Aegis Padlock 3.0

User's Manual

APRICORN

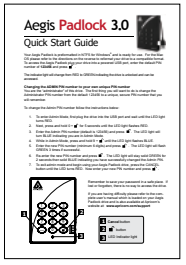
THE LEADER IN PERSONAL STORAGE

Table of Contents

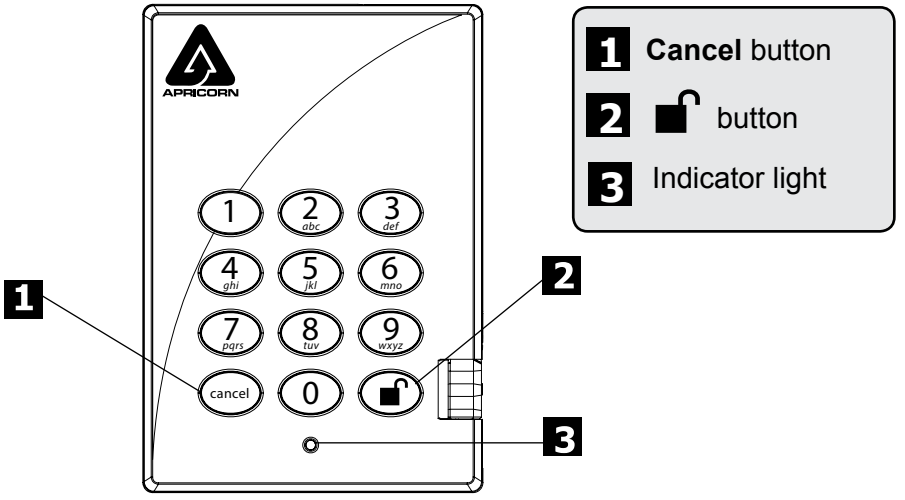
About the Aegis Padlock Portable Secure Hard Drive

Looking for an effortless way to secure your data? The Aegis Padlock Secure Drive is the ultimate portable hard drive and secure storage system. With an easy-to-use keypad design and software free setup, the Aegis Padlock Secure Drive enables you to access the drive with your own unique pin. Featuring 256 bit hardware encryption and a super-fast USB 3.0 connection, the Aegis Padlock provides seamless real-time encryption, keeping your data safe even if the hard drive is removed from its enclosure.

Package contents



Aegis Padlock button panel



The **"Cancel"** button can be used to:

- Cancel current operation
- Return to the previous step when you knowingly entered a wrong password
- Exit the Admin Mode

The button can be used to access the Aegis Padlock and it can also be used as an OK acknowledgement in the following operations:

- Entering a password
- Confirming a new password

The indicator light displays the following colors to indicate the various modes of operation:

- RED: Standby Mode
- BLUE: Admin Mode
- GREEN: User Mode

The indicator light has other display methods to indicate different status of the Aegis Padlock. Details are provided later in this chapter.

Aegis Padlock - Getting Started

Before you begin

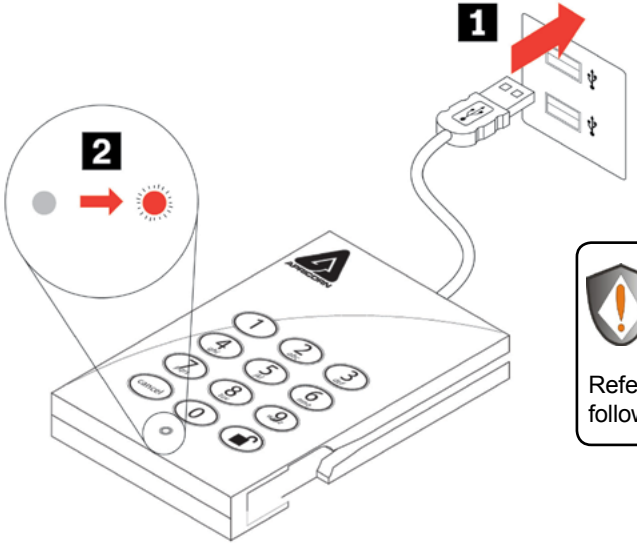
Be sure to review the following information before you begin to use the Aegis Padlock.

Attention: Use only the included cables with your Aegis Padlock. You might damage the drive if you use a cable not included with the Aegis Padlock.

The Aegis Padlock is designed for portable use without an AC power adapter and in most cases will be able to power on a single USB port. In the event that the Aegis Padlock is unable to power on a single USB connection, use the included USB Y-cable.

Connecting the Aegis Padlock

1. Attach the integrated USB cable of the Aegis Padlock drive to an available USB port on your computer, as shown below.
2. The Aegis Padlock indicator light should glow RED.



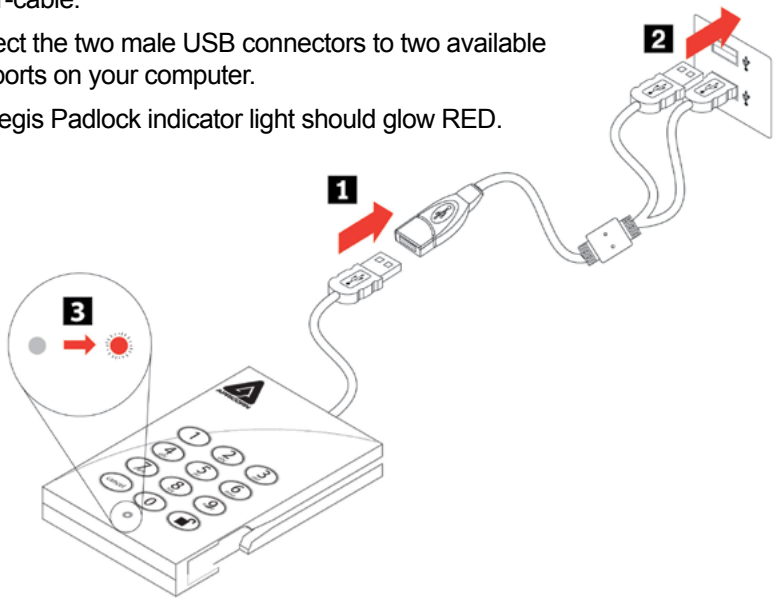
If the Indicator light does not power, use the included USB Y-cable.

Refer to directions on the following page

Connecting the Aegis Padlock with USB Y-Cable

If the indicator light does not power on a single USB connection, use the included USB Y-cable.

1. Attach the Aegis Padlock's integrated USB cable to the female connector of the USB Y-cable.
2. Connect the two male USB connectors to two available USB ports on your computer.
3. The Aegis Padlock indicator light should glow RED.



How do I use the Aegis Padlock the first time?

You can use it in one of the following ways:

- Enter the Admin Mode with **123456** (default administrator password), and then you are able to change the Admin Password or create a User Password.
- Directly enter the Secure User Mode with **123456** (default Admin Password) to use the Aegis Padlock.

What if I forget the User Password?

Use your Admin Password to enter Admin Mode, and then create another User Password in Admin Mode.

Using the Aegis Padlock

Entering and exiting the Standby Mode, Admin Mode, and User Mode

Entering the Standby Mode

The Standby Mode is the default working mode of the Aegis Padlock and is the gateway to other working modes.

To enter the Standby Mode, attach the Aegis Padlock to your computer. The drive automatically goes into Standby Mode and the indicator light turns RED. In this mode, the Aegis Padlock is locked. It cannot be recognized by **My Computer** and it does not provide either the regular functions or the encryption function. However, it enables you to enter and switch between the Admin Mode and the User Mode.

Attention: To switch between the Admin Mode and the User Mode, you are required to switch to the Standby Mode first, and then you can enter the mode of your choice.

Entering the User Mode

To enter the User Mode, do the following:

1. Attach the Secure Hard Drive to your computer. It enters the Standby Mode.
2. Enter the User Password or the Admin Password (the default Admin Password is **123456**) and press . The indicator light turns GREEN indicating that the drive is in the User Mode. If the indicator light flashes RED, you need to re-enter the correct password.

Exiting the User Mode

To exit the User Mode, double-click the **Safely Remove Hardware** icon from the Microsoft® Windows® desktop, and then remove the Aegis Padlock from your computer.

Attach the Aegis Padlock to your computer again and the indicator light turns RED. This indicates that you are in the Standby Mode.

Entering the Admin Mode

Note: The Aegis Padlock cannot be recognized by the operating system in the Admin Mode.

To enter the Admin Mode, do the following:

1. Attach the USB cable to an available USB port on your computer. The Aegis Padlock goes into the Standby Mode, and the indicator light turns RED.
2. Press and hold + 0 for five seconds until the indicator light flashes RED. This indicates that you can enter the Admin Password.
3. Enter the Admin Password and press . The default Admin Password is **123456**. The Secure Hard Drive is in Admin Mode when the indicator light has changed to BLUE.

Exiting the Admin Mode

To exit the Admin Mode, press the **"Cancel"** button in the Admin Mode until the indicator light turns RED. This indicates that you are in the Standby Mode.

Note: If the indicator light flashes RED for a few seconds, indicating the Aegis Padlock has returned to the Standby Mode, go back to Step 2. This is due to one of the following conditions:

- You entered an incorrect Admin Password in Step 3.
- No activity was detected within two minutes in the Admin Mode.

Password Management

This section provides information about managing your password in the Admin Mode and User Mode.

Changing the Admin Password

You can change the Admin Password by doing the following:

1. Enter Admin Mode (refer to page 9 for details).
2. Press and hold + 9 until the indicator light flashes BLUE.
3. Enter the new password and press (The Password must be a minimum of 6 digits and a maximum of 16 digits). The indicator light flashes GREEN three times. See note below.
4. Re-enter the new Admin Password and press . The indicator light stays solid GREEN for two seconds and then solid BLUE indicating that the Admin Password has been changed successfully.

Note: If the indicator light flashes RED three times, this indicates that the password is less than 6 digits or more than 16 digits. Enter a password that contains 6 – 16 digits after the indicator light flashes BLUE intermittently.

1. If the indicator light flashes RED intermittently and then BLUE intermittently, go back to step 3. This is due to one of the following conditions:
   - You waited longer than 10 seconds before entering a password.
   - The new password was entered incorrectly.
2. If no activity is detected within two minutes in the Admin Mode, the Aegis Padlock will return to the Standby Mode.

Adding a new User Password

You can add a new User Password by doing the following:

1. Enter the Admin Mode (refer to page 9 for details).
2. Press and hold + 1 until the indicator light flashes BLUE intermittently.
3. Enter a User Password and press (a minimum of 6 digits and a maximum of 16 digits) The indicator light flashes GREEN three times.
4. Re-enter the new User Password and press . If the indicator light stays solid GREEN for two seconds and then solid BLUE, the User Password was added successfully.

Deleting the User Passwords

You can delete all User Passwords by doing the following:

1. Enter the Admin Mode (refer to page 9 for details).
2. Press and hold 7 + 8 + for five seconds until the indicator light flashes BLUE intermittently. After the indicator light flashes GREEN three times and then BLUE intermittently.
3. Press and hold 7 + 8 + a second time for five seconds until the indicator light goes on solid GREEN for two seconds and then back to solid BLUE, this indicates that the User Passwords were deleted successfully.

Changing the User Password

You can change the User Password by doing the following:

1. Enter User Mode (refer to page 8 for details).
2. Press and hold + 1 until the indicator light flashes RED.
3. Enter your old password and press . The indicator light will turn GREEN, then change to flashing BLUE.
4. Enter the new password and press (The Password must be a minimum of 6 digits and a maximum of 16 digits). The indicator light will flash GREEN three times.
5. Re-enter the new User Password and press . The indicator light stays solid GREEN indicating that the User Password has been changed successfully.

Setting the Unattended Auto Lock Feature

To protect against unauthorized access if the drive is unlocked and unattended, the Aegis Padlock can be set to automatically lock after a pre-set amount of time.

In its default state, the Aegis Padlock 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 use the following steps:

1. Enter the Admin mode by pressing and holding + 0 for five seconds until the indicator light flashes RED. This indicates that you can enter the Admin Password.
2. Enter the Admin Password and press . The drive is in Admin Mode when the indicator light has changed to BLUE.
3. Once in Admin mode, press + 6. The indicator light 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:

Auto Lock Timeout Table:

1 = 5 min
2 = 10 min
3 = 20 min
0 = OFF

The default is 0 (OFF)

5. After you have input the number, the indicator light should flash GREEN 3 times to indicate that you have successfully set the Unattended Auto Lock feature.

Aegis Padlock Brute Force Protection

What is Brute Force Attack?

A brute force attack is a method of defeating a cryptographic scheme by systematically trying a large number of possibilities; for example, a large number of the possible keys in a key space in order to decrypt a message. In most schemes, the theoretical possibility of a brute force attack is recognized, but it is set up in such a way that it would be computationally infeasible to carry out. Accordingly, one definition of “breaking” a cryptographic scheme is to find a method faster than a brute force attack.

How does the Aegis Padlock protect against brute force attack?

1. With the drive locked and in the standby state the indicator light is solid RED.
2. After five failed attempts to enter the correct user or admin password, the keypad will not respond and indicator light will turn off. The drive will need to be unplugged from the USB port and replugged. This will be repeated for the next five PIN entry attempts.
3. Following the 10th incorrect PIN entry, the keypad will lock and the indicator light will begin blinking quickly. Even after unplugging and replugging in the unit, the drive will remain locked and the indicator light will continue to blink rapidly.
4. Here are the steps to allow the user to unlock the keypad for 10 more attempts to unlock this drive.
    a. Unplug the device from the computer
    b. Push and hold the number five key and plug-in the drive
    c. The indicator light will be blinking alternating RED and GREEN rapidly
    d. Enter the code **5278879** and press
    e. The keypad will unlock and will be in the standby state with the indicator light solid RED, this will allow only 10 more attempts
    g. After a total of 20 Attempts the drive will remain locked with the indicator light flashing RED quickly. You must now go through the reset process and reformat the drive to be able to use the drive again. (see page 15)

Setting a Self Destruct Password

The Aegis Padlock has the ability to set a password that will reset the encryption key if needed. By resetting the encryption key all data on the drive will be lost and cannot be recovered.

After initiating the Self Destruct sequence, the PIN used to initiate the self destruct sequence will become the default Admin password. The drive will need to be initialized and reformatted. For directions see page 15.

To set a Self Destruct password please use the following steps:

1. Enter the Admin mode by pressing and holding + 0 for five seconds until the indicator light flashes RED. This indicates that you can enter the Admin Password.
2. Enter the Admin Password and press . The drive is in Admin Mode when the indicator light has changed to BLUE.
3. Once in Admin mode, press + 3. The indicator light should start flashing RED and BLUE intermittently.
4. Input in the PIN that you would like to use as the Self Destruct password and press .

Note: The PIN must be a minimum of 6 digits in the length (16 max) and cannot match any Admin or User codes already used by the drive.

In the future, a User or Admin code can not be set to the same number as used by the Self Destruct password.

5. The Aegis Padlock will then check against known PINs to make sure that it is not already in use. If in use the indicator light will flash RED 3 times and the drive will go into Standby mode. If this happens please re-enter the Admin mode (step 1) and repeat the process with a new code.
6. If the Self Destruct password is accepted the indicator light flashes GREEN three times.
7. Immediately re-enter the new PIN and press . If the indicator light stays solid GREEN for two seconds and then goes to solid BLUE, the Self Destruct PIN was added successfully.
8. To delete the Self Destruct password, you will need to delete all of the User Passwords. Please refer to the instructions on page 11 - Deleting User Passwords.

Completely resetting the Aegis Padlock

If you forget all the User Passwords or Admin Passwords, you can perform a complete reset to remove all the User Passwords, and restore the Admin Password to the default **123456**.

Attention: Completely resetting the Aegis Padlock will reset the encryption key, in effect making all the data on the drive unrecoverable. You will need to partition and format the Aegis Padlock with disk management applications.

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

1. Press and hold the **"Cancel"** button while you attach the Aegis Padlock to an available USB port on your computer. The indicator light will flash BLUE and RED alternately.

   Note: If no activity is detected for 30 seconds in this step, the Aegis Padlock will go into the Standby Mode.

2. Press and hold **"Cancel"** + + 2 for 10 seconds until the indicator light flashes RED and BLUE intermittently, and then stops on a solid color. The indicator light will then turn solid GREEN for two seconds, followed by solid RED. You have successfully reset the Aegis Padlock.

Initializing and formatting the Aegis Padlock after a complete reset

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

To initialize your Aegis Padlock, do the following:

1. After a complete reset, attach the Aegis Padlock to the computer.
2. Wait 5 seconds for the computer to recognize the device.
3. Enter the default User Password **123456** and press to enter the User Mode.
4. Right-click **My Computer**, and then click **Manage** from the Windows desktop.

5. In the Computer Manage window, click **Disk Management**. In the Disk Management window, the Aegis Padlock is recognized as an unknown device that is uninitialized and unallocated.
6. Do the following to make the drive recognized as a basic drive.
   - If the Initialize and Convert Disk Wizard window opens, click **Cancel**, then 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**.
7. Right-click in the blank area under the Unallocated section, and then select New Partition. The Welcome to the New Partition Wizard window opens.
8. Click **Next**.
9. Select Primary partition and click **Next**.
10. If you need only one partition, accept the default partition size and click **Next**.
11. Click **Next**.
12. Create a volume label, select Perform a quick format, and then click **Next**.
13. Click **Finish**.
14. Wait until the format process is complete. The Aegis Padlock will be recognized and it is 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 before hibernating, suspending, or logging off from the Windows operating system.

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

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

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

- away from your computer
- using the switching user function by sharing a computer with others

Troubleshooting

This section contains troubleshooting information for the Aegis Padlock. If you encounter any of the following problems when using the Aegis Padlock, refer to the corresponding answers.

Q: How do I use the Aegis Padlock the first time?

A: You can use it in one of the following ways:

- Enter the Admin Mode with **123456** (default administrator password), and then you are able to change the Admin Password or create a User Password
- Directly enter the Secure User Mode with **123456** (default Admin Password) to use the Aegis Padlock

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

A: Use your Admin Password to enter Admin Mode, and then create another User Password in Admin Mode.

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

A: There is no other way to retrieve the Admin Password except a complete reset of the Aegis Padlock. After a complete reset, all data will be lost and you will need to initialize, allocate and format the Aegis Padlock manually. Then you will be able to use the default Admin Password **123456**.

Q: Why did the operating system not recognize the Aegis Padlock after I enter the User Mode and completely reset the computer?

A: You need to initialize, allocate and format the Aegis Padlock manually. For more information, refer to **Initializing and formatting the Hard Drive after a complete reset** in this manual.

Q: How do I use the Aegis Padlock without a password?

A: As a full disk encryption product, the Aegis Padlock can never be used without a password.

Q: What encryption algorithm is used in this product?

A: Depending on your model the Aegis Padlock uses either AES 128-bit or 256-bit algorithm.

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

A: Ensure that you have administrator privileges. You can use only the administrator account to initialize, partition or format the Aegis Padlock in the Admin Mode.

Technical Support

Apricorn provides the following helpful resources for you:

1. Apricorn's Website (**http://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 Standard Time Monday through Friday

Warranty and RMA information

One Year Limited Warranty:
Apricorn offers a 3-year limited warranty on the Aegis Padlock 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

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