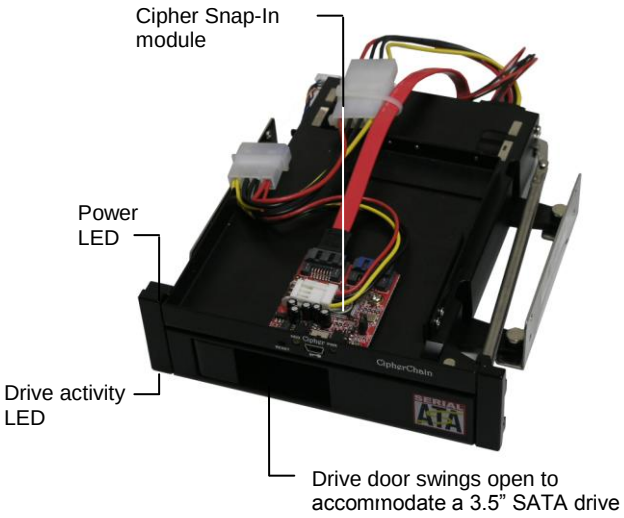
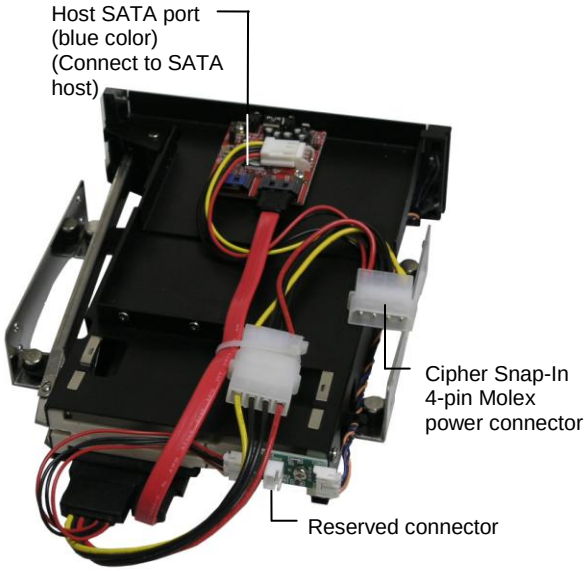
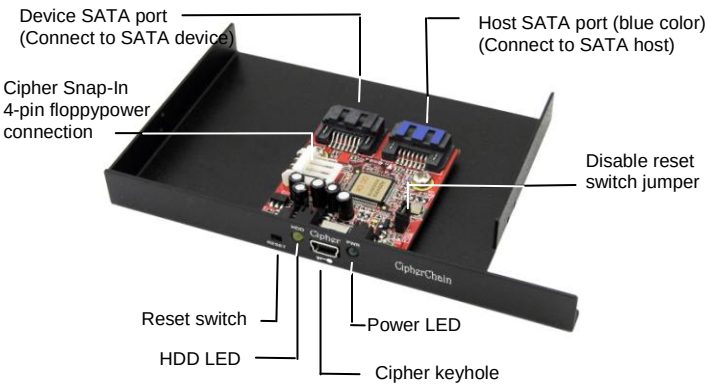
ADDONICS TECHNOLOGIES
Model: CSN256





I. Detailed Description of Cipher Snap-In Module:



Disable reset switch jumper – By default, Cipher Snap-In reset switch is enabled. To disable reset, remove the jumper. Disabling the reset switch is recommended if the Cipher Snap-In is connected to a boot drive or non-hotswap SATA controller card.

Reset switch – Under certain applications, the RESET button enables the adding and removing of hard drives without restarting the system. Following is an example of such an application:

a. When the Cipher Snap-In is connecting a removable drive system to a SATA port that supports hot swap, the drive can be removed without powering off the computer. However the drive icon will still be there as the system does not realize a hard drive is removed from the system. In addition, the key code still resides inside the Cipher Snap-In. Resetting will turn off the Cipher Snap-In, clear the key code and remove the drive icon. We recommend resetting the Cipher Snap-In whenever a hard drive is removed from a system to ensure better security.

b. Likewise when a new hard drive is added to a removable drive system. The Cipher Snap-In can be initialized again by pressing the RESET button while with the Cipher key inserted. Note that if the new hard drive is not encrypted or the Cipher key does not match what is on the encrypted hard drive, it will show up as an unallocated drive under the drive management screen and no drive icon will show up in My Computer folder. So it is very important to make sure that the correct Cipher key is used on the hard drive. ***Proceeding to initialize the hard drive will erase all the data beyond any possibility of recovery.***

Green Power LED: In order to turn on the power to the Cipher Snap-In, the cipher key must be inserted prior to power on the system or resetting the Cipher Snap-In. If the power LED does not light up, the system will not detect the hard drive connected to the Cipher Snap-In.

Yellow Power LED: Lights up when there is drive activity.

ADDONICS TECHNOLOGIES
Model: CSN256

II. Basic Hardware Installation

1. Mount the Cipher Snap-In into a 5.25" drive bay on the PC case.
2. Connect the Cipher Snap-In 4-pin Molex power connector to the system's power supply to provide power to the hard drive and CipherChain module.
3. Connect the Host SATA port (port with Blue color) on the Cipher Snap-In to the onboard SATA port of the motherboard or an add-in SATA controller card using a SATA cable.

III. How to operate the Cipher Snap-In:

Note: Hot swapping refers to the ability to plug and unplug the component without rebooting.

For a SATA port that supports hotswap and the **system is turned on**.

1. Insert the AES 256-bit cipher key into the cipher keyhole on the Cipher Snap-In.
2. Slide the 3.5" SATA hard into the Cipher Snap-In.
3. Observed that the green Power LED should light up. If it does not, re-insert the cipher key and re-power the drive by removing it from the Cipher Snap-In.
4. For new drive, go to the operating system's management utility to partition, format and mount the encrypted drive.
5. Go to File Manager and view the encrypted drive.

For SATA port that does NOT support hotswap and the **system is turned off**.

1. Insert the AES 256-bit cipher key into the cipher keyhole on the Cipher Snap-In.
2. Slide the 3.5" SATA hard into the Cipher Snap-In.
3. Power on the system.
4. Observed that the green Power LED should light up. If it does not, re-insert the cipher key restart your system.
5. For new drive, go to the operating system's management utility to partition, format and mount the encrypted drive.
6. Go to File Manager and view the encrypted drive.

Note: You may remove the cipher key from the Cipher Snap-In once the Cipher Snap-In is powered on. All the files being transferred into the drive are still encrypted even if the cipher key is removed.

Best Practices:

- Create a label to identify the SATA storage device and the Cipher key used to encrypt the device.
- Always keep a spare master key in a safe place.

For additional information about the Cipher Snap-In, refer to the Cipher Snap-In manual on the CD or download a copy from www.addonics.com

Procedure on using an existing boot drive in the Cipher Snap-In

In case you plan to use an existing boot drive on the Cipher Snap-In so you can encrypt it, by just inserting the existing boot drive on the Cipher Snap-In does NOT encrypt it.

You would need to either do a fresh install of the operating system on another drive that is on the Cipher Snap-In or would first clone the boot drive by placing a second drive on the Cipher Snap-In then duplicate the boot drive using a cloning software.

TECHNICAL SUPPORT

Email: http://www.addonics.com/sales/query/
Internet: http://www.addonics.com

Technical Support (8:30 am to 6:00 pm PST)
Phone: 408 433-3855
Email: http://www.addonics.com/support/query/