



# APRICORN NVX Hardware Encrypted USB Storage Device Instruction Manual

[Home](#) » [APRICORN](#) » [APRICORN NVX Hardware Encrypted USB Storage Device Instruction Manual](#) 



Aegis NVX™  
AES 256 Bit XTS Military Grade  
Hardware-Encrypted NVMe SSD with USB 10Gbps High Speed  
Type-C Connector



## Contents

- [1 Maximum Data Security at Breakneck Speeds](#)
- [2 Aegis NVX™](#)
- [3 TECHNICAL SPECIFICATIONS](#)
- [4 Documents / Resources](#)
  - [4.1 References](#)

## Maximum Data Security at Breakneck Speeds

The next generation of Aegis Secure Drives incorporates all of the upper level security features you've come to expect from Apricorn with a patented proprietary NVMe architecture to deliver 256-bit hardware encryption at transfer speeds of up to 1000Mb/s.

### Speed, Action.

Finally an encrypted hard drive that stays well ahead of your r/w speed demands. Whether you're pulling huge amounts of forensic data in a tight timeframe or shooting at your HD Camera's highest resolutions and fastest frame speeds, all of your data is being encrypted on its path to storage at speeds of up to 1000Mb/s. And with 5 available PINs, access to the device's contents is limited to those who are authorized within the workflow.

### Built for Anywhere.

Smaller than most smartphones, the NVX is built to go wherever you do, fitting right into your workspace; from your pocket, media case, backpack, and most media storage cradles. Extreme temperatures, rugged terrains, and hard knocks are what it's made for.

Available in 500GB, 1TB, and 2TB capacities, the NVX ships with a molded protective case (not that it needs one) a C-to-C extension cable, and a C-to-A adapter/extension cable.

### Serious Materials.

The crush-resistant enclosure is milled from solid 6061 aircraft-grade aluminum alloy, with stainless breakaway fasteners and a new moisture resistant rubberized keypad. Inside, the components are further protected with hardened epoxy potting. The rugged integrated USB 10Gbps type-C connector cable securely tucks away when not in use.

### No Software, No Prob.

Apricorn's unique hardware based approach delivers the highest levels of data security and workflow compatibility. Like all Aegis secure drives, the NVX is software-free and hardware-encrypted, making it completely cross-compatible. 100% of its authentication and encryption processes take place within the device itself.



The Safest Place on Earth for Your Data.

## Aegis NVX™

NVMe SSD with AES 256-Bit XTS Hardware-Encrypted USB 3.2 Gen-2 10Gbps with USB Type-C Connector  
Milled from a Solid Block of Aircraft Grade Aluminum with Breakaway Fasteners and Epoxy Threadlock  
Wear-Resistant Membrane Style Keypad/10k Press Tested  
Software-Free/Locked-Down Firmware to Prevent Introduction of Malware Such as BadUSB



Our patented firmware delivering the industry's most advanced feature set– the heart and soul of every Apricorn device.

### **Separate Admin and User Modes/PINs**

Admin (Device Configuration) Mode and User Access Mode. The Admin mode controls the universal programmable settings of the device and can only be accessed with the Admin PIN. The User mode is for general external drive usage like read /write, unlock / lock, and certain other functions. The User mode is accessible via a User PIN or the Admin PIN. Up to four User PINs may be enrolled.

### **Admin Forced Enrollment**

Eliminates factory default PIN vulnerability by forcing the enrollment of an Admin PIN prior to use. As with all Apricorn Aegis secure devices, there are no default passwords, and no back-doors. In order to use any Apricorn secure drive, the Admin must first establish a complex PIN.

### **User Forced Enrollment**

Beyond the admin PIN, one additional PIN can be generated to access the device's data. This User PIN can be set up by the admin at initial setup, or the device can be deployed in a state of User Forced Enrollment, allowing the user to establish his or her own PIN prior to use.

### **Data Recovery PINs**

Programmed by the admin at time of setup to permit regaining access to the drive by creating a state of User Forced Enrollment in which a new User PIN can be created without affecting the drive's existing data or the Admin PIN.

### **Two Read-Only Modes**

Universal Read Only: set by the admin from within the admin mode and can't be modified or disabled by anyone but the admin. The second (User) mode can be set and disabled by a user but can also be enabled or disabled by the admin.

### **Programmable PIN Length**

Admin Designates Minimum and Maximum PIN Lengths (between 7 and 16 Characters). The longer the PIN, the more secure the data on the device becomes. For example, the odds of brute force success go from 1/10,000,000 with a 7-digit PIN to 1/100,000,000 with an 8 digit PIN. In cases where the User sets up his or her own PIN from User Forced Enrollment, the Admin can still affect User password length requirements

### **Unattended Auto Lock**

Programmable Length of Time of Inactivity Permitted Before Drive Locks Itself. All Aegis Secure Drives will automatically lock once disconnected from a computer's USB port or the power to that USB port is interrupted, or after a pre-programmed period of inactivity.

### **Lock Override**

Allows Drive to Remain Unlocked During USB Port Re-Enumeration (Virtual Machine, Remote Boot). Designated for specific cases in which the drive needs to remain unlocked through USB port re-enumeration such as during reboot, or passing through a virtual machine.

### **Self-Destruct PIN**

When Programmed and Activated, Performs a Crypto- Erase and Becomes New Access PIN. The last line of defense for data security when the device's physical security is at risk. The Self-Destruct PIN defends against these physically compromising situations by erasing the drive's contents, leaving it in normal working order appearing yet to be deployed.

### **Brute Force Defense**

Programmable Number of Consecutive Invalid PIN Attempts Permitted (4-20) Before Crypto-Erase. If the device comes under a physical brute force attack, once the programmed number (between 4 and 20) of consecutive incorrect password entries has been attempted, the device will delete its own encryption key and destroy the ability to decrypt its stored data.

### **Provision Lock**

Patented setting where the admin can designate whether the device will permit itself to be reset by a User or after a brute force attempt. If Provision Lock is enabled, any attempt at complete reset will "brick" the device for good.

## **TECHNICAL SPECIFICATIONS**

### **CAPACITIES**

NVMe SSD: 500GB, 1TB, 2TB

### **TRANSFER RATE**

NVMe SSD: up to 1000MB/s\*

### **INTERFACE**

USB 10Gbps TYPE-C

### **DIMENSIONS and WEIGHT**

67mm x 120mm x 15mm | 184.27g

2.63" x 4.72" x 0.59" | 6.5oz

### **POWER SUPPLY**

100% bus powered

### **OPERATING TEMPERATURE RANGES**

-40° to 158°F (-40°C to 70°C)

### **OPERATING HUMIDITY RANGES**

95% @ temps under 131°F (55°C)

### **CRUSH RESISTANT**

up to 6500 LBS

### **SHOCK SSD**

NON-OPERATING: 1500G .5ms

OPERATING: 1500G .5ms

### **WARRANTY**

3-Year Limited

### **SYSTEM COMPATIBILITY**

WINDOWS, MAC OS, LINUX, ANDROID, CITRIX any machine that supports a USB mass storage device

### **SKU NUMBERS**

NVMe SSD: ANVX-500, ANVX-1TB, ANVX-2TB

### **ECCN / HTS / CAGE CODE**

5A992.c / 8523.51.0000 / 3VYK8

### **STANDARDS / CERTIFICATIONS**

IP-67

TAA COMPLIANT



**PACKAGE CONTENTS**

Aegis NVX, C-TO-C Extension Cable  
Aegis NVX, C-TO-A Adapter / Extension Cable  
Multi-Language Quick-Start Guide



\* To achieve these speeds, your computer’s internal hard drive must also be an SSD; all transfer rates will be limited by computer’s internal HDD One gigabyte (GB) = one billion bytes; accessible capacity will be less and actual capacity depends on the operating environment and formatting.

©2023 Apricorn. 12191 Kirkham Rd., Poway, CA. 92064  
800.458.5448

[apricorn.com](http://apricorn.com)

Patents: [apricorn.com/patents](http://apricorn.com/patents)



**Documents / Resources**



[APRICORN NVX Hardware Encrypted USB Storage Device](#) [pdf] Instruction Manual  
NVX Hardware Encrypted USB Storage Device, NVX, Hardware Encrypted USB Storage Device, Encrypted USB Storage Device, Storage Device

**References**

- [▲ Apricorn | Home](#)
- [▲ Patents](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.