Cigent pre-boot authentication (PBA) and
Cigent Secure SSD

Cigent Single and Multidrive PBA Installation Guide and User Manual

Sep 2024
Build 30
PBA Version 1.0.6

1 Table of Contents

2 Introduction 3
3 Initial Installation 4
3.1 Initial installation overview 4
3.2 Drive installation 4
3.3 Configure UEFI and BIOS Settings 4
3.4 Operating System installation 5
3.5 Create a bootable USB 3.0 thumb drive 5
3.6 Boot to the USB thumb drive 5
3.7 Install the PBA 6
3.7.1 Primary and Secondary drive overview 6
3.8 Initial login 9
4 Using the Administrative Console 10
4.1 Dashboard 11
4.2 Maintenance 12
4.2.1 Disable PBA 12
4.2.2 Uninstall PBA 13
4.2.3 Erase Entire Disk 13
4.3 Users 15
4.3.1 Authentication options and requirements 16
4.3.2 Add User 17
4.3.3 Edit User 18
4.3.4 Remove User 18
4.4 Drives 20
4.4.1 View protected drives 20
4.4.2 Remove Secondary drive(s) 20
4.4.3 Add Secondary drive(s) 22
4.4.4 Import Secondary drive(s) 23
4.5 Settings 27
4.5.1 Settings - Login 27
4.5.2 Settings - Password 28
4.5.3 Settings - Other 29

5 Reinstallation of the Cigent PBA 30
6 Re-enabling the Cigent PBA 33
7 Updating the Cigent PBA software 34
8 Logging in and Logging Out 35
8.1 Logging in with a username and password 35
8.2 Logging in with a Smart Card 36
8.3 Logging in with a Security Key 36
8.4 Logging in with Two Factor Authentication 38
8.5 Logging out of the PBA Administrative console 39
9 Troubleshooting 40
9.1 Replacing or recovering from a drive failure 40
9.1.1 Replacing or recovering from a failed secondary drive. 40
9.1.2 Replacing or recovering from a failed primary drive. 40

Known Issues

1. The Users page does not show an indication that a user was configured with a security key.
2. Caps Lock and Num Lock do not light up when active, however they are working properly.

2 Introduction

When combined with a supported self-encrypting drive (SED) like the Cigent Secure SSD, Cigent pre-boot authentication (PBA) creates a highly secure data at rest (DAR) solution protecting data against unauthorized access.

Before starting any operating system or virtual machine stored on the drive users must first authenticate using a username/password, smart card or security key. Users remain authenticated until the drive is powered off.

The following guide helps you install the Cigent Secure SSD(s) and Cigent PBA software. It also details how to configure users and options in the PBA administrative console.

3 Initial Installation

3.1 Initial installation overview

You can obtain a copy of the PBA software from:

- https://support.cigent.com After registering, the download will be available under the Cigent PBA section.
- If you have a Data Defense subscription, you can download the Cigent PBA from the downloads page of the Cigent Management console.

3.2 Drive installation

Install the Cigent Secure SSD(s) into your system following your computer manufacturer's instructions.

3.3 Configure UEFI and BIOS Settings

Prior to installation of the PBA software, it is important to ensure certain bios settings are configured properly. Incorrect configuration may prevent installation altogether or disable certain features within the PBA afterwards.

Not every setting is supported by every manufacturer. If the setting is not supported by your BIOS, it can be ignored.

SATA/NVMe Operation – AHCI (REQUIRED)
SATA/NVMe Operation sets the operating mode of the integrated storage device controller with a choice between AHCI (Advanced Host Controller Interface) and RAID (Redundant Array of Independent Disks.) It is usually found under the Storage section of the BIOS. This must be set to AHCI for the PBA software to recognize the SED.

Block SID Authentication - OFF (REQUIRED)
TCG storage devices (like self-encrypting drives) will block all attempts to authenticate the SID authority. This is a security mechanism that prevents malicious software from placing a password on the drive preventing access. Once PBA is installed, this protection is no longer required as the software will set the password appropriately as part of installation. Note that setting this off is not always permanent therefore install the PBA on the next restart otherwise it may set back to on automatically.

Secure Boot – ON (RECOMMENDED)

Prevents unauthorized operating systems from running at boot time. Setting Secure Boot to ON is a best practice and although it is not required for installation of the PBA, it is required if you plan to use the TPM authentication option.

3.4 Operating System installation

Install any operating system or virtual machines.

3.5 Create a bootable USB 3.0 thumb drive

To install the Cigent PBA you will need to create a bootable USB thumb drive containing the Cigent PBA software. Cigent provides a utility to help you create a bootable usb thumb drive containing the Cigent PBA software. Warning: All data on the USB thumb drive will be erased.

NOTE: You can use the same usb thumb drive to install multiple drives which means you only have to create the usb drive once.

1. Extract the file from the provided zip and ensure all files remain in the same directory.
2. Insert a USB 3.0 thumb drive into your computer.
3. Start an Administrator command window and change directory to the location of loader software.
4. Run PBALoader_Multi.exe -i
5. Choose the number next to the correct USB thumb drive (if more than 1)
6. Select 1 for Load operation.
7. You should see 2 entries. Type the number next to pba.bin and press enter.
   Note: The pba_custom.bin is a Cigent Self-Signed version requiring keys (provided) be imported into the bios secure boot menu prior to running installer. Contact support for additional information.
8. Confirm your selection by typing ‘YES’ then enter.

The process can take several minutes to complete. Once successful you may remove the USB thumb drive and proceed to the next step.

3.6 Boot to the USB thumb drive

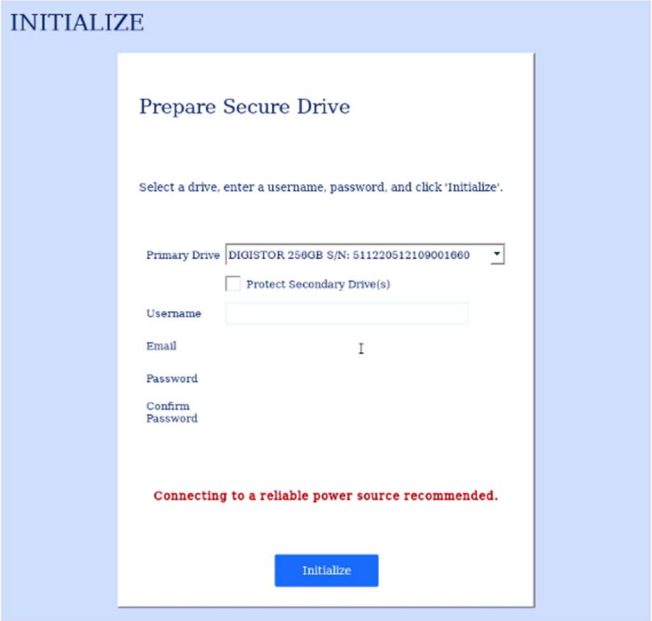
1. Ensure the power is turned off.
2. Insert the bootable USB thumb drive into the computer with the Cigent Secure SSD.
3. Turn on the computer and press the appropriate key for your computer to display the boot menu. The typical keys are F1, F2, F10, F12 or Esc.
4. Choose the USB thumb drive from the menu and proceed to boot.

3.7 Install the PBA

3.7.1 Primary and Secondary drive overview

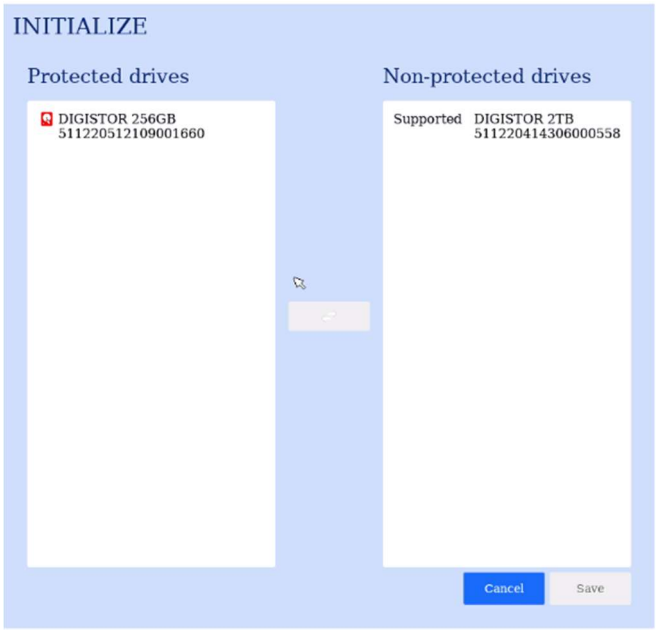
The PBA can protect multiple drives with a single installation. In a system with more than one protected drive, one drive will be designated primary, and the others will be secondary. The PBA installs and boots from the primary drive. Secondary drives can be added, removed and imported from other installations. During installation, the admin must designate a primary drive. The impact of being primary affects the process of replacement or recovery from a drive failure. Regardless of whether a primary or secondary drive fails, the system can be recovered.

1. The Secure Setup screen will be displayed.

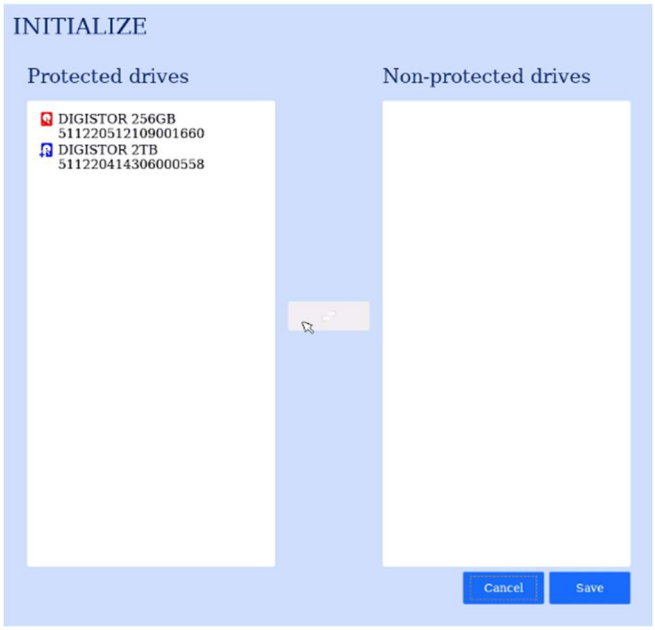


2. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will boot.

3. On a system with more than one drive:
    a. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will boot.
    b. Check “Protect Secondary Drives” to open the Add Secondary Drives dialog.

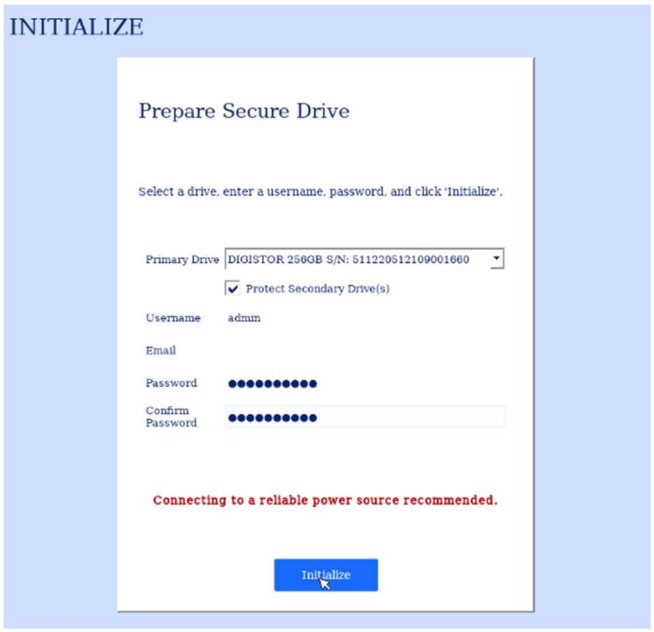


c. Select drives from the Non-protected drives list and click the double arrow button to move them to Protected drives.

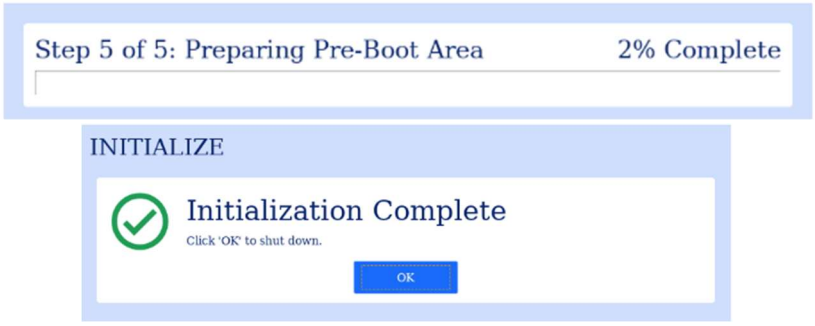


d. Select the secondary drives to protect and click Save.

4. Enter a username, email (optional) and password. (See Username and Password Requirements in Add User section for details.)
5. Then click Initialize.



The installation process can take 10 minutes or more. Do not interrupt or power off the computer during this time.



Once complete, power off the computer.

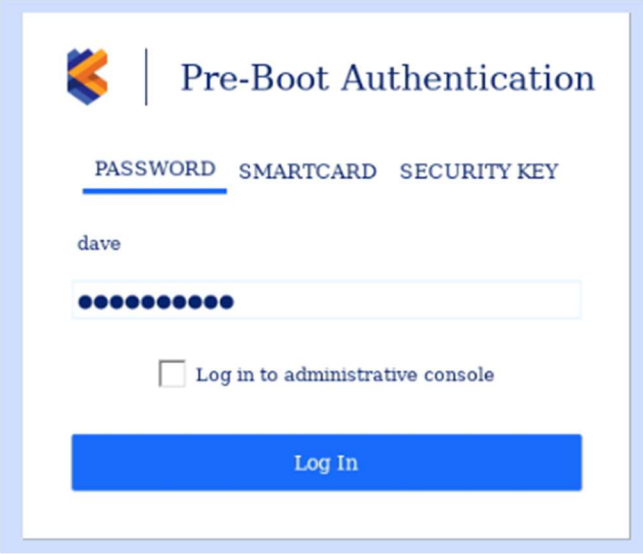
Your PBA is now installed and ready for use.

Remove the USB thumb drive and power up the system.

3.8 Initial login

The user credentials used to install the PBA software have administrative role by default. You should login at least once before entering the administrative console to test if the system successfully starts the operating system.

1. Turn on the computer. The Cigent PBA will automatically load.
2. On the login screen, enter the credentials you used during the PBA installation process.
3. Click Log In.

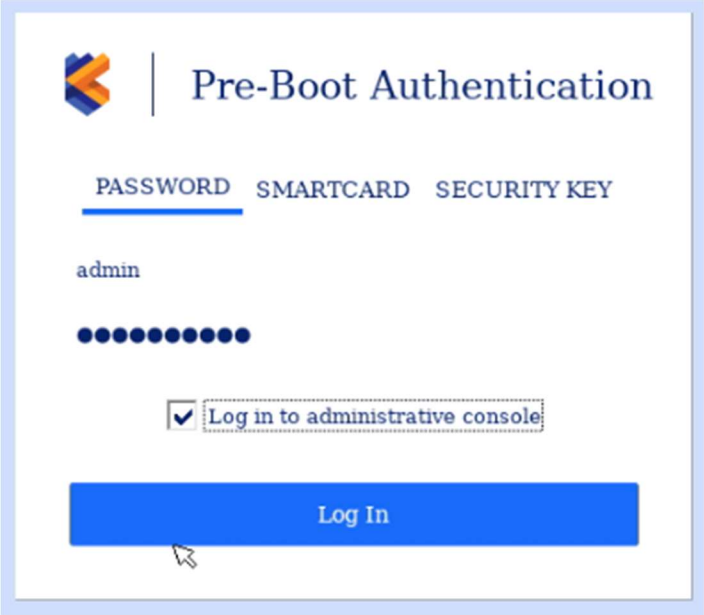


For details on how to log in to the administrative console, see section Using the Administrative Console.

4 Using the Administrative Console

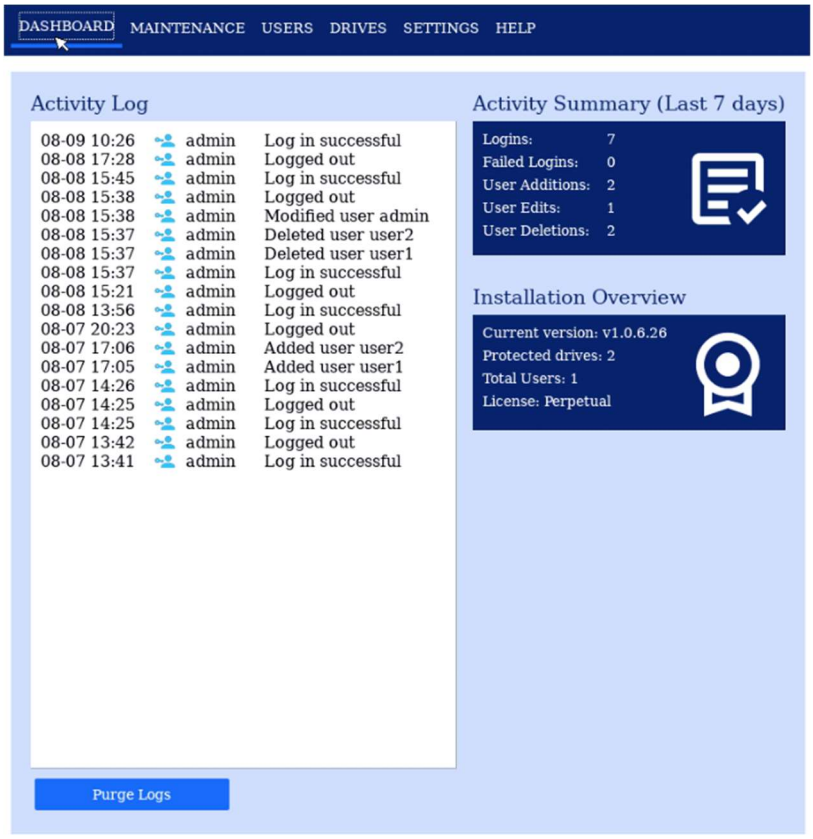
The administrative console allows administrators to manage users, perform maintenance tasks, and view activity logs pertaining to the PBA environment.

You can enter the administrative console from the login page by checking the “Log in to administrative console” checkbox before clicking Log In.



4.1 Dashboard

The administrative console allows you to manage users, perform maintenance tasks and view activity logs pertaining to the PBA environment.



The dashboard shows PBA related activity in time order with the most recent activity at the top. Administrators can see all activity while normal users can only see activity for which they are the subject of the activity. Administrators can also purge the logs as desired.

The following activities are recorded:

- ✓ Successful login
- ✓ Failed Login
- ✓ Logoff successful
- ✓ Added user
- ✓ Edited user
- ✓ User deleted
- ✓ Authentication Keys Change

The Summary widget provides version and user login information as well as a summary of user activity for the last 7 days.

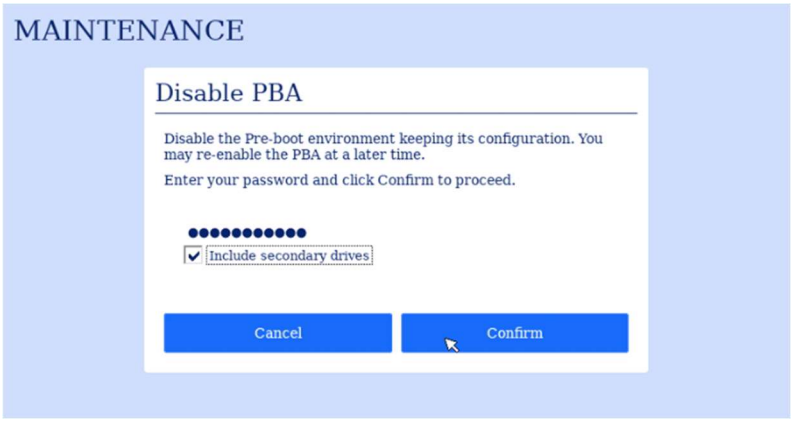
4.2 Maintenance

The maintenance page allows administrators to uninstall the PBA environment, disable the PBA, and completely erase the drive.

4.2.1 Disable PBA

Disabling the PBA temporarily allows the system to boot directly to the operating system without the need to authenticate. This can be useful for administrators during update operations that require repeated restarts of the system. All settings and configuration will be preserved while disabled. Re-enabling the PBA will require authentication as an existing administrative user. See Re-enable PBA for details.

Multidrive systems: Enable *Include secondary drives* option(recommended) to temporarily remove protection from non-primary drives in addition to the primary.

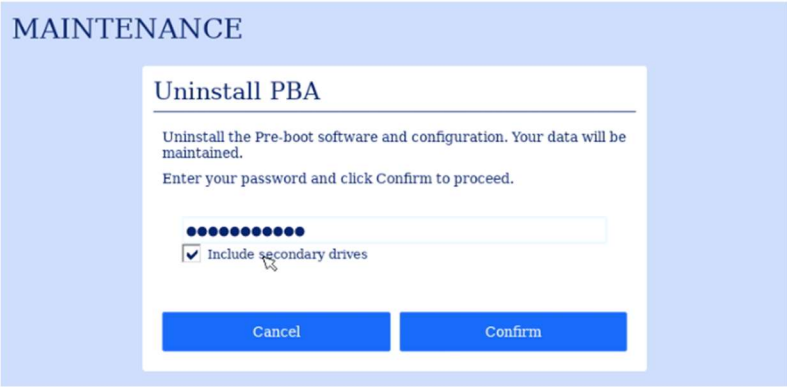


1. Click *Disable PBA*.
2. Enter your administrator password.
3. Click *Confirm*.

4.2.2 Uninstall PBA

You can completely uninstall the Cigent PBA software which removes all files, configuration and user information. Your operating system environment will be preserved and boot normally.

Multidrive systems: Enable *Include secondary drives* option(recommended) to remove protection from non-primary drives in addition to the primary.



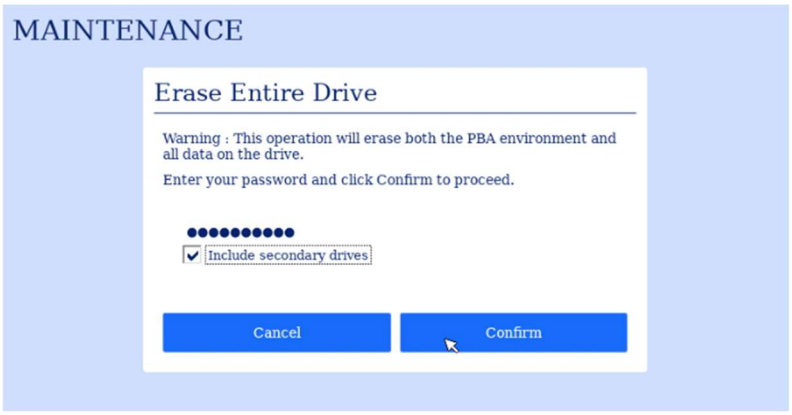
1. Click *Uninstall PBA*.
2. Enter your administrator password.
3. Click *Confirm*.

WARNING: The uninstallation of the PBA proceeds immediately after clicking *Confirm*.

4.2.3 Erase Entire Disk

The Erase Entire Drive feature allows administrators to reset the drive(s) back to factory state and ensures all data on the disk is completely erased and unrecoverable. Once complete, the drive can be safely repurposed.

Multidrive systems: Enable *Include secondary drives* option(recommended) to erase non-primary drives in addition to the primary.



The following actions are performed during the Erase Entire Disk procedure:

- The Data Encryption Key (DEK) of the SED is changed. This is also known as Crypto-Erase.
- The PBA executes a Format NVM with the sanitize option. The Cigent Secure SSD has an enhanced feature called Full Flash Overwrite which will zero every block on the drive.
- The Erase Verification firmware feature is used to ensure all mapped and unmapped blocks have been erased.

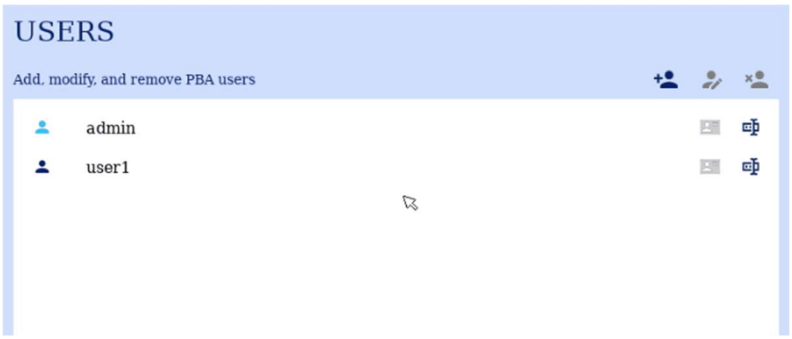
1. Click *Erase Entire Disk*.
2. Enter your administrator password.
3. Click *Confirm*.

WARNING: The **Erase Entire Drive** proceeds immediately after clicking Confirm and cannot be stopped or canceled.

Once complete, power off the system.

4.3 Users

The Users page allows administrators to add, modify, and delete user accounts from the PBA environment. Non-administrative users can use this page to change their password and modify other forms of authentication.



Roles and Capabilities

Capability	Administrator Role	User Role
Purge Logs	Yes	No
Uninstall PBA	Yes	No
Change Authentication Keys	Yes	No
Erase Entire Drive	Yes	No
Add User	Yes	No
Edit User	Yes	Only their own
Remove User	Yes	No
Modify Settings	Yes	No

4.3.1 Authentication options and requirements

Each PBA user can be configured with three different authentication options including password, smartcard and security key. Password is always required. Smartcard and security key authentication are optional. As of this release, only Smartcard can be used for a two-factor authentication setup (requiring both a password and smartcard to succeed.) Security key will be added as an option in an upcoming release.

Password Requirements

Requirement	Username	Password
Length	1-40	8-128
Uppercase letter: A-Z	May contain	Must contain at least 1
Lowercase letter: a-z	May contain	Must contain at least 1
Number: 0-9	May contain	Must contain at least 1
Special character: ~! @#$^&*()_-+=[]:<>.	May contain	Must contain at least 1

Smartcard

Any smartcard or device supporting NIST SP 800-73-4 – *Interfaces for Personal Identity Verification* are supported. This includes Common Access Cards (CACs) and multiprotocol security keys that support the PIV interface (for example Swissbit iShield and Yubikey 5 series.) Authentication requires the presence of the device as well as an 8 number PIN. The PIN is setup separately from the PBA.

To add a smartcard to a user, ensure the smart card is inserted and click *Scan*. The dropdown will show supported certificates on the card. Enter the already configured PIN before saving the changes.

Security Key

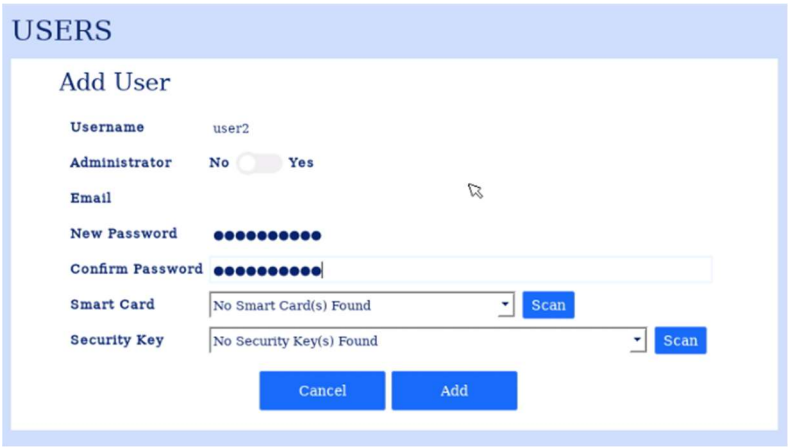
Any device supporting the FIDO2 U2F protocol are supported (for example Swissbit iShield and Yubikey 5 series.) There are three options for authentication using a security key – Auto, Touch and PIN. The Auto option simply requires that the key is inserted at the time of boot, no user interaction is required. Touch requires the security key to be inserted and will prompt the user to touch the key before proceeding. PIN requires the security key to be inserted and will

prompt the user for a previously chosen PIN. The PIN is configured when adding a security key to a user.

To add a security key to a user first insert the security then click Scan. Ensure the correct security key is selected and choose the type of authentication. For PIN, enter and confirm a 6-to-63-digit number.

4.3.2 Add User

The Add User page is used to add a new user using password, smartcard or security key. If the "Require Two-Factor Authentication" setting is set to Yes, all newly added users must have both password and smartcard.



1. Enter a unique username.
2. Set the Administrator role as desired.
3. Enter an email address. (Optional)
4. Enter and confirm a password.
5. (Optional) Select the smart card certificate from the menu and enter the PIN.
6. (Optional) Select the Security key. Choose Auto, Touch or PIN.
7. Click *Add*.

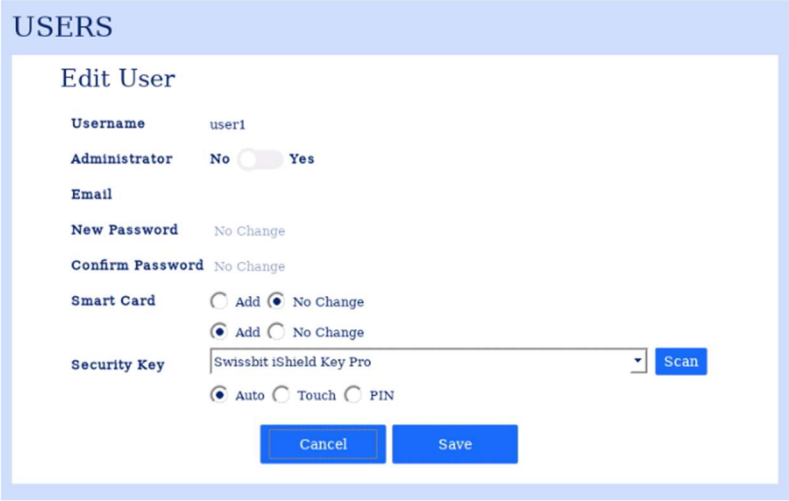
Click the Scan button next to Smartcard or Security Key if your device is not listed after inserting the card or key.

4.3.3 Edit User

The Edit User page is used by administrators to make changes to any user in the system including themselves. It is also used by non-administrators to change their own password.

Administrators can change the following user attributes:

- Role
- Email Address
- User Password
- Add or Remove a Smart Card
- Add or Remove a Security Key



1. Select an existing user from the table and click the edit user icon.
2. Change one or more user attributes.
3. Click Save.

Note that to Add a Smart Card or Security Key to an existing user, the device should be inserted before entering the page. If you do not see the device listed after inserting it, click Scan.

4.3.4 Remove User

Removing a user will permanently delete a user from the PBA environment. Users will no longer be able to authenticate to the PBA to access the protected operating system nor the PBA administrative console.

1. Select an existing user or users from the table and click the remove user icon.

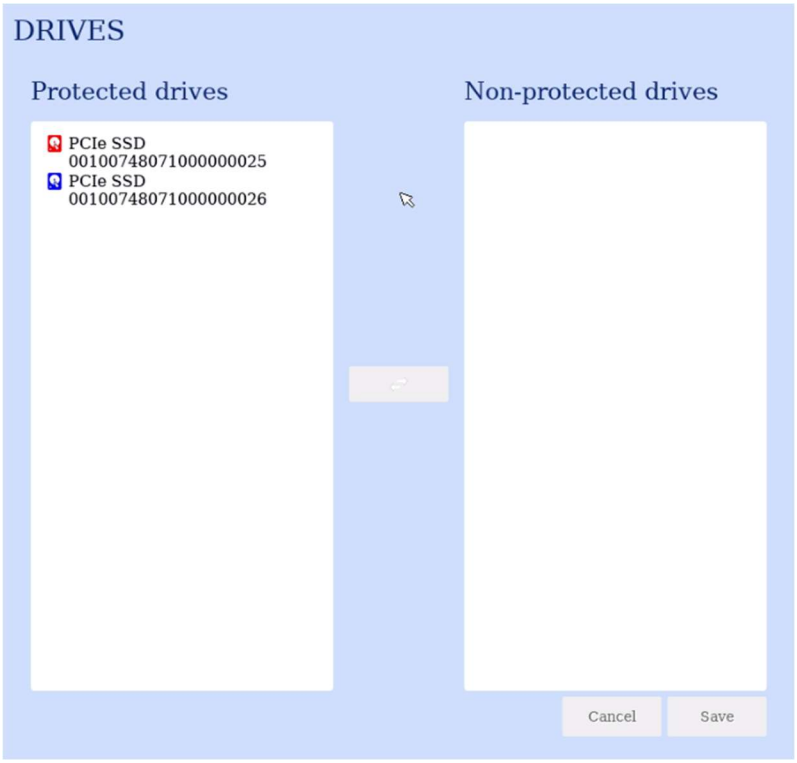
2. Click Remove.

4.4 Drives

The Drives page shows information about the drive(s) being protected by the PBA. On systems with more than one drive this page allows administrators to add, remove and import drives from the environment. The standard license allows up to 5 drives in a non-hardware RAID configuration.

4.4.1 View protected drives

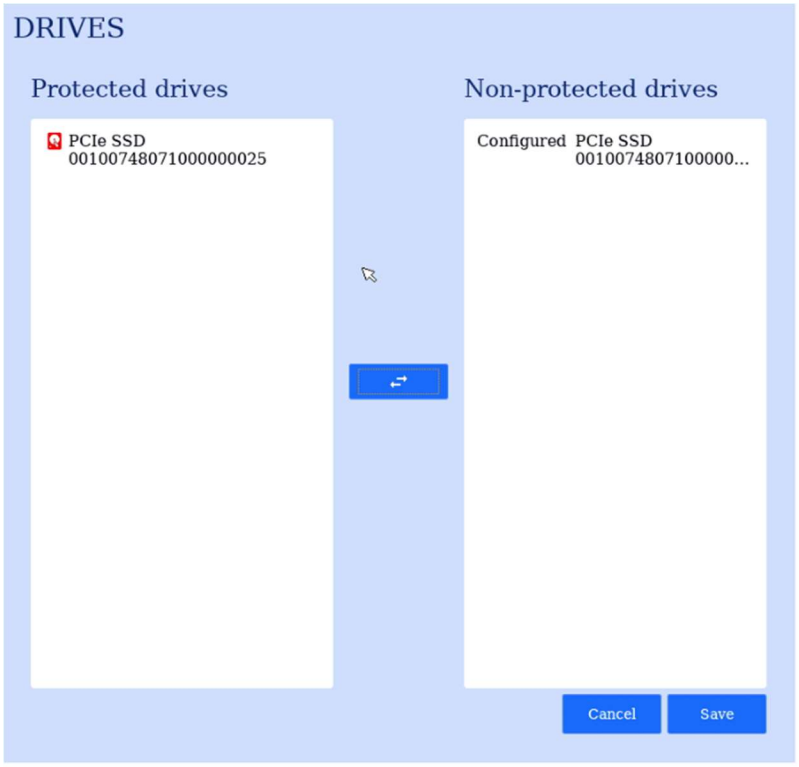
The *Protected drives* column shows details of the drives under the protection of PBA including model number and serial number. The primary drive is indicated with a red icon and all secondaries, if present, are blue. The *Non-protected drives* column shows drives recently removed from protection or available to import. Selecting one or more drives and clicking the double arrow button will move drives between columns. When updates are complete, click the *Save* button.



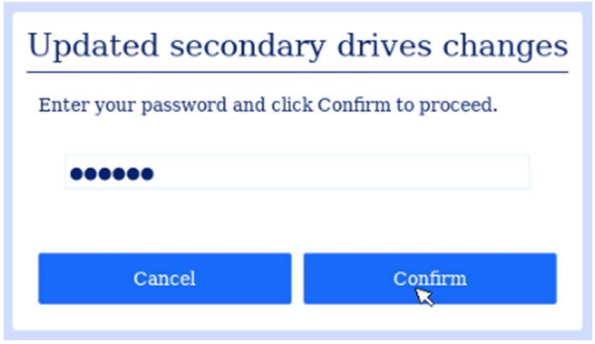
4.4.2 Remove Secondary drive(s)

To remove protection from a secondary drive(s) perform the following.

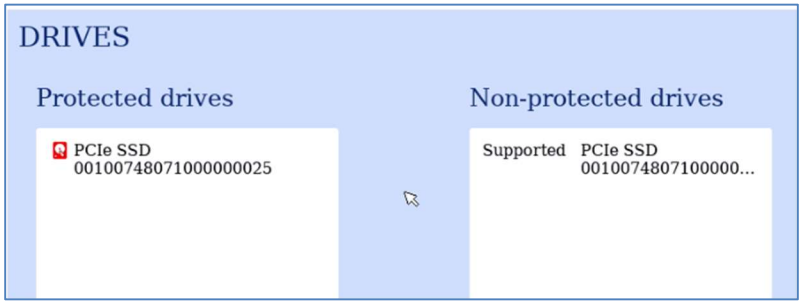
1. Select one or more secondary drives from the *Protected drives* column.
2. Click the double arrow button.



3. Click Save
4. Enter your password and click Confirm.



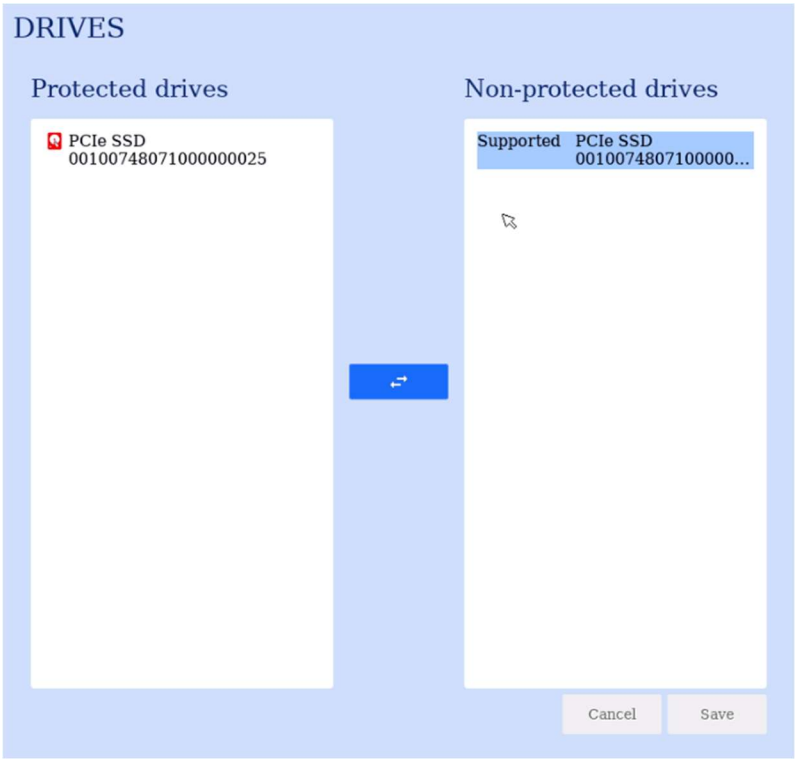
The drive will now show as Supported indicating it is no longer protected but could be added to the protected drives list.



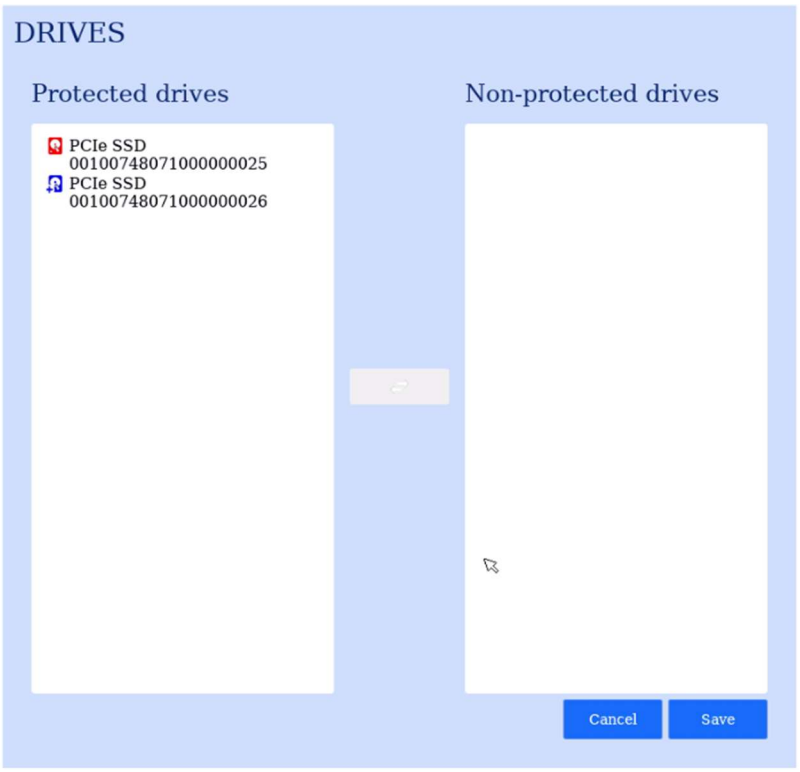
4.4.3 Add Secondary drive(s)

If an additional drive was added to the system or you wish to add a previously removed drive back under protection, perform the following.

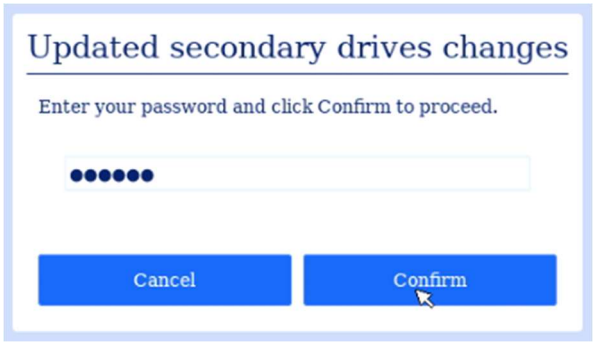
1. Select one or more drives shown as Supported from the Non-Protected column.



2. Click the double arrow button to move the drive(s) to the *Protected drives* column.



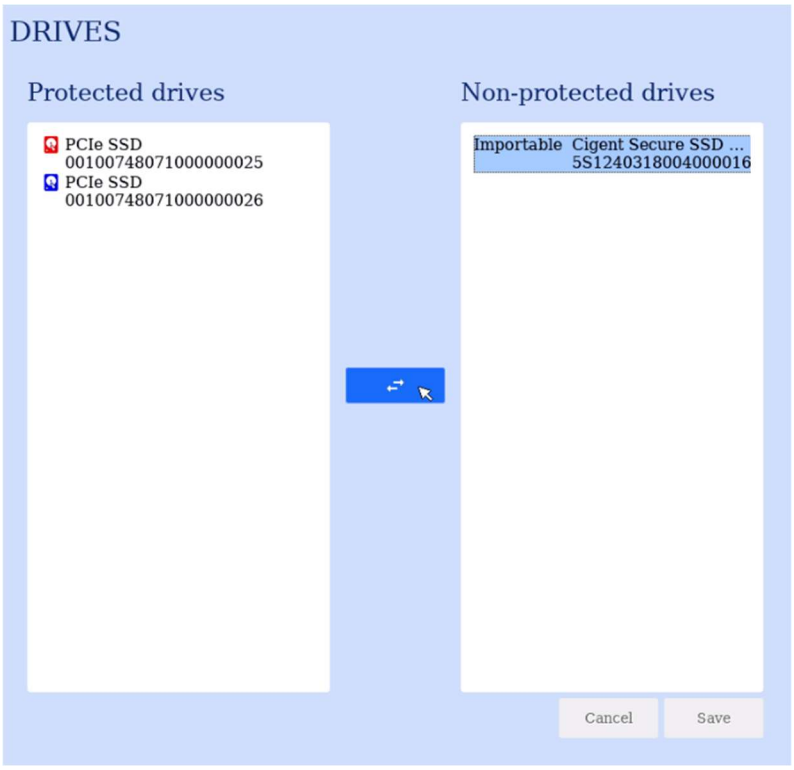
3. Click Save.
4. Enter your password and click Confirm.



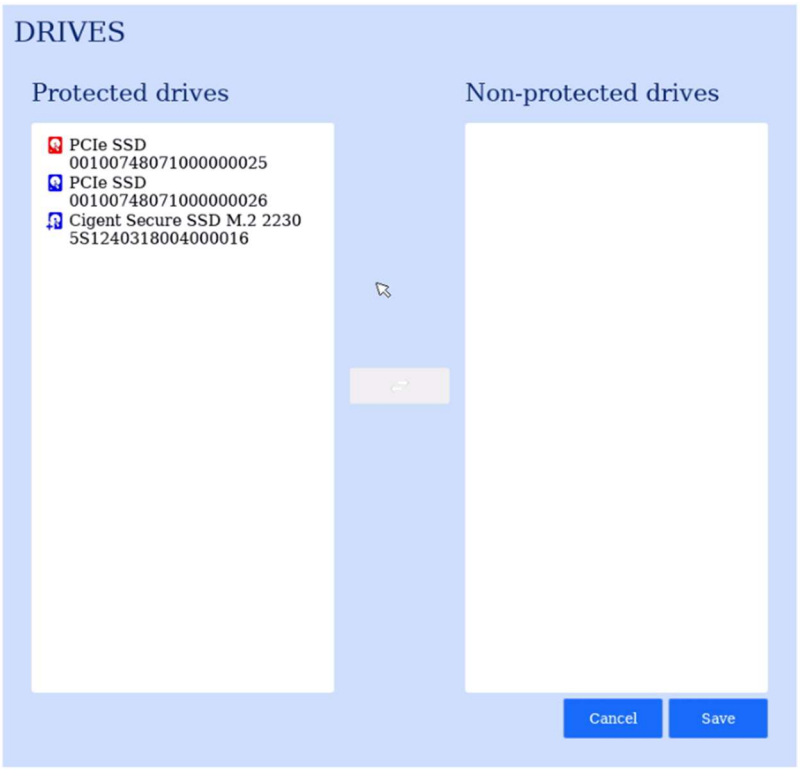
4.4.4 Import Secondary drive(s)

You can import secondary drives that were protected in another system. You would also use the import capability if the primary drive was removed or had failed and needed to be replaced. (See Troubleshooting section at the end of this document.)

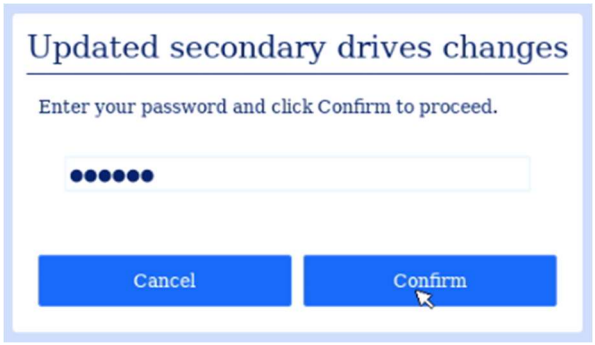
1. Select one or more drives labeled Importable from the Non-protected drive list.



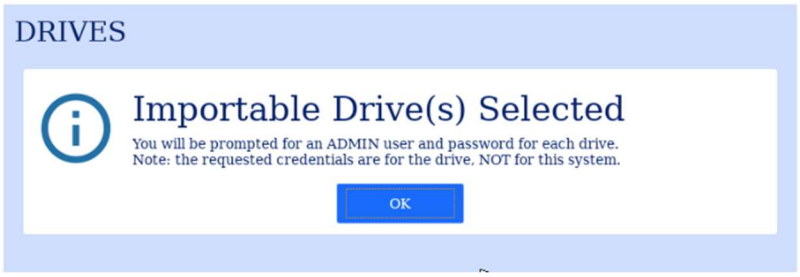
2. Click the double arrow button to move the drive to the Protected drives column.



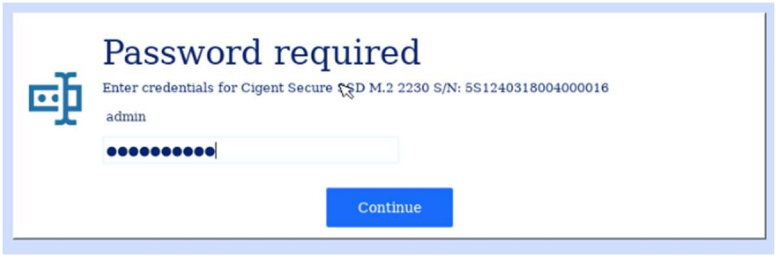
3. Click Save.
4. Enter your password and click Confirm.



5. Click Ok.

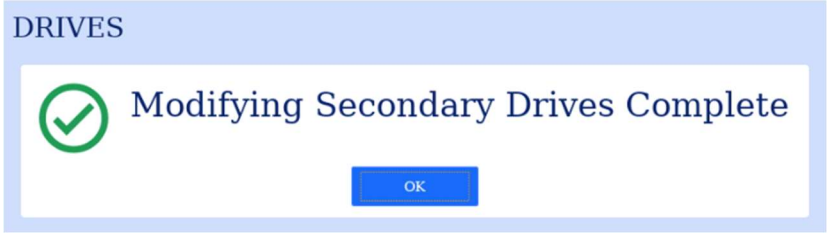


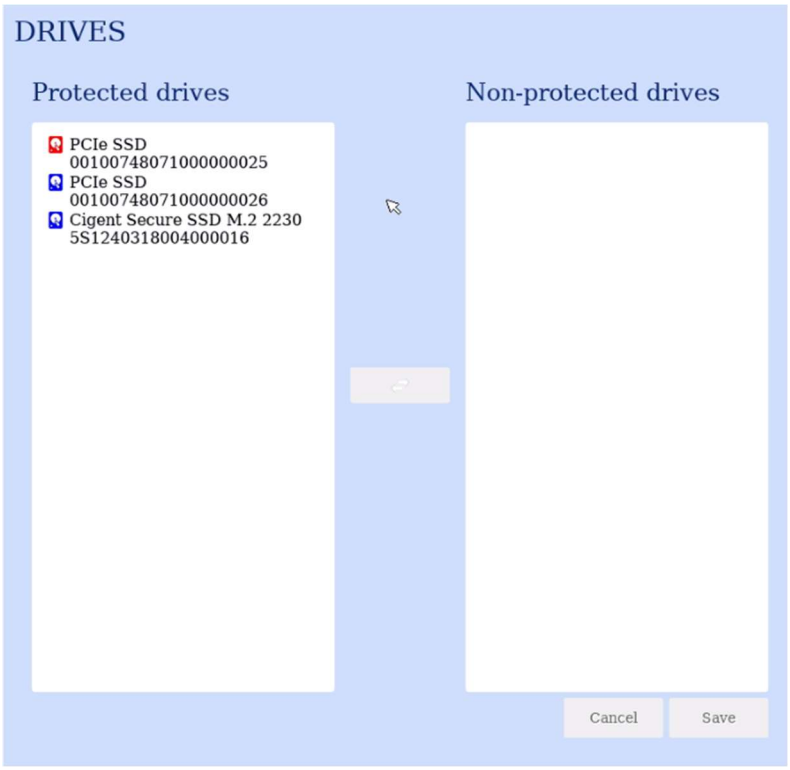
6. Enter administrator credentials from the source PBA then click Continue. (NOTE: These are the credentials from the PBA installation where this drive was originally configured, not the credentials for the running PBA.)



7. Click Continue. Repeat for each drive selected.

8. Click Ok.

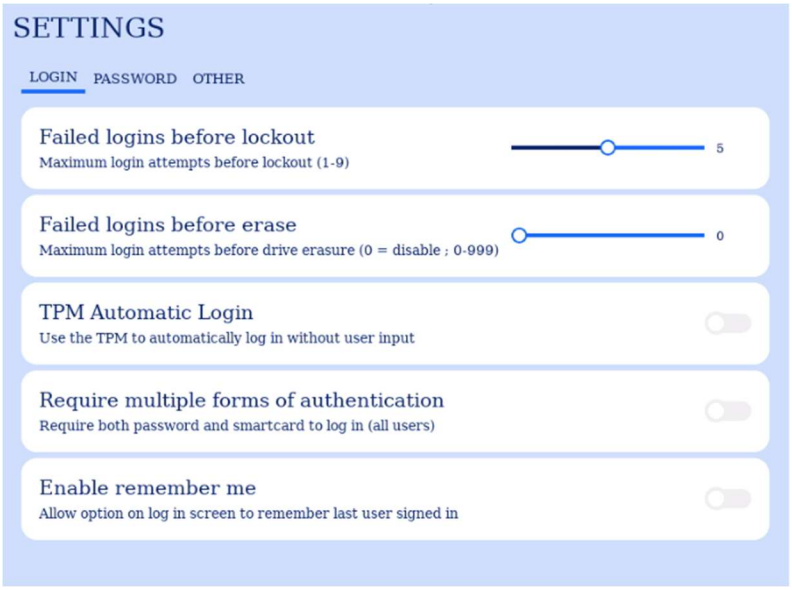



DRIVES
Protected drives
Non-protected drives
PCIe SSD
00100748071000000025
PCIe SSD
00100748071000000026
Cigent Secure SSD M.2 2230
5S1240318004000016
Cancel
Save

4.5 Settings

The Settings page allows administrators to customize certain behavior of the application to match their security requirements. After changing settings, be sure to click Save to update the system.

4.5.1 Settings - Login



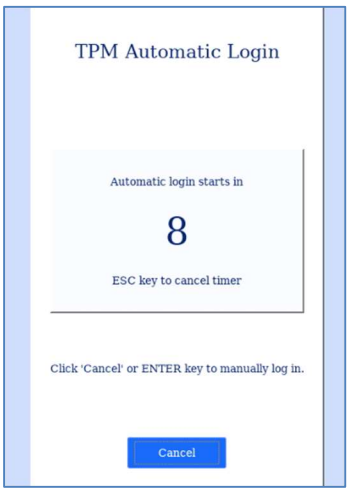
Failed logins before lockout
The number of consecutive failed login attempts (across all users) before a restart is required. Only attempts with valid usernames are considered towards failures.
Min: 1 *Max*: 10

Failed logins before erase
The number of consecutive failed login attempts before the disk is automatically erased. Only attempts with valid usernames are considered towards failures.
Min: 0 (Disabled) *Max*: 999

TPM automatic authentication
Automatically authenticate to the PBA using the TPM (Trusted Platform Module.) When enabled, the login screen will pause for 10 seconds before attempting to unlock the drives using TPM authentication. Users can interrupt the automatic log in and enter their own credentials. This feature is useful for systems that are located where users are not always present and may experience temporary power loss. Only the TPM present when the feature is enabled will be

able to automatically log in. If the drive is placed in another computer, a user must enter credentials.

Note: This feature requires that Secure Boot be enabled in the BIOS before it can be enabled.

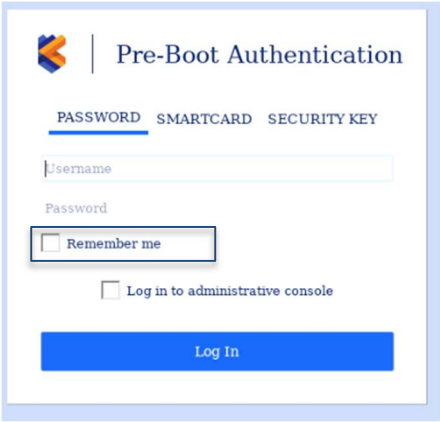


Require multiple forms of authentication

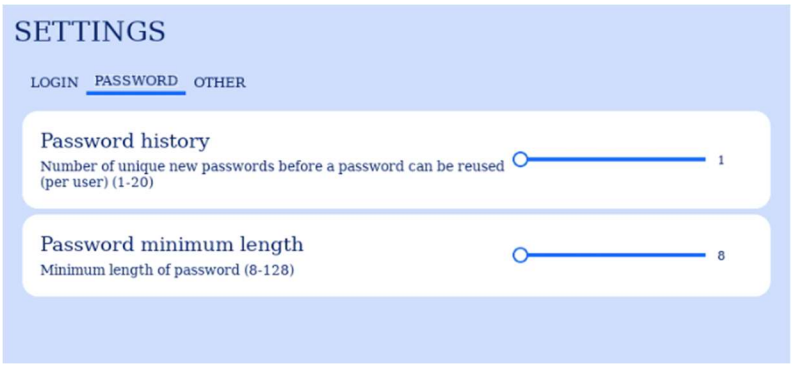
Require both password and smartcard authentication to log in. This can only be enabled if all currently defined users have both a password and smart card configured. If some users do not, you must require that they configure a smartcard or delete the user first.

Enable remember me

Enabling this setting will display an additional option on the PBA Login screen to automatically fill in the username field with the last successful login's username. This is a time saving feature on systems where the same user logs in on a regular basis.



4.5.2 Settings - Password

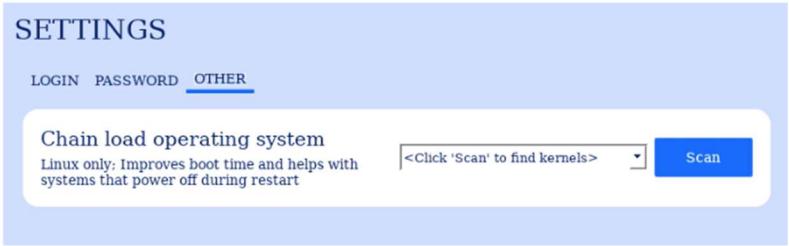


Password history
The number of unique passwords per user before a password can be reused.
Min: 1 *Max*: 20

Password minimum length
The minimum password length required for each user. The requirement will be enforced the next time an existing user changes their password or a new user is added.
Min: 1 *Max*: 128

4.5.3 Settings - Other

Chain load operating system
Chain loading is when a boot loader loads another boot loader to begin the boot process. This process greatly reduces the time needed to start the target operating system. Currently, Cigent PBA supports chain loading to Linux only. Click Scan to initiate a search for available kernels on the boot drive. Once complete, select the desired kernel from the list and click Save.



5 Reinstallation of the Cigent PBA

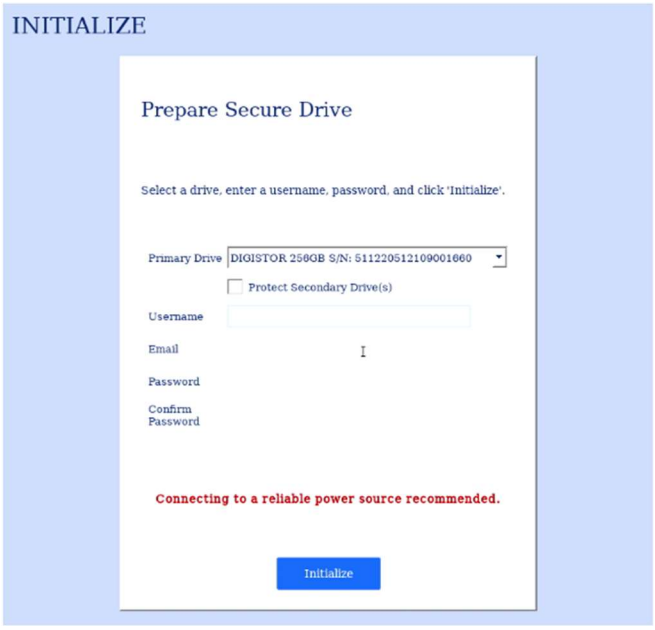
Reinstallation of the Cigent PBA software will be necessary if you used the **Erase Entire Drive** or **Uninstall PBA** features from the maintenance page or erased the drive using another utility.

The reinstallation process is the same as the process you followed to initially install the Cigent PBA.

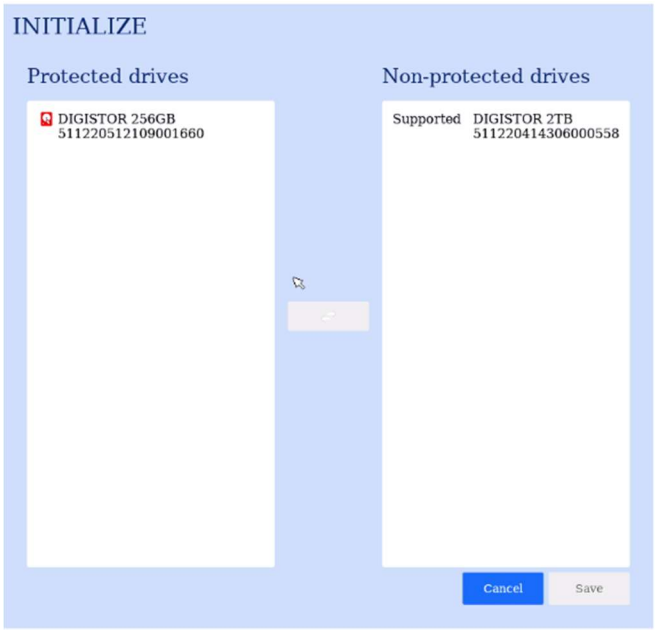
1. Create a bootable USB thumb drive containing the Cigent PBA software. (See section Create a bootable USB 3.0 thumb drive **)**

> **Note:** You can use the same bootable USB drive you used to enable the Cigent PBA if you still have it.

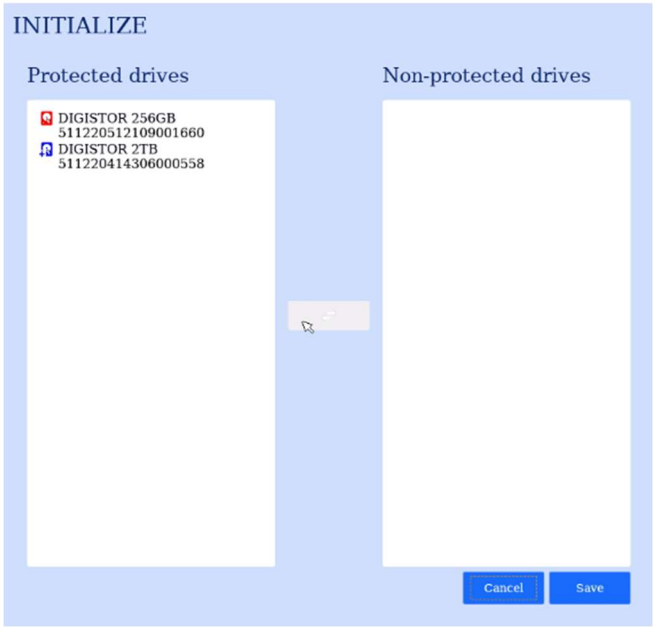
2. Boot from the USB thumb drive.
3. The Prepare Secure Drive screen will be displayed.



4. On a system with more than one drive:
    a. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will boot.
    b. Check “Protect Secondary Drives” to open the Add Secondary Drives dialog.

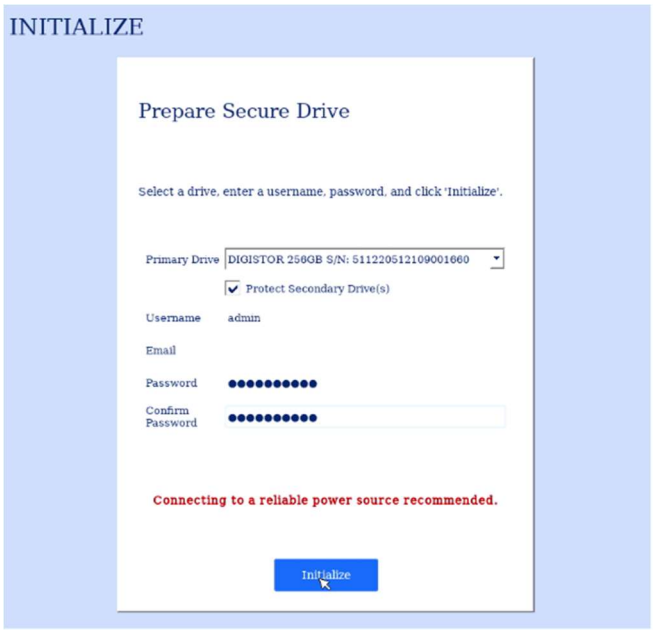


c. Select some or all of the drives from the Non-protected drives list and click the double arrow button to move them to Protected drives.

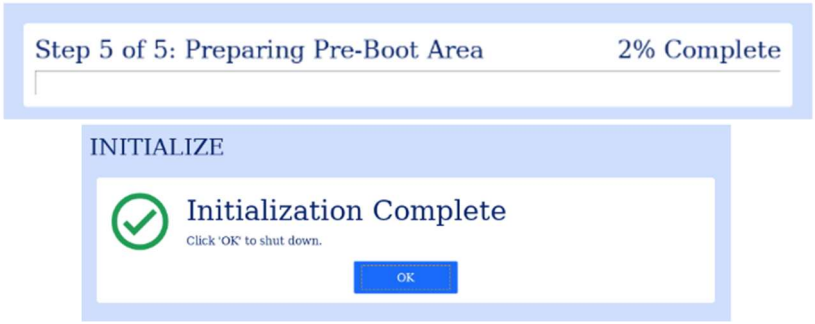


d. Select the secondary drives to protect and click Save.

5. Enter a username, email (optional) and password. (See Username and Password Requirements in Add User section for details.)
6. Then click Initialize.



The installation process can take 10 minutes or more. Do not interrupt or power off the computer during this time.



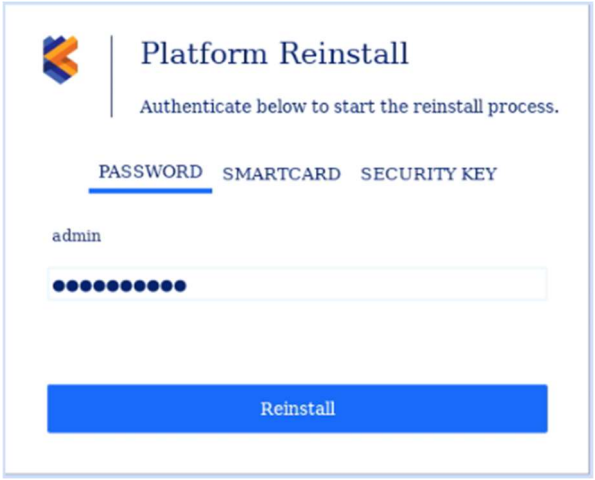
Once complete, power off the computer.
Remove the USB thumb drive from the computer.

6 Re-enabling the Cigent PBA

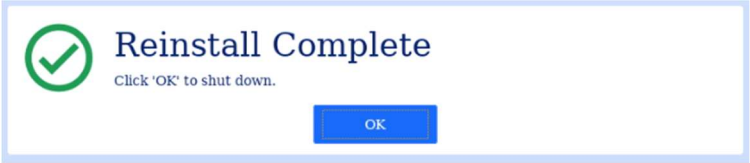
To re-enable PBA after temporarily disabling it from the maintenance page you will need the following:

1. An installation USB drive of the same version of Cigent PBA installed on the device
   (See section Create a bootable USB 3.0 thumb drive)
2. Administrator credentials to the disabled PBA environment

When you are ready to re-enable the PBA boot to the USB drive. The system will detect that a PBA environment is already installed and present a reinstallation login screen.



Enter valid administrator credential and click Reinstall. It should only take a few seconds to enable the PBA. Click OK to shut down.



The PBA environment should once more present the normal login screen.

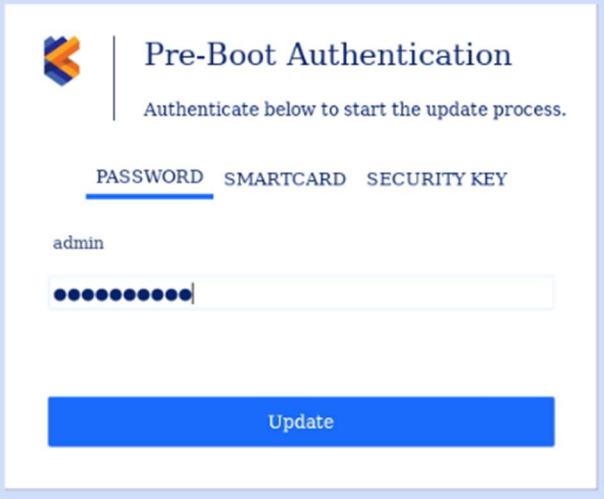
7 Updating the Cigent PBA software

For information on obtaining the newest version of the Cigent PBA software see section Initial installation overview.

To update the Cigent PBA software to a newer version you will need the following:

1. An installation USB drive of the newer version of Cigent PBA installed on the device (See section Create a bootable USB 3.0 thumb drive)
2. Administrator credentials to the PBA environment

When you are ready to update the Cigent PBA software, boot to the USB drive containing the newer version of the software. The system will detect that a PBA environment is already installed and present an upgrade login screen.



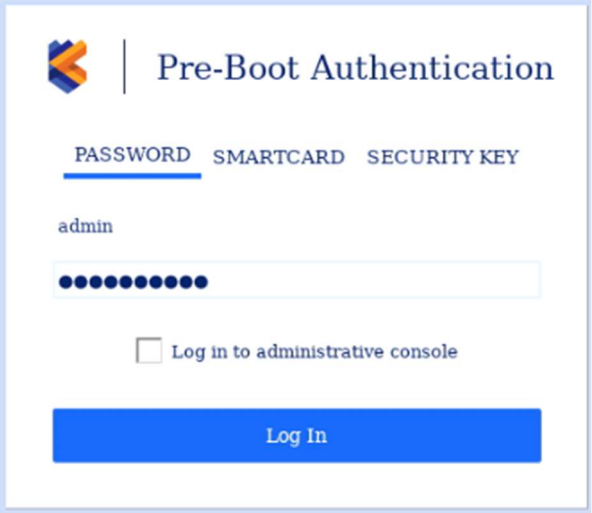
Enter valid administrator credentials and click Update. The process will take about 10 minutes to complete. Once complete shutdown the system and remove the USB drive.

The PBA environment should once more present the normal login screen.

8 Logging in and Logging Out

8.1 Logging in with a username and password

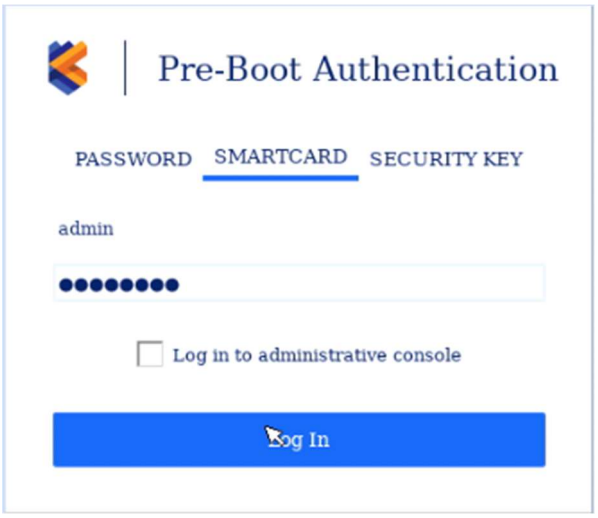
1. Power on the computer and wait for the PBA authentication screen to appear.
2. Enter your username and password.
3. Click Log in.



If the authentication is successful, your system will reboot and automatically start your operating system.

8.2 Logging in with a Smart Card

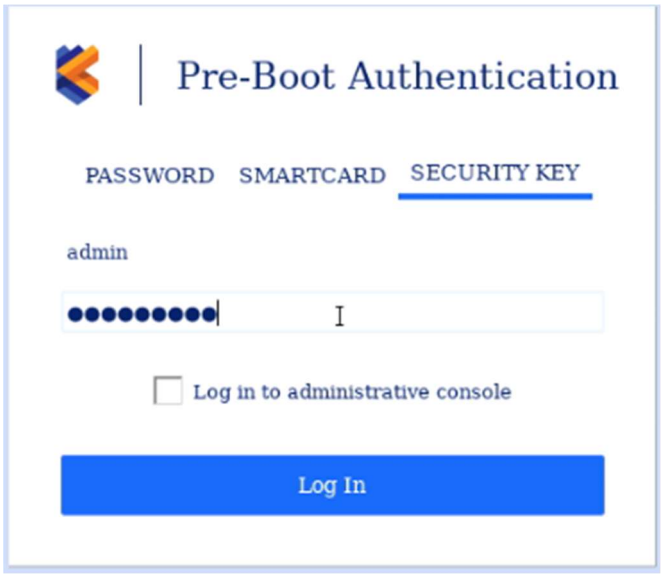
1. Power on the computer and wait for the PBA authentication screen to appear.
2. Click Smart Card.
3. Enter your Username and PIN.
4. Click Log In.



If the authentication is successful, your system will reboot and automatically start your operating system.

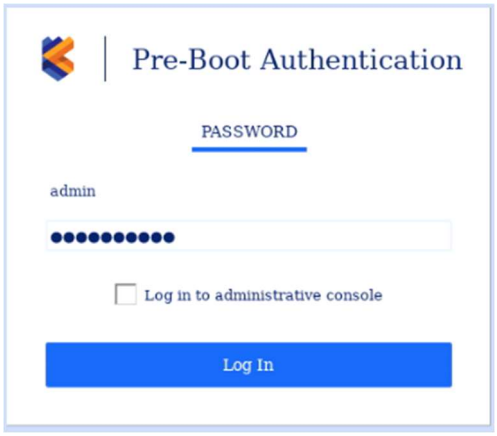
8.3 Logging in with a Security Key

1. Power on the computer and wait for the PBA authentication screen to appear.
2. Click Security Key.
3. Enter your Username.
4. Enter a PIN if the security key was configured with a PIN.
5. Click Log In.

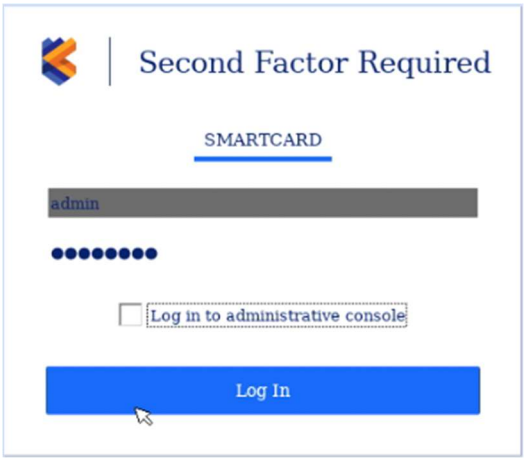

Pre-Boot Authentication
PASSWORD
SMARTCARD
SECURITY KEY
admin
Log in to administrative console
Log In

8.4 Logging in with Two Factor Authentication

When the “Require Two-Factor Authentication” setting is enabled, all users must authenticate with a password and smartcard. The Login page will first ask for the password then the smartcard PIN. If both factors are verified, the login will be successful.



1. Power on the computer and wait for the PBA authentication screen to appear.
2. Enter the username and password.
3. Click Log In.



4. Insert your smartcard.
5. Enter the PIN.
6. Click Log In.

If the authentication is successful, your system will reboot and automatically start your operating system.

8.5 Logging out of the PBA Administrative console

When you have finished using the administrative console you must Power Off using the button at the bottom left corner of the screen. There is no explicit log off capability. If you wish to enter the operating system, you power off, then power on.

9 Troubleshooting

9.1 Replacing or recovering from a drive failure

In a system where the PBA is protecting more than one drive, the recovery procedure will depend on whether the drive to be replaced was primary or secondary. A failure of the primary drive will result in a system that is unable to boot to the PBA. A system with a failed secondary drive will still boot to the PBA. Follow the appropriate procedure below depending on whether the primary or secondary is being replaced or has failed.

9.1.1 Replacing or recovering from a failed secondary drive.

1. Shutdown the system.
2. Install the replacement SSD.
3. Power on the system.
4. Log in to the PBA administrative console and navigate to the Drives page.
5. Add the new secondary drive following instructions in 4.4.1.2 **Add Secondary drive(s)**.
6. Shutdown and restart the system.

9.1.2 Replacing or recovering from a failed primary drive.

1. Shutdown the system.
2. Create a bootable thumb drive with the same version of PBA software on it as was previously installed. (Following instructions in section 3.5 **Create a bootable USB 3.0 thumb drive**)
3. Boot to the USB thumb drive.
4. Install the PBA to the primary drive. Note the secondary drives will NOT display for selection as they already contain a PBA environment. For instructions on how to install the PBA see section 3.7 **Install the Cigent PBA.**
5. Boot the system.
6. The Login page should indicate Secondary drive(s) found.
7. Log into the PBA administrative console and navigate to the Drives page.
8. Import each of the secondary drives one at a time. For instructions on importing secondary drives, see section 4.4.1.3 **Import Secondary drive(s)**

For more information about Cigent Secure SSDs please visit www.cigent.com

©2023 Cigent Technology Inc. All rights reserved. Cigent is a registered trademark of Cigent Technology Inc. in the United States and other jurisdictions.