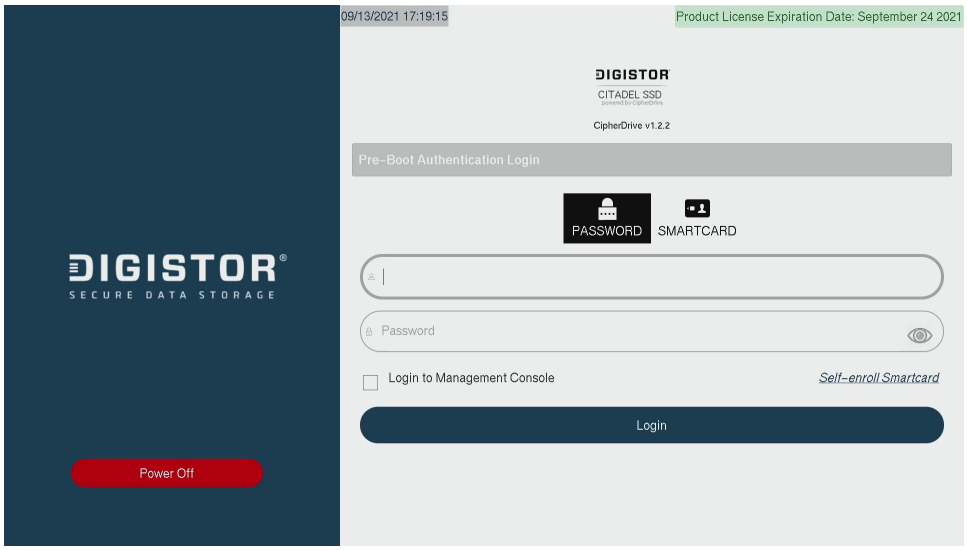
DIGISTOR®

SECURE DATA STORAGE



Citadel K Series

User Manual and Software Only Installation Guide

A9-4400-01-5 Rev 1.3

©2021-2022 CRU Data Security Group, LLC. ALL RIGHTS RESERVED.

This User Manual contains proprietary content of CRU Data Security Group, LLC (“CDSG”) which is protected by copyright, trademark, and other intellectual property rights.

Use of this User Manual is governed by a license granted exclusively by CDSG (the “License”). Thus, except as otherwise expressly permitted by that License, no part of this User Manual may be reproduced (by photocopying or otherwise), transmitted, stored (in a database, retrieval system, or otherwise), or otherwise used through any means without the prior express written permission of CDSG. Use of the full SSD product is subject to all of the terms and conditions of this User Manual and the above referenced License.

DIGISTOR® (collectively, the “Trademarks”) are trademarks owned by CDSG and are protected under trademark law. This User Manual does not grant any user of this document any right to use any of the Trademarks. CipherDrive is a registered trademark of KLC Group, LLC.

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.

In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:

1. Ensure that the case of your attached drive is grounded.
2. Use a data cable with RFI reducing ferrites on each end.
3. Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
4. Reorient or relocate the receiving antenna.

Table of Contents

1. Introduction 5
1.1. Safety Information 5
2. Drive Installation 6
2.1. M.2 SSDs (NVMe or SATA) 6
2.2. 2.5-inch SATA SSD 7
3. Install the PBA Software 8
3.1. Download the PBA Software 8
3.2. Create a Bootable USB Thumb Drive 8
3.3. Configure UEFI/BIOS Settings 9
3.3.1. For All Computers 9
3.3.2. For Dell Computers 9
3.4. Install an Operating System or Virtual Environment 11
3.5. How to Boot into the Thumb Drive 11
3.6. Install the PBA Software 11
3.6.1. Single Drive Software Installation 12
3.6.2. Multi-Drive Software Installation 13
3.7. First Time Login 15
3.8. Upgrade to a Permanent License 16
3.8.1. Collect System Information 16
3.8.2. Complete the License Upgrade 17
4. Pre-Boot Authentication Interface 18
4.1. Logging In 18
4.1.1. Logging In with a Username and Password 18
4.1.2. Logging In with a Smart Card 19
4.1.3. Logging in with Two-Factor Authentication 20
4.2. Logging Out 21
4.3. Dashboard 21
4.4. User 22
4.4.1. User Roles 22
4.4.2. Add a User 23
Add a Password User 23
Add a Smart Card User 24
Add a Two-Factor User 25
Bulk Import Users 26
How to Create a Bulk User Import File 27
4.4.3. Edit a User 28
Edit a Password User 28
Edit a Smart Card User 29
4.4.4. Delete a User 29
4.5. Settings 30
4.5.1. Configuration 30
4.6. Maintenance 32
4.6.1. Backup Database 32
4.6.2. Erase Disk 32
4.6.3. Change DEK 33
4.6.4. Change AK 34
4.6.5. License Upgrade 34
Generate a License Request 35
Upgrade License 36

4.6.6. Upgrading the PBA Software 36
Via the Settings Console 37
Via Command Line 38
4.6.7. Temporarily Deactivate the PBA 40
4.6.8. Uninstall the PBA Software 41
4.6.9. Export Configuration 42
4.6.10. Update Disclaimer 43
4.7. Logs 44
4.7.1. Activity Log 44
4.7.2. Login Log 45
4.7.3. Exception Log 46
4.7.4. Admin Log 47
4.7.5. Latest Log 48
4.7.6. Purge Log 49
4.7.7. Log Filter 50
4.8. Disk Information 51
5. Other Features 52
5.1. Dead Man's Switch Operation 52
5.1.1. What to Do After Using the Dead Man's Switch 52
5.2. Two-factor Authentication Recovery 52
5.3. Deploy the Same Configuration Across Multiple Systems 53
5.4. Reset an SSD 54
5.4.1. Download the PBA Software 55
5.4.2. Create a Bootable USB Thumb Drive 55
5.4.3. How to Boot into the Thumb Drive 56
5.4.4. Wipe the SSD 56
5.5. Reactivate the Citadel SSD 57
5.5.1. Download the Activation Software 57
5.5.2. Create a Bootable USB Thumb Drive 57
5.5.3. How to Boot into the Thumb Drive 58
5.5.4. Activate the SSD 58
6. Troubleshooting 60
6.1. How to Recover Your PBA Software License File 60
6.2. How to Replace a Bad Secondary SSD 61
6.3. Create a Bootable USB Thumb Drive 62
7. Product Support 64

1. INTRODUCTION

DIGISTOR Citadel K Series PBA Software, powered by CipherDrive™, protects against unauthorized access using pre-boot authentication (PBA) built into your self-encrypting drive.

Once fully set up and configured, the PBA software will require you to securely authenticate access to the drive before any operating system or virtual machine stored on the SSD can start up. Then after you authenticate and sign in, changes can be made to the drive in real-time until the host computer is powered off.

This User Manual will help you install the PBA software. It also includes instructions for using the software's Management Console, including managing users and user roles and configuring the PBA for smart card or password access.

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.

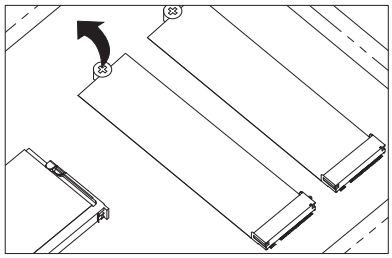
2. DRIVE INSTALLATION

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

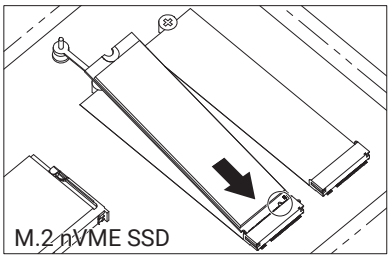
Choose the installation instructions appropriate to the type of SSD you have.

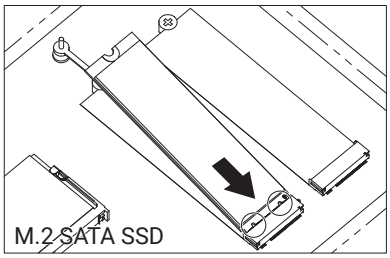
2.1. M.2 SSDS (NVME OR SATA)

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

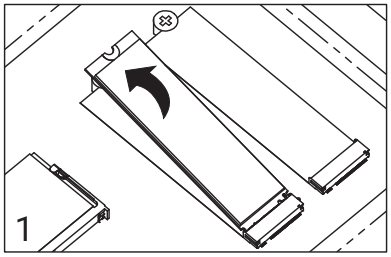


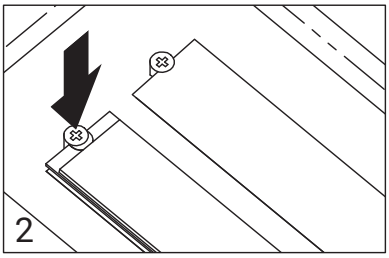
2. Insert your SSD into an open M.2 slot in your computer. Be sure to align the notch(es) on the gold contacts of the SSD module with the notch(es) on the empty slot.





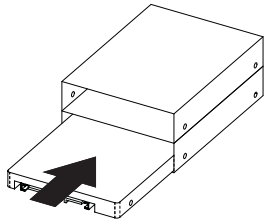
3. Secure the SSD. Hold the SSD flat against the slot bay (Figure 1) and reinsert the screw back into the rear of the slot (Figure 2).



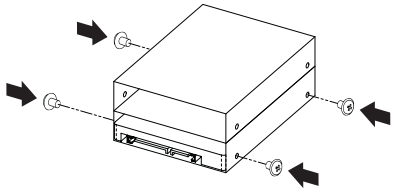


2.2. 2.5-INCH SATA SSD

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

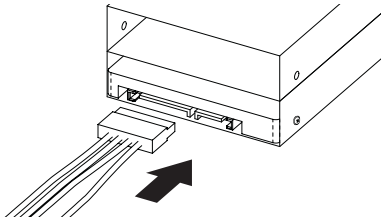


1

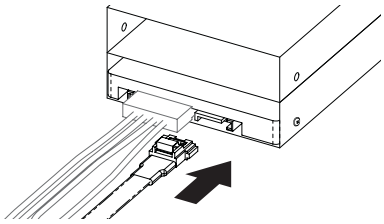


2

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



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



3. INSTALL THE PBA SOFTWARE

These instructions will show you how to create a bootable USB thumb drive, when to install your operating system or virtual machine during the PBA software installation process, how to activate the DIGISTOR SSD's PBA capability, as well as how to log in using the PBA software.

3.1. DOWNLOAD THE PBA SOFTWARE

1. Navigate to digistor.com/citadel-software-only-install and locate the PBA software download. The downloads should be located at the top of the page.

2. Choose the version that you purchased a license for and save it to a place on your computer.

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.

3. Open the ZIP file containing the PBA software you downloaded and extract the folder inside to your computer's desktop.

4. Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

> **IMPORTANT**
> Do not copy the folder itself over to the thumb drive. Your system will 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 Product Support, page 64.

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**, **Esc**, **F2**, or **F12** repeatedly while your computer boots.

1. If you have an option for "UEFI Boot Path Security" or something like it, be sure to change it to **Never**.
2. If you have an option to allow OPAL hard drive SID authentication, be sure to **enable it**.
3. Ensure that your "SATA Operation" is set to **AHCI**.
4. If you have a system that supports CPUs with high core counts, such as a server, the UEFI will likely have an option for "X2Apic Mode" in its processor settings section. Set “X2Apic Mode” to **Disabled**.
5. If you have a discrete video card, ensure your primary display detection is set to **Auto**.
6. Disable "Secure Boot".

> **NOTE**
> Secure Boot **is** supported, but only once the PBA software is completely installed. You may re-enable Secure Boot after you have completed installation of the PBA software and your operating system.

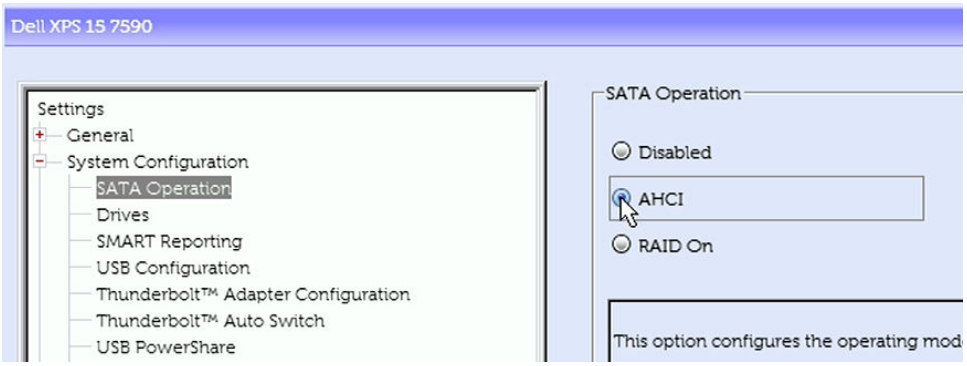
3.3.2. FOR DELL COMPUTERS

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** repeatedly while your computer boots.

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

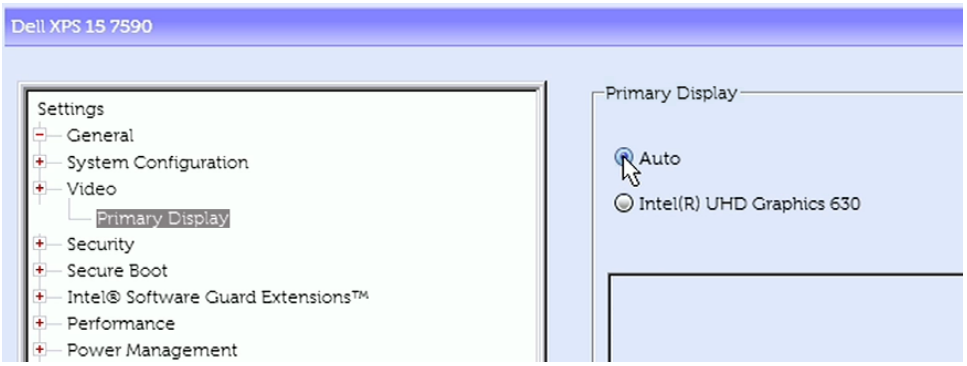
2. If you have an option to allow OPAL hard drive SID authentication, be sure to **enable it**.

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



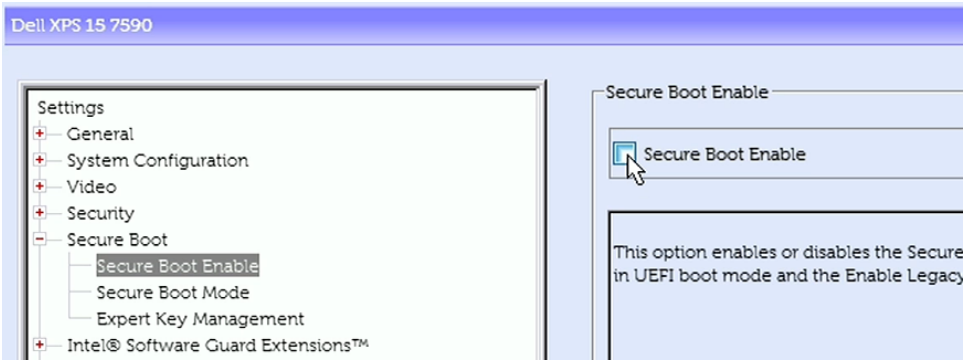
4. If you have a system that supports CPUs with high core counts, such as a server, the UEFI will likely have an option for "X2Apic Mode" in its processor settings section. Set “X2Apic Mode” to **Disabled**.

5. 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.



6. 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**
> Secure Boot **is** supported, but only once the PBA software is completely installed. You may re-enable Secure Boot after you have completed installation of the PBA software and your operating system.



3.4. INSTALL AN OPERATING SYSTEM OR VIRTUAL ENVIRONMENT

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.

3.5. HOW TO BOOT INTO THE THUMB DRIVE

1. Ensure that the computer is turned off.
2. Insert the bootable USB drive you created in the steps above into the computer and turn it on.
3. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.
4. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.
5. A Linux BASH prompt will load. Press **Enter** to activate the console.

3.6. INSTALL THE PBA SOFTWARE

To install the PBA software, follow the instruction set below for the version you have a license for.

- Single Drive License
- Multi-Drive License

3.6.1. SINGLE DRIVE SOFTWARE INSTALLATION

1. Boot into the thumb drive using the steps above.
2. Type in the command below that applies to the type of SSD you have. Please note that the following text is case sensitive.

CAUTION

The following commands will only work when your 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 (examples: /nvme0, /nvme1, /sda) for your SSD. To do so, type **sedutil-cli --scan** and press **Enter**.

Please note that with this version of the PBA software, only the drive you select during this process will be protected by pre-boot authentication and encryption.

If you need more help, contact Technical Support (see Product Support, page 64).

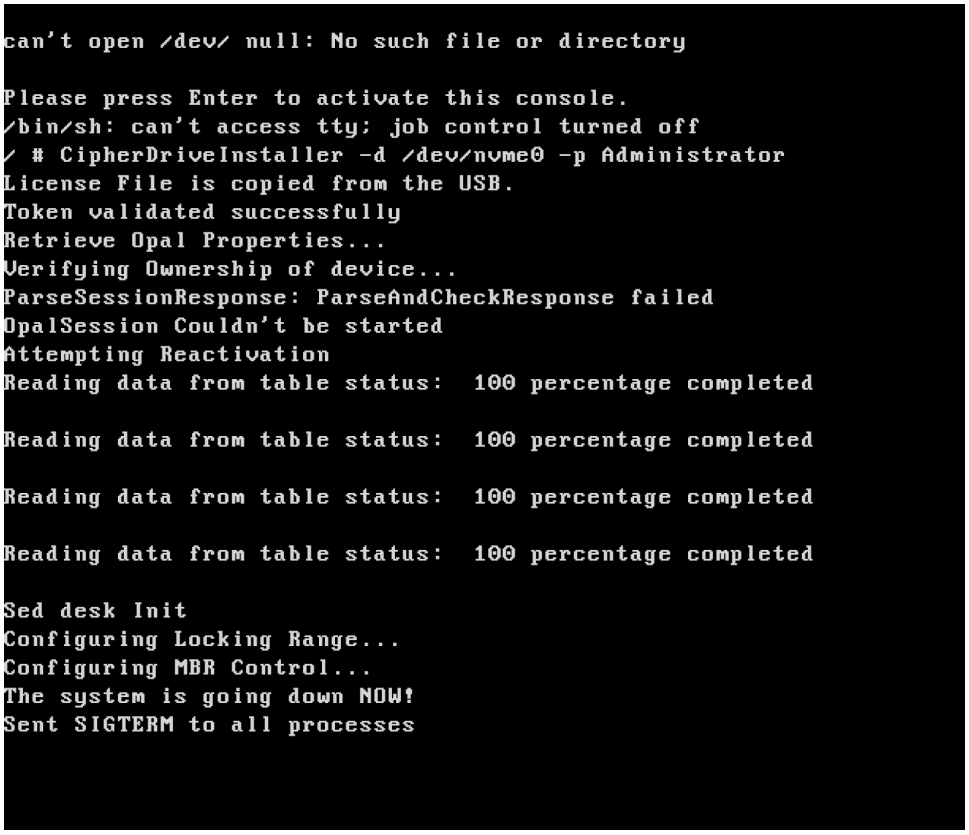
- M.2 NVMe SSD:
  CipherDriveInstaller -d /dev/nvme0 -p <password>
- SATA 2.5-inch or M.2 SATA SSD:
  CipherDriveInstaller -d /dev/sda -p <password>

NOTE

<password> is the Administrator password. The default Administrator password is **Administrator**, and it is *case-sensitive*.

IMPORTANT

If you are using the default Administrator password, you should change it as soon as possible by logging into the PBA software's Management Console.



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

The PBA software has been installed! You can now start using the pre-boot authentication feature.

3.6.2. MULTI-DRIVE SOFTWARE INSTALLATION

1. Boot into the thumb drive using the steps above.
2. Type **sedutil-cli --scan** and press **Enter** to display the paths for each drive you have installed in the system.
3. Use the following command syntax to install the PBA software on the primary SSD with a chained pre-boot authentication on the secondary SSDs. Please note that the following text is case sensitive:

   CipherDriveInstaller -d <primary SSD location>,<secondary SSD location A>,<secondary SSD location B>,<etc> -p <password>

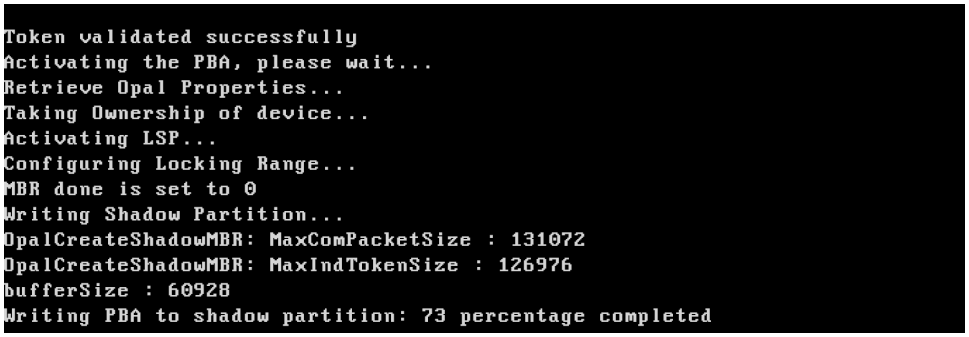
NOTE

<primary SSD location> refers to the drive path for the primary SSD (ex. /dev/nvme0). <secondary SSD location A> is the drive path for the first secondary SSD, <secondary SSD location B> is the drive path for the next secondary SSD, and so on. **<password>** is the Administrator password. The default Administrator password is **Administrator**, and it is *case-sensitive*.

Example: CipherDriveInstaller -d /dev/sda,/dev/sdb -p Administrator

IMPORTANT

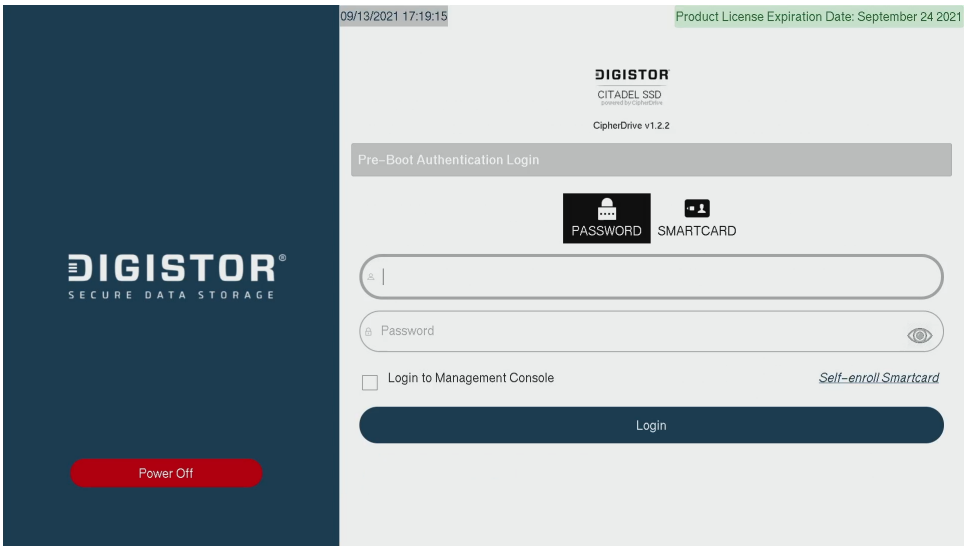
If you are using the default Administrator password, you should change it as soon as possible by logging into the PBA software Management Console.



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

The PBA software has been installed! You can now start using the pre-boot authentication feature.

3.7. FIRST TIME LOGIN



1. If you haven't already, turn on the computer. The SSD pre-boot authentication 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:
   - 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 immediately change the Administrator password to maintain operational security. To do so, log into the Management Console by ensuring the **Management Console box** is checked when you log in. The Management Console allows you to manage users and settings for the PBA software.
>
> DIGISTOR also recommends using a proper, secure password and to not use the Administrator account for everyday use.

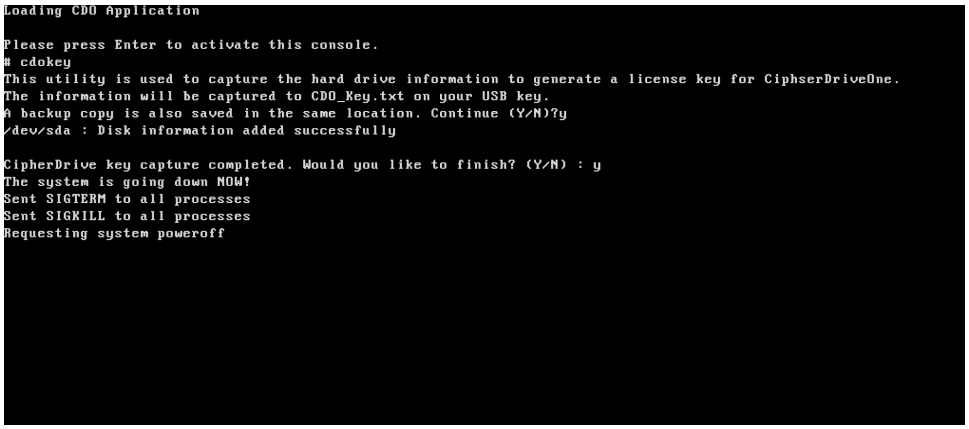
3.8. UPGRADE TO A PERMANENT LICENSE

The PBA Software you downloaded and installed comes with a temporary evaluation license. When the evaluation license expires, you will still be able to log in but you won't be able to use the Management Console, which is how you change settings and edit or add users.

Follow the instructions in this section to upgrade your license to a permanent one that's keyed to your system configuration.

3.8.1. COLLECT SYSTEM INFORMATION

1. Ensure that the computer is turned off.
2. Insert the bootable USB drive you created in the steps above into the computer and turn it on.
3. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.
4. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.
5. A Linux BASH prompt will load. Press **Enter** to activate the console.
6. Type **cdokey** and press **Enter**. Your system information will be collected and saved to the thumb drive as "CDO_Key.txt".
7. You will be prompted, "CipherDrive key capture completed. Would you like to finish? (Y/N)." Type **Y** and press **Enter**.



8. The computer will shut down. Wait for the machine to shut down before removing the thumb drive.
9. If you only need to collect system information for this computer, continue on to the next step.

   Otherwise, follow the above steps for each additional machine. The disk information for each computer will be appended to the "CDO_Key.txt" file every time you use the utility.
10. Save a copy of "CDO_Key.txt" in a safe place for your records.
11. Send "CDO_Key.txt" to your DIGISTOR sales representative. They will return a permanent license file in 3-5 days that's keyed to your system configuration.

3.8.2. COMPLETE THE LICENSE UPGRADE

1. Copy the license file you received from DIGISTOR onto a USB thumb drive formatted as FAT32.
2. Insert the thumb drive into the computer with the SSD installed in it.
3. If you haven't already, log into the Management Console. See Logging In with a Username and Password, page 18.
4. Navigate to **Maintenance > License Upgrade**, and click on the **Upgrade license tab**.
5. Select the thumb drive where the license file is stored from the **Device Name field**.
6. Click the **Choose File button** and find the license file. Select it and click **Open**.

   NOTE
   Sometimes the "Open" dialog box will display the root of the computer system instead of the contents of the thumb drive. If this happens to you, open the **/mnt** folder and then open the folder inside corresponding to the thumb drive to find its contents.

7. Click the **Upgrade License button**.
8. A dialog box will pop up. Enter your password and click **Continue**.

The license will be updated. For changes to take effect, log out and log back in again.

4. PRE-BOOT AUTHENTICATION INTERFACE

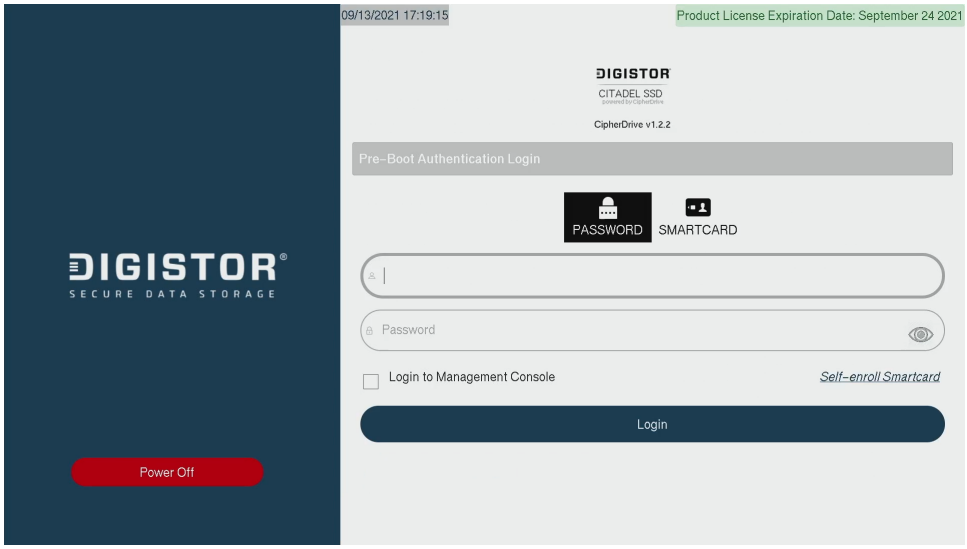
The PBA Interface consists of the **Login Screen** and the **Management Console**, which you can optionally choose to enter from the Login Screen instead of booting into your computer's operating system or virtual machine.

The Management Console allows you to view data and logs about the PBA, edit your user profile, and allows users with the Administrator or Security Officer roles to perform various administrative and maintenance tasks.

4.1. LOGGING IN

4.1.1. LOGGING IN WITH A USERNAME AND PASSWORD

1. Power the computer on. The computer will boot into the SSD's pre-boot authorization screen.



2. Make sure the **Password button** is selected.

3. Type the default username and password into the "Username" and "Password" fields, respectively.

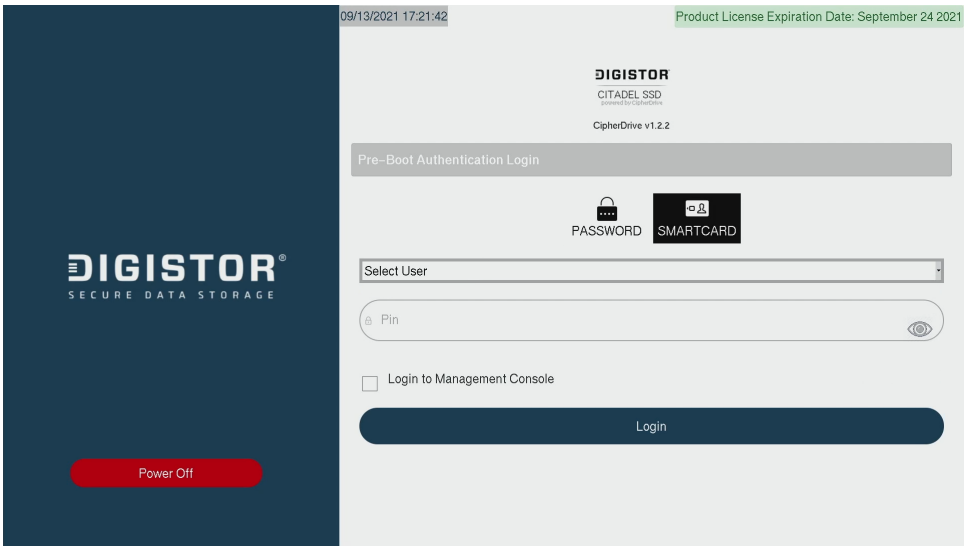
4. If allowed by policy, you can check **Remember Me** so the software will remember your username between logins.

5. If you want to load into the Management Console instead of your operating system, check **Management Console**. Otherwise, leave it unchecked.

6. Click the **Login button**.

You will now be logged in.

4.1.2. LOGGING IN WITH A SMART CARD



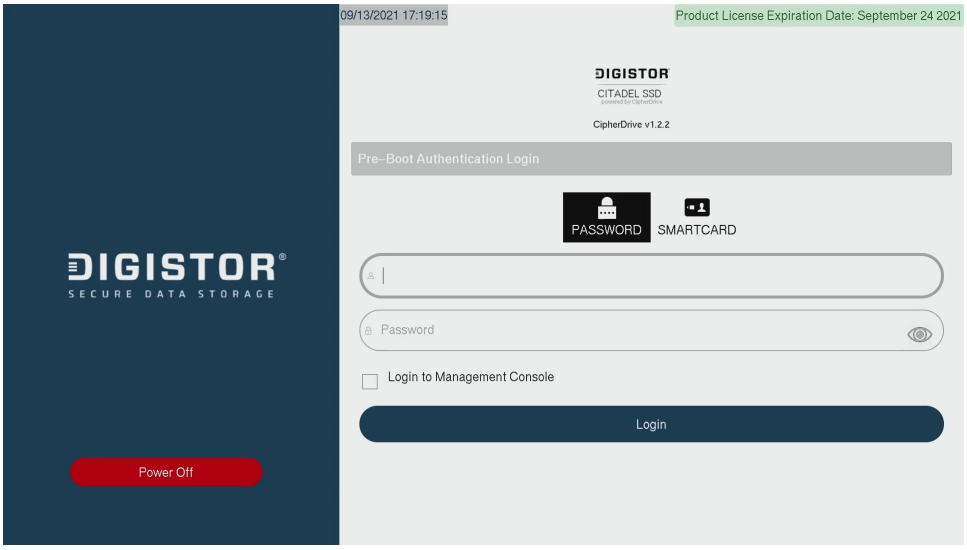
1. Power the computer on. The computer will boot into the SSD's pre-boot authorization screen.
2. Insert the smart card into the card reader.
3. Make sure the **Smart Card button** is selected.
4. Select the username from the drop-down menu.

> **NOTE**
> The usernames in the menu are pulled from the installed certificates on the smart card.

5. Enter the PIN for the card.
6. If you want to load into the Management Console instead of your operating system, check **Management Console**. Otherwise, leave it unchecked.
7. Click the **Login button**.

You will now be logged in.

4.1.3. LOGGING IN WITH TWO-FACTOR AUTHENTICATION



When two-factor authentication (also called multi-factor authentication) is enabled, the user is required to use both the password and smart card login methods.

1. Power the computer on. The computer will boot into the SSD's pre-boot authorization screen.
2. Type the default username and password into the "Username" and "Password" fields, respectively.
3. If allowed by policy, you can check **Remember Me** so the software will remember your username between logins.
4. Click the **Next button**. The Smart Card login screen will now appear.
5. Select the username from the drop-down menu.

> **NOTE**
> The usernames in the menu are pulled from the installed certificates on the smart card.

6. Enter the PIN for the card.
7. If you want to load into the Management Console instead of your operating system, check **Management Console**. Otherwise, leave it unchecked.

> **NOTE**
> A single-factor SmartCard user will only be able to configure Login and viewing options such as Logs. Only users with a password will be able to access the full suite of management features.

8. Click the **Login button**.

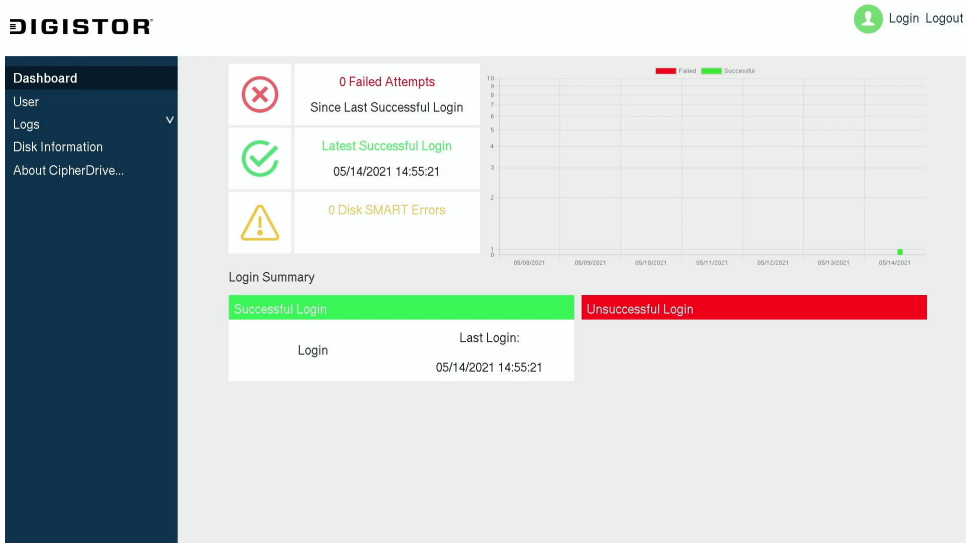
You will now be logged in.

> **WARNING**
> If you've enabled this setting without having an account set up with both a password and smart card, you will be unable to log in or access the Settings Console. You will need to use the Administrator Backdoor method to log in or access Settings Console. See Two-factor Authentication Recovery, page 52.

4.2. LOGGING OUT

You can log out from the Management Console by clicking the **Logout button** on the top right of the screen at any time. This will take you back to the login screen so you can log in and proceed to your operating system.

4.3. DASHBOARD

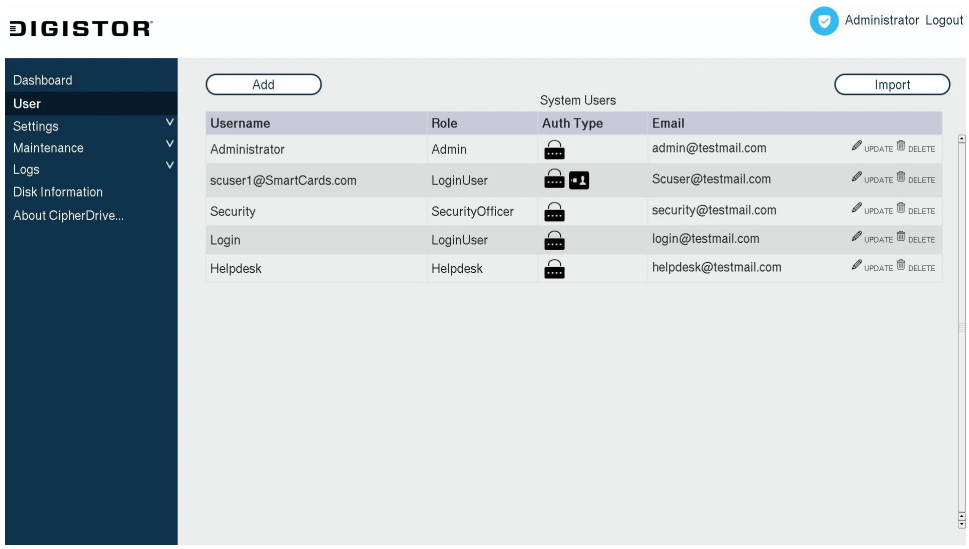


The "Dashboard" screen shows a quick overview of the following events:

- Number of failed login attempts since the last successful login
- Last successful login time and date
- S.M.A.R.T. error count reported by the disk
- Graph of the previous seven (7) days of failed, successful, and total login attempts
- The last successful and unsuccessful login attempts of distinct users

NOTE
Admin and Security Officer accounts can view the successful and failed attempts of all users.

4.4. USER



The "User" screen allows you to add a new user account, delete an account, or modify an existing account.

4.4.1. USER ROLES

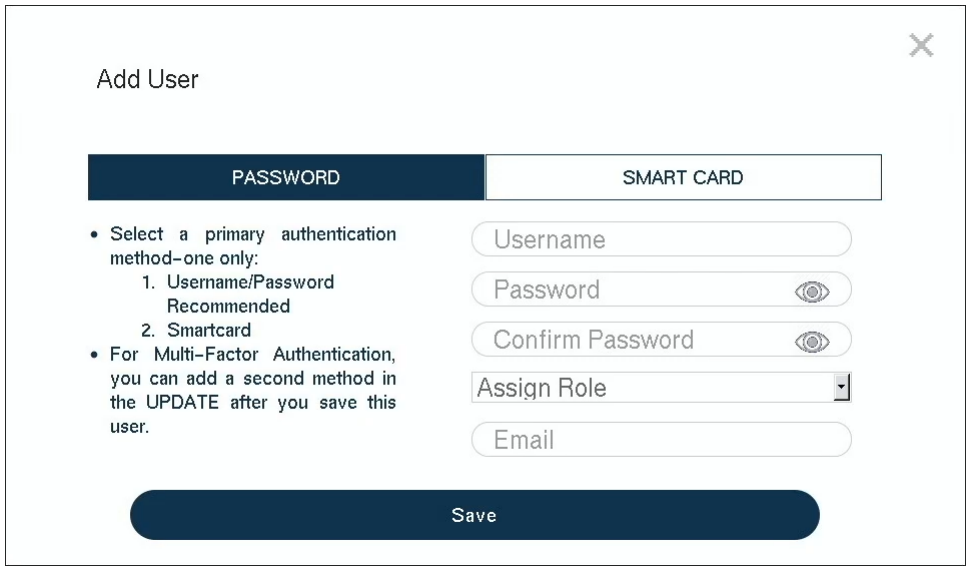
Here are the available user roles (user account types) and what each is allowed to do:

User Role	Add User Account	Update User Account	Delete User Account	Purge Logs	Erase Disk	Change DEK* or AK*	Upgrade, Deactivate or Uninstall PBA*	License Upgrade
Login User		Own Account Only						
Help Desk		Login & Help Desk Accounts Only	✓					
Security Officer		✓	✓	✓	✓	✓		
Admin-istrator	✓	✓	✓		✓	✓	✓	✓

*DEK means "Data Encryption Key", AK means "Authentication Key", and PBA means "Pre-boot Authentication"

4.4.2. ADD A USER

ADD A PASSWORD USER



1. On the "User" screen, click the **Add button**.
2. Make sure the **Password tab** is selected.
3. Enter a unique username for the user account in the **Username field**.

> **IMPORTANT**
> The username must be less than 40 characters. Uppercase, lowercase, numbers, and special characters are allowed.

4. Enter the initial password for the account in the **Password field**.

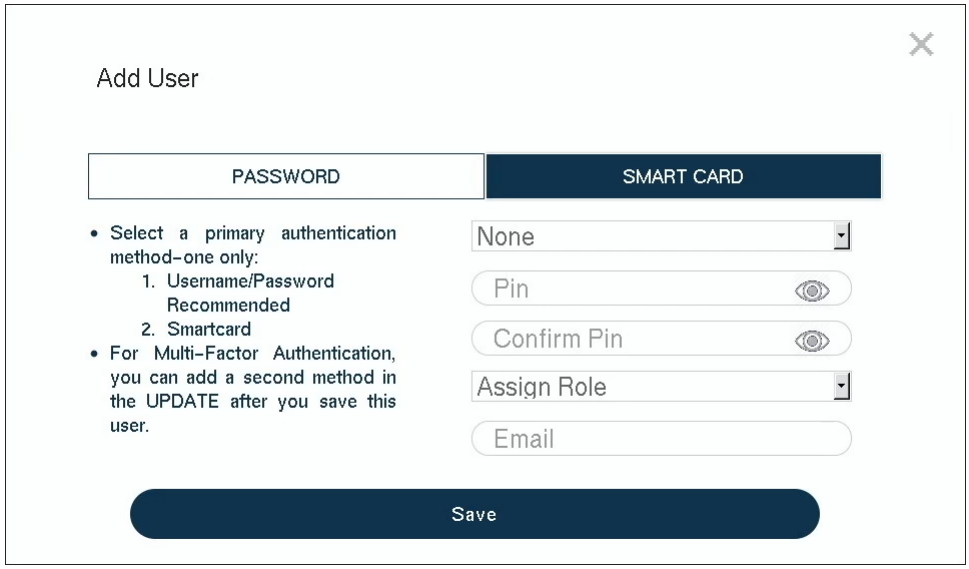
> **IMPORTANT**
> The username must be less than 128 characters. Uppercase, lowercase, numbers, and special characters are allowed.

5. Re-enter the password in the **Confirm Password field**.
6. Select the user role from the **Assign Role drop-down box**.
7. Enter the email address to be associated with the user account in the **Email field**.
8. Click the **Save button**.

9. A new window will pop up. Enter your password in the appropriate field and click **Continue** to verify that you have registered the credentials correctly.

The user account is now ready for use.

ADD A SMART CARD USER



NOTE
A single-factor SmartCard user will only be able to configure Login and viewing options such as Logs. Only users with a password will be able to access the full suite of management features.

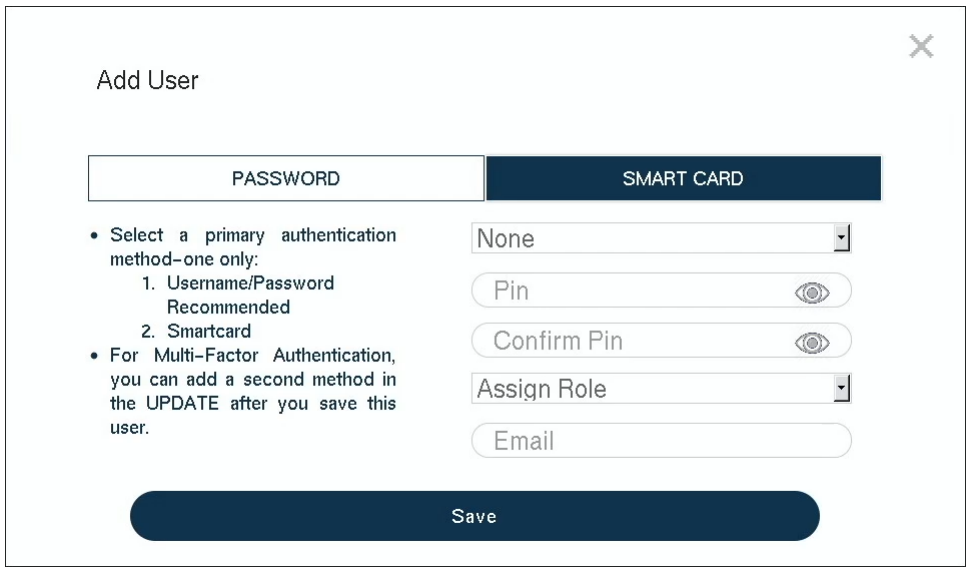
1. Make sure you have access to the card as well as the PIN for the card.
2. On the "User" screen, click the **Add button**.
3. Make sure the **Smart Card tab** is selected.
4. Insert the smart card into the card reader.
5. Select the username to be registered with the software from the drop-down menu at the top of the window. This list shows all the usernames contained on the smart card.
6. Enter the PIN into the **PIN field**.

IMPORTANT
The PIN must be less than 20 characters long.

7. Re-enter the PIN into the **Confirm PIN field**.
8. Select the user role from the **Assign Role drop-down box**.
9. Enter the email address to be associated with the user account in the **Email field**.
10. Click the **Save button**.
11. A new window will pop up. Enter your password in the appropriate field and click **Continue** to verify that you have registered the credentials correctly.

The user account is now ready for use.

ADD A TWO-FACTOR USER



This section shows you how to set up a user with both a password and smart card authentication.

IMPORTANT

Two-Factor Authentication (also called multi-factor authentication) must be enabled in order for user accounts to be required to login with both a password and a smart card. Otherwise they can log in with either one or the other. To enable Two-Factor Authentication, turn on "Enforce 2-Factor Authentication" on the Configuration screen here: Configuration, page 30

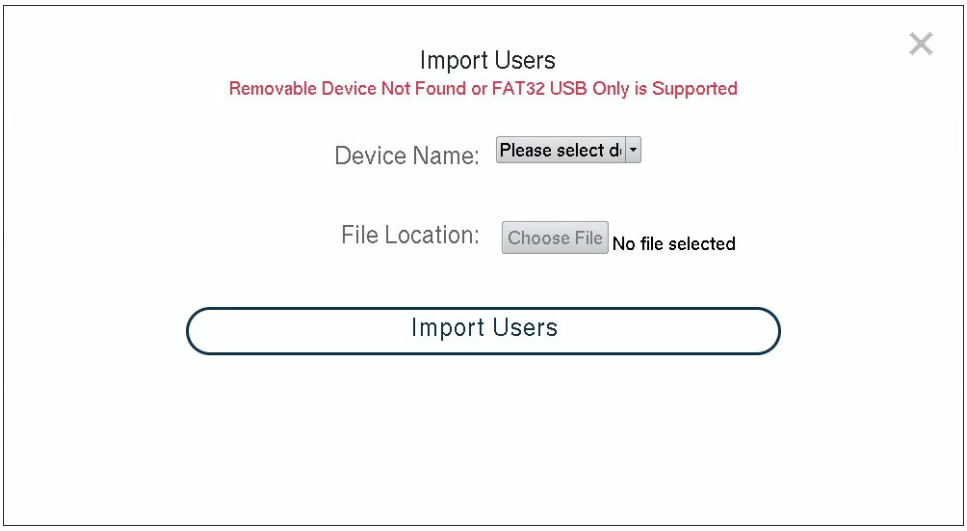
1. Insert the smart card into the card reader.
2. Set up your primary authentication method first.

- If a password will be your primary authentication, follow the instructions for adding a Password user. See Add a Password User, page 23.
- If a smart card will be your primary authentication, follow the instructions for adding a Smart Card user. See Add a Smart Card User, page 24.

3. Next, set up your secondary method by editing the user and adding the appropriate credentials to the user.
   - If a password is your secondary authentication, follow the instructions for editing a Password user. See Edit a Password User, page 28.
   - If a smart card is your secondary authentication, follow the instructions for editing a Smart Card user. See Edit a Smart Card User, page 29.

The user account is now ready for use.

BULK IMPORT USERS



The "Import" function lets you quickly import a set of users to multiple non-networked (air-gapped) systems so you don't have to manually add them one by one to each system.

1. On the "User" screen, click the **Import button** in the top right to open the "Import Users" dialog box.
2. Select the device from the **Device Name drop-down box** to find the USB thumb drive or external hard drive containing the list of users you want to import.

> **NOTE**
> If you need to create a list, see How to Create a Bulk User Import File, page 27.

3. Click the **Choose File button** and select the list of users you want to import. It will be formatted as a TXT file.

NOTE
Sometimes the "Open" dialog box will display the root of the computer system instead of the contents of the thumb drive. If this happens to you, open the **/mnt** folder and then open the folder inside corresponding to the thumb drive to find its contents.

4. Click the **Import Users button**. The users in the TXT file will now be imported onto the PBA.

TIP
Another way to add users is to fully configure a system with a set of users with their valid credentials and then export an encrypted copy that can be imported in another computer. See Export Configuration, page 42.

HOW TO CREATE A BULK USER IMPORT FILE

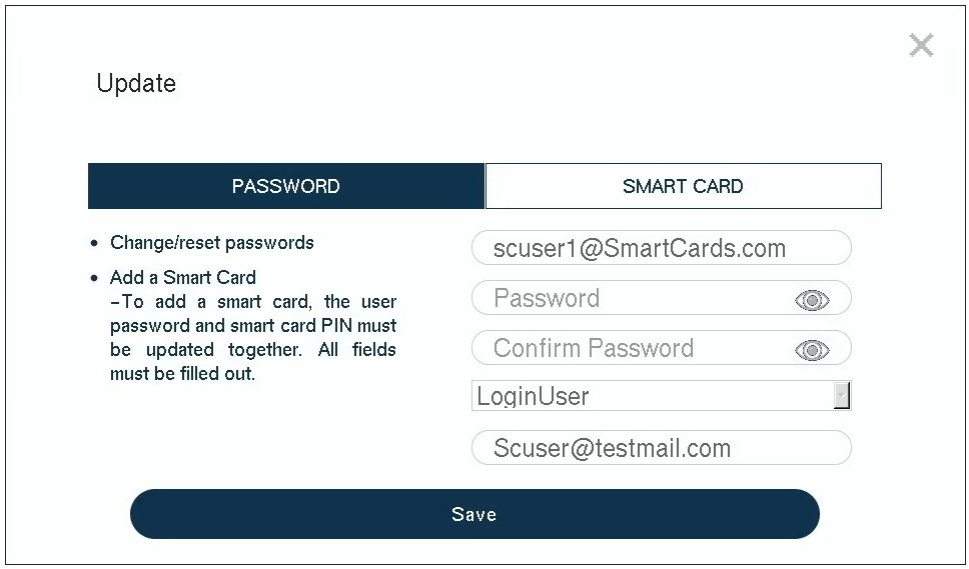
1. Use the following example below to create a JSON-formatted TXT file to bulk import users into your SSD.
2. Place the file onto a USB thumb drive or external drive formatted as FAT32.
3. Follow the instructions for bulk importing users (see Bulk Import Users, page 26).

JSON Example

```
{
'Data':[
    {'UserName': 'Bob', 'Role': 'Admin', 'Email': 'bob@test.com'},
    { 'UserName': 'Alice', 'Role': 'LoginUser', 'Email': 'alice@test.com'},
    { 'UserName': 'Hobbs', 'Role': 'SecurityOfficer', 'Email': 'hobbs@test.com' },
    { 'UserName': 'Steve', 'Role': 'Helpdesk', 'Email': 'steve@test.com'}
]
}
```

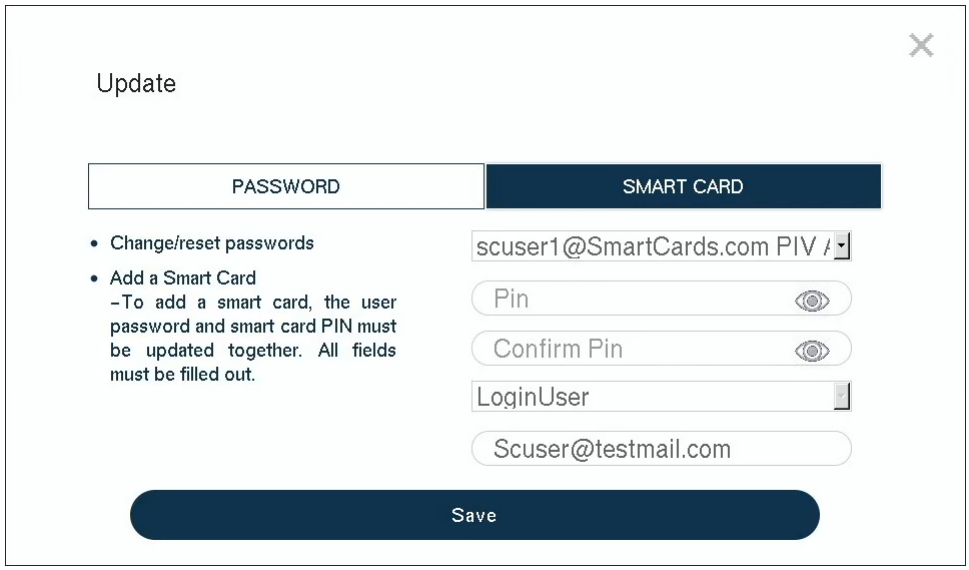
4.4.3. EDIT A USER

EDIT A PASSWORD USER



1. On the "User" screen, locate the user account you wish to edit and then click the **Edit button** next to it.
2. The "Edit User" window will open. Ensure the **Password tab** is selected.
3. Modify the information you need to change or update.
    - If you are an Admin or Security Officer, you can modify the user's password, role, and email address.
    - If you are a Help Desk user, you can modify the user's password and email address.
    - If you are a standard Login User, you can edit your own password and email address.
4. When you are finished, click the **Save button**.
5. A new window will pop up. Enter your password in the appropriate field and click **Continue** to verify that you have registered the credentials correctly.

EDIT A SMART CARD USER



1. On the "User" screen, locate the user account you wish to edit and then click the **Edit button** next to it. If you are a Login User you can only edit your own account.
2. The "Edit User" window will open. Ensure the **Smart Card tab** is selected.

> **IMPORTANT**
> Only users who log in via a password are able to edit smart card users.

3. Modify the information you need to change or update.
   - If you are an Admin or Security Officer, you can modify the user's password, role, and email address.
   - If you are a Help Desk user, you can modify the user's password and email address.
   - If you are a standard Login User, you can edit your own password and email address.
4. When you are finished, click the **Save button**.
5. A new window will pop up. Enter your password in the appropriate field and click **Continue** to verify that you have registered the credentials correctly.

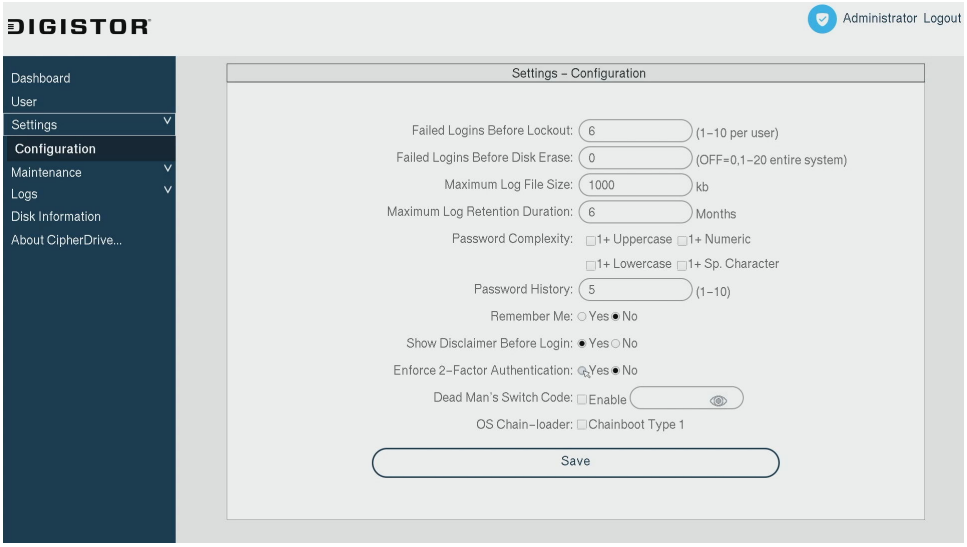
4.4.4. DELETE A USER

1. On the "User" screen, locate the user account you wish to delete and then click the **Delete button** next to it.
2. A confirmation dialog box will appear, asking if you're user you want to delete the user. Click **Yes**.

The user will now be deleted.

4.5. SETTINGS

4.5.1. CONFIGURATION



The "Configuration" page allows you to view and customize the following settings that determine how the SSD PBA behaves. When you are finished, click the **Save button** to save your changes.

- **Failed Logins Before Lockout:** When a user reaches this number of consecutive failed login attempts, further login is disabled until the system is rebooted.
- **Failed Logins Before Disk Erase:** When a user reaches this number of consecutive failed login attempts, the disks protected by the system will be erased.
- **Maximum Log File Size:** The maximum size the log file is allowed to be. The oldest records will be deleted to ensure the log file stays under this file size.
- **Maximum Log Retention Duration:** The amount of time the oldest logs will be kept.

> **NOTE**
> Logs are retained based on whichever condition (Maximum Log File Size or Maximum Log Retention Duration) occurs earlier.

- **Password Complexity:** Check these boxes to enforce different levels of password complexity.
  - **1+ Uppercase:** Requires passwords to have at least one uppercase character.
  - **1+ Lowercase:** Requires passwords to have at least one lowercase character.
  - **1+ Numeric:** Requires passwords to have at least one numeral.
  - **1+ Sp. Character:** Requires passwords to have at least one special character, which include @, %, $, !, and so on.

- **Password History:** The number of previously used unique passwords that should be remembered by the system before a user can use the same password again.
- **Remember Me:** Select **Yes** to enable usernames to be remembered in between sessions. Select **No** to disable this behavior.

> **NOTE**
> This setting does *not* remember passwords.

- **Show Disclaimer Before Login:** Select **Yes** to set the disclaimer screen to appear prior to the login screen. Select **No** to set the disclaimer screen to show after the login screen.
- **Enforce 2-Factor Authentication:** Select **Yes** to require both a password and smart card to log in. Select **No** to allow users to log in using only a password or only a smart card.

> **WARNING**
> Enabling this setting without having your account set up with both a password and smart card will result in you being unable to log in or access the Management Console. You will need to use the Multi-factor Authentication Recovery method to log in or access Management Console. See Two-factor Authentication Recovery, page 52.

- **Dead Man's Switch Code:** The Dead Man's Switch is only to be used in an emergency situation. For example, when user is threatened by an assailant with a gun and is pressured to login. Using the Dead Man's Switch will erase all crypto keys and make it impossible to unlock the disk. Data will be lost permanently.

  Check the **Enable box** to enable the switch. Type the code you wish to set as the Dead Man's Switch into the text box.

  To learn how to use the Dead Man's Switch, see Dead Man's Switch Operation, page 52.

> **NOTE**
> This setting is only visible to users with the Administrator or Security Officer role.

- **Recovery:** Check the **Enable box** to allow users with the Administrator or Security Officer roles to use the Export Configuration and Database Backup features. This field maps directly to the “-n noexport” installer option.

> **NOTE**
> This setting is only visible to users with the Security Officer role.

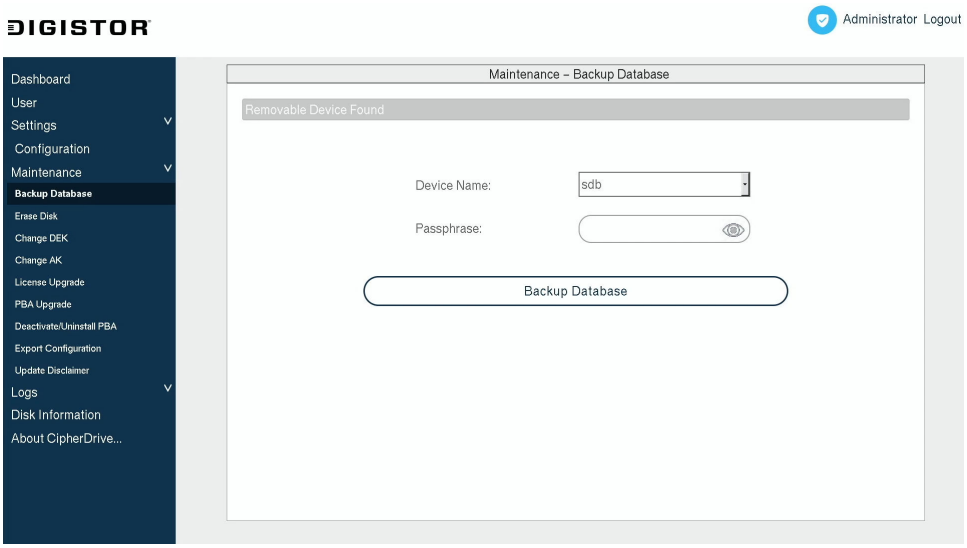
- **OS Chain-loader:** On certain systems, disks will lose power during the chain-booting process after login, resulting in the PBA being loaded repeatedly. On such systems, if this option is enabled, chain-loading will be used for handover from PBA to the protected OS.

Check the **Chainboot type 1 box** to enable this setting.

Once this option is enabled, the PBA will display the kernels available for chain-loading after you log in. Select the kernel and click **OK**.

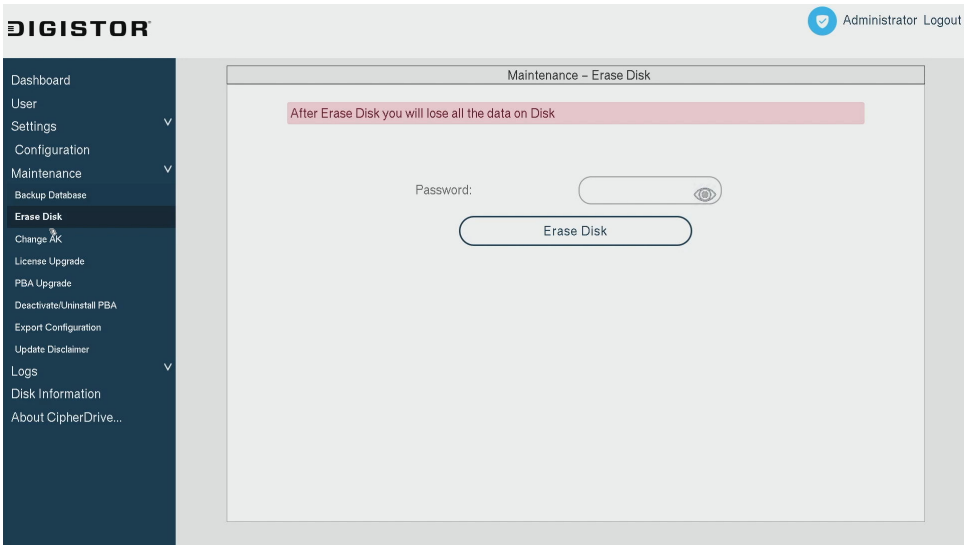
4.6. MAINTENANCE

4.6.1. BACKUP DATABASE



The "Backup Database" screen is used to export configuration and log data. This feature is planned to be fully implemented in a future version of the PBA software.

4.6.2. ERASE DISK



The "Erase Disk" screen lets a Security Officer erase everything on the protected drive(s) and resets them to the factory default state without the Pre-Boot Authentication (PBA) software installed. This screen is only visible to users with the "Security Officer" role.

WARNING

This process **will** erase all the data on the SSD, **including the PBA software**!

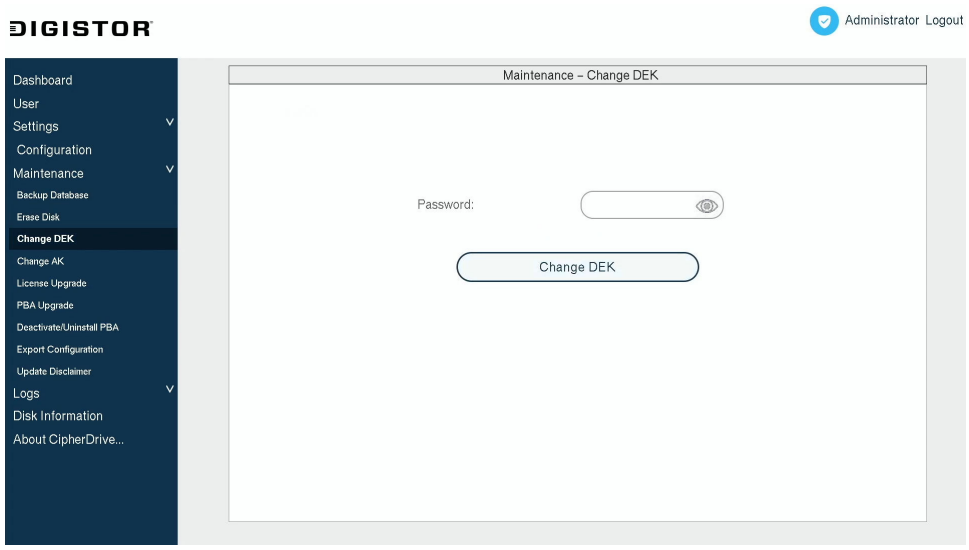
To securely erase the entire drive, you will have to use this process. Be sure to have your license file on hand if you wish to reinstall the PBA software. If you don't have your license file, see Troubleshooting, page 60 for instructions on how to recover your license file.

If you want to uninstall the PBA software but preserve your data, see Uninstall the PBA Software, page 41.

1. On the "Maintenance" > "Erase Disk" screen, enter your password into the **password field**.
2. Click the **Erase Disk button**.
3. A confirmation box will open asking if you really want to continue. Click **Yes** to continue.

The drive contents will be erased.

4.6.3. CHANGE DEK

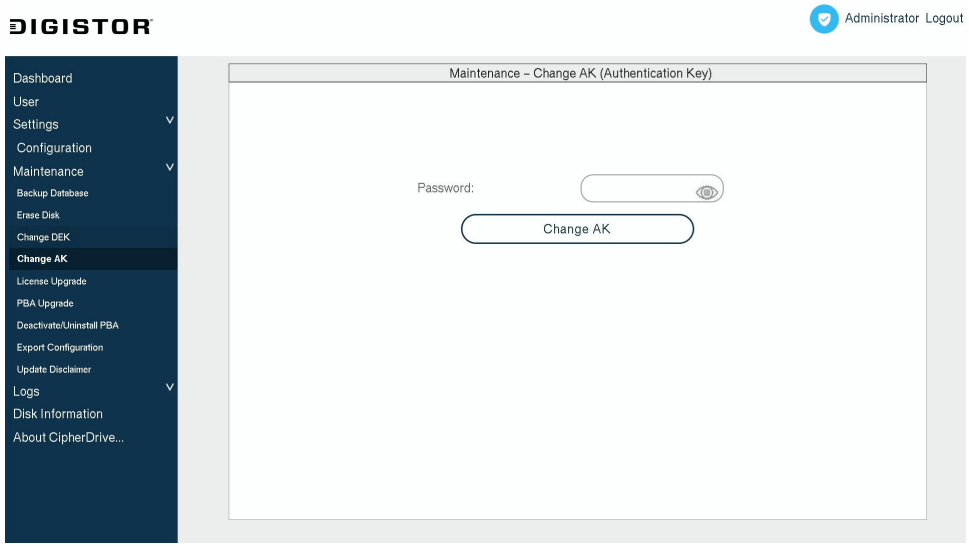


The "Change DEK" screen lets a Security Officer change the protected drive(s)' data encryption key (DEK). This is the actual key used to encrypt the data on the protected drive(s). This screen is only visible to users with the "Security Officer" role.

NOTE
This operation may also be called "SED Gen Key" or "Crypto-Erase" elsewhere.

1. On the "Maintenance" > "Change DEK" screen, enter your password into the **password field**.
2. Click the **Change DEK button**.
3. A window will pop up warning that the operation will cryptographically and irreversibly erase the protected drive(s). Click **Yes** to change the DEK and erase the drive contents.

4.6.4. CHANGE AK



The "Change AK" screen lets an Administrator or Security Officer change the authentication keys (AK's) for all users. An AK ensures that a user is who they say they are. You should change the AK's if you suspect any AK to be compromised. This role is only visible to users with the Administrator or Security Officer roles.

1. On the "Maintenance" > "Change AK" screen, enter your password into the **password field**.
2. Click the **Change AK button**.
3. A window will pop up warning that the operation will change the AK's used to access the protected drive(s) and that the change is non-destructive and all of the content on the protected drive(s) will remain intact. Click **Yes** to change the AK.

4.6.5. LICENSE UPGRADE

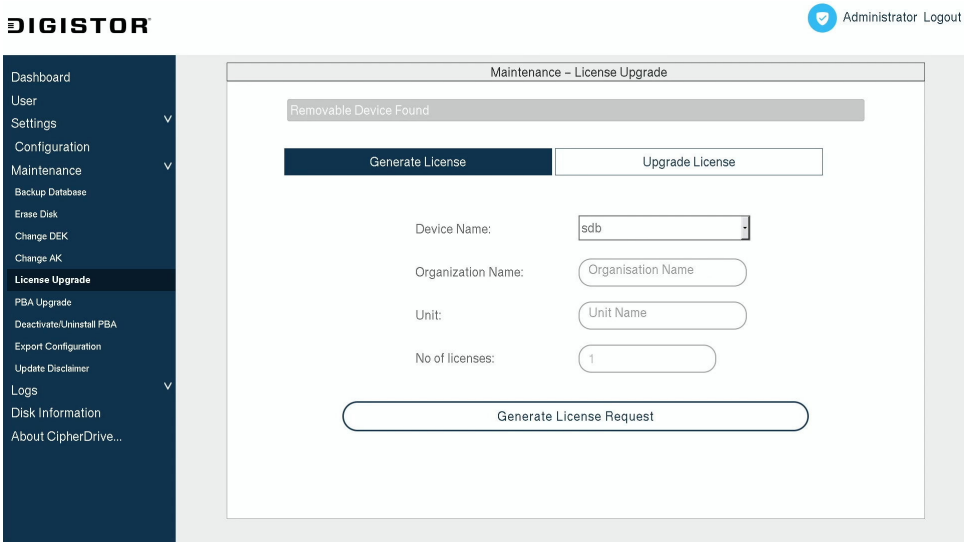
Each SSD comes with a full license so generally you will not need to upgrade or change your license.

Licensing consists of two operations. First, you will need to generate a license request that is unique to the computer where the PBA will be used. This license string can be exported to a network folder for automatic

processing by a licensing agent on the network or by manually giving the file to an administrator who will process the file and send back a file with an activation key.

Secondly, you'll have to import the key into the PBA to remove the trial period and enable the full suite of features available.

GENERATE A LICENSE REQUEST

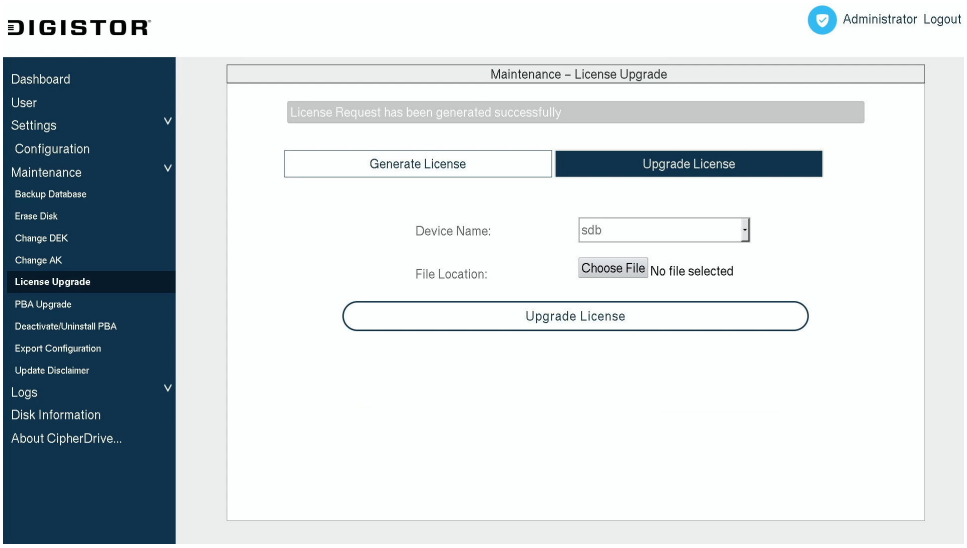


1. Insert a thumb drive formatted to FAT32 into your computer.
2. On the "Maintenance" > "License Upgrade" screen, select the **Generate License tab**.
3. From the **Device Name drop-down box**, choose the thumb drive you inserted to the computer in Step 1. It may take a few seconds for the list of available devices to appear.
4. Enter your company name in the **Organisation Name field**.
5. If applicable, enter your company department or unit name into the **Unit field**.
6. Enter the number of licenses you need in the **No of licenses field**.
7. Click the **Generate License Request button** to create a license request file on the selected drive.
8. Send the license request file to Technical Support. See Product Support, page 64.
9. When you receive the license from Technical Support, continue onto the Upgrade License section (see Upgrade License, page 36).

NOTE

The license Technical Support will send you also determines the data encryption key size used for the encryption/decryption of data. The default size is 256-bits. If you need a different size, please include the request when you contact Technical Support.

UPGRADE LICENSE



1. Using a computer, place the license file you saved from a previous installation or received from Technical Support onto a USB thumb drive formatted as FAT32.
2. Insert the thumb drive into the computer with the SSD installed in it.
3. On the "Maintenance" > "License Upgrade" screen, select the **Upgrade License tab**.
4. Select the thumb drive where the license file is stored from the **Device Name field**.
5. Click the **Choose File button** and find the license file. Select it and click **Open**.

> **NOTE**
> Sometimes the "Open" dialog box will display the root of the computer system instead of the contents of the thumb drive. If this happens to you, open the **/mnt** folder and then open the folder inside corresponding to the thumb drive to find its contents.

6. Click the **Upgrade License button**.
7. A dialog box will pop up. Enter your password and click **Continue**.

The license will be updated. For changes to take effect, log out and log back in again.

4.6.6. UPGRADING THE PBA SOFTWARE

There are two methods to upgrade the SSD's PBA software: through the Management Console or through a USB boot disk while using a command line utility.

VIA THE SETTINGS CONSOLE

1. Go to digistor.com/citadel-downloads and download the latest version of the Citadel PBA software that you have a license for.

2. Open the ZIP file containing the PBA software you downloaded from digistor.com/citadel-downloads and extract the folder inside to your computer's desktop.

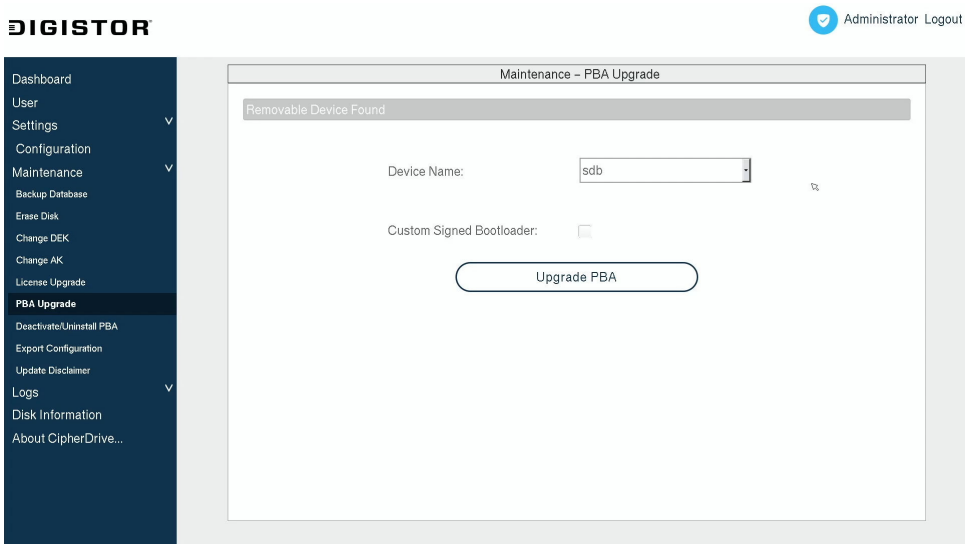
3. Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

> **IMPORTANT**
> Do not copy the folder itself over to the thumb drive. Your system will be unable to boot from it if you do.

4. If there are any changes in customization information (your organization name, your IT support number, or disclaimer), then copy the license file you received from Technical Support to the root location of the thumb drive as well. Otherwise, continue onto the next step.

5. Insert the thumb drive into the computer with the SSD you are upgrading.

6. On the Settings Console, go to the **Maintenance > PBA Upgrade screen**.



7. Choose the thumb drive that contains the PBA software from the **Device Name drop-down box**. It may take a few seconds for the list of available devices to appear.

8. Check the **Custom Signed Bootloader checkbox** if you know you are using a custom signed bootloader. Otherwise, continue to the next step.

9. Click the **Upgrade PBA button**.

10. A dialog box will pop up. Enter an Administrator password and click **Continue**.

The SSD will now be upgraded. After the upgrade is complete, the computer will power off.

VIA COMMAND LINE

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.

3. Open the ZIP file containing the PBA software you downloaded and extract the folder inside to your computer's desktop.
4. Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

> **IMPORTANT**
> Do not copy the folder itself over to the thumb drive. Your system will be unable to boot from it if you do.

5. Copy the license file that you received upon purchasing the SSD to the root of the thumb drive.

> **NOTE**
> Make note of the license file's filename because you will need it later to install the PBA software.

You now have a bootable thumb drive. If you require more help, please contact Technical Support. See Product Support, page 64.

HOW TO BOOT INTO THE THUMB DRIVE

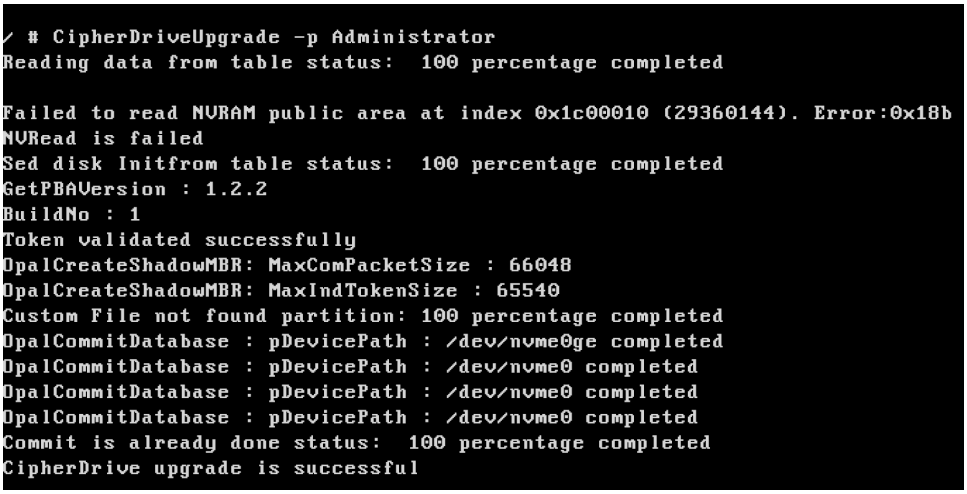
1. Ensure that the computer is turned off.
2. Insert the bootable USB drive you created in the steps above into the computer and turn it on.

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

EXECUTE THE UPGRADE

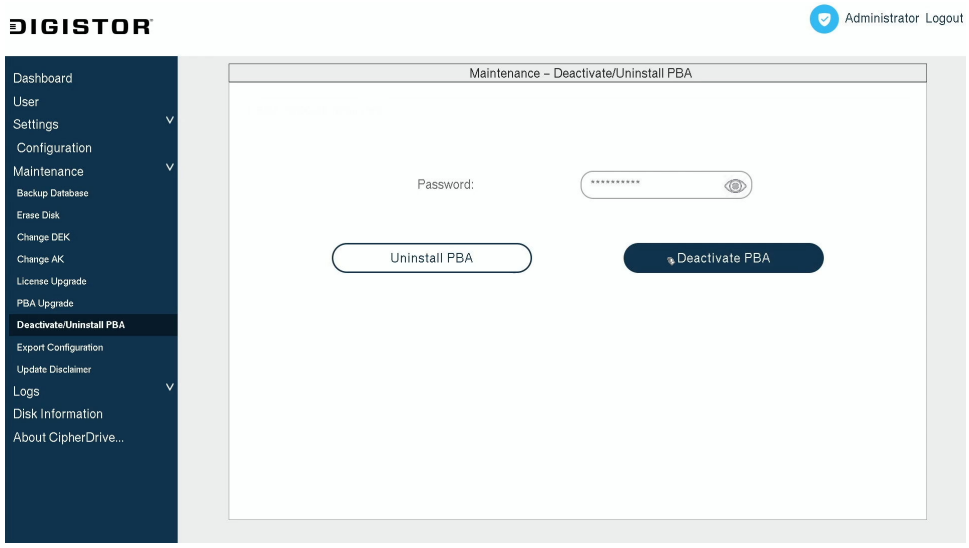
- Type in the following command: **CipherDriveUpgrade -p <password>**

> **NOTE**
> **<password>** is the Administrator password.



The software will now be updated. When you see the message "CipherDrive upgrade is successful", power off the computer.

4.6.7. TEMPORARILY DEACTIVATE THE PBA



The SSD PBA software can be temporarily disabled by an authorized administrator to allow maintenance of the computer's OS. This may be necessary for OS updates that require multiple reboots, or when you need uninterrupted booting and reading from a USB thumb drive or CD. Once work on the host OS is completed, you can reactivate the SSD PBA software (see Reactivate the Citadel SSD, page 57).

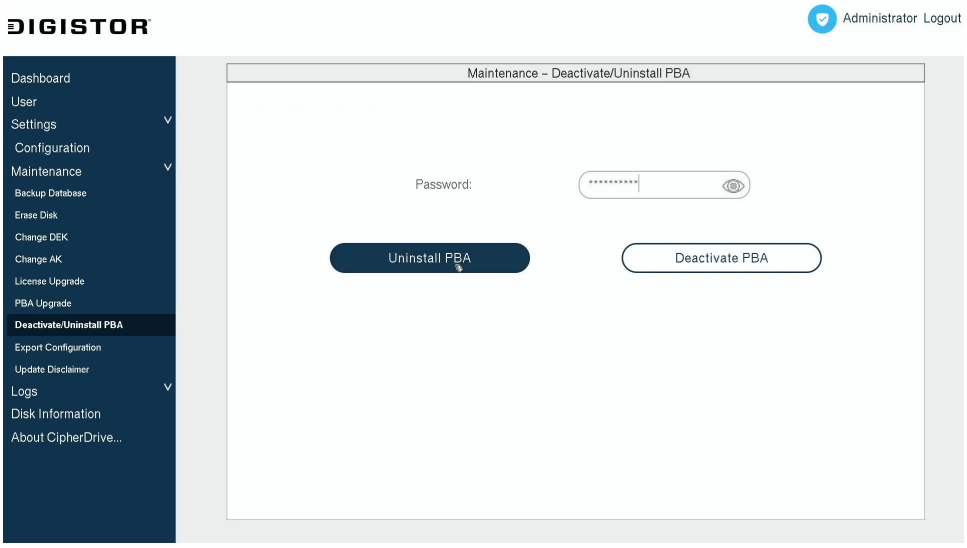
NOTE
This operation does **not** destroy any data, user profiles, or settings. It is only visible to users with the Security Officer or Administrator roles.

1. On the "Maintenance" > "Deactivate/Uninstall PBA" screen, enter your Administrator password into the **password field**.
2. Click the **Deactivate PBA button**.
3. A confirmation dialog box will pop up asking if you're sure you want to continue. Click **Yes** to deactivate.

The SSD PBA software has now been deactivated.

When you need to reactivate the SSD, see Reactivate the Citadel SSD, page 57 and follow the instructions.

4.6.8. UNINSTALL THE PBA SOFTWARE



You can completely uninstall the SSD PBA software, which will completely remove all settings, users, and files from the SSD.

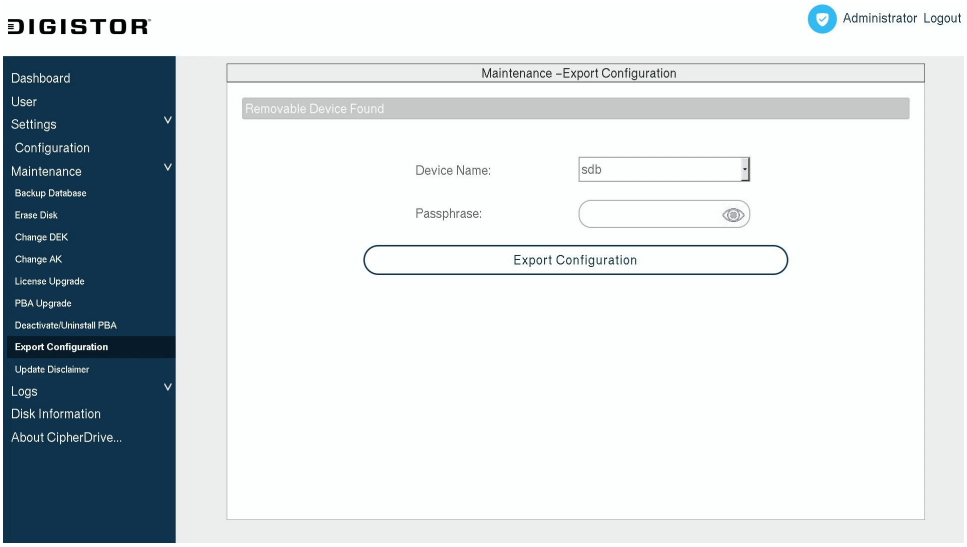
WARNING

DIGISTOR does **not** recommend performing this action unless a Technical Support agent directs you to do so.

1. On the "Maintenance" > "Deactivate/Uninstall PBA" screen, enter your Administrator password into the **password field**.
2. Click the **Uninstall PBA button**.
3. A confirmation dialog box will pop up asking if you're sure you want to continue. Click **Yes** to uninstall.

The SSD PBA software will now be uninstalled.

4.6.9. EXPORT CONFIGURATION



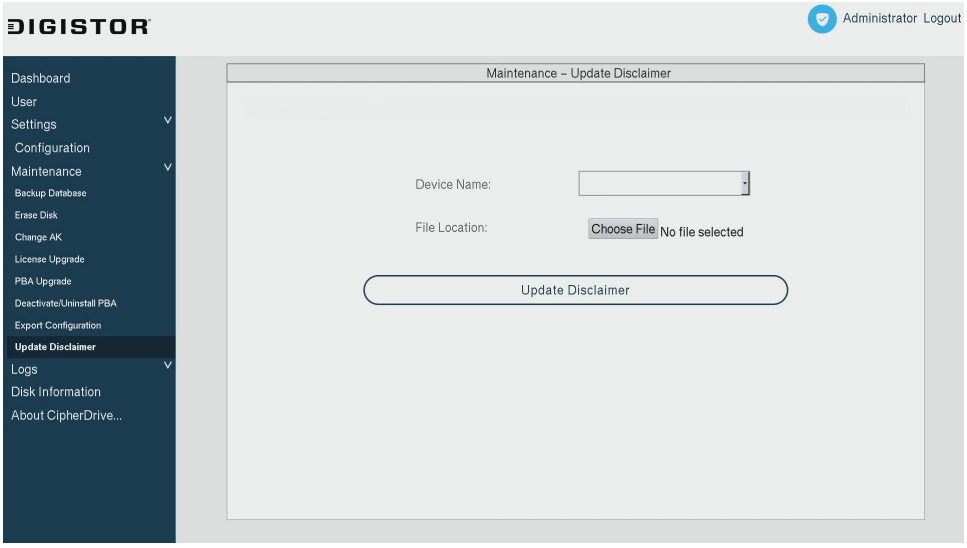
The "Export Configuration" feature is used to deploy a large number of devices with the same configuration on all of them. The configuration file includes both users and settings and will be named "CDExportDB".

This screen is only visible to users with Administrator or Security Officer roles.

1. Insert a thumb drive formatted to FAT32 into your computer.
2. On the "Maintenance" > "Export Configuration" screen, choose the device or drive to store the configuration file on from the **Device Name drop-down box**. It may take a few seconds for the list of available devices to appear.
3. Type in a passphrase that will be used to encrypt the configuration file into the **Passphrase text box**.
4. Click the **Export Configuration button**.
5. A dialog box will pop up. Enter your password and click **Continue** to confirm your credentials.

The "CDExportDB" configuration file has now been exported to the root of the thumb drive. To deploy it to a large number of devices, see Deploy the Same Configuration Across Multiple Systems, page 53.

4.6.10. UPDATE DISCLAIMER



You can upload your own Disclaimer text using the Update Disclaimer Screen. This text displays on the first boot of a Citadel protected device, right before you enter the Login Screen.

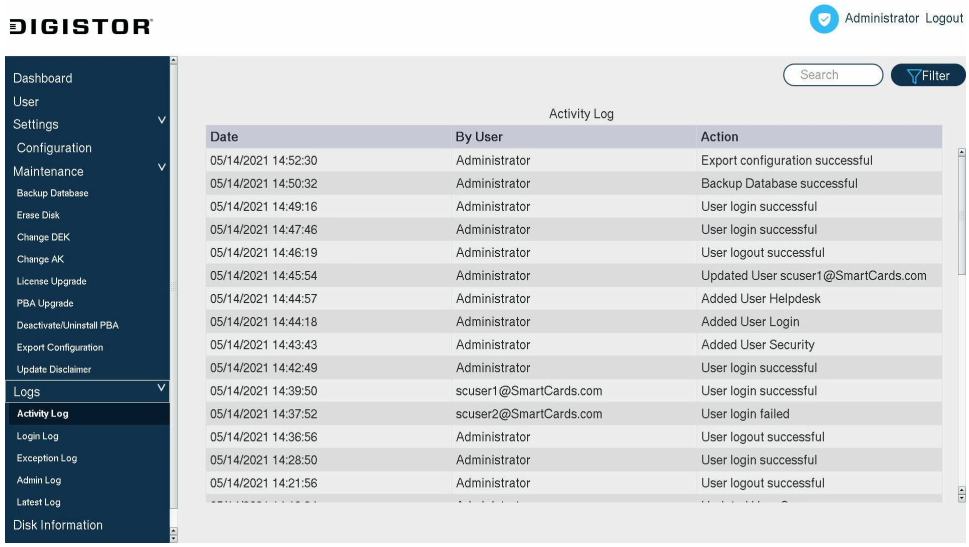
1. Using a computer, write your Disclaimer text into a .TXT file.
2. Using a computer, place the Disclaimer text file you created onto a USB thumb drive formatted as FAT32.
3. Insert the thumb drive into the computer with the SSD installed in it.
4. On the "Maintenance" > "Update Disclaimer" screen, select the thumb drive where the license file is stored from the **Device Name field**.
5. Click the **Choose File button** and find the license file. Select it and click **Open**.

> **NOTE**
> Sometimes the "Open" dialog box will display the root of the computer system instead of the contents of the thumb drive. If this happens to you, you can find the thumb drive's contents in the 'mnt' folder.

6. Click the **Update Disclaimer button**.
7. A dialog box will pop up. Enter your password and click **Continue**.

4.7. LOGS

4.7.1. ACTIVITY LOG



The "Activity Log" screen includes every log that exists in the SSD PBA software's database. To access the "Activity Log" screen, click on **Logs** on the left-hand menu and then click on **Activity Log**.

You can search for specific log messages by using the **Search text box** in the top right of the screen and you can filter log messages by date range and username by clicking on the **Filter button** in the top right. See Log Filter, page 50.

Here are the types of logs available from this screen:

Login Messages

- User login successful
- User login failed
- User logoff successful

> **NOTE**
> This log message means that the user has exited the PBA Settings Console and booted into the host system. This log message is not recorded unless the user has already first entered the Settings Console.

User Management Messages

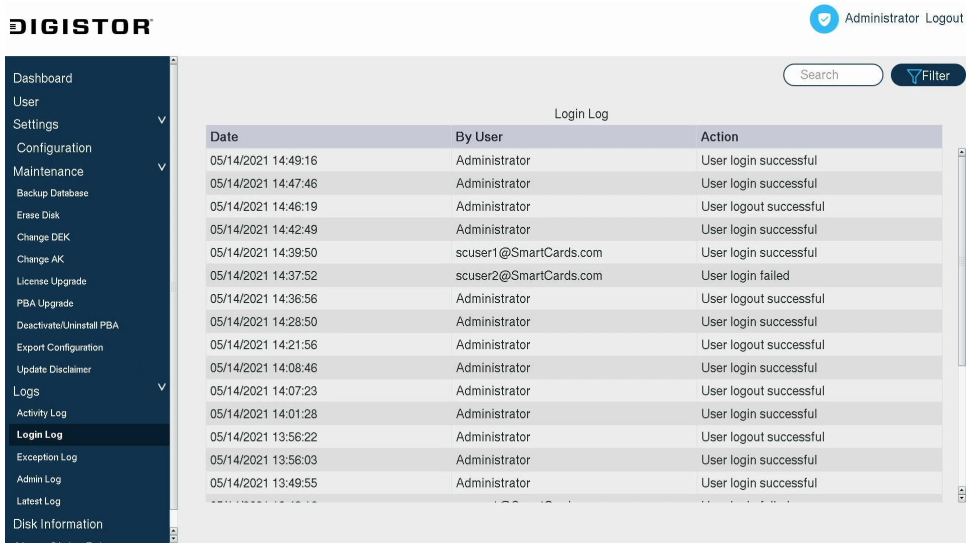
- Added user
- Edited user
- Failed to add user
- Failed to delete user

- Failed to edit user
- User deleted

Maintenance Messages

- Incorrect JSON data for import users

4.7.2. LOGIN LOG



The "Login Log" screen includes successful and unsuccessful login and logout events of the SSD. To access the "Login Log" screen, click on **Logs** on the left-hand menu and then click on **Login Log**.

You can search for specific log messages by using the **Search text box** in the top right of the screen and you can filter log messages by date range and username by clicking on the **Filter button** in the top right. See Log Filter, page 50.

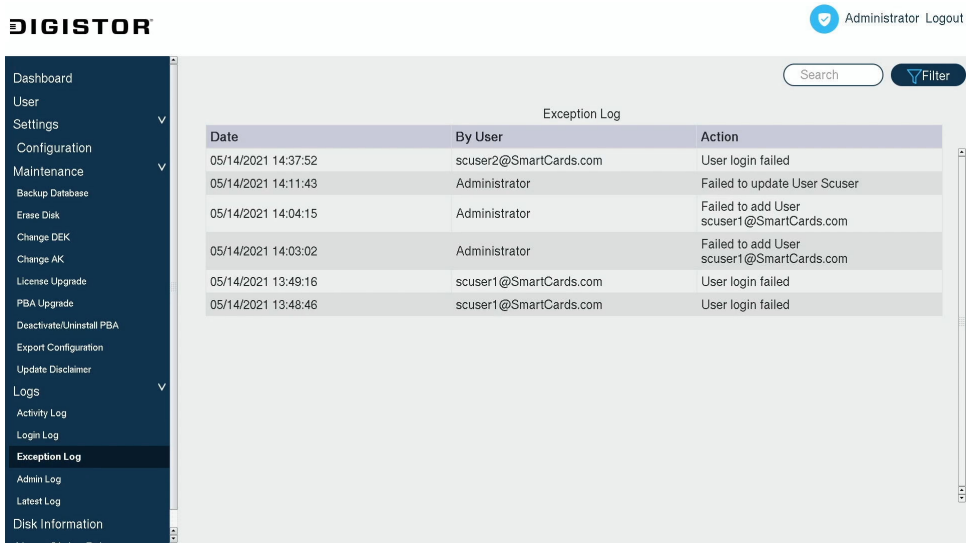
Here are the types of logs available from this screen:

- User login successful
- User login failed
- User logoff successful

NOTE

This log message means that the user has exited the PBA Settings Console and booted into the host system. This log message is not recorded unless the user has already first entered the Settings Console.

4.7.3. EXCEPTION LOG



The "Exception Log" screen includes all failed actions. To access the "Exception Log" screen, click on **Logs** on the left-hand menu and then click on **Exception Log**.

You can search for specific log messages by using the **Search text box** in the top right of the screen and you can filter log messages by date range and username by clicking on the **Filter button** in the top right. See Log Filter, page 50.

Here are the types of logs available from this screen:

- Failed to add user
- Failed to delete user
- Failed to edit user
- Incorrect JSON data for import users
- User login failed

4.7.4. ADMIN LOG

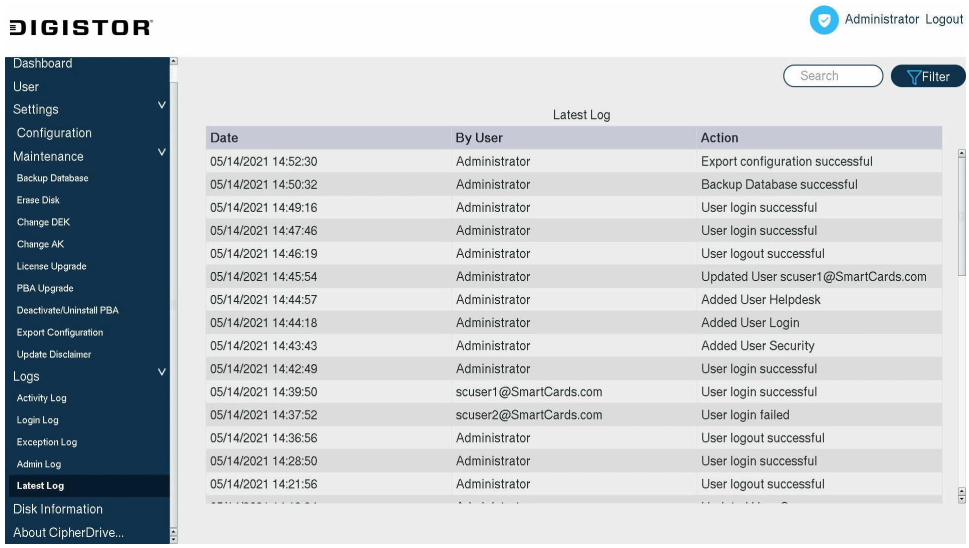
The "Admin Log" screen includes all administator actions carried out by the administrator on their account. To access the "Admin Log" screen, click on **Logs** on the left-hand menu and then click on **Admin Log**.

You can search for specific log messages by using the **Search text box** in the top right of the screen and you can filter log messages by date range and username by clicking on the **Filter button** in the top right. See Log Filter, page 50.

Here are the types of logs available from this screen:

- Added user
- Edited user
- User deleted

4.7.5. LATEST LOG



The "Latest Log" screen includes all logs generated for the current day. To access the "Admin Log" screen, click on **Logs** on the left-hand menu and then click on **Latest Log**.

You can search for specific log messages by using the **Search text box** in the top right of the screen and you can filter log messages by date range and username by clicking on the **Filter button** in the top right. See Log Filter, page 50.

Here are the types of logs available from this screen:

Login Messages

- User login successful
- User login failed
- User logoff successful

> **NOTE**
> This log message means that the user has exited the PBA Settings Console and booted into the host system. This log message is not recorded unless the user has already first entered the Settings Console.

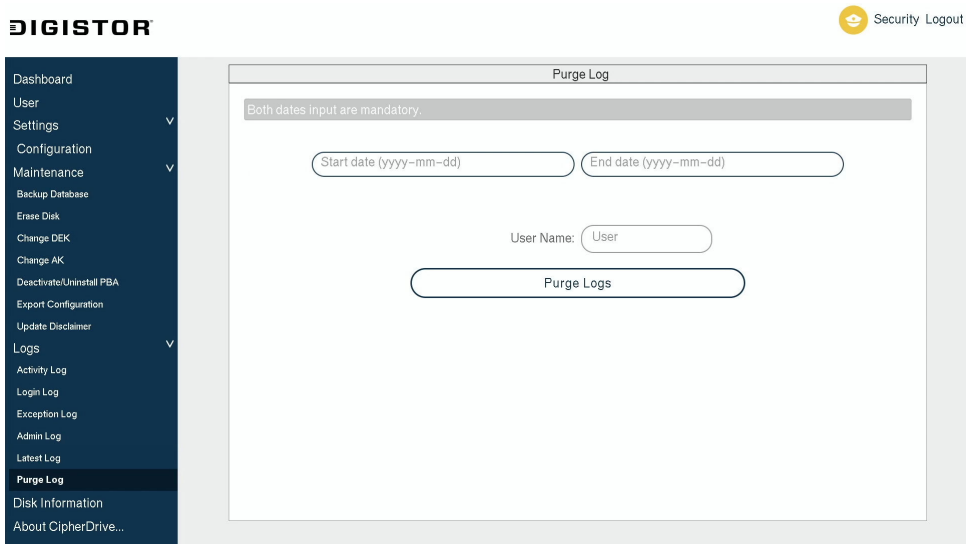
User Management Messages

- Added user
- Edited user
- Failed to add user
- Failed to delete user
- Failed to edit user
- User deleted

Maintenance Messages

- Incorrect JSON data for import users

4.7.6. PURGE LOG

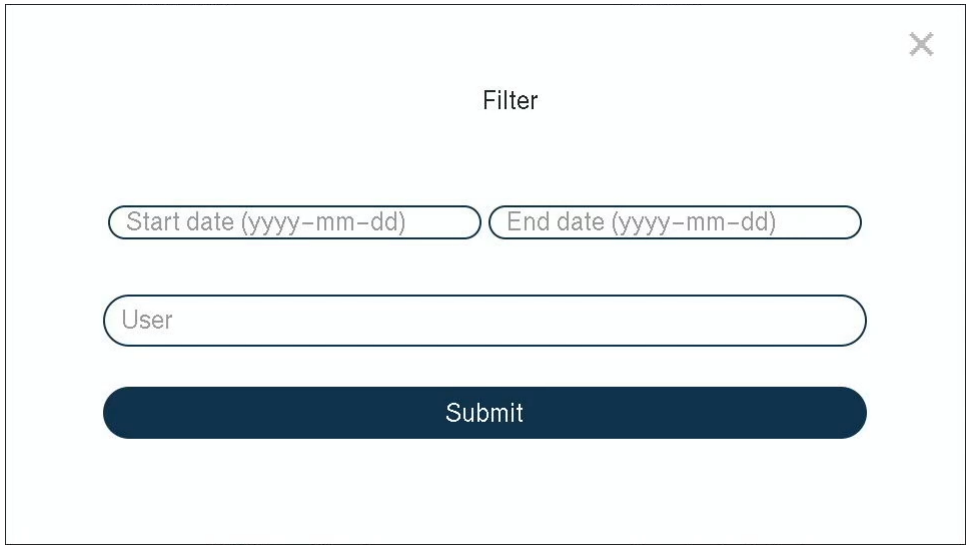


The "Purge Log" screen allows Security Officer users to delete logs by date range and/or username.

1. Click on the **Start Date text box**. You'll be shown a pop-up calendar. Click on your desired start date for the date range you want to search within.
2. Click on the **End Date text box** and choose your desired end date from the pop-up calendar.
3. If desired, type in the user account name whose logs you want to purge.
4. Click the **Purge Logs button**.
5. A confirmation box will pop up asking if you are sure you want to continue. Click **Yes**.

The logs within the selected date range and belonging to the chosen user account have now been deleted.

4.7.7. LOG FILTER

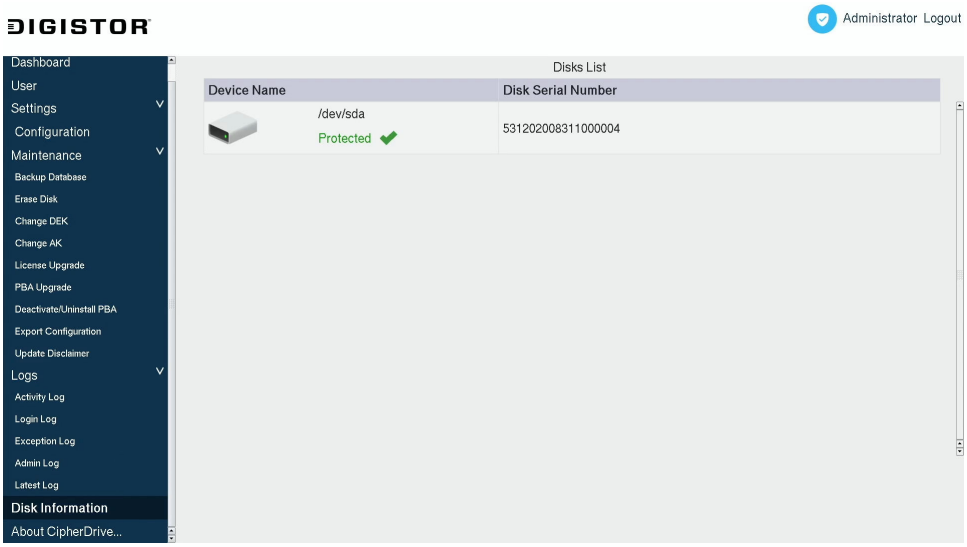


You can sort and filter the display of logs by date and/or username with the log filter. This feature is available on all log screens except the "Purge Log" screen.

1. Click on the **Filter button** in the top right.
2. Click on the **Start Date text box**. You'll be shown a pop-up calendar. Click on your desired start date for the date range you want to search within.
3. Click on the **End Date text box** and choose your desired end date from the pop-up calendar.
4. If desired, type in the user account name whose logs you want to display.
5. Click the **Submit button**.

A list of logs matching the criteria you entered will appear.

4.8. DISK INFORMATION



The "Disk Information" screen shows a list of available disks installed on the computer and displays each one's device name, serial number, and protection status.

5. OTHER FEATURES

5.1. DEAD MAN'S SWITCH OPERATION

The Dead Man's Switch is used when a threatened user wants to destroy the disk authentication keys and make the protected drives' contents impossible to recover. For example, when user is threatened by a man with a gun and is pressured to login.

1. Enter the login user’s username and password at the login screen.
2. In the password field, after entering the user’s password, **don’t press enter/logon**! Instead, continue by entering the Dead Man's Switch code directly following the user’s password characters.
3. Now click the **Logon button**.

The PBA will destroy all the authentication keys without acknowledgment of any sort. This will make it impossible to access the protected drive(s).

5.1.1. WHAT TO DO AFTER USING THE DEAD MAN'S SWITCH

Unfortunately there is no way to recover the data on the protected disks. You will have to reset the SSD, which will cryptographically erase the protected disks and revert them back to factory settings so you can reuse them and reinstall the PBA software.

To reset the SSD, see Reset a SSD.

5.2. TWO-FACTOR AUTHENTICATION RECOVERY

This feature is intended to allow you to log in if you accidentally enable two-factor authentication (also called multi-factor authentication) without also having a user account set up for two-factor authentication.

DANGER

Because the Administrator account can be accessed in this way, DIGISTOR recommends that you do not use this account for everyday access or share its credentials with anyone. You should also use a proper, secure password and store it in a secure location. The security of your data depends on it!

To log into a two-factor enabled system when no two-factor enabled account exists, follow these instructions:

1. On the "Login" screen, type the username **Administrator** into the **Username field**.
2. Type the Administrator account's password into **Password field**.
3. Check the **Management Console checkbox**.

4. Click the **Next button**. The Smart Card login screen will now appear.

5. Skip selecting a username or entering your PIN. Instead, click the **Login button**.

You will now be logged into the Management Console on the Administrator account. Now you can disable two-factor authentication if necessary by going to "Settings" > "Configuration". See Configuration, page 30.

5.3. DEPLOY THE SAME CONFIGURATION ACROSS MULTIPLE SYSTEMS

Follow these instructions to duplicate an entire Citadel configuration from one system to another, including settings and user accounts. This is helpful if you are deploying a large number of Citadel protected systems.

TIP

You may wish to refer to the full installation instructions for the version of the PBA software you've licensed, which are located at digistor.com/citadel-downloads. The procedure for installing the PBA software with an exported configuration is identical with the exception of the command to install the PBA software (seen below).

1. In the PBA software's Management Console, navigate to **Maintenance > Export Configuration**. Follow the instructions there to export a 'CDExportDB' configuration file, or see Export Configuration, page 42.

2. Install the new SSD into the second system.

3. If you haven't already, create a bootable USB thumb drive with the full version of the PBA software on it. Ensure you've chosen the version you have a license for. For instructions on how to download the PBA software and create a bootable USB thumb drive, see Create a Bootable USB Thumb Drive, page 38.

4. Copy the 'CDExportDB' configuration file you exported in Step 1 onto the root of the USB thumb drive.

5. Insert the thumb drive into the computer system. Then power on or reboot it.

6. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.

7. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.

8. A Linux BASH prompt will load. Press **Enter** to activate the console.

9. Type in the command below to install the PBA software with the configuration you exported. Please note that the following text is case sensitive.

> **CAUTION**
> If you have multiple drives, you must ensure you are using the correct Linux boot path for the replacement drive (examples: /nvme1, /sdb) for your SSD. To do so, type **sedutil-cli --scan** and press **Enter**.
>
> If you need more help, contact Technical Support (see Product Support, page 64).

CipherDriveInstaller -d <drive boot path> -p <password> -db CDExportDB -ps <passphrase>

> **NOTE**
> **<drive boot path>** refers to the drive path of the SSD you're installing the PBA software on (Examples: /dev/nvme1, /dev/sda, /dev/sdb). **<password>** is the Administrator password and it is *case-sensitive*. **<passphrase>** is the passphrase you placed on your database when you exported it.

10. The computer will power off once the command has been processed. Power it back on and boot into the **Management Console**. The settings and users from the source Citadel system can now be found here.

5.4. RESET AN SSD

> **WARNING**
> This process **will** erase all the data on the SSD, **including the PBA software**!
>
> If you want to uninstall the PBA software but preserve your data, see Uninstall the PBA Software, page 41.

If you are unable to access your system with your Administrator password, then it may be necessary to reset the SSD.

The following sections show you how to prepare and wipe a SSD.

> **IMPORTANT**
> Before beginning this process, be sure that you have the following information on hand:
>
> - **The PSID number for each SSD you have:** The PSID is located on the physical label of the SSD.
> - **Your license file:** This file was sent to you upon purchase of your SSD. If you no longer have a copy of the license file, see Troubleshooting, page 60 for instructions on how to recover your license file.

5.4.1. DOWNLOAD THE PBA SOFTWARE

Visit digistor.com/citadel-downloads and choose the full installation of the PBA software that you have a license for.

NOTE
Do not download the Citadel Activation software. This software is used to activate brand new SSD's.

5.4.2. 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.

3. Open the ZIP file containing the PBA software you downloaded and extract the folder inside to your computer's desktop.
4. Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

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

5. Copy the license file that you received upon purchasing the SSD to the root of the thumb drive.

NOTE
Make note of the license file's filename because you will need it later to install the PBA software.

You now have a bootable thumb drive. If you require more help, please contact Technical Support. See Product Support, page 64.

5.4.3. HOW TO BOOT INTO THE THUMB DRIVE

1. Ensure that the computer is turned off.
2. Insert the bootable USB drive you created in the steps above into the computer and turn it on.
3. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.
4. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.
5. A Linux BASH prompt will load. Press **Enter** to activate the console.

5.4.4. WIPE THE SSD

WARNING

This process **will** erase all the data on the SSD, **including the PBA software**!

To securely erase the entire drive, you will have to use this process. Be sure to have your license file on hand if you wish to reinstall the PBA software. If you don't have your license file, see Troubleshooting, page 60 for instructions on how to recover your license file.

If you want to uninstall the PBA software but preserve your data, see Uninstall the PBA Software, page 41.

1. Type **sedutil-cli --scan** and press **Enter** to display the paths for each drive you have installed in the system.
2. Use the following command syntax to wipe your SSD. Please note that the following text is case sensitive:

   CipherDriveInstaller -d <SSD location> -r <SSD PSID>

   NOTE

   <SSD location> is the location of the drive you wish to wipe (ex. /dev/nvme0>). **<SSD PSID>** is the PSID number physically located on the SSD.

3. Repeat Step 2 for each protected SSD in your computer system.

You have now reset your SSD! You can now reinstall the PBA software using your bootable thumb drive. For instructions, see Install the PBA Software, page 8.

IMPORTANT
After you reinstall the PBA software, you will need to import your license file that Technical Support sent you to continue using the SSD past the trial period. To do so, see Upgrade License, page 36.

If you need assistance, please contact Technical Support (see Product Support, page 64).

5.5. REACTIVATE THE CITADEL SSD

If you have temporarily deactivated your SSD, you can reactivate it by following these instructions.

NOTE
If you wish to temporarily deactivate the PBA software on the SSD and keep its settings and user database intact, see Temporarily Deactivate the PBA, page 40. While the SSD is deactivated, you can install a new operating system or virtual machine on the system or perform complex software updates on the system that may require many reboots or require uninterrupted booting/reading from a CD or thumb drive.

Once work on the host system is completed the PBA software can be reactivated again.

5.5.1. DOWNLOAD THE ACTIVATION SOFTWARE

Download the SSD activation software from digistor.com/citadel-activation and save it to a place on your computer. The download should be located at the top of the page.

5.5.2. 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.

3. Open the ZIP file containing the PBA software you downloaded from digistor.com/citadel-activation and extract the folder inside to your computer's desktop.

4. Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

> **IMPORTANT**
> Do not copy the folder itself over to the thumb drive. Your system will 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 Product Support, page 64.

5.5.3. HOW TO BOOT INTO THE THUMB DRIVE

1. Ensure that the computer is turned off.

2. Insert the bootable USB drive you created in the steps above into the computer and turn it on.

3. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.

4. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.

5. A Linux BASH prompt will load. Press **Enter** to activate the console.

5.5.4. ACTIVATE THE SSD

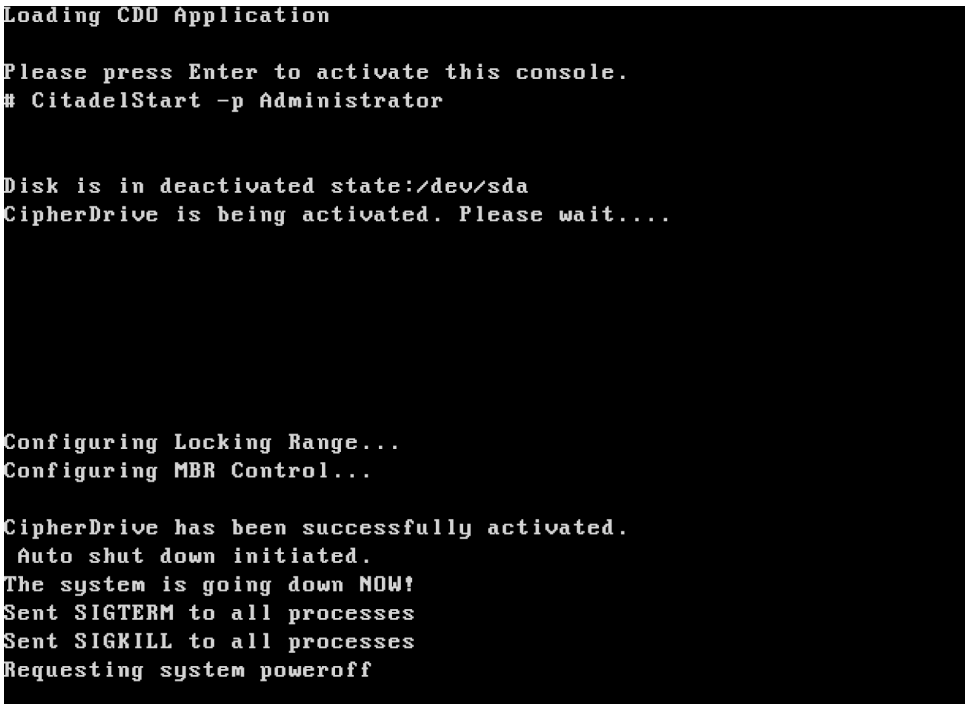
1. Boot into the thumb drive using the steps above.

2. Type in the command below to run the activation software. Please note that the following text is case sensitive.

   CitadelStart -p <password>

> **NOTE**
> **<password>** is the Administrator password. The default Administrator password is **Administrator**, and it is *case-sensitive*.

> **IMPORTANT**
> If you are using the default Administrator password, you should change it as soon as possible by logging into the SSD Management Console.



3. The software will activate the pre-boot authentication and will automatically shut down the computer when finished. Remove the USB thumb drive and reboot the system.

The SSD has been activated!

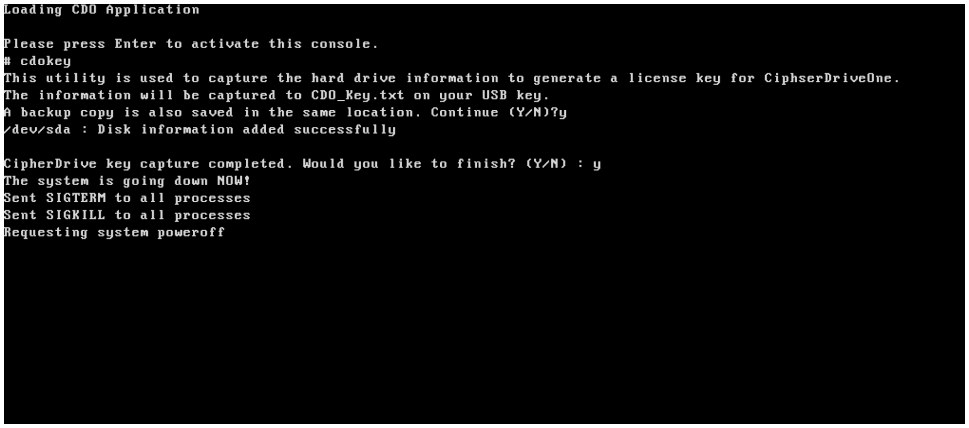
6. TROUBLESHOOTING

6.1. HOW TO RECOVER YOUR PBA SOFTWARE LICENSE FILE

If you had to wipe the SSD, your PBA software will require reinstallation. However, before you can unlock the full functionality of the PBA software you must install the license file.

To recover your license file, follow these instructions:

1. Ensure that the computer is turned off.
2. Insert a bootable USB drive into the computer and turn it on. If you don't have a bootable USB drive, see Create a Bootable USB Thumb Drive, page 62 for instructions on how to create one.
3. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.
4. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.
5. A Linux BASH prompt will load. Press **Enter** to activate the console.
6. Type **cdokey** and press **Enter**. Your system information will be collected and saved to the thumb drive as "CDO_Key.txt".
7. You will be prompted, "CipherDrive key capture completed. Would you like to finish? (Y/N)." Type **Y** and press **Enter**.



8. The computer will shut down. Wait for the machine to shut down before removing the thumb drive.
9. If you only need to collect system information for this computer, continue on to the next step.

   Otherwise, follow the above steps for each additional machine. The disk information for each computer will be appended to the "CDO_Key.txt" file every time you use the utility.
10. Save a copy of "CDO_Key.txt" in a safe place for your records.

11. Send "CDO_Key.txt" to your DIGISTOR tech support along with an explanation of why you are requesting recovery of your license file. They will return a copy of your permanent license file in 3-5 days that's keyed to your system configuration. To contact support, see Product Support, page 64.

12. Once you receive the license file back, follow one of these instruction sets depending on your situation:

    - If you have not yet reinstalled the PBA software: See Install the PBA Software, page 8
    - If you have already reinstalled the PBA software: See Upgrade License, page 36.

You may need to install the license file into your existing

6.2. HOW TO REPLACE A BAD SECONDARY SSD

If a secondary Citadel SSD on a Citadel multi-drive system (a system with more than one Citadel drive installed) has gone bad and needs to be replaced, you can follow these steps to successfully secure the new SSD seamlessly in place into the citadel multi-drive system.

1. In the PBA software's Management Console, navigate to **Maintenance > Export Configuration**. Follow the instructions there to export a 'CDExportDB' configuration file, or see Export Configuration, page 42.

2. Install the replacement SSD into the computer in the default manufactured state (deactivated and unlocked).

3. If you haven't already, create a bootable USB thumb drive with the **multi-drive version of the PBA software** on it. For instructions on how to download the PBA software and create a bootable USB thumb drive, see Create a Bootable USB Thumb Drive, page 38.

4. Copy the 'CDExportDB' configuration file you exported in Step 1 onto the root of the USB thumb drive.

5. Insert the thumb drive into the computer system. Then power on or reboot it.

6. Continually press the key for accessing your motherboard's boot menu while the computer starts up. The key to access it differs on different models, but the most common keys are **F2**, **F10**, **F12**, or **Esc**.

7. The motherboard's boot menu will appear. Choose the USB thumb drive from the list of boot options.

8. A Linux BASH prompt will load. Press **Enter** to activate the console.

9. Type in the command below to replace the bad disk with a new one. Please note that the following text is case sensitive.

CAUTION

Since you have multiple drives, you must ensure you are using the correct Linux boot path for the replacement drive (examples: /nvme1, /sdb) for your SSD. To do so, type **sedutil-cli --scan** and press **Enter**.

If you need more help, contact Technical Support (see Product Support, page 64).

CipherDriveInstaller -d <new ssd location> -p <password> -dbp CDExportDB -ps <passphrase>

> **NOTE**
> **<new ssd location>** refers to the drive path of the SSD that is replacing the bad SSD (Examples: /dev/nvme1, /dev/sda, /dev/sdb). **<password>** is the Administrator password and it is *case-sensitive*. **<passphrase>** is the passphrase you placed on your database when you exported it.

10. The computer will power off once the command has been processed. Power it back on and boot into the **Management Console**.

11. Navigate to **Disk Information** on the sidebar menu. This page should now display the replacement SSD as protected.

6.3. CREATE A BOOTABLE USB THUMB DRIVE

1. Go to digistor.com/citadel-downloads and choose the appropriate setup instructions page for your version of SSD.

2. On the setup page, download the installation package located at the top of the page and save it to a place on your computer.

3. Insert a USB thumb drive into your computer.

4. 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.

5. Open the ZIP file containing the PBA software you downloaded from digistor.com/citadel-downloads and extract the folder inside to your computer's desktop.

6. Navigate into the folder you extracted and copy the contents to the thumb drive, including any individual files as well as the “EFI” folder.

> **IMPORTANT**
> Do not copy the folder itself over to the thumb drive. Your system will 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 Product Support, page 64.

7. 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 or call us at 1-408-796-5140.