

Aegis Secure Key 3.0

User's Manual



Remember to save your PIN in a safe place.
If PIN is lost or forgotten, there will be no
way to access data on the key.



Data Security at Your Fingertips

Table of Contents

About the Aegis Secure Key 3.0	4
PIN Requirements	4
Battery Note	4
Waking the Key	5
First-Time Use	5
Admin Mode	5
LED States and Their Meaning	6
Locking the Key	6
Unlocking the Key	6
Establishing a New User PIN	7
Deleting the User PIN	8
Changing the User PIN	8
Changing the Admin PIN	8
Setting One-Time Use Recovery PINs	9
Using One-Time Use Recovery PINs	9
Setting Read-Only or Read / Write Modes from Admin Mode	10
Setting Read-Only or Read / Write Modes from the User Mode	11
Setting LED Flicker / Button Press Indicator Mode	12
Setting Minimum PIN Length Requirement	12
Setting the Unattended Auto-Lock Feature	12
Setting a Self-Destruct PIN	13
Aegis Secure Key Brute-Force Protection	14
Performing a Complete Reset	15
Initializing after Performing a Complete Reset	16
Hibernating or Logging Off from the Operating System	17
Aegis Secure Key Setup for Mac OS	17
Diagnostic Mode	18
Lock-Override Mode	19
Troubleshooting / FAQs	20-21
Technical Support	22
Warranty and RMA information	22

Copyright © Apricorn 2022. All rights reserved.

Windows is a registered trademark of Microsoft Corporation.
All other trademarks and copyrights referred to are the property of their respective owners.

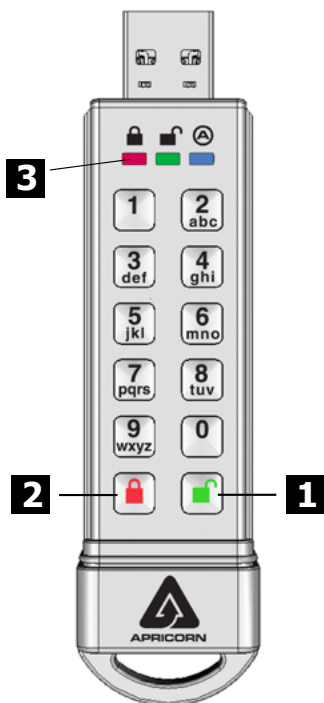
Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.



DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID

Last Revised June 14, 2018

About the Aegis Secure Key 3.0



Note: It's normal for this device to be warm to the touch during use.

- 1**  UNLOCK button
- 2**  LOCK button
- 3** LED Indicator lights

PIN Requirements

PINs must be a minimum of seven digits and a maximum of 16 digits.

Cannot contain all sequential numbers (e.g., 01234567, 9876543) and cannot contain all of the same number (e.g., 1111111, 2222222.)

Note: Sequentially, 0 occurs before 1, not after 9.

Important:

With its flash key size, the Aegis Secure Key also has relatively small buttons. For greater ease and better control of key commands, enter all PINs and command codes onto the Secure Key's keypad **PRIOR** to plugging the device into the USB port for use. Failure to do so may damage the USB port and cause the key to not function properly.



Battery Note

The Aegis Secure Key has an internal rechargeable battery with a smart-charging circuit. For safety, each key ships with a partial charge. Before initial use, we recommend plugging the key into a powered USB port for 80 minutes to fully charge the battery. The battery will automatically charge whenever it is plugged into a powered USB port, regardless of its operational mode. In standby mode, the **RED** LED fades in and out slowly to indicate that it's charging and glows solid **RED** to indicate that it's fully charged. If the battery is completely discharged, the key will go through a self-test (indicated by a **RED**, **GREEN**, and **BLUE** LED sequence) when plugged into a USB port.

Waking the Secure Key

When the Secure Key is not in use, it will enter a sleep state. While in this state, the device is locked and cannot be accessed.

To wake the key so it can accept keypad inputs, press the **UNLOCK** button once. The **RED** LED will glow solidly (standby state.)

Note: If the key has never been used, the **BLUE** and **GREEN** LEDs will glow solidly indicating that the Admin PIN must first be established before the key can be used.

First-Time Use

Each Aegis Secure Key is shipped without a preset Personal Identification Number (PIN) installed on the key. A 7 to 16-digit Admin PIN must be established before the key can be used. This Admin PIN can be used to set any and all of the Admin Mode Features of the key, as well as to access the key's data.



NOTE: if you are using the Aegis Configurator to set up your Aegis Secure Key or any other Apricorn secure drive, first ensure that the device to be configured has the “configurable” logo on the belly label and second, DO NOT perform any of 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. Wake up the key by pressing the **UNLOCK** button. Both the **BLUE** and **GREEN** LEDs will glow solidly.
2. Press **UNLOCK + 9** at the same time. The **BLUE** LED will glow solidly and the **GREEN** LED will be blinking.
3. Enter the series of numbers that you will use for the Admin PIN (See PIN requirements on p. 4) and press the **UNLOCK** button.*
4. Re-enter that same PIN and press the **UNLOCK** button again. The **GREEN** LED will illuminate for one second followed by the **BLUE** LED glowing solidly by itself.
5. The key is now in Admin mode and other Admin features can be set (e.g., adding a User.)
6. To exit the Admin mode, press the **LOCK** button. The key will return to the locked standby state. If no action is taken within 30 seconds, the key 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.*

Admin Mode

To set up any of the key's Admin functions, the Admin mode must first be entered. Once in the Admin mode, each of the key's functions can be addressed with the appropriate button commands. While in the Admin mode, the data on the key will not be accessible.

Prior to your first use of the Aegis Secure Key, you must first set an Admin PIN. Immediately after setting up your Admin PIN, you may then continue setting up other functions. If you do nothing for a period of 30 seconds, the key will revert to its standby state.

To re-enter the Admin mode, perform the following steps below.

1. Press and hold **UNLOCK + 0** for five seconds until the **RED** LED blinks. (This indicates that you can enter the Admin PIN.)
2. Enter the Admin PIN and press the **UNLOCK** button.
3. Admin Mode is indicated by a solid **BLUE** LED.
4. To exit the Admin Mode, either allow 30 seconds of inactivity or press the **LOCK** button.

LED States and Their Meaning

	Slow Fading RED	Battery charging (when plugged into USB port)
	No LEDs	Key locked and asleep
	Blinking RED	Error / incorrect key entry; Mode Not Available; User PIN Change
	Solid RED	Locked / Standby state; Awaiting PIN entry
	Blinking GREEN	Key-entry accepted
	Solid BLUE / Blinking GREEN	Waiting for New User or Admin PIN to be established
	Solid BLUE	Admin Mode
	Solid GREEN	Key unlocked
	Slow Blinking BLUE	Key unlocked in Lock-Override Mode
	Solid GREEN / Slow Blinking RED	Key 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 key (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

Unlocking the Key

1. Press the **UNLOCK** button to wake the key from sleep (as described above.)
The **RED** LED will glow solidly.
2. Enter either a User PIN or Admin PIN and press the **UNLOCK** button. If the PIN is accepted, the **GREEN** LED will rapidly blink three times, then will slow down to one blink per second until it's plugged into a USB port, at which time will glow solidly.
(If the PIN is incorrect, the **RED** LED will blink.)
3. A blinking **GREEN** LED indicates that the key is unlocked and ready for use. The key is now ready to plug into a USB port and will function as an external drive. If it's not plugged into a USB port within 30 seconds, the key will lock itself and return to its sleep state.

Locking the Key

Press the **LOCK** button. When successfully locked, The **RED** LED will glow solidly, indicating that it's in its standby state.

The Aegis Secure Key will not be recognized by the operating system while in its standby state.

Note: If data is still being written to the key, the Secure Key will wait until that operation is completed and then it will lock automatically.

Establishing a User PIN

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

The Aegis Secure Key can have one Admin and one User, making a total of two working PINs. Adding a User is a perfect way to securely share the key or deploy it for use where the User does not require access to the key's Admin features. While the User has limited functionality and no Admin rights to the key, they can still access its data, change their own User PIN, and set the key 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 **UNLOCK + 0** for five seconds; With **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button. The **BLUE** LED will glow solidly.
2. Press the **UNLOCK + 1** buttons together until the **BLUE** LED glows solidly and the **GREEN LED** starts blinking.
3. Enter the User PIN* and press **UNLOCK**. The **GREEN** LED will blink three times by itself, then the **BLUE** LED will glow solidly as the **GREEN** LED continues blinking.
4. Re-enter that same User PIN and press **UNLOCK**. The **GREEN** LED will glow solidly for three seconds verifying that the User PIN was successfully added, and then will be replaced by the **BLUE** LED glowing solidly, indicating that the key 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 PIN 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 **UNLOCK + 0** for five seconds; With **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** 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 **LOCK** button to return the key to its locked state. The key is now in *User Forced Enrollment State*, allowing a User to establish his own User PIN.

USER-GENERATED USER PIN IN FORCED ENROLLMENT STATE

1. Press **UNLOCK** and ensure that the **BLUE** and the **GREEN** LEDs are glowing solidly.
2. Press **UNLOCK + 1** and ensure that the **BLUE** LED continues glowing solidly while the **GREEN** LED blinks. Enter the new User PIN and press the **UNLOCK** button. The **GREEN** LED will blink three times by itself and then will be joined by the **BLUE** LED glowing solidly.
3. Within 30 seconds, enter that same User PIN once more, and press the **UNLOCK** 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 minimum PIN length is 7 characters, and a maximum of 16.**

Deleting the User PIN

You can delete the User PIN by doing the following:

1. Enter the Admin mode. (Hold **UNLOCK + 0** for five seconds. With the **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will now glow solidly.
2. Press and hold the **7 + 8** buttons 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 and hold the **7 + 8** buttons again for five seconds. The **GREEN** LED will glow solidly for two seconds.
4. The key will return to Admin mode indicated by the **BLUE** LED glowing solidly.

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

Changing the User PIN

The User PIN can be changed within the User mode (key 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.

You can change the User PIN by doing the following:

1. Unlock the Aegis Secure Key with the User PIN. (the **GREEN** LED will blink)
2. Press and hold **UNLOCK + 1** for five seconds (the **RED** LED will blink)
3. Enter the current User PIN and press the **UNLOCK** button. (the **BLUE** LED will glow solidly and the **GREEN** LED will blink.)
4. Enter the new User PIN and press the **UNLOCK** button (the **GREEN** LED will blink three times, followed by the **BLUE** LED glowing solidly and the **GREEN** LED blinking.)
5. Re-enter the new User PIN and press the **UNLOCK** button (the **GREEN** LED will glow solidly 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 key is in the Admin mode.

1. Enter the Admin mode. (Hold **UNLOCK + 0** for five seconds – with the **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
2. Press **UNLOCK + 9**. The **BLUE** LED will glow solidly and the **GREEN** LED will blink.
3. Enter the new Admin PIN and press the **UNLOCK** button. The **GREEN** LED will blink three times.
4. Re-enter the new Admin PIN and press the **UNLOCK** button. The **GREEN** LED will glow solidly for two seconds and then return to the Admin mode, indicated by the **BLUE** LED glowing solidly.

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 Secure Key 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 Secure Key, it will no longer be available. NOTE: The Recovery PIN will not unlock the device, but will place the Secure Key into a User Forced Enrollment state, where the User can then establish a new User PIN and then access the Key's data.

1. Enter the Admin mode. (Hold **UNLOCK + 0** for five seconds. With the **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will now glow solidly.
2. Press the **UNLOCK + 8** buttons. The **GREEN** LED will blink three times by itself, and then will be joined by a solid **BLUE** LED.
3. Enter the Recovery PIN and press the **UNLOCK** button. If PIN is accepted, the **GREEN** LED will blink three times.
4. Repeat by entering that same Recovery PIN and pressing the **UNLOCK** button again. If PIN is accepted for the final time, the **GREEN** LED will blink three times and the Secure Key will then return to the Admin mode indicated by a solid **BLUE** LED.
5. To add more Recovery PINs, repeat steps 2-4. When finished, press the **LOCK** button to return Key to its Standby mode.

Using a One-Time-Use Recovery PIN

Deploying a Recovery PIN will put the Secure Key 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 Secure Key in Standby mode, press and hold the **UNLOCK + 7** buttons together for five seconds and release once the **RED** LED starts blinking.
2. Enter a recovery PIN (from Admin) and press the **UNLOCK** button. The **GREEN** LED will blink three times by itself, and then will be joined by a solid **BLUE** LED indicating the Key is in User Forced Enrollment mode.
3. Enter a new User PIN and press the **UNLOCK** button. The **GREEN** LED will blink three times if accepted.
4. Re-enter that same new User PIN and press the **UNLOCK** button again to verify it. If accepted, the **GREEN** LED will blink three times and then the Secure Key will return to its Standby state, indicated by the **RED** LED glowing steadily. The Secure Key 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 keys, this feature is especially useful if you need to access data on the key 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 key to a *Read-Only* mode for both the Admin and the User. When set by the Admin, the Admin is the only one that can change the key back to *Read / Write* mode.

When the key is unlocked in *Read-Only* mode and inserted into a USB port, the **GREEN** LED will glow solidly and the **RED** LED will blink once every three seconds.

To set the Key to Read-Only:

1. Enter the Admin mode. (Hold **UNLOCK + 0** for five seconds – with **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
2. Press and hold the **r + o** (7 + 6) buttons together for three seconds. The **GREEN** LED will blink three times.
3. The key will return to Admin mode. The **BLUE** LED will glow solidly.
4. Until changed, the key can only be read.

To return the Key to Read / Write:

1. Enter the Admin mode. (Hold **UNLOCK + 0** for five seconds – with the **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
2. Press and hold the **r + w** (7+ 9) buttons together; the **GREEN** LED will blink three times.
3. The key will return to Admin mode, indicated by the **BLUE** LED glowing solidly and the key will be restored to its normal *Read / Write* condition.

Important Note

Setting the key to *Read/Write* from the Admin mode will globally override a *Read-Only* mode that has been set by the User.

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

NOTE: When changing *Read-Only* or *Read / Write* settings, do not make these changes with the key attached to an operating system. This may cause confusion within the operating system about the proper status of the key and the key may not function properly until the operating system has been restarted.

This mode will allow the User to set the *Read / Write* status of the key, without having access to the Admin functions.

When the key is unlocked in *Read-Only* mode and inserted into a USB port, the **RED** LED will blink once every three seconds while the **GREEN** LED will glow solidly.

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

To Set the Key to Read-Only:

1. Press the **UNLOCK** button to wake the key. The **RED** LED will glow solidly.
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 **UNLOCK**. The **GREEN** LED will blink.
4. The Key will be in a *Read-Only* state the next time it is unlocked.

To Return the Key to Read / Write:

1. Press the **UNLOCK** button to wake the key. The **RED** LED will glow solidly.
2. Press and hold **r + w** (7+ 9) for three seconds. The **GREEN** LED will blink three times.
3. Enter the User / Admin PIN and press **UNLOCK**. The **GREEN** LED will glow solidly.
4. Key will return to unlocked mode and can now be written to, indicated by the blinking **GREEN** LED.

Important Note

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

To set the key 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 **UNLOCK + 0** buttons for five seconds – with **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** 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 Secure Key'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 **UNLOCK + 0** for five seconds – with **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
2. Press the **UNLOCK + 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 Secure Key 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 key is unlocked and unattended, the Aegis Secure Key can be set to automatically lock after a predetermined period of inactivity. In its default state, the Aegis Secure Key'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 **UNLOCK + 0** for five seconds – with **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
2. Once in the Admin mode, press **UNLOCK + 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 the key 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 solidly.

Setting a Self-Destruct PIN

The Secure Key's Self-Destruct PIN defends against physically compromising situations by erasing the key's contents and leaving it to look as if it never had any data written to it.

USE WITH CAUTION When this mode is activated and the key is unlocked with the Self-Destruct PIN, it will effectively perform a crypto-erase on the key, 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 entered, the key will unlock and the **GREEN** LED will glow solidly as if the key is being normally unlocked. The key, however, will need to be partitioned and reformatted before it can be used again. Additionally, The previous Admin and User codes will be deleted in the crypto-erase process and the Self-Destruct PIN will then become the new Admin PIN to unlock the key.

The Self-Destruct feature can only be enabled or disabled by the Admin. However, the Self-Destruct PIN can be generated by either the Admin or the User. If the *Admin* generates the Self-Destruct PIN, only the Admin can change that PIN. If the *User* generates the Self-Destruct PIN, both the User and the Admin can change the PIN.

Note: The Self-Destruct PIN must be different from the Admin PIN, User PIN, and Recovery PINs.

1. By default, the Self-Destruct feature is disabled. To allow the Secure Key to be set with a Self-Destruct PIN, Enter the Admin mode. (Hold **UNLOCK + 0** for five seconds – while the **RED** LED is blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
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 Key is in the Admin mode. If the intent is for the Self-Destruct PIN to be set up at another time by the User, press the **LOCK** button and refer to the **User Setting Self Destruct PIN** instructions below. Otherwise, continue to step 3.
3. Press **UNLOCK + 3** until the **RED** and **BLUE** LEDs blink alternately.
4. Enter the Self-Destruct PIN and press **UNLOCK**. 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 **UNLOCK**. The **GREEN** LED will glow solidly for a few seconds and then will return to either the Admin mode (indicated by the **BLUE** LED glowing solidly) 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.

Aegis Secure Key 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 Secure Key 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 Secure Key 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 key will only allow up to ten additional attempts before the key 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 **UNLOCK** button.
--You will now have ten additional attempts.
6. When the key 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 **UNLOCK + 0** for five seconds – with the **RED** LED blinking, enter the Admin PIN and press the **UNLOCK** button.) The **BLUE** LED will glow solidly.
3. Press and hold the **UNLOCK + 5** button for three seconds. The **RED** LED will double-blink.
4. 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 key 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 Secure Key in an unformatted condition.

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

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

1. Press and hold **UNLOCK + LOCK + 2** together for ten seconds. The **RED** and **BLUE** LEDs will blink alternately.
2. The **GREEN** LED will glow solidly for three seconds, followed by the **GREEN** and **BLUE** LEDs glowing solidly when complete.
3. A new Admin PIN will need to be entered and the key will need to be reformatted.

Initializing and Formatting the Aegis Secure Key After a Complete Reset

A complete reset of the Aegis Secure Key will erase all information and partition settings. You will need to initialize and format the Aegis Secure Key again after reset.

To initialize your Aegis Secure Key, perform the following steps:

1. After a complete reset, press **UNLOCK + 9**.
The **BLUE** LED will glow solidly and the **GREEN** LED will be blinking.
2. Enter the new Admin PIN and press the **UNLOCK** button. If accepted, the **GREEN** LED will quickly blink three times, then return to the **BLUE** LED glowing solidly and the **GREEN** LED blinking.
3. Re-enter the Admin PIN and press the **UNLOCK** button. If accepted, the **GREEN** LED will be solid for two seconds.
4. The **BLUE** LED will glow solidly for 30 seconds (or until the **LOCK** button is pressed, which will return the key to its standby state.)
5. The Admin PIN is now set and will allow access to the key or the Admin features.
6. To **UNLOCK** the key, enter the new Admin PIN and press **UNLOCK**.
7. Windows 7 and earlier: Right-click **My Computer**, and then click **Manage** from the Windows desktop.
Windows 8: 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 Secure Key is recognized as an unknown device that is uninitialized and unallocated.
9. Perform the following to make the key recognizable as a basic key.
 - 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. 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 Secure Key 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 Secure Key before hibernating, suspending, or logging off from the Windows operating system.

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

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



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

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

Aegis Secure Key Setup for Mac® OS

Your Aegis Secure Key is pre formatted in NTFS for Windows. To reformat the key 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 Secure Key:

1. Select the **Aegis Secure Key** from the list of keys and volumes. Each key in the list will display its capacity, manufacturer, and product name, such as 232.9 Apricorn Secure Key.
2. Click the **Erase** tab.
3. Enter a name for the key. The default name is **Untitled**. The key's name will eventually appear on the desktop.
4. Select a volume format to use. The **Volume Format** dropdown menu lists the available key 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. Press **UNLOCK**, then press **LOCK + 1**, then press and hold **0** for five seconds. The **RED** and **BLUE** LEDs will blink alternately.
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 solidly. (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 solidly.)
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, **Unlock Button** = 11 blinks, **Lock Button** = 12 blinks.)
4. To exit the Diagnostic Mode, wait for the 20 second timeout to return the key to its normal operation.

Self-Diagnostics:

During the initial power up, after the key has been plugged into a USB port, the key 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 key 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 key can no longer function.

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

Lock-Override Mode

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

NOTE: When in this mode, the key 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 key 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 key 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 **UNLOCK + 0** for five seconds until the **RED** LED blinks, then enter the Admin code and press the **UNLOCK** button. The **BLUE** LED will glow solidly.)
2. Press and hold **7 + 1** for three seconds. the **GREEN** LED will blink three times, then the **BLUE** LED will glow solidly.
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 **UNLOCK + 0** for five seconds until the **RED** LED blinks. Then enter the Admin code and press the **UNLOCK** button. The **BLUE** LED will glow solidly.)
5. Press and hold **7 + 0** for three seconds. The **GREEN** LED will blink three times then the **BLUE** LED will glow solidly.
6. To verify, unlock the key in User mode and check that the **BLUE** LED is no longer blinking.

FAQs

This section contains troubleshooting information for the Aegis Secure Key. More can be found in the FAQs section on apricorn.com

Q: What can I do if I forget the User PIN?

A: Use the Admin PIN to enter the Admin Mode and create another User PIN or (if programmed at configuration) utilize one of the data recovery PINs programmed into the device to create a state of User forced enrollment. Once a new user PIN is created, the User will regain access the device's data.

Q: What can I do if I forget the Admin PIN?

A: In the case of forgotten Admin and User PINs, if data recovery PINs were programmed into the drive at the time of setup, then you can use one of them to create a state of User Forced Enrollment and generate a new User PIN to gain access to (and back up) the drive's contents. Once complete, you must then perform a complete reset of the Aegis Secure Key where all PINs and data will be erased and you will need to reconfigure / reformat the Aegis Secure Key, creating a new Admin PIN which will allow you to reload the previously backed-up data onto the device.

Q: Why did the operating system not recognize the Aegis Secure Key, after I did a complete re-set of the drive?

A: You need to initialize, allocate and format the Aegis Secure Key manually. For more information, refer to *Initializing and Formatting the Aegis Secure Key After a Complete Reset* in this manual.

Q: How do I use the Aegis Secure Key without a PIN?

A: As a full disk encryption product, the Aegis Secure Key can never be used without a PIN.

Q: What encryption algorithm is used in this product?

A: The Aegis Secure Key uses AES 256-bit algorithm.

Q: Why could I not initialize, partition, or format the Aegis Secure Key?

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: The key seems warm to the touch, is this normal?

A: Yes. The SSD in the case runs hotter than a standard flash key. The cooling features use the case to dissipate the heat.

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. If you forget the PIN and do not have an Admin PIN, the key can be reset so it can be used again, but the data cannot be recovered.

Q: Why does the LED indicate an error when I try to change the PIN?

A: PIN requirements for this key 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 seven 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: 5A992c and HTS code 8523.51.0000

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 Secure Key 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, NEGLIGENCE, 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, ALTERATION 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.

Quick Reference Guide for Programming Key Combinations

Standby Mode

- 7+6 = Read-Only On
- 7+9 = Read-Only Off
- 🔒 +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
- 🗑️ + 7 = Set Recovery PIN
- 🗑️ + 8 = 1X Use to 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



APRICORN

© Apricorn 2022. All rights reserved.
12191 Kirkham Road
Poway, CA, U.S.A. 92064
1-858-513-2000 www.apricorn.com