DIGISTOR®

SECURE DATA STORAGE

Citadel SSD

Setup Guide

A9-4400-01-1 Rev 1.0

Product Warranty: CDSG warrants this product to be free of significant defects in material and workmanship for a period of three (3) years from the original date of purchase. CDSG's warranty is nontransferable and is limited to the original purchaser.

Limitation of Liability: The warranties set forth in this agreement replace all other warranties. CDSG expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CDSG dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CDSG or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CDSG product or service, even if CDSG has been advised of the possibility of such damages. In no case shall CDSG's liability exceed the actual money paid for the products at issue. CDSG reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

1. Introduction

This DIGISTOR Citadel SSD is powered by CipherDrive pre-boot authentication (PBA) built into the self-encrypting drive. You will need to activate the PBA *after* you install an operating system or virtual machine.

Once reactivated, the Citadel SSD will require you to securely authenticate the drive with an AES 256-bit encryption key before any data can be accessed and before any operating system or virtual machine stored on the SSD can start up. Once authenticated, changes can be made to the drive in real-time until the host computer is powered off.

This guide will help you install your Citadel SSD and reactivate it.

1.1. Safety Information

Please read the following before handling this product.

1. Do not drop the product, submit it to impact, or pierce it.
2. The circuit boards within this product are susceptible to static electricity. Proper grounding is strongly recommended to prevent electrical damage to the product or other connected devices, including the computer host.
3. Avoid placing this product close to magnetic devices, high voltage devices, or in an area exposed to heat, flame, direct sunlight, dampness, moisture, rain, vibration, shock, dust, or sand.
4. To avoid overheating, this product should be operated in a well-ventilated area.
5. Before starting any type of hardware installation, please ensure that all power switches have been turned off and all power cords have been disconnected to prevent personal injury and damage to the hardware.

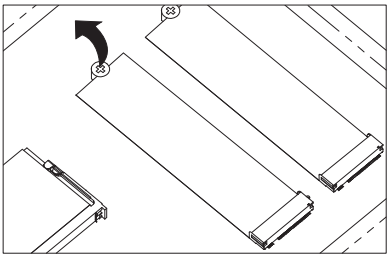
2. Drive Installation

These instructions will help you install the Citadel SSD into your computer. If you purchased a computer with a Citadel SSD pre-installed, you can skip this section.

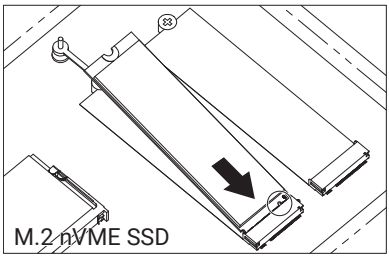
Choose the installation instructions appropriate to the type of Citadel SSD you have.

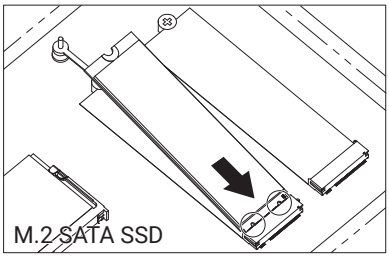
2.1. M.2 SSDs (NVMe or SATA)

1. Remove the screw from the SSD slot you intend to use if there is one present.

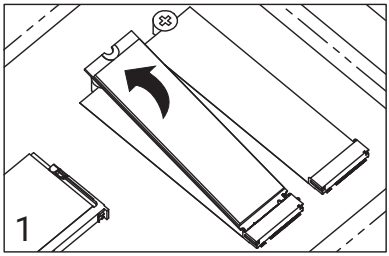


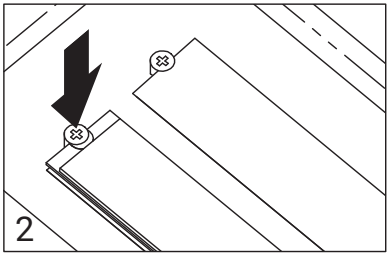
2. Insert the Citadel SSD into an open M.2 slot in your computer. Be sure to align the notch(es) on the gold contacts of the SSD module with the notch(es) on the empty slot.





3. Secure the Citadel SSD. Hold the Citadel SSD flat against the slot bay (Figure 1) and reinsert the screw back into the rear of the slot (Figure 2).

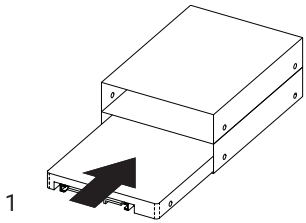


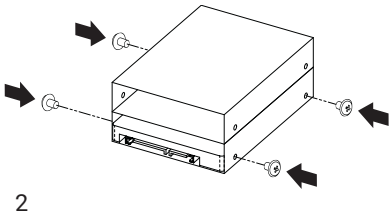


The Citadel SSD must now be reactivated. Please continue to the next section (see Section 3: Reactivate the Citadel SSD, page 7).

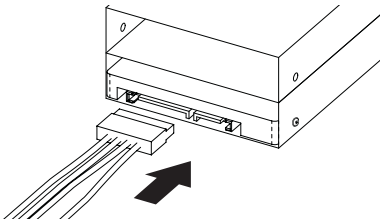
2.2. 2.5-inch SATA SSD

1. Insert the Citadel SSD into an open 2.5-inch drive bay in your computer (Figure 1). Then secure the Citadel SSD with four screws (Figure 2) or via the computer chassis' built-in tension clip.

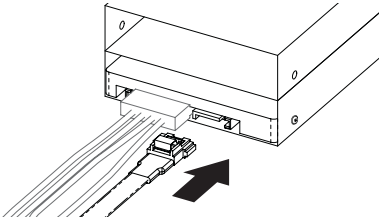




2. Attach a SATA power connector from your computer to the SATA power port on the rear of the Citadel SSD.



3. Attach a SATA data cable to the SATA port on the rear end of the Citadel SSD and the other end to the computer's motherboard.



The Citadel SSD must now be reactivated. Please continue to the next section (see Section 3: Reactivate the Citadel SSD, page 7).

3. Reactivate the Citadel SSD

3.1. Download the Activation Software

Download the Citadel SSD activation software from cru.bz/citadel and save it to a place on your computer. This download should be located at the top of the page.

3.2. Create a Bootable USB Thumb Drive

1. Insert a USB thumb drive into your computer.
2. Format a USB thumb drive to the FAT32 file system.

CAUTION
Be sure you backup any files on the drive because they will be erased!

IMPORTANT
Ensure that no other partitions or files exist on the thumb drive! If you have multiple partitions on the thumb drive, you may have to use other tools to delete them such as "Disk Management" which is built into Windows 8.1 and Windows 10.

3. Open the ZIP file you downloaded and extract the "COPY_TO_USB" folder to your computer.
4. Navigate into the "COPY_TO_USB" folder. Copy the contents of the "COPY_TO_USB" folder to the thumb drive.

IMPORTANT
Do not copy the “COPY_TO_USB” folder itself over to the thumb drive. Your system will probably be unable to boot from it if you do.

You now have a bootable thumb drive. If you require more help, please contact Technical Support. See Section 5: Product Support, page 14.

3.3. Configure UEFI/BIOS Settings

You will need to properly configure your BIOS or UEFI in order to properly boot from the thumb drive. To do so, follow the instruction set below that's applicable to your situation. Specific instructions have been provided for Dell computers, as well as a generic instruction set for all other computers.

3.3.1. For All Computers

Follow these steps to ensure your computer's BIOS or UEFI settings are configured correctly. To access the BIOS or UEFI, you may have to press **Delete**, **F2**, or **F12** when starting your computer up.

1. If you have an option for "UEFI Boot Path Security" or something like it, be sure to change it to **Never**.
2. Ensure that your "SATA Operation" is set to **AHCI**.
3. If you have a discrete video card, ensure your primary display detection is set to **Auto**.
4. Disable "Secure Boot".

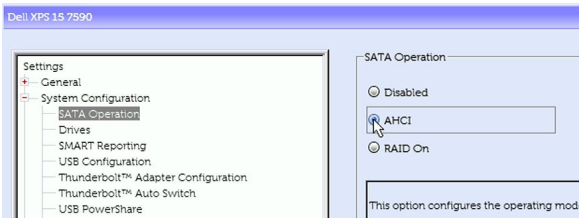
> **NOTE**
> The Citadel SSD **does** support Secure Boot, but only once activated. You may reenable Secure Boot after you finish reactivating the Citadel SSD.

3.3.2. For Dell Computers

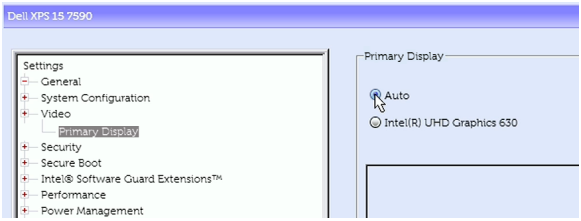
Follow these steps to ensure your Dell computer's UEFI settings are configured correctly. To access the UEFI, you may have to press **F2** or **F12** when starting your computer up.

1. Navigate to "General > UEFI Boot Path Security" and change it to **Never**.

2. Navigate to "System Configuration > SATA Operation" and change it to **AHCI**.

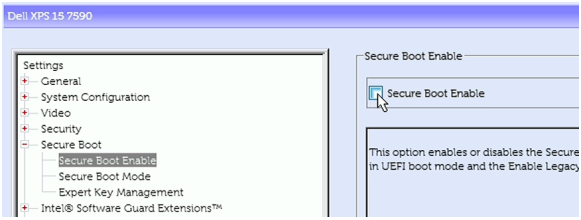


3. If your Dell computer has an upgraded video card, navigate to "Video > Primary Display" and ensure it is set to **Auto**. Otherwise, this option will not be available and you can continue onto the next step.



4. Navigate to "Secure Boot > Secure Boot Enable" and **uncheck the box** next to the "Secure Boot" option to disable it. A dialog box may pop up warning you that disabling Secure Boot will reduce system security. Click **Yes** to disable it.

> **NOTE**
> The Citadel SSD **does** support Secure Boot, but only once activated. You may reenable Secure Boot after you finish activating the Citadel SSD.



3.4. How to Boot into the Thumb Drive

1. Insert the bootable USB drive with the Citadel SSD activation software into the computer and turn it on.
2. Continually press the key for accessing your motherboard's boot menu while the computer starts up. This key to access it differs on different models, but the most common keys are F12, F10, F2, or Esc.
3. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.
4. A Linux BASH prompt will load. Press **Enter** to activate the console.

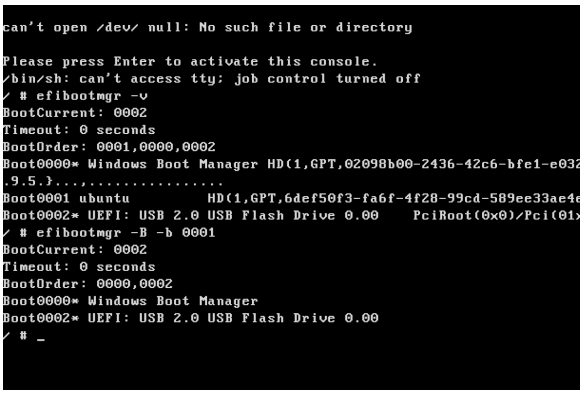
3.5. Remove Existing Boot Sequences

IMPORTANT

You only need to follow this section if your computer has been previously used for several different operating systems. You may skip this step if your computer is brand new.

However, if your computer *does* have a previous operating system and you wish to keep it, you can also skip this step. Please note that DIGISTOR does not recommend keeping previous operating systems as a best practice.

1. Boot into the thumb drive using the steps above. See Section 3.4: How to Boot into the Thumb Drive, page 9.
2. Type in **efibootmgr -v** and press **Enter**. You will see text similar to that seen in the screenshot below.



3. If you see any boot sequences (indicated by "Boot0000", "Boot0001", etc.), use the following command to delete them, where <xxxx> is the four digit number that corresponds to the boot sequence you wish to delete: **efibootmgr -B -b <xxxx>**.
4. When you have finished deleting the existing boot sequences, turn off the computer.

3.6. Install an Operating System or Virtual Environment

Your Citadel SSD has been shipped to you deactivated and unlocked. Install any operating system (OS) or virtual machine (VM) at this time.

TIP
If you need to turn on a Trusted Platform Module (TPM), Virtualization Support, or Trusted Execution, you can turn them on in the UEFI.

After you have installed the OS or VM, perform a cold reboot by turning your computer off and back on again and test the OS or VM.

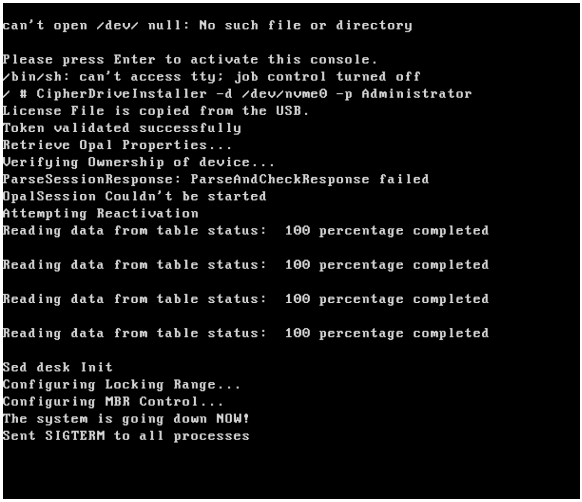
3.7. Activate the Citadel SSD

1. Boot into the thumb drive using the steps above. See Section 3.4: How to Boot into the Thumb Drive, page 9.
2. Type in the command below that applies to the type of Citadel SSD you have. Please note that the following text is case sensitive.

CAUTION
The following commands will only work when your Citadel SSD is the only SATA or NVMe drive installed in the system. If you have multiple drives, please ensure you are using the correct Linux boot path for your Citadel SSD. To do so, type **sedutil-cli –-scan** and press **Enter**. If you need more help, contact Technical Support for help.

- M.2 NVMe SSD:
  CipherDriveInstaller -d /dev/nvme0 -p Administrator
- SATA 2.5-inch or M.2 SATA SSD:
  CipherDriveInstaller -d /dev/sda -p Administrator

NOTE
The default password is **Administrator**, and it is *case-senstive*. You can change it once you log into the Citadel SSD software dashboard.



3. The computer will shut down automatically. Remove the USB thumb drive and reboot the system.

The Citadel SSD has been activated!

4. First Time Login

IMPORTANT
Before attempting to log in, make sure you have first activated your Citadel SSD. See Section 3: Reactivate the Citadel SSD, page 7.

1. If you haven't already, turn on the computer. The Citadel SSD software will load.
2. Click the **Accept button** at the bottom of the Disclaimer screen that appears.
3. Log into the default Administrator account. Use the following credentials, which are case sensitive:
   - Username: **Administrator**
   - Password: **Administrator**

NOTE
Usernames and passwords are case sensitive.

The computer will appear to reboot and your OS or VM will now start up.

NOTE
You should change the administrator password as soon as possible to maintain operational security. To do so, log into the dashboard by ensuring the **Settings Console box** is checked when you log in.

5. Product Support

Your investment in DIGISTOR products is backed up by our free technical support for the lifetime of the product. Contact us through our website, digistor.com/support, call us at 1-800-816-0225 or e-mail us at support@digistor.com.