Enter the Admin mode. (Hold ☝ + 0 for five seconds. With the **RED** LED blinking, enter the Admin PIN and press the ☝ button.) The **BLUE** LED will now glow steadily.

2. Press the **7 + 8** buttons together for five seconds. The **GREEN** LED will blink three times and then will be followed by the **RED** and **BLUE** LEDs blinking alternately.

3. Press the **7 + 8** buttons together again for five seconds. The **GREEN** LED will glow steadily for a second or two.

4. The drive will return to Admin mode indicated by the **BLUE** LED glowing steadily.

    NOTE: Deleting the User PIN will also delete the Self-Destruct PIN and all recovery PINs (if any have been set.)

Changing a User PIN

1. Unlock the Aegis Fortress L3 with the User PIN. (The **GREEN** LED will blink)

2. Press the ☝ + 1 buttons together for five seconds (the **RED** LED will blink)

3. Enter the current User PIN and press the ☝ button. (The **BLUE** LED will glow steadily and the **GREEN** LED will blink.)

4. Enter the new User PIN and press the ☝ button (the **GREEN** LED will blink three times, followed by the **BLUE** LED glowing steadily and the **GREEN** LED blinking.)

5. Re-enter the new User PIN and press the ☝ button (the **GREEN** LED will glow steadily for a second or two, then will return to the User mode)

Setting One-Time-Use Recovery PINs

The Admin has the ability to set Recovery PINs that will allow a User to access data on the device in the event of a forgotten PIN. The Admin can establish up to four one-time-use Recovery PINs. Once a Recovery PIN has been used to access the Aegis Fortress, it will no longer be available. NOTE: The Recovery PIN will not unlock the device, but will place the drive into a User Forced Enrollment state, where the User can then establish a new User PIN and regain access the device's data.

1.   Enter the Admin mode. (Hold 🔓 + 0 for five seconds. With the **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will now glow steadily.

2.   Press the 🔓 + 8 buttons. The **GREEN** LED will blink three times by itself, and then will be joined by a steady **BLUE** LED.

3.   Enter the Recovery PIN and press the 🔓 button. If PIN is accepted, the **GREEN** LED will blink three times.

4.   Repeat by entering that same Recovery PIN and pressing the 🔓 button again. If PIN is accepted for the final time, the **GREEN** LED will illuminate for a second or two and the device will then return to the Admin mode indicated by a steady **BLUE** LED.

5.   To add more Recovery PINs, repeat steps 2-4. When finished, press the 🔒 button to return drive to its Standby mode.

Using a One-Time-Use Recovery PIN

Deploying a Recovery PIN will put the device into a state of User Forced Enrollment and that recovery PIN will no longer be useable. Additionally, once in a state of User Forced Enrollment, the previous User PIN will no longer be recognized as a valid PIN for drive authentication and a new User PIN must be created.

1.   With the drive in Standby mode, press and hold the 🔓 + 7 buttons together for five seconds and release once the **RED** LED starts blinking.

2.   Enter a recovery PIN (from Admin) and press the 🔓 button. The **GREEN** LED will blink three times by itself, and then will be joined by a steady **BLUE** LED indicating the drive is in User Forced Enrollment mode.

3.   Enter a new User PIN and press the 🔓 button. The **GREEN** LED will blink three times if accepted.

4.   Re-enter that same new User PIN and press the 🔓 button again to verify it. If accepted, the **BLUE** LED will illuminate for a second or two, followed by the **GREEN** LED which will then be replaced by the **RED** LED glowing steadily, indicating that the device has returned to its Standby state. The contents of this drive will now be accessible using this new User PIN.

Setting Read-Only or Read / Write Modes From the Admin Mode

With a large number of viruses and Trojans that attach themselves to USB devices, this feature is especially useful if you need to access data on the drive when used in a public setting. Additionally, *Read-Only* is an important feature for forensic applications, where data must be preserved in its original, unaltered state and can't be overwritten or modified.

The Admin can set the drive to a *Read-Only* mode for both the Admin and the Users. When set by the Admin, the Admin is the only one that can change the drive back to *Read / Write* mode.

When the drive is unlocked in *Read-Only* mode, the **GREEN** LED will glow steadily and the **RED** LED will blink once every three seconds.

To Set the Drive to Read-Only:

1. Enter the Admin mode. (Hold 🔓 **+ 0** for five seconds – with **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will glow steadily.

2. Press and hold the **r + o** *(7 + 6)* buttons together until the **GREEN** LED blinks three times.

3. The drive will return to Admin mode. The **BLUE** LED will glow steadily.

4. Until changed, the drive can only be read.

To Return the Drive to Read / Write:

1. Enter the Admin mode. (Hold 🔓 **+ 0** for five seconds – with the **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will glow steadily.

2. Press and hold the **r + w** *(7+ 9)* buttons together until the **GREEN** LED blinks three times.

3. The drive will return to Admin mode, indicated by the **BLUE** LED glowing steadily and the drive restored to its normal *Read / Write* condition.

Important Note

Setting the drive to Read / Write from Admin mode will globally override any User Read-Only settings.

Setting Read-Only or Read / Write From the User mode

This mode allows the User to set the *Read / Write* status of the drive without having access to the Admin functions.

When the drive is unlocked in *Read-Only* mode the **RED** LED will blink once every three seconds while the **GREEN** LED will glow steadily.

If the drive is set to *Read-Only* in the Admin mode, the User cannot override that setting. Only the Admin can return the drive to *Read / Write* Mode.

To Set the Drive to Read-Only:

1. Plug device into USB port. The **RED** LED will glow steadily.

2. Press the **r + o** *(7 + 6)* buttons together for three seconds.
    The **GREEN** LED will blink three times.

3. Enter the User / Admin PIN and press 🔓. The **GREEN** LED will blink.

4. The drive will be in the *Read-Only* state and will remain until it's changed.

To Return the Drive to Read / Write:

1. Plug device into USB port. The **RED** LED will glow steadily.

2. Press the **r + w** *(7+ 9)* buttons together for three seconds.
    The **GREEN** LED will blink three times.

3. Enter the User / Admin PIN and press 🔓.
    The **GREEN** LED will glow steadily.

4. Drive will return to unlocked mode and can now be written to, indicated by the blinking **GREEN** LED.

Important Note

Any changes to the Read-Only or Read / Write settings in User Mode will only affect the user that unlocked the drive, any other users will be unaffected.

To set the drive in the Read-Only mode for all users, set the Read-Only mode using the Admin function.

Setting LED Flicker / Button Press Indicator

Creates a flickering effect in LED lights indicating positive button presses

1. Enter the Admin mode. (Hold 🔓 **+ 0** buttons for five seconds – with **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will glow solidly.

2. Once in the Admin mode, press **0 + 3** together to enable LED Flicker mode.

3. To disable LED Flicker mode, (while in Admin mode) press the **0 + 4** buttons together.

Setting Minimum PIN Length Requirement

The Aegis Fortress L3's minimum PIN length default setting is 7, however, for greater security, a longer minimum PIN setting of up to 16 characters can be implemented.

1. Enter the Admin mode. (Hold 🔓 **+ 0** for five seconds – with **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will glow solidly.

2. Press the 🔓 **+ 4** buttons; The **RED** LED will blink.

3. Pressing two digits, enter the new minimum PIN length; e.g.: 08 = 8 characters, 11 = 11 characters, etc.

4. If accepted, the **GREEN** LED will blink three times and the Aegis Fortress will return to the Admin mode, indicated by the **BLUE** LED glowing solidly. If the numeric entry is below 07, or greater than 16, the **RED** LED will blink three times indicating entry error and your command will not be accepted.

Setting the Unattended Auto-Lock Feature

To protect against unauthorized access if the drive is unlocked and unattended, the Aegis Fortress can be set to automatically lock after a pre-set amount of time. In its default state, the Aegis Fortress Unattended Auto Lock feature is turned off. The Unattended Auto Lock can be set to activate after 5, 10 or 20 minutes.

To set the Unattended Auto Lock please uses the following steps:

1. Enter the Admin mode by pressing and holding 🔓 **+ 0** for five seconds until the LED flashes **RED**. This indicates that you can enter the Admin PIN.

2. Enter the Admin PIN and press 🔓. The drive is in Admin Mode when the LED has changed to solid **BLUE**.

3. Once in Admin mode, press 🔓 **+ 6**. The LED should start flashing **RED** and **BLUE** intermittently.

4. Press one of the numbers below that corresponds to amount of time you would like the drive to lock after no activity:

    1=5 minutes

    2=10 minutes

    3=20 minutes

    0=OFF

    The Default is OFF for this feature.

5. After you have entered the desired amount of allowable inactivity, the **GREEN** LED will blink three times indicating command acceptance, and then will return to the Admin mode, indicated by the **BLUE** LED glowing steadily.

Lock-Override Mode

Certain users may encounter a case where they need the drive to remain unlocked during a reboot, passing the device through a virtual machine or other similar situations which, under normal circumstances, would cause the drive to lock. To help facilitate this use case, "Lock-Override Mode" will allow the drive to remain unlocked through USB port re-enumeration and will not lock again until USB power is interrupted.

NOTE: When in this mode, the drive is vulnerable to being moved from one computer and connected to another computer provided USB power is uninterrupted. Due to this vulnerability, we strongly recommend this mode be used ONLY in circumstances where the drive can be physically secured (as in a locked Server Room) or in a place where it can be visually monitored while in this mode. Use of a powered hub or a Y-cable increases this security risk.
Always return the drive to the default *Lock-Override Mode OFF* when returning to normal service.

To set the "Lock-Override" to *On*:

1. Enter the Admin Mode (Press and hold � **+ 0** for five seconds until the **RED** LED blinks, then enter the Admin code and press the ☝ button. The **BLUE** LED will glow steadily.)

2. Press the **7 + 1** together until the **GREEN** LED blinks three times. The **BLUE** LED will glow steadily.

3. When the device is unlocked and attached to a USB port in "Lock-Override Mode", the **BLUE** LED will blink once every three seconds to alert you that "Lock-Override" mode is active.

Note: If "Unattended Auto-Lock" mode has been turned on, "Lock-Override" will not override it; the device will lock itself upon reaching the selected amount of inactivity. If you need the Fortress to stay unlocked, Enter the Unattended Auto-Lock Feature and set the lock timer to **"0"** (0 = OFF) See Page 10.

To turn Lock-Override Mode off and return to normal operation:

4. Enter the Admin Mode (Press and hold ☝ **+ 0** for five seconds until the **RED** LED blinks. Then enter the Admin code and press the ☝ button. The **BLUE** LED will glow steadily.)

5. Press the **7 + 0** together until the **GREEN** LED blinks three times. The **BLUE** LED will glow steadily.

6. To verify, unlock the key in User mode and check that the **BLUE** LED is no longer blinking.

Aegis Fortress L3 Brute Force Protection

What is Brute Force Attack?

A *Brute-Force Attack* is a means of breaching a cryptographic data defense scheme by systematically running an astronomical number of decryption possibilities. With AES 256 having never been cracked, the data stored on an Apricorn secure device is going to be more than well-protected against brute-force. But brute-force attacks aren't necessarily aimed at the bulk of the data itself, but rather, at the drive's access PINs. After all, PINs are usually the weakest links of any data protection plan, and as such, PINs are essentially all that a brute-force attack needs to decrypt.

Brute Force Feature

1. After three unsuccessful attempts, the Aegis Fortress will add additional time delays to each subsequent try thereafter. The **RED** LED will blink the number of failed attempts after three, all the way up to the tenth (and final) try.

2. After up to ten unsuccessful attempts, the keypad will lock up, no functions will work, and the **RED** LED will blink at a rate of three flashes per second.

3. From this point, the drive will only allow up to ten additional attempts before the drive assumes that it is under brute-force attack and automatically deletes all of its data.

4. To gain these ten extra attempts, press the ☌ **+ 5** buttons together until the **RED** and **GREEN** LEDs blink alternately.

5. Enter the code "*LastTry*" **(5278879)** and press the ☌ button.
    --You will now have ten additional attempts.

6. When the drive is successfully unlocked, the Brute-Force counter will return to zero.

The number of attempts possible, both before and after the LastTry (5278879) code is entered, can be set (in Admin Mode) between two and ten attempts.

Setting the before/after attempts to the minimum of two would allow for a total of four attempts (two before entering the last try code and two after.)

To reduce the number of Brute-Force attempts:

1. Enter the Admin mode. (Hold ☌ **+ 0** for five seconds – with the **RED** LED blinking, enter the Admin PIN and press the ☌ button.) The **BLUE** LED will glow steadily.

2. Press the ☌ + **5** buttons together until the **RED** LED double-blinks.

3. Press the number of before/after attempts desired on the numeric keypad (2 - 9). The **GREEN** LED will blink the same number of times to correspond to the number you have entered (for example: the **8** button will result in eight blinks, and yield eight attempts *before* the LastTry code and another eight attempts *after*, yielding a total of 16.) To return the drive to its default setting, press the **1** then **0** keys to change the number back to ten attempts.

    Note: The number of before and after attempts are the same, i.e., 4 before / 4 after, 8 before / 8 after, etc.

Setting a Self-Destruct PIN

For certain users, it's important to have a "last-resort" level of security where sensitive data falling into the wrong hands must be avoided. The Fortress' Self-Destruct PIN defends against physically compromising situations by erasing the device's contents, leaving it to look as if it never had any data written to it. ***USE WITH CAUTION*** When this mode is activated and the device is unlocked with the Self-Destruct PIN, it will effectively perform a crypto-erase, deleting all of its data. Additionally, the encryption key will be deleted and a new encryption key will be created to take its place. When this Self-Destruct PIN is deployed, the device will unlock and the **GREEN** LED will glow solidly as if the key is being normally unlocked. The device, however, will need to be partitioned and formatted before it can be used again. The previous Admin and User codes will be deleted in the crypto-erase and the Self-Destruct PIN will then become the new Admin PIN to unlock the device.
The self-destruct PIN can be set by either the Admin or the User. If the Admin sets the self-destruct PIN, only the Admin can disable or change the PIN. If the User sets the self-destruct PIN, both the User and the Admin can change or overwrite the PIN.
Note: The Self-Destruct PIN must be different from the Admin PIN and User PIN.

1. By default, the Self-Destruct feature is disabled. To allow the Aegis Fortress to be set with a Self-Destruct PIN, Enter the Admin mode. (Hold 🔓 **+ 0** for five seconds – with **RED** LED blinking, enter the Admin PIN and press the 🔓 button.) The **BLUE** LED will glow steadily.

2. Press the **7 + 4** buttons together*. The **GREEN** LED will blink three times and at this point, the Self Destruct PIN can now be set by the Admin while the drive is in the Admin mode, or it can be set up at another time by the User (after the drive is unlocked with the User PIN) with the following steps.

3. Press 🔓 **+ 3** until the **RED** and **BLUE** LEDs begin to blink alternately.

4. Enter the Self-Destruct PIN and press 🔓. The **GREEN** LED will blink three times and then will return to **RED** and **BLUE** LEDs blinking alternately.

5. Re-enter the Self-Destruct PIN and press 🔓. The **GREEN** LED will momentarily glow steadily and then will return to either the Admin mode (indicated by the **BLUE** LED glowing steadily) or the unlocked state if created by User.

6. To enable or disable the Self-Destruct PIN, enter the Admin mode and press the **7 + 4** buttons together for a second or two; successful enablement will be indicated by three **GREEN** LED blinks. successful disablement of Self Destruct mode (press and hold the **7 + 4** buttons again) is indicated by three **RED** LED blinks.

Self-Destruct PIN Set by the User
If the device is enabled for Self-Destruct Mode by the Admin, unlock the device with the User PIN and follow steps 3 - 5. Additionally, the User can change their Self-Destruct PIN by following these same steps. Note that the mode can't be enabled or disabled in the User mode.

Performing a Complete Reset

NOTE: A complete reset will erase encryption keys and PINs and leave the Aegis Fortress in an unformatted condition.

There may be circumstances (forgotten PIN, redeployment, return to factory default settings) when you need to completely reset the drive. The complete reset feature will perform a crypto-erase on the drive, generate a new encryption key, delete all users, and return all of the settings to factory default.

To perform a complete reset of the drive, perform the following:

1. Press and hold 🔓 **+** 🔒 **+ 2** together for several seconds. The **RED** and **BLUE** LEDs will blink alternately.

2. Release all buttons when the **GREEN** and **RED** LEDs glow steadily which will continue for several seconds, followed by the **GREEN** LED glowing steadily for several seconds, and then will be followed finally by the **GREEN** and **BLUE** LEDs glowing steadily, indicating that the reset is complete.

3. A new Admin PIN will need to be entered and the drive will need to be reformatted.

Initializing and Formatting After Performing a Complete Reset

A complete reset of the Fortress L3 will erase all information and partition settings. You will need to initialize and format the device as follows.

Plug device into USB Port. Both the **BLUE** and **GREEN** LEDs will glow steadily.

Press 🔓 **+ 9** at the same time. The **BLUE** LED will glow steadily and the **GREEN** LED will blink.

1. Enter the series of numbers that you will use for the Admin PIN and press the 🔓 button.*

2. Re-enter that same PIN and press the 🔓 button again. The **GREEN** LED will illuminate for one second, then replaced by the **BLUE** LED glowing steadily.

3. The drive is now in Admin mode where Admin features can be set (e.g., adding a User.)

4. If no further user(s) or functions are to be added, you can exit the Admin mode by pressing the 🔒 button and the drive will return to the locked standby state. If no action is taken within 30 seconds, the drive will return to its locked sleep state.
   *_*GREEN LED will blink if the PIN is accepted; If the PIN is NOT accepted, the RED LED will blink-- see PIN requirements below._*

5. UNLOCK the drive by entering the new Admin PIN and pressing 🔓.

6. Open Disk Management

7. Windows 7 : Click "Start", then right click "My Computer", select "Manage". A window will pop-up, select "Disk Management" from the left-most pane.

8. Windows 8+ : Right click "Start", select "Disk Mangement"

9. Right click box that reads, "Not Initialized" and select, "Initialize Disk". Click, "Ok" in the window that pops up.

10. Right click box that reads, "Unallocated" and select, "New Simple Volume". Follow the "New Simple Volume Wizard" prompts to complete format.

11. Wait until the format process is complete. The Aegis Fortress will be recognized and available for use.

Hibernating, Suspending, or Logging-Off from the Operating System

Be sure to save and close all the files on your Aegis Fortress before hibernating, suspending, or logging off from the Windows operating system.

It is recommended that you lock the Aegis Fortress manually before hibernating, suspending, or logging off from your system.

To log off the Aegis Fortress, double-click Safely Remove Hardware on the Windows desktop and remove the Aegis Fortress from your computer.

Attention: To ensure the data integrity of your Aegis Fortress, be sure to lock or log off your Aegis Fortress if you are:
- Away from your computer
- Using the switching user function by sharing a computer with others

Aegis Fortress Setup for Mac OS®

Your Aegis secure drive is preformatted in NTFS for Windows. To reformat the drive to a Mac compatible format please read the below.

Once the drive is unlocked, open Disk Utility from Applications/Utilities/ Disk Utilities and perform the following.

1. Select the Aegis Fortress L3 from the list of drives and volumes. Each drive in the list will display its capacity, manufacturer, and product name, such as 232.9 Apricorn Fortress.

2. Click the 'Erase' tab.

3. Enter a name for the drive. The default name is Untitled. The drive's name will eventually appear on the desktop.

4. Select a volume format to use. The Volume Format dropdown menu lists the available drive formats that the Mac supports. The recommended format type is 'Mac OS Extended (Journaled).'

5. Click the 'Erase' button. Disk Utility will unmount the volume from the desktop, erase it, and then remount it on the desktop.

Diagnostic Mode

The keypad has a manual diagnostic mode built-in to verify proper keypad function and troubleshooting purposes. This mode will not allow access to any data or admin function. It can only be used to identify the firmware level and to test button recognition.

To enter the diagnostic function:

1. From standby mode, press 🔒 **+ 1**, release, then press and continue to hold the **0** button as the **RED** and **BLUE** LEDs blink alternately. Once all three LEDs illuminate steadily, release the **0** button.

2. The **BLUE** LED will blink a number of times to represent the number of both the major and minor revisions. The decimal point will be represented by a single **RED** LED blink. Upon completion, the **BLUE** LED will glow steadily. *(Example: **VERSION 4.1** would be indicated by four **BLUE** LED blinks, one **RED** LED blink, one **BLUE** LED blink, and one **RED** LED blink, then revert to the **BLUE** LED glowing steadily.)*

3. To check the keypad's button functionality, press each button and the number of the button pressed will be expressed by the **RED** LED blinking. (Example: **1 Button**= 1 blink, **2 Button** = 2 blinks, **3 Button** = 3 blinks...**0 Button** = 10 blinks, 🔒 **Button** = 11 blinks, 🔓 **Button** = 12 blinks.)

4. To exit the Diagnostic Mode, either unplug the device from its USB port or hold the 🔒 **Button** for ~7 seconds to return the key to its normal operation.

Self-Diagnostics:

During the initial power up, after the drive has been plugged into a USB port, the drive will perform self-diagnostics on the encryption algorithm and critical hardware components. If the **RED** LED blinks at a rate of one blink per second for 15 seconds, returns to standby and will not unlock, unplug the drive from USB port and try again. If the **RED** LED continues to blink in the manner mentioned above and won't unlock upon USB re-insertion, a critical component has failed and the drive can no longer function.

If the drive blinks a triple-**RED** LED pattern that is repeated every two seconds when unlocked, a failure has occurred that will not immediately stop the device from working nor affect the security of the device, but should be considered as a warning that the device needs to be replaced in the near future. Additionally, Admin features may be limited in this mode.

If either condition should appear, remove the drive from the USB port and allow the drive to go to sleep, and try to unlock the drive again. The event of either diagnostic failure will be very rare, but if the drive cannot recover, it must be replaced.

Quick Reference Guide for Programming Key Combinations

Standby Mode

- 7+6 = Read-Only On

- 7+9 = Read-Only Off

- 🔓 + 7 = Use Data Recovery PIN

- 🔓 + 🔒 +2 (hold for 10 secs) = Complete Reset

- 🔒 +1 then hold 0 = Diagnostic Mode

User Mode

- 🔓 + 1 = Enter User PIN (from forced enrollment state)

- 🔓 + 3 = Set Self-Destruct PIN

ADMIN Mode

- 🔓 + 0 = Enter Admin Mode

- 🔓 + 1 = Create User PIN

- 🔓 + 2 = not used

- 🔓 + 3 = Set Self Destruct PIN Admin or User setup

- 🔓+ 4 = Set Minimum PIN length

- 🔓 + 5 = Set Brute Force Attempts

- 🔓 + 6 = Auto Lock

- 🔓 + 8 = Enter Recovery PIN

- 🔓 + 9 = Enter / Change Admin PIN

- 7+1 = Turn Lock Override On

- 7+0 = Turn Lock Override Off

- 7+ 4 = Disable / Enable Self-Destruct PIN

- 7+6 = Read-Only On

- 7+9 = Read-Only Off

- 7+8 = Erase User and Self-Destruct PIN's

- 0+1 = Set Forced-Enrollment for User

- 0+3 = Turn On LED Flicker When Entering PIN from Standby

- 0+4 = Turn Off LED Flicker When Entering PIN from Standby

Technical Support

Apricorn provides the following helpful resources for you:

1. Apricorn's Website: **https://www.apricorn.com**

2. Tech Support / FAQs: **apricorn.com/faqs**

3. E-mail us at **support@apricorn.com**

4. Or call the Technical Support Department at **1-800-458-5448**

Apricorn's Technical Support Specialists are available from 8:00

a.m. to 5:00 p.m., Pacific Standard Time, Monday through Friday

Warranty and RMA information

Three Year Limited Warranty:
Apricorn offers a 3-year limited warranty on the Aegis Fortress against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from Apricorn or an authorized reseller.

Disclaimer and terms of the warranties:
THE WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE DISPLAYING THE DATE OF PRODUCT PURCHASE.

APRICORN WILL, AT NO ADDITIONAL CHARGE, REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF APRICORN.

THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM APRICORN OR AN AUTHORIZED RESELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLECT, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE: 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY APRICORN; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERNATION OR REPAIR BY ANYONE OTHER THAN APRICORN AND SHALL BE VOID. THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.

NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF APRICORN OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR.

APRICORN SHALL NOT BE LIABLE BY VIRTUE OF THIS WARRANTY, OR OTHERWISE, FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE INCLUDING ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, WHETHER OR NOT APRICORN WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

APRICORN