Aegis Secure Key 3NX

Quick Start Guide

First-Time Use / Admin Mode Setup

NOTE: if you are setting up your Secure Key 3NX with the Aegis Configurator (sold separately), DO NOT perform the following Manual Admin and USER PIN SETUP steps below; The Aegis Configurator will only recognize devices in their factory "out of box" state or devices that have been completely reset.
Each Aegis Secure Key is shipped without a preset Personal Identification Number (PIN.) To prepare the Key for use, the user must first establish an Admin PIN that is between 7and 16 digits in length. PINs cannot contain all consecutive numbers or all the same numbers *(e.g. 123456789, 987654321 or 11111111, 22222222, etc.* This Admin PIN is used to set the Secure Key's various Admin features and also serves as the first of two User PINS for the Secure Key's standard operation.

To Set Up the Admin PIN:
1. Wake up the Secure Key by pressing 🔓.
   (BLUE and GREEN LEDs will glow solidly, indicating no Admin PIN has been established.)
2. Press 🔓 **+ 9** simultaneously.
   (BLUE LED will glow solidly and GREEN LED will blink.)
3. Enter the PIN to be used as your Admin code and press 🔓.
   (If PIN is accepted, BLUE LED will turn off momentarily and GREEN LED will blink 3 times by itself, then will continue blinking as the BLUE LED glows solidly.)*
4. Quickly re-enter that same PIN once more and press 🔓
   (BLUE LED will turn off momentarily and GREEN LED will illuminate for one second until replaced by the BLUE LED glowing solidly, indicating that the Admin PIN has been set and the Secure Key is in Admin mode, ready to add another User PIN [see reverse] or for setting up features.)
5. To exit the Admin mode, press 🔒 *(RED LED will glow solidly)* or wait 30 seconds and Secure Key will return to sleep mode.
6. If no additional user is to be added or no further Admin features are to be set, your Aegis Secure Key setup is now complete and ready for use.

Battery Note
The Aegis Secure Key has an internal rechargeable battery with a smart-charging circuit and will automatically charge whenever it's plugged into a powered USB port. After initial Admin PIN setup, when plugged into a powered USB port while in standby mode, the Red LED will pulse to indicate that it's charging and will glow solidly once fully charged. Since the Secure Key ships with a partial charge, plug it into a powered USB port for 60-80 minutes to give the battery a full charge before initial setup (RED LED will still be blinking.)

Adding a New User PIN

There are two ways to establish a User PIN: Admin-generated while in Admin Mode, and User-generated while Secure Key is placed in User Forced Enrollment State.

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.

* If PIN is unacceptable, Red LED will blink 3 times and return to solid BLUE / blinking GREEN LEDs.

IMPORTANT:
Do NOT press any buttons while the Secure Key is plugged into a USB port. Doing so may cause damage to the USB port and Secure Key USB Connector.

Adding a New User PIN (cont'd)

CREATING FORCED ENROLLMENT STATE ALLOWING USER TO GENERATE USER PIN
Note: This can only be done if there isn't already a User PIN established on the key using the method above.
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.

Locking the Key

To lock the key, simply press the 🔒 button. When locked, the **RED** LED will glow solidly.

If data is still being written to the Secure Key, it will wait for this operation to be completed before the locking operation takes place. The 🔒 button can also be used to exit out of the Admin mode.

Note: The Aegis Secure Key will not be recognized by any operating system in its locked state.

Unlocking the Key

1. Beginning in standby mode, press the 🔓 button to wake the drive. *(The RED LED will glow solidly.)*
2. Enter either an Admin PIN or User PIN and press the 🔓 button.
   (If the PIN is accepted, the GREEN LED will quickly blink four times, then continue to blink slowly until it's plugged into a USB port, after which will then glow solidly;
   If the PIN is incorrect, the RED LED will blink three times and then glow solidly.)
3. Upon correct PIN entry, the key will be unlocked and ready for use. If it is not plugged into a USB port within 30 seconds, the key will return to sleep mode and automatically lock itself.

Formatting For Mac OS

The Aegis Secure Key 3NX comes preformatted in FAT32 for complete cross-platform compatibility and is ready for use. For a strictly Mac OS environment, you should first reformat the drive to Mac OS Extended (journaled). Once the drive is unlocked and inserted into a USB port, open the **Mac Disk Utility** from **Applications/Utilities/Disk Utilities** and perform the following:
1. Select the Aegis Secure Key from the list of drives and volumes.
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.

Technical Support
Apricorn provides the following helpful resources:
1. Apricorn's Website (**http://www.apricorn.com**)
2. E-mail us at **support@apricorn.com**
3. Call Technical Support at **1-800-458-5448** from 8:00 a.m. to 5:00 p.m. PST, M - F

(Rev 0) 04/15/2018