Aegis Padlock DT FIPS

User's Manual

Remember to memorize / save your authentication and recovery PINs in a safe place.

APRICORN

Data Security at Your Fingertips

Table of Contents

First-Time Use	4
Locking the Drive	4
Unlocking the Drive	4
LED States and Their Meaning	5
Admin Mode	5
Adding a New User PIN (Via Admin Mode)	6
Adding a New User PIN (Via User Forced Enrollment Mode)	6
Deleting the User PIN	7
Changing the User PIN	7
Changing the Admin PIN	7
Setting One-Time-Use Recovery PINs	8
Using One-Time-Use Recovery PINs	8
Setting Read-Only or Read / Write Modes from Admin Mode	9
Setting Read-Only or Read / Write Modes from the User Mode	10
Setting LED Flicker / Button Press Indicator Mode	11
Setting Minimum PIN Length Requirement	11
Setting the Unattended Auto-Lock Feature	11
Setting a Self-Destruct PIN	12
Aegis Padlock DT FIPS Brute-Force Protection	13
Performing a Complete Reset	14
Initializing and Formatting After a Complete Reset	15
Hibernating or Logging Off from the Operating System	16
Aegis Padlock DT Setup for Mac OS	16
Diagnostic Mode	17
Lock-Override Mode	18
Troubleshooting / FAQs	19
Quick Reference Guide for Key Command Programming	20
Warranty and RMA information	21

Package contents

- Aegis Padlock DT FIPS
- AC Adapter
- USB 3.0 data cable (backwards compatible with USB 2.0)
- Quick Start Guide

Revised June 2018

First-Time Use

Before you begin, ensure that the USB cable is connected, the power cable is connected to the drive and plugged into an outlet, and the power switch is turned ON.
Each Aegis Padlock DT FIPS is shipped without a preset Personal Identification Number (PIN) installed on the device. A 7- to 16-digit Admin PIN must first be established before the drive can be used. This Admin PIN can be used to set any and all of the Admin Mode Features of the drive, as well as to access its data. **Note: PINs can't be repeating or sequential numbers such as 0123456, 987654321, or 1111111, 2222222, etc.**

NOTE: if you are using the Aegis Configurator to set up your Aegis Padlock DT FIPS or any other Apricorn secure drive, you must first ensure that the device to be configured has the "configurable" logo on the belly label and second, DO NOT perform any of the the following Manual Admin and USER PIN SETUP steps below; The Aegis Configurator will execute these setup steps and will only recognize devices in their factory "out of box" state or devices that have been completely reset.

To Set Up the Admin PIN:

1. Plug device into USB Port. Both the **BLUE** and **GREEN** LEDs will glow steadily.
2. Press 🔓 **+ 9** at the same time. The **BLUE** LED will glow steadily and the **GREEN** LED will blink.
3. Enter the series of numbers that you will use for the Admin PIN and press the 🔓 button.*
4. Within 30 seconds, 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.
5. The drive is now in Admin mode where Admin features can be set (e.g., adding a User.)
6. To exit the Admin mode, press the **CANCEL** button. 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-- return to step 4 to resume the Admin PIN setup process.***

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.

Locking the Drive

Press the **CANCEL** button. When successfully locked, The **RED** LED will glow steadily, indicating that it's returned to its standby state.
The Aegis Padlock DT will not be recognized by the operating system while in its standby state.

Note: If data is still being written to the key when the CANCEL button is pressed, the Padlock DT will wait until that operation is completed before the lock command is executed.

Admin Mode

To set up any of the drive's Admin functions, 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. While in the Admin mode, the actual data on the drive will not be accessible.
Prior to your first use of the Aegis Padlock DT, you must first create the Admin PIN. Immediately after setting the Admin PIN, you may then continue setting up other functions. If you'd like to skip the function setup, or do it at another time, either press the CANCEL button or do nothing for a period of 30 seconds and the key will revert to its standby state.
To re-enter the Admin mode, 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 **CANCEL** button.

LED States and Their Meaning

○ ○ ○	No LEDs	Drive locked, power switch is off, device unplugged
🔴 ○ ○	Blinking **RED**	Error / incorrect button entry; Mode Not Available; User PIN Change
🔴 ○ ○	Solid **RED**	Locked / Standby state; Awaiting PIN entry
○ 🟢 ○	Blinking **GREEN**	Button-entry accepted
○ 🟢 🔵	Solid **BLUE** / Blinking **GREEN**	Waiting for New User or Admin PIN to be established
○ ○ 🔵	Solid **BLUE**	Admin Mode
○ 🟢 ○	Solid **GREEN**	Drive unlocked
○ ○ 🔵	Slow Blinking **BLUE**	Drive unlocked in Lock-Override Mode
🔴 🟢 ○	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 key 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

Establishing a User PIN

If no additional Users beyond the Admin will be permitted to access the drive's data, disregard this page's contents as it relates only to the "User" PINs.

The Aegis Padlock DT can have one Admin and four additional Users, making a total of five authentication PINs.
Adding a User is a perfect way to securely share the drive or deploy it for use where the Users do not require access to the drive's Admin features. While the Users have limited functionality and no Admin rights to the drive, they can still access all of its data, change their own User 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. Within 30 seconds, re-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 steadily.
2. Press **0 + 1** and the **GREEN** LED will blink three times, then will be replaced by **BLUE** LED glowing steadily. Press the **CANCEL** button to return the drive to its locked state. The drive is now in *User Forced Enrollment State*, allowing the first User to establish his own User PIN.

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 key's data can now be accessed using either the User PIN or the Admin PIN.

* **Note: Default setting for PIN length is 7 characters min. / 16 max. PINs can't be consecutive numbers (0123456) or repeating the same number (2222222).**

Deleting the User PIN

You can delete the User PIN by doing the following:

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 two seconds.
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 the User PIN

The User PIN can be changed within the User mode (drive unlocked, **GREEN** LED blinking)

*Note: The Admin PIN cannot be changed while in the User mode. The Admin PIN can only be changed from within the Admin mode-- See below.
You can change the User PIN by doing the following:

1. Unlock the Aegis Padlock DT 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 two seconds, then will return to the User mode, indicated by the **GREEN** LED blinking.)

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 **UNLOCK + 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.

Setting One-Time-Use Recovery PINs

Gives the Admin the ability to set Recovery PINs that will allow a User to access data on the Padlock DT FIPS in the event of a forgotten PIN by creating a new state of User Forced Enrollment in which a new User PIN can be established without wiping any data off of the drive. The Admin can establish up to four ***one-time-use*** Recovery PINs. Once a Recovery PIN has been used to access the drive, 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 then access the drive'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 blink three times and the Padlock DT 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 **CANCEL** button to return drive to its Standby mode.

Using a One-Time-Use Recovery PIN

Remember that using a Recovery PIN to set the Padlock DT into User Forced Enrollment renders that Recovery PIN spent / unavailable for future use.

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 **GREEN** LED will blink three times and then the Padlock DT will return to its Standby state, indicated by the **RED** LED glowing steadily. The contents of this drive will now be accessible using this new User PIN.

Setting Read-Only or Read / Write modes from 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 for three seconds. The **GREEN** LED will blink 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; the **GREEN** LED will blink 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 the Admin mode will globally override a *Read-Only* mode that has been set by a User.

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. Start with the drive in stand-by mode (indicated by the **RED** LED glowing 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 a *Read-Only* state the next time it is unlocked.

To Return the Drive to Read / Write:

1. Press the 🔓 button to wake the key. 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

Setting the drive to *Read/ Write* from the User mode will not override a *Read-Only* setting that was placed by the Admin.

To set the drive to be in *Read-Only* mode for both the User and the Admin, 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 steadily.
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 Padlock DT's minimum PIN length default setting is 7, however, for even 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 steadily.
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 drive will return to the Admin mode, indicated by the **BLUE** LED glowing steadily. 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 key is unlocked and unattended, the Aegis Padlock DT can be set to automatically lock after a predetermined period of inactivity. In its default state, the drive's *Unattended Auto-Lock* feature is turned off.
The *Unattended Auto-Lock* can be set to activate after 5, 10 or 20 minutes of inactivity.

To set the *Unattended Auto-Lock,* perform the following steps:

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. Once in the Admin mode, press 🔓 **+ 6**.
   The **RED** and **BLUE** LEDs will blink alternately.
3. Press one of the numbers below that corresponds to the amount of inactivity you would like to set for the drive to lock itself:

   0 = OFF (The Default is OFF for this feature.)

   1 = 5 minutes

   2 = 10 minutes

   3 = 20 minutes
4. 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.

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 Padlock DT's Self-Destruct PIN defends against physically compromising situations by erasing the key'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 drive is unlocked with the Self-Destruct PIN, it will effectively perform a crypto-erase on the drive, 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 drive will unlock and the **GREEN** LED will glow steadily as if the drive is being normally unlocked. The drive, 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 drive.
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 Padlock DT 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 **UNLOCK + 3** for five seconds. The **RED** and **BLUE** LEDs will 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 glow steadily for three seconds 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.
7. **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.

Aegis Padlock DT 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 a Padlock DT FIPS 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 Padlock 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 and hold the **5** button and then press the **UNLOCK** button 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 and hold the 🔓 + **5** button for three seconds.
   The **RED** LED will double-blink.
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.

Performing a Complete Reset

NOTE: A complete reset will erase encryption keys and PINs and leave the Aegis Padlock DT FIPS 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 the **CANCEL** button and turn the power switch to the ON position. Release the **CANCEL** button once the power-up self-test concludes (when only the **RED** LED glows steadily.)
2. Within five seconds of releasing the **CANCEL** button, press and hold 🔓 **+ CANCEL + 2** together for about ten seconds, until the **RED** and **BLUE** LEDs blink alternately, then release all buttons.
3. The **GREEN** and **RED** LEDs will glow steadily for several seconds, followed by the **GREEN** LED glowing steadily for several seconds, followed finally by the **GREEN** and **BLUE** LEDs glowing steadily which indicates that the reset is complete.
4. A new Admin PIN will need to be entered and the drive will need to be reformatted.

Initializing and Formatting the Aegis Padlock DT FIPS After a Complete Reset

A complete reset of the Aegis Padlock DT FIPS will erase all information and partition settings. You will need to initialize and format the drive again after reset.

To initialize your Padlock DT, perform the following steps:

1. After a complete reset, press 🔓 **+ 9**.
   The **BLUE** LED will glow steadily and the **GREEN** LED will be blinking.
2. Enter the new Admin PIN and press the 🔓 button. If accepted, the **GREEN** LED will quickly blink three times, then return to the **BLUE** LED glowing steadily and the **GREEN** LED blinking.
3. Re-enter the Admin PIN and press the 🔓 button. If accepted, the **GREEN** LED will be solid for two seconds.
4. The **BLUE** LED will glow steadily for 30 seconds (or until the **CANCEL** button is pressed, which will return the drive to its standby state.)
5. The Admin PIN is now set and will allow access to the drive or the Admin features.
6. To **UNLOCK** the drive, enter the new Admin PIN and press 🔓.
7. Windows 7 and earlier: Right-click ***My Computer,*** and then click ***Manage*** from the Windows desktop.

   Windows 8, 8.1, or 10: Right-click left corner of desktop and select ***Disk Management.***
8. In the ***Computer Manage*** window, click ***Disk Management.*** In the ***Disk Management*** window, the Aegis Padlock 3 is recognized as an unknown device that is uninitialized and unallocated.
9. Perform the following to make the drive recognizable as a basic drive.
   - If the ***Initialize and Convert Disk Wizard*** window opens, click ***Cancel*** and initialize the disk manually using the following steps:
     a. Right-click ***Unknown Disk*** and then select ***Initialize Disk***.
     b. In the ***Initialize Disk*** window, click **OK**.
10. Right-click in the blank area under the Unallocated section, and then select *New Partition* or *New Simple Volume* (depending on your OS.) The ***Welcome to the New Partition Wizard*** window opens.
11. Click ***Next***.
12. Select ***Primary Partition*** and then click ***Next***.
13. If you need only one partition, accept the default partition size by clicking ***Next***.
14. Click ***Next***.
15. Create a volume label, select ***Perform a quick format,*** and then click ***Next***.
16. Click ***Finish***.
17. Wait until the format process is complete. The Aegis Padlock DT 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 Padlock 3 before hibernating, suspending, or logging off from the Windows operating system.

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

To log off the Aegis Padlock 3, double-click ***Safely Remove Hardware*** on the Windows desktop and remove the **Aegis Padlock 3** from your computer.

Attention: To ensure the data integrity of your Aegis Padlock 3, be sure to lock or log off your Aegis Padlock 3 if you are:

- Away from your computer
- Using the switching user function by sharing a computer with others

Aegis Padlock DT FIPS Setup for® Mac OS

Your Aegis Padlock 3 is pre-formatted in NTFS for Windows. To reformat the drive to a Mac compatible format please perform the following:

Once the key is unlocked, open ***Disk Utility*** from Applications/Utilities/Disk Utilities.

To format the Aegis Padlock 3:

1. Select the **Aegis Padlock 3** from the list of keys and volumes. Each drive in the list will display its capacity, manufacturer, and product name, such as 232.9 Apricorn Padlock 3.
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 key issues. 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 **LOCK + 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, **CANCEL Button** = 12 blinks.)
4. To exit the Diagnostic Mode, wait for the 20 second timeout or hold the **CANCEL 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.

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 and hold **7 + 1** for three seconds. The **GREEN** LED will blink three times, then the **BLUE** LED will glow steadily.
3. When the key 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 key will lock itself upon reaching the selected amount of inactivity. If you need the key 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 and hold **7 + 0** for three seconds. The **GREEN** LED will blink three times then 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.

Troubleshooting / FAQs

This section contains troubleshooting information and FAQs for the Aegis Padlock 3.

Q: What can I do if I forget the User PIN?
A: Use your Admin PIN to enter the Admin Mode and create another User PIN. Additionally you may access the drive by enabling a recovery PIN and establishing a new USER PIN.

Q: What can I do if I forget the Admin PIN?
A: Using a valid User PIN or a data recovery PIN to access the data on the drive, back up all of the data onto another device. Once the device’s data has been backed up, you’ll need to perform a complete reset of the Aegis Padlock DT FIPS, after which, all data and PINs will be zeroed out, leaving the drive ready to be reformatted and reconfigured with a new Admin PIN.

Q: Why did the operating system not recognize the Aegis Padlock DT, after I did a complete re-set of the drive?
A: You need to initialize, allocate and format the Aegis Padlock DT manually. For more information, refer to *Initializing and Formatting the Aegis Padlock DT After a Complete Reset* in this manual.

Q: How do I use the Aegis Padlock without a PIN?
A: As a full disk encryption product, the Aegis Padlock can never be used without a PIN.

Q: What encryption algorithm is used in this product?
A: The Aegis Padlock uses AES 256-bit algorithm.

Q: Why could I not initialize, partition, or format the Aegis Padlock?
A: Ensure that you have administrator privileges. You will need Admin privileges to use the Disk Management Utility.

Q: The LED is blinking RED and I can’t enter a code. Why?
A: Somebody has tried to access the key and the code has been entered 10 times incorrectly (see Brute Force section of this manual.)

Q: Is there any way to recover my data if I forget the PIN?
A: If an Admin PIN has been previously set, the Admin PIN can be used to unlock the key and recover the data. Additionally, if recovery PINs have been set and haven’t been previously depleted in the past (up to 4x) you can access the data on your drive using this route. If you don’t have any recovery PINs set or they’re depleted, and do not have an Admin PIN, the data cannot be recovered but the drive can be reset with new PINs and it can then be used again.

Q: Why does the LED indicate an error when I try to change the PIN?
A: PIN requirements for this drive must meet a minimum security level. There are several combinations that are not allowed, such as repeating numbers or sequential numbers. The PIN must be a minimum of six digits, and not longer than 16 digits.

Q: What are the ECCN and HST codes used for shipping this device outside of the United States?

A: ECCN: 5A992.c and HTS code 8473.50.3000

Quick Reference Guide for Programming Key Combinations

Standby Mode

- 7+6 = Read-Only On
- 7+9 = Read-Only Off

Cancel +1 then hold 0 = Diagnostic Mode

User Mode

- Unlock + 1 = Enter User PIN (from forced enrollment state)
- Unlock + 3 = Set Self-Destruct PIN

ADMIN Mode

- Unlock + 0 = Enter Admin Mode
- Unlock + 1 = Create User PIN
- Unlock + 2 = not used
- Unlock + 3 = Set Self Destruct PIN Admin or User setup
- Unlock+ 4 = Set Minimum PIN length
- Unlock + 5 = Set Brute Force Attempts
- Unlock + 6 = Auto Lock
- Unlock + 7 = Set Recovery PIN
- Unlock + 8 = 1X Use to Enter Recovery PIN
- Unlock + 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**)

This gives you the ability to check for up-to-date information

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

3. 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 Time, Monday through Friday

Warranty and RMA information

Three Year Limited Warranty:
Apricorn offers a 3-year limited warranty on the Aegis Padlock DT FIPS 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.

12191 Kirkham Road
Poway, CA, U.S.A. 92064
1-858-513-2000 www.apricorn.com