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

Cigent Single and Multidrive PBA Installation Guide and User Manual

Mar 2026

PBA Version 2.0.1.17

Table of Contents

Known Issues

1. Caps Lock and Num Lock do not light up when active, however they are working properly.

1 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, USB token 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.

1.1 Transition to Compliant Power Saving State

The pre-boot authentication (PBA) environment is designed to ensure that no sensitive information remains in volatile memory after it is no longer needed. This includes cryptographic keys, user credentials, and any authentication artifacts.
Upon shutdown or transition into a low-power state, the PBA software performs an orderly cleanup of sensitive material. The system is considered to have fully transitioned into the Compliant power saving state when all volatile memory used by the PBA has been reliably cleared.

Expected Transition Time
Based on internal testing and implementation behavior, the transition time for the Target of Evaluation (TOE) to enter the Compliant power saving state—i.e., the time required for volatile memory to be cleared—is as follows:

- Time to complete memory sanitization: typically under 1 second after PBA exit is initiated.
- This process is triggered automatically as part of the normal shutdown or handoff sequence to the BIOS/Firmware/OS bootloader.

Additional Notes

- Sanitization routines include zeroization of all sensitive memory buffers used during authentication.

2 Initial Installation

2.1 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.

2.2 Drive installation

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

2.3 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.

2.4 Operating System installation

Install any operating system or virtual machines.

2.5 Create a bootable USB 3.0 flash drive

To install the Cigent PBA you will need to create a bootable USB flash drive containing the Cigent PBA software. Cigent provides a utility to help you create this bootable USB flash drive.

Warning: All data on the selected USB flash drive will be erased.

Note: You can use the same USB flash drive to install multiple systems. You only need to create the installer once.

Prerequisites

- USB flash drive (USB 3.0 or later recommended)
- Administrator command prompt
- Extracted Cigent PBA loader package

Procedure

Step 1- Extract the files from the provided ZIP archive and ensure all files remain in the same directory.

Step 2 - Insert the USB flash drive into your computer.

Step 3 - Open an **Administrator** Command Prompt and change directory to the location of the loader software.

Step 4 – Choose Installation Mode

At this point, you may choose between:

- **Interactive Mode (Recommended for Standard Installations)**
- **Manual Mode (Required for Advanced Options)**

Option A – Interactive Mode (Recommended)

Interactive Mode simplifies the process and is suitable for most installations that do **not** require advanced features such as RAID, open primaries, controller-based locks, or license injection.

Run:

PBALoader.exe -i

The utility will:

1. Display a list of discovered USB flash drives.
2. Prompt you to select the target USB flash drive.
3. Prompt for the operation, choose Load.
4. Prompt you to select the PBA package to write:
    - **Microsoft-Signed PBA (pba_v2.0.1.15.bin)**
    - **Cigent Self-Signed PBA (custom_pba_vX.X.X.XX.bin)**
5. Ask for confirmation before writing.

Enter YES to begin writing the PBA image.

Warning: All data on the selected drive will be erased.

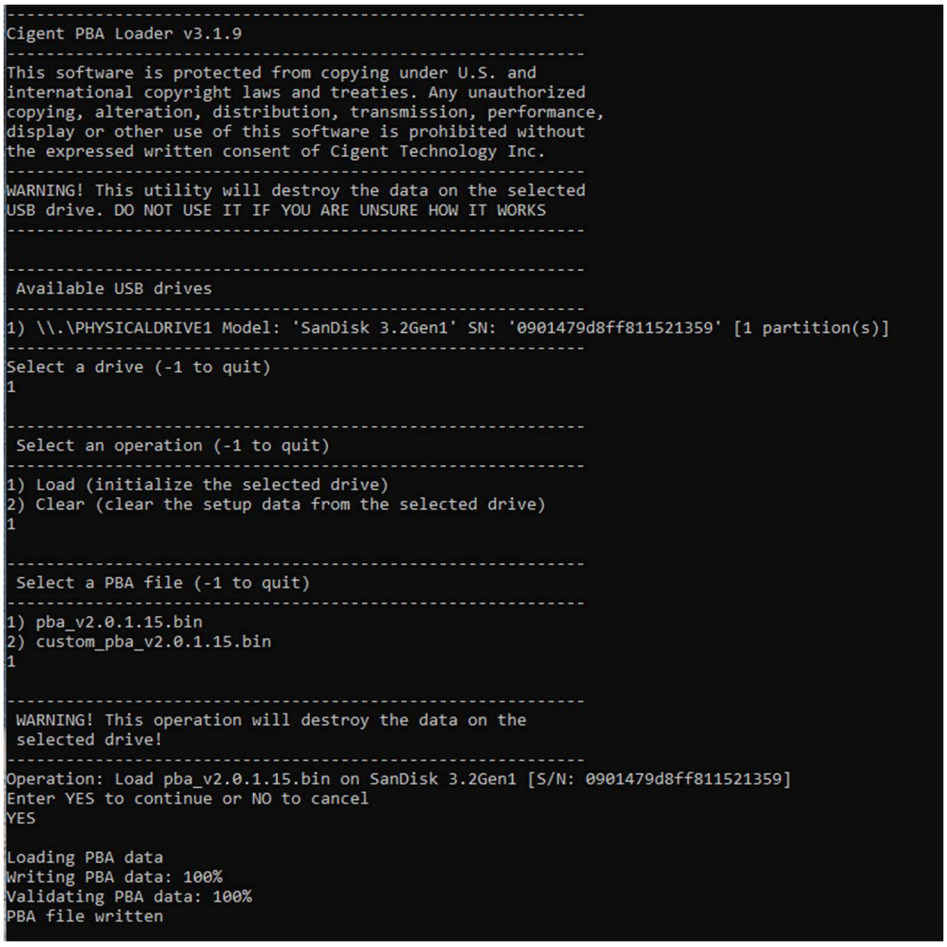


Figure 1 Example - PBALoader Interactive Mode

The process may take several minutes to complete. Once successful, remove the USB flash drive and proceed to **step 2.6.**

When to Use Interactive Mode

Use Interactive Mode for:

- Standard installations
- Typical single-drive or common multi-drive systems
- Installations not requiring:
  - -lic
  - -raid
  - -addl_algos
  - -ctlk
  - -open

Option B – Manual Mode (Advanced)

Use Manual Mode if advanced configuration options are required.

Run: PBALoader.exe -l

This will list available drives. Note the physical drive number of the USB flash drive.

Run: PBALoader.exe -d \\.\PHYSICALDRIVE**X** -load pba_v2.0.1.15.bin

Replace **X** with the physical drive number identified in Step 4.

Optional Parameters (Manual Mode Only)

a) -lic <license file>
   Provide a license file if needed.
b) -raid
   Add this option if the host has more than 5 drives to be protected or if some drives are connected to a supported RAID controller.
c) -addl_algos
   Enables additional smartcard certificate support including EC286, EC384, RSA4096
d) -ctlk
   Use controller-based locks. Advanced option for supported RAID controllers. Contact support for guidance.
e) -open
   Forces the PBA to be loaded on a drive without provisioning the drive (the MBR data is written only to the beginning of the drive). This is used for systems that will not boot a locked drive (even if the MBR shadow is visible and should boot).

Notes When Using the -open Parameter

- The drive will **NOT** be protected.
- The drive will not contain critical data (the database remains on a secondary drive).
- Only drives without partitions are allowed as open primaries.
- The install process overwrites the first **256 MiB** of the drive.
- Erasing an open primary overwrites only the first 256 MiB.

Example Usage with -open

1. Install two drives in the system.
2. Install an OS on one of the drives.
3. Create installer USB:
   PBALoader.exe -d \\.\PHYSICALDRIVE1 -load pba_v2.0.1.15.bin -open -raid
4. Boot to the PBA installer drive.
5. Load PBA:
   - Select the non-OS drive as the open primary
     (The beginning of the drive must be erased or contain no partitions.)
   - Select the OS drive as a secondary.
   - Complete the installation.
6. Reboot into UEFI.
7. Set boot order: place the OS before the open primary.

Important: The open primary will ALWAYS boot (unlike the normal shadow MBR which hides its boot data after login).

Additional Notes

The file custom_pba_v2.0.1.15.bin is a Cigent self-signed version. The keys provided must be imported into the BIOS Secure Boot menu prior to running the installer. Contact support for additional information.

The process can take several minutes to complete. Once successful, remove the USB flash drive and proceed to step 2.6.

2.6 Boot to the USB thumb drive

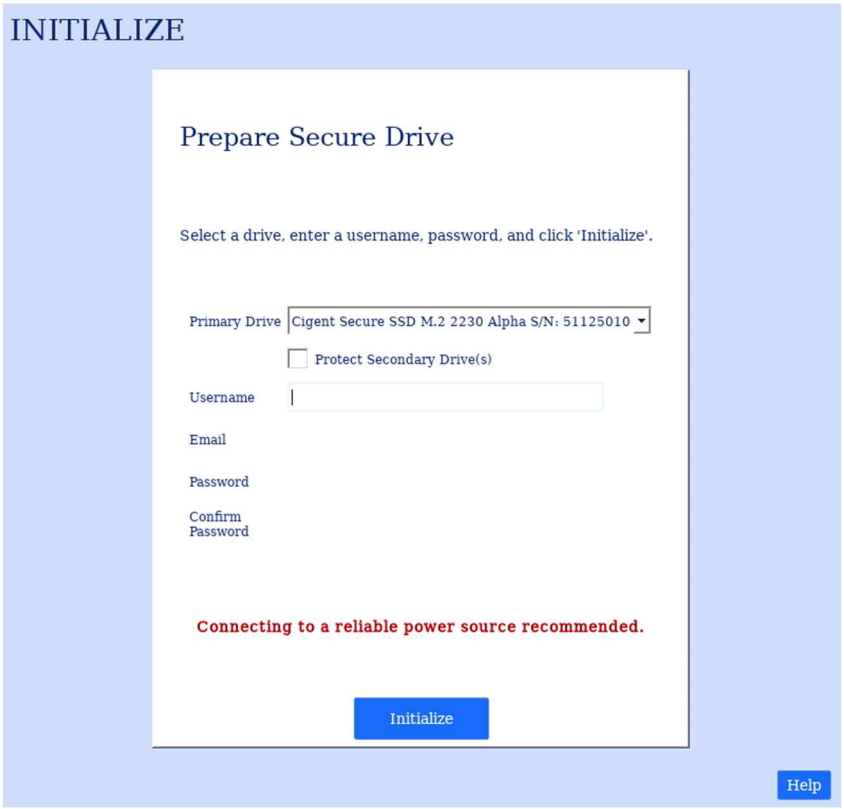
1. Ensure the power is turned off.
2. Insert the bootable USB thumb drive into the computer with the Cigent Secure SSD.
3. Turn on the computer and press the appropriate key for your computer to display the boot menu. The typical keys are F1, F2, F10, F12 or Esc.
4. Choose the USB thumb drive from the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

2.7 Install the PBA

2.7.1 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.

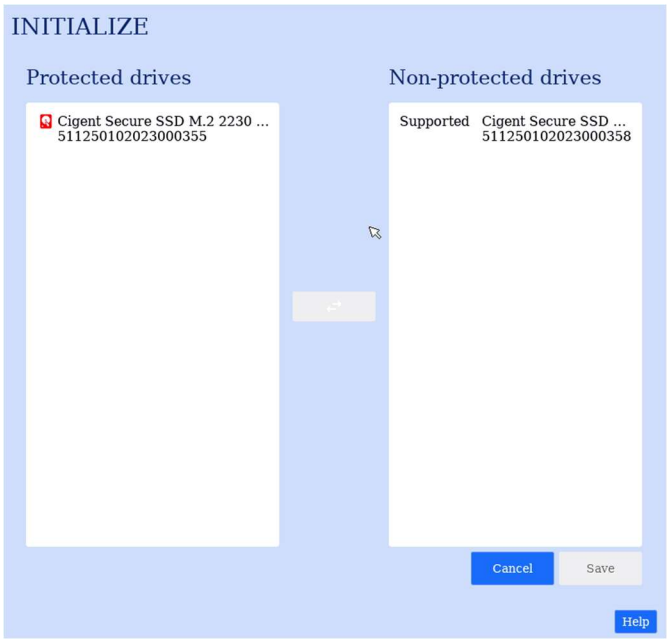


2. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will boot.

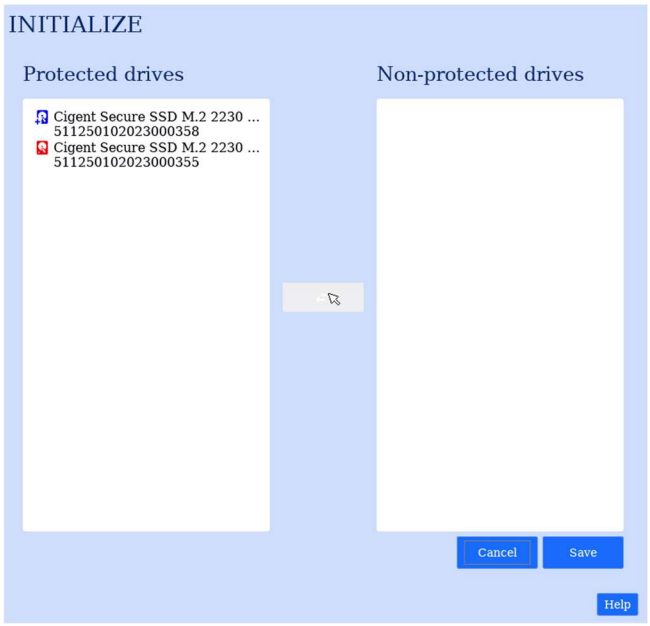
3. On a system with more than one drive:
    a. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will boot.

       NOTE:
       - When loading the PBA using a loader created with the -open flag, select the desired open primary as the main drive and select the other drives to protect as secondaries. Note that the first secondary in the list is the one that will hold the database.
       - When loading the PBA using a loader created with the -open flag, the initial boot should be into UEFI to ensure the boot order is correct. The drive with OS should boot before open primary. This is important because the open primary will ALWAYS boot (unlike the normal shadow MBR which hides its boot data after login).

    b. Check “Protect Secondary Drives” to open the Add Secondary Drives dialog.

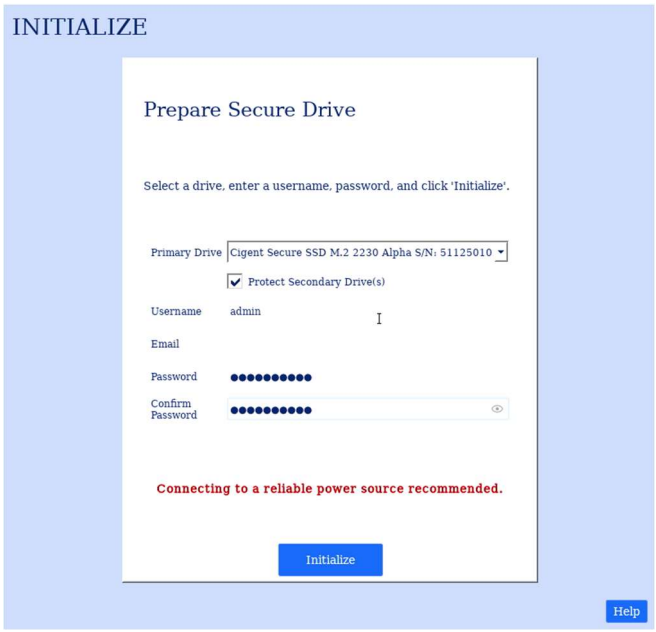


    c. Select drives from the Non-protected drives list and click the double arrow button to move them to Protected drives.



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 (NOTE: Update is applicable when upgrading during activation.)



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

Once complete, the login page will immediately display. Proceed to **Initial Login** section for more information.

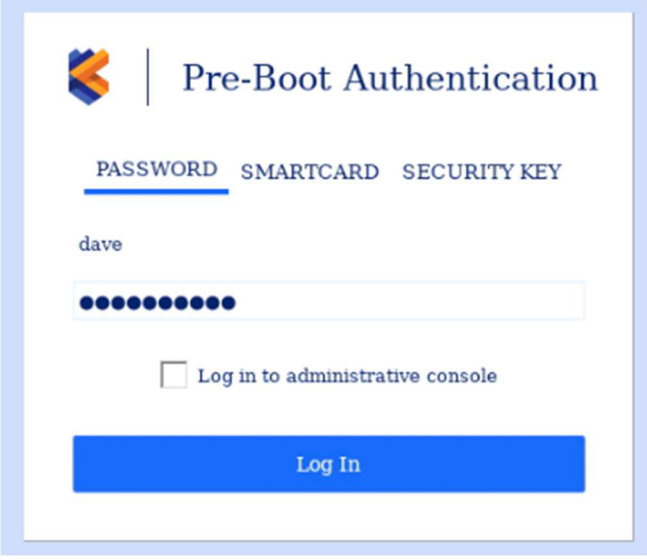
Be sure to remove the USB thumb drive.

Your PBA is now installed and ready for use.

2.8 Initial login

The user credentials used to install the PBA software have the 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. On the login screen, enter the credentials you used during the PBA installation process.
2. Click Log In.

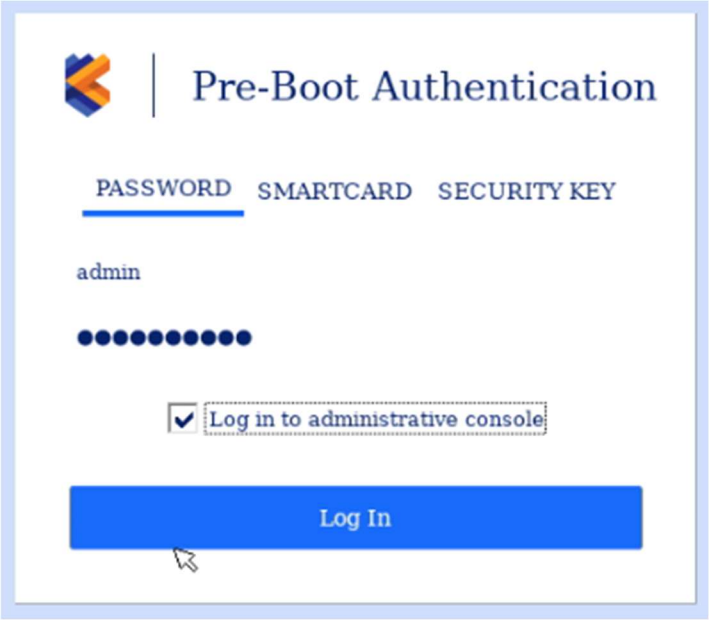


For details on how to log in to the administrative console, see section Using the Administrative Console.

3 Using the Administrative Console

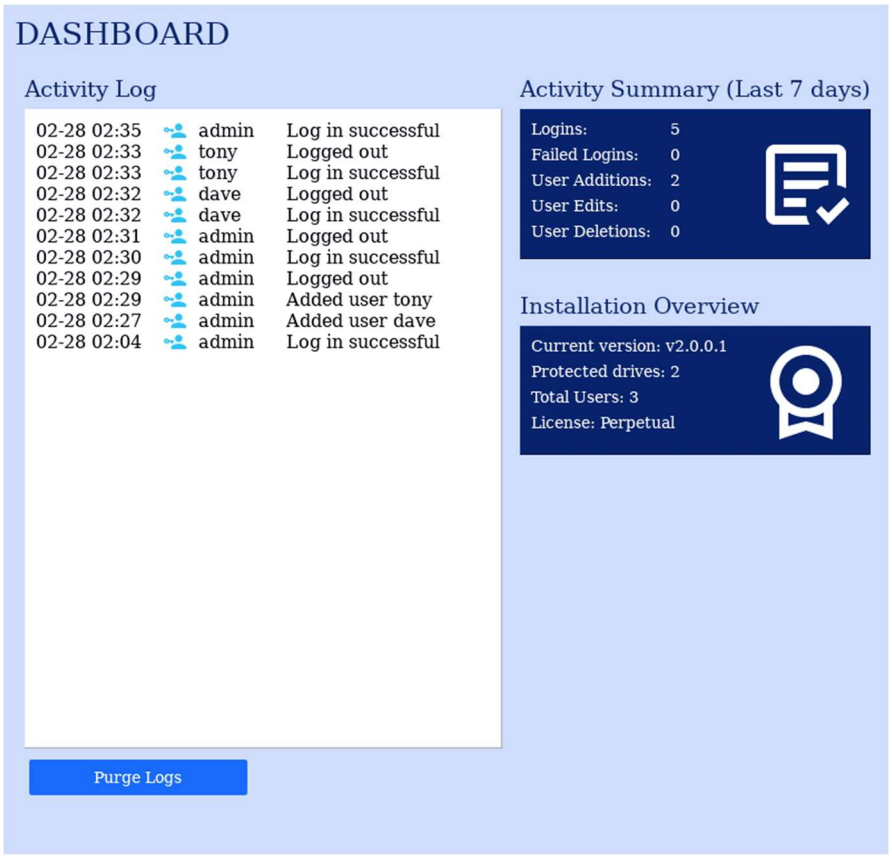
The administrative console allows administrators to manage users, perform maintenance tasks, and view activity logs pertaining to the PBA environment.

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



3.1 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.

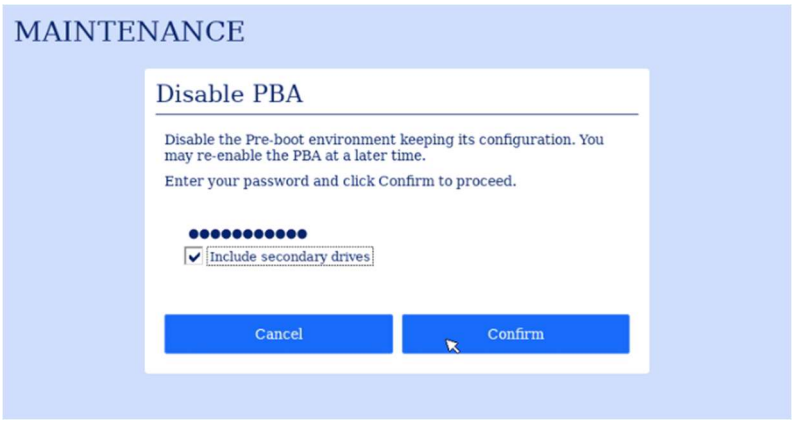
3.2 Maintenance

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

3.2.1 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.

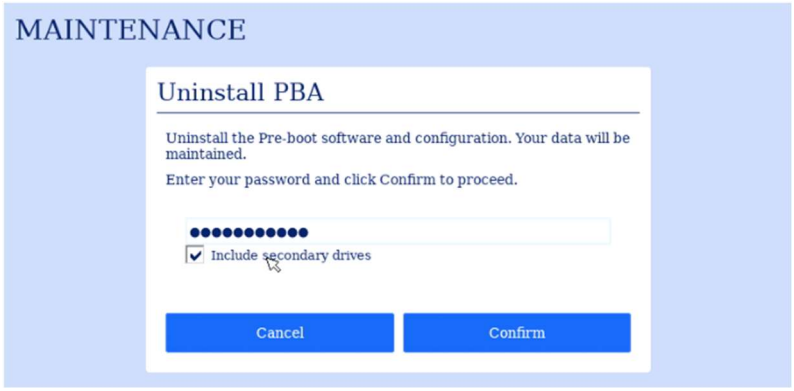


1. Click *Disable PBA*.
2. Enter your administrator password.
3. Click *Confirm*.

3.2.2 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.



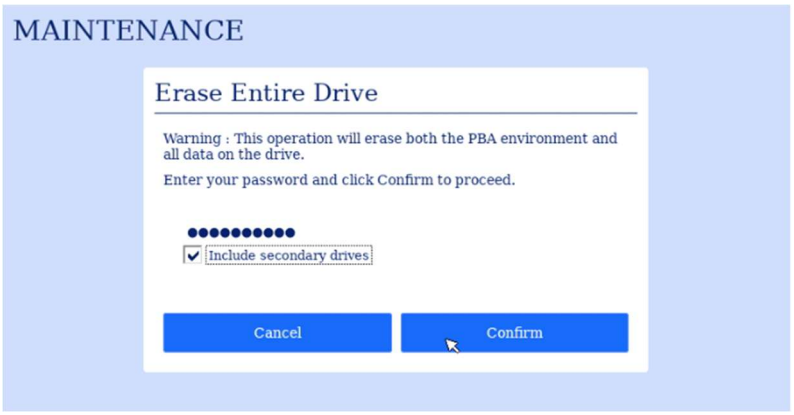
1. Click *Uninstall PBA*.
2. Enter your administrator password.
3. Click *Confirm*.

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

3.2.3 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.

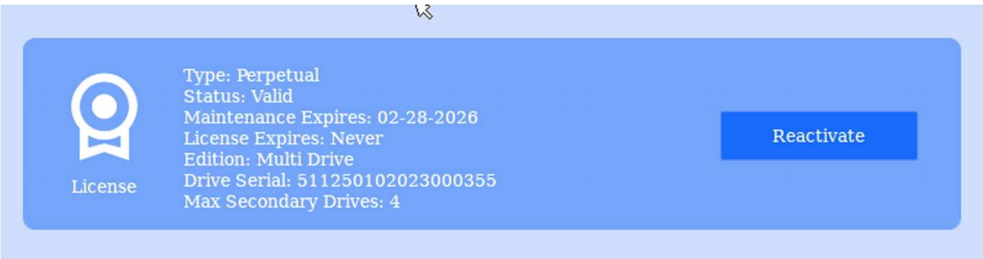
1. Click *Erase Entire Disk*.
2. Enter your administrator password.
3. Click *Confirm*.

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

Once complete, power off the system.

3.2.4 Reactivate/Activate

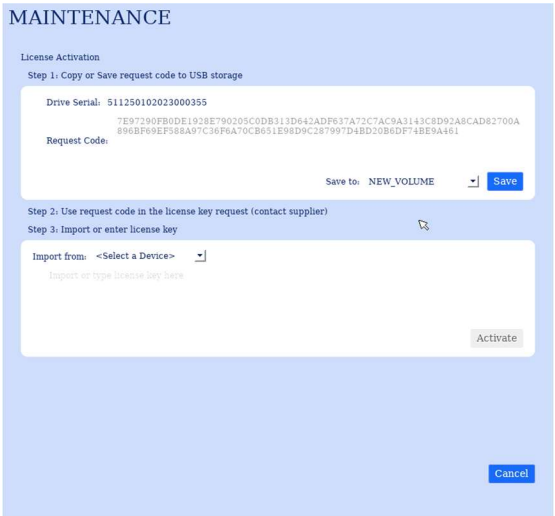
PBA usage and access to features is controlled by a license key. Installation on Cigent drives automatically enables a perpetual license allowing up to 4 secondary drives. The maintenance period will expire one year from installation after which upgrades will no longer be supported, however the PBA will continue to function normally.



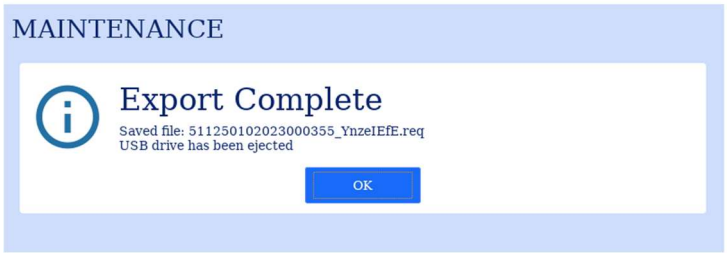
If additional secondary drives or RAID support is required a license key will need to be requested using the license activation process.

You will need a FAT32 formatted usb drive to store the request code and to import the activation code from. Alternatively, you can manually copy the request code and enter the activation code.

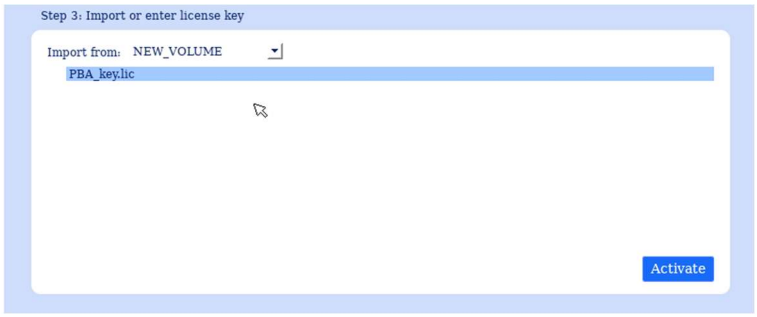
1. Insert the USB drive.
2. Click Reactivate



3. Click Save to place the request code to your USB drive.



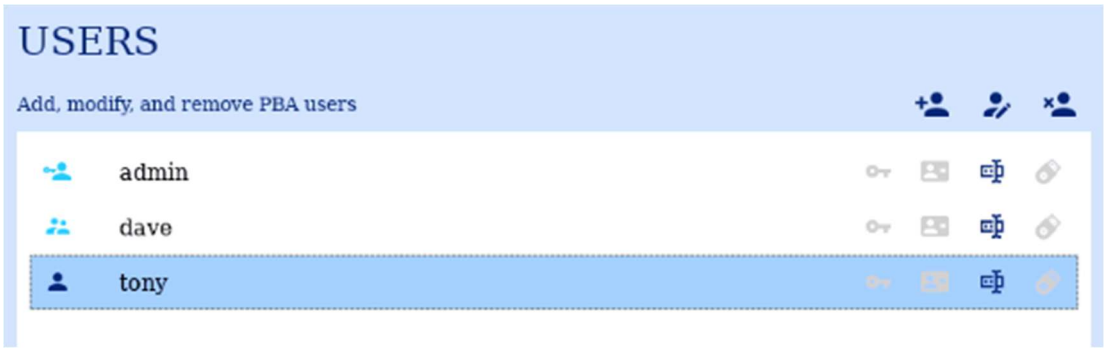
4. Send the request code file to your supplier. Note the request file will be saved with a REQ extension.
5. Once the license key is received, copy it to the usb drive and use the Import from dialog to select the file. License keys typically have a LIC extension.



6. Click Activate.

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

3.3.1 Authentication options and requirements

Each PBA user can be configured with four different authentication options including password, smartcard and security key and USB token. Password is always required. Smartcard, security key and USB token authentication are optional. Both Smartcard and Security Key (PIN or Touch) can be used for a two-factor authentication setup (requiring both a password and second factor.)

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 PIN. The PIN is set up 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.

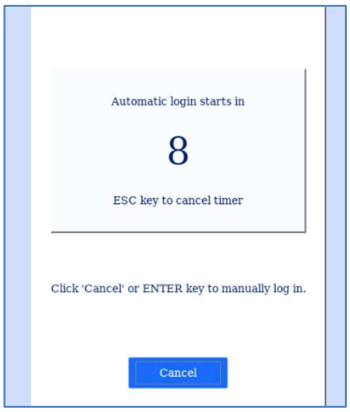
Note: Support of Smartcards using EC256, EC384 and RSA4096 require the **-addl_algos** parameter to PBALoader during USB flash drive creation.

USB Token

USB token authentication requires a dedicated storage device which if present during boot time will automatically login as the user. During setup a user specific key will be placed on the

storage device. More than one key can be stored on a single device allowing a user to authenticate on multiple systems with a single token.
Note all data will be destroyed during setup and no user data can be stored on the device. The USB token device should be dedicated to this usage and not be used for other purposes like storing data. Formatting the drive will delete all keys.

When the system is powered on and the PBA finds a valid USB token, automatic login will be initiated.



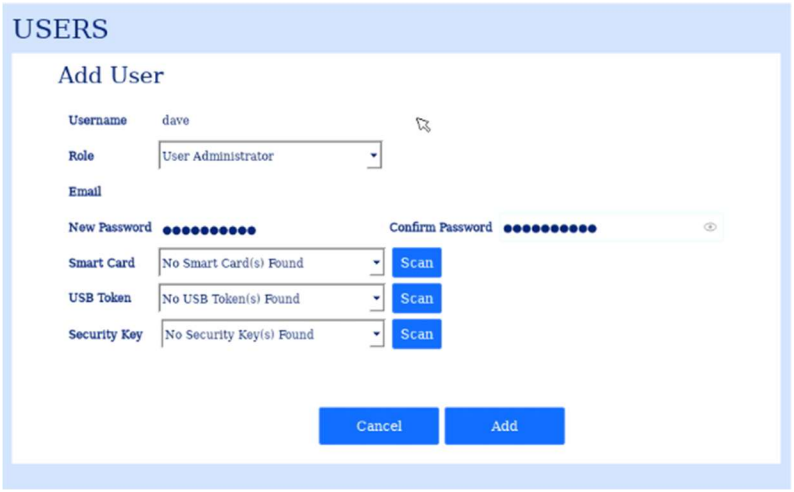
Note: After login has been completed, the USB token should be removed from the system for security reasons.

Security Key
Most devices supporting the FIDO2 U2F protocol are supported (Swissbit iShield and Yubikey 5 series are tested and supported.) 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.

3.3.2 Add User

The Add User page is used to add a new user using password, smartcard, USB token or security key. If the "Require Two-Factor Authentication" setting is set Smartcard or Security Key, all newly added users must have both password and the second factor when being added.



1. Enter a unique username.
2. Select role (Administrator, User Administrator, User) 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 a USB Token.
7. (Optional) Select the Security key. Choose Auto, Touch or PIN.
8. Click *Add*.

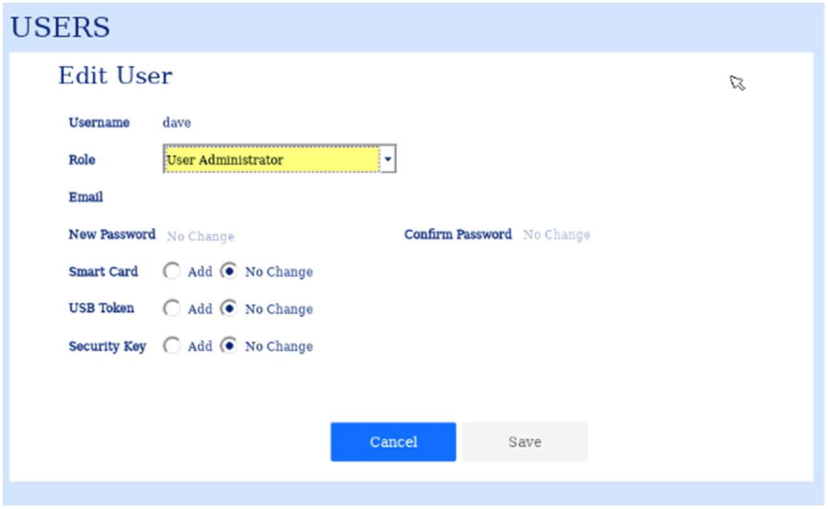
Click the Scan button next to Smartcard, USB Token or Security Key if your device is not listed after inserting the card, token or key.

3.3.3 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 USB token
- 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.

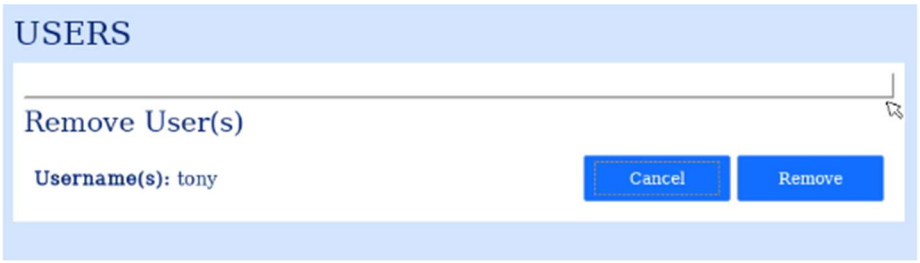
Note that to Add a Smart Card, USB Token or Security Key to an existing user, the device should be inserted before entering the page. If you do not see the device listed after inserting it, click Scan.

3.3.4 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.

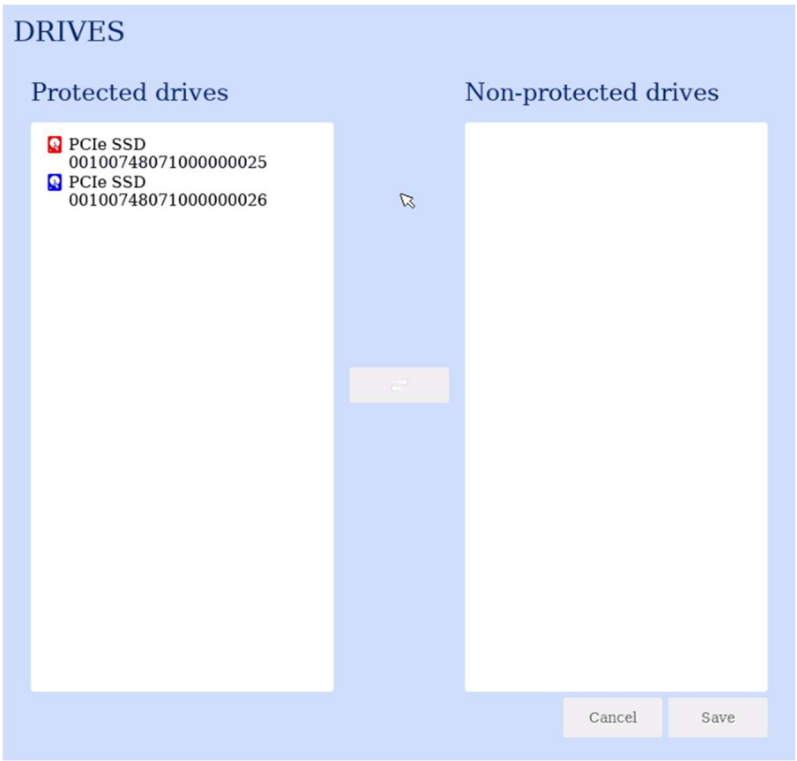


3.4 Drives

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.

3.4.1 View protected drives

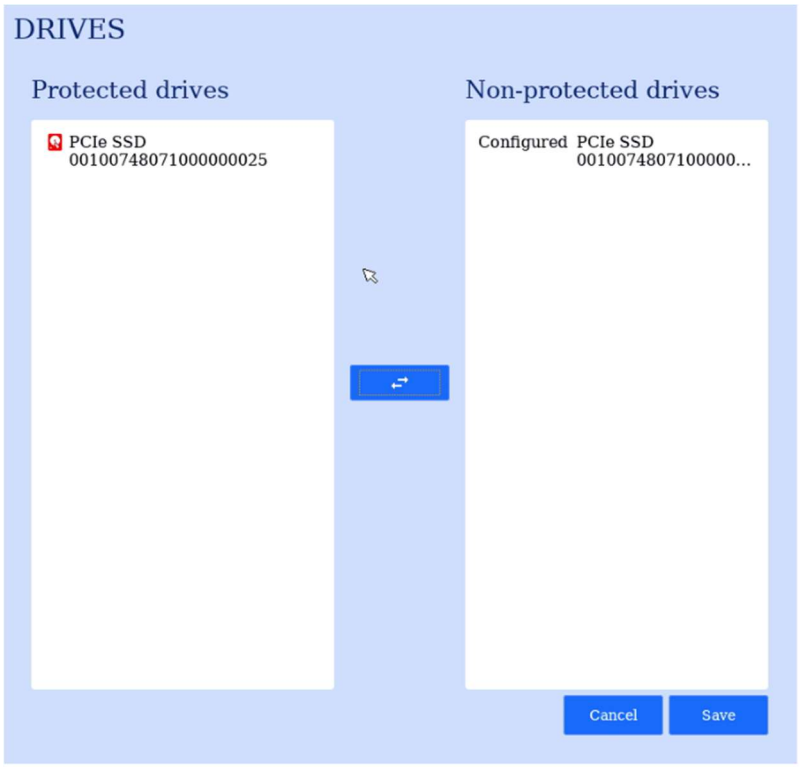
The *Protected drives* column shows details of the drives under the protection of PBA including model number and serial number. The primary drive is indicated with a red icon and all secondaries, if present, are blue. The *Non-protected drives* column shows drives recently removed from protection or 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.



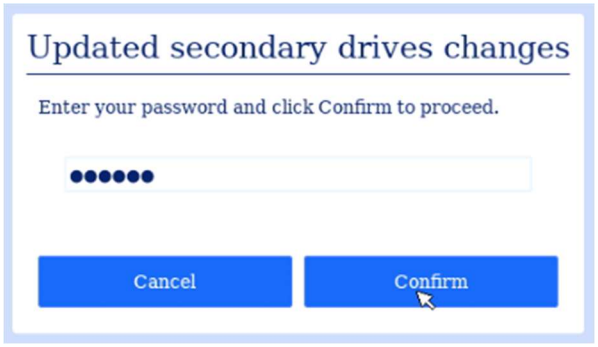
3.4.2 Remove Secondary drive(s)

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.

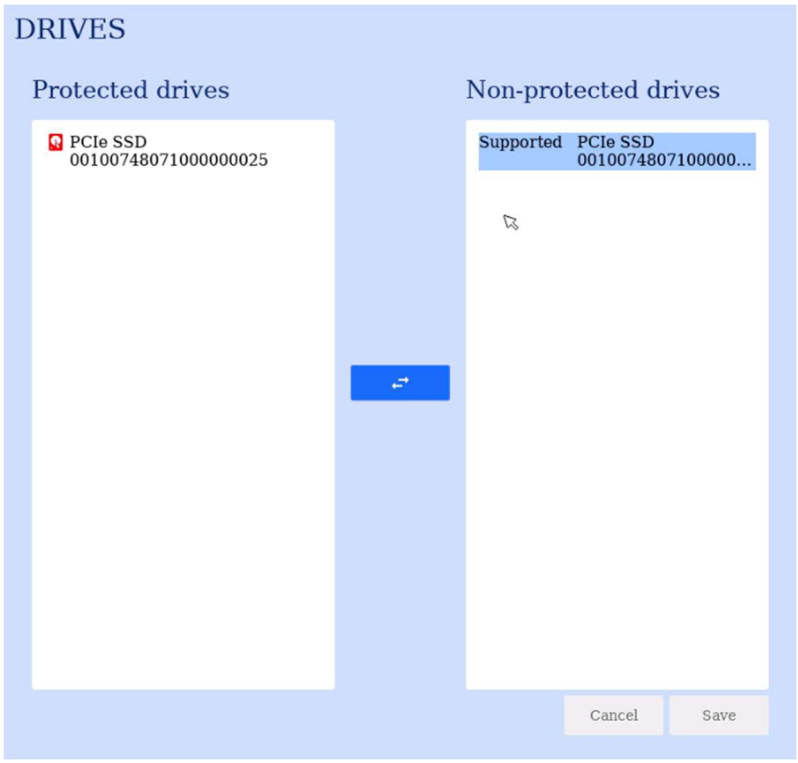


The drive will now show as Supported indicating it is no longer protected but could be added to the protected drives list.

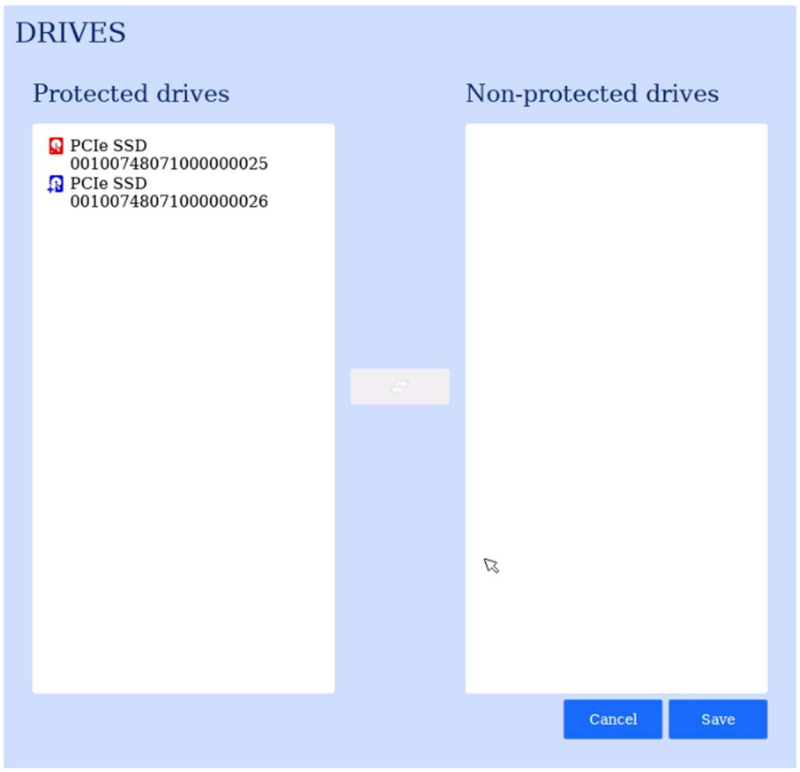
3.4.3 Add Secondary drive(s)

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

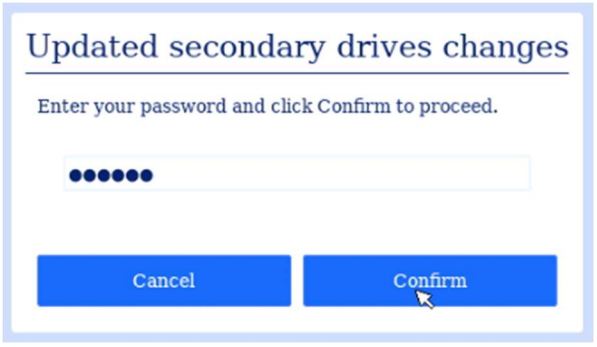
1. Select one or more drives shown as Supported from the Non-Protected column.



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



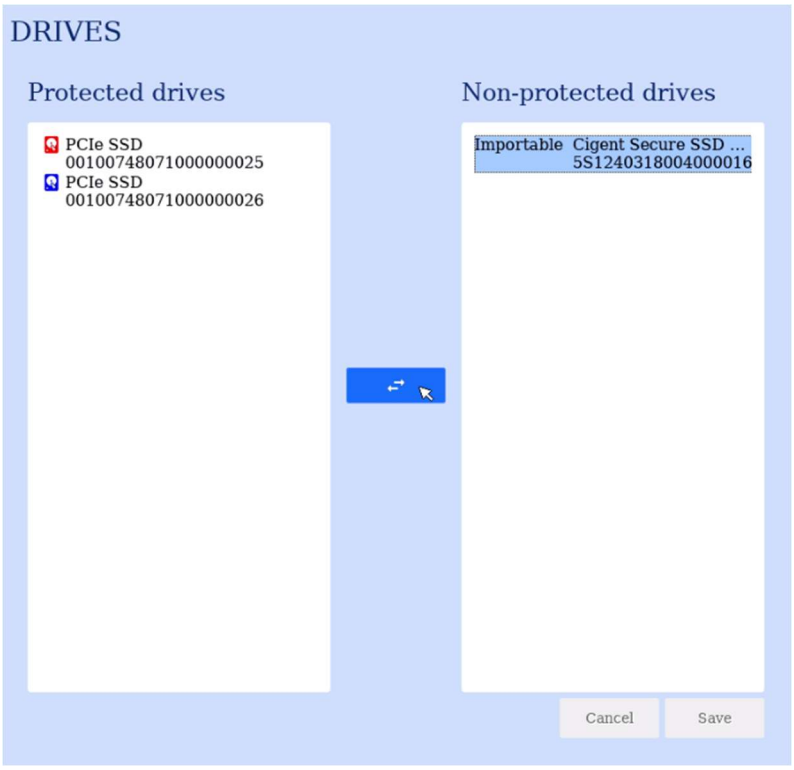
3. Click Save.
4. Enter your password and click Confirm.



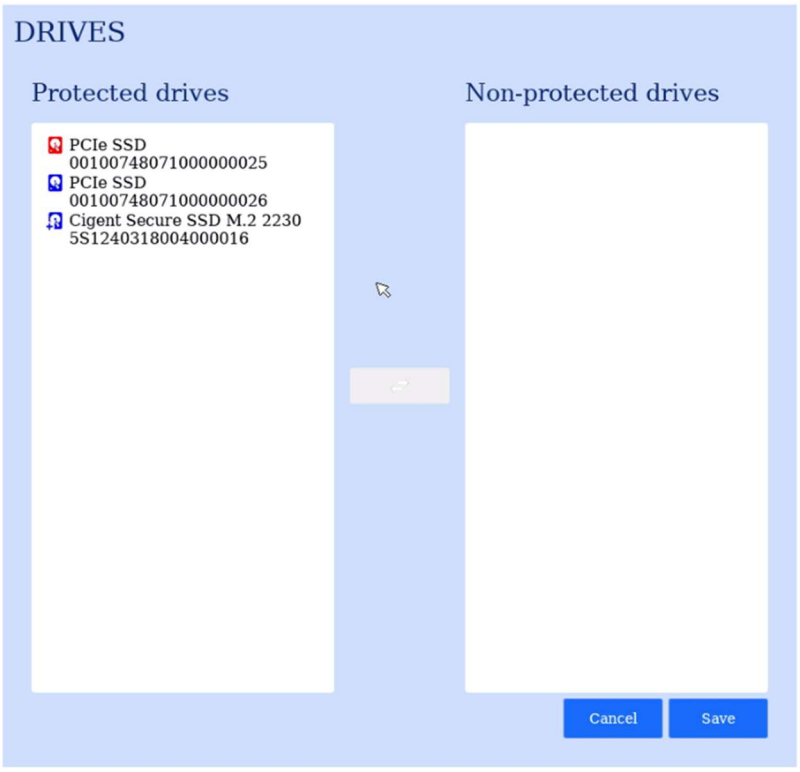
3.4.4 Import Secondary drive(s)

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.)

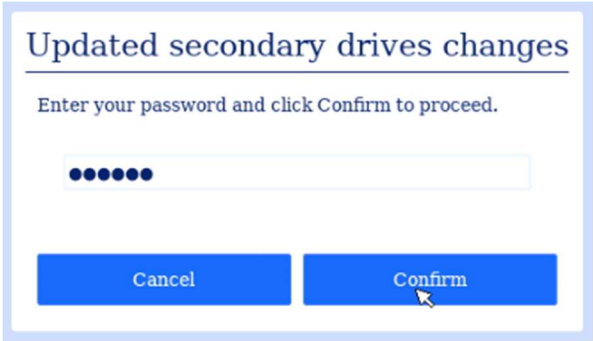
1. Select one or more drives labeled Importable from the Non-protected drive list.



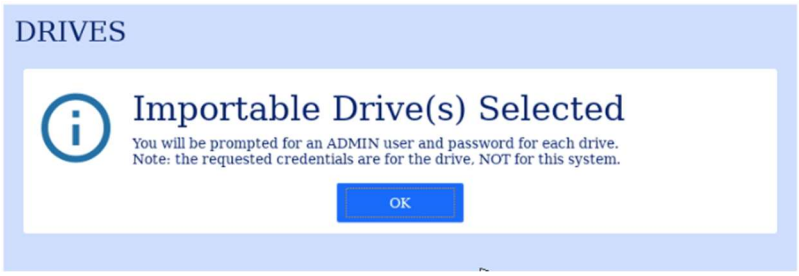
2. Click the double arrow button to move the drive to the Protected drives column.



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



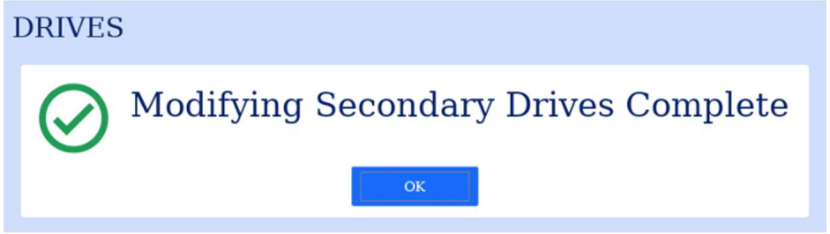
5. Click Ok.

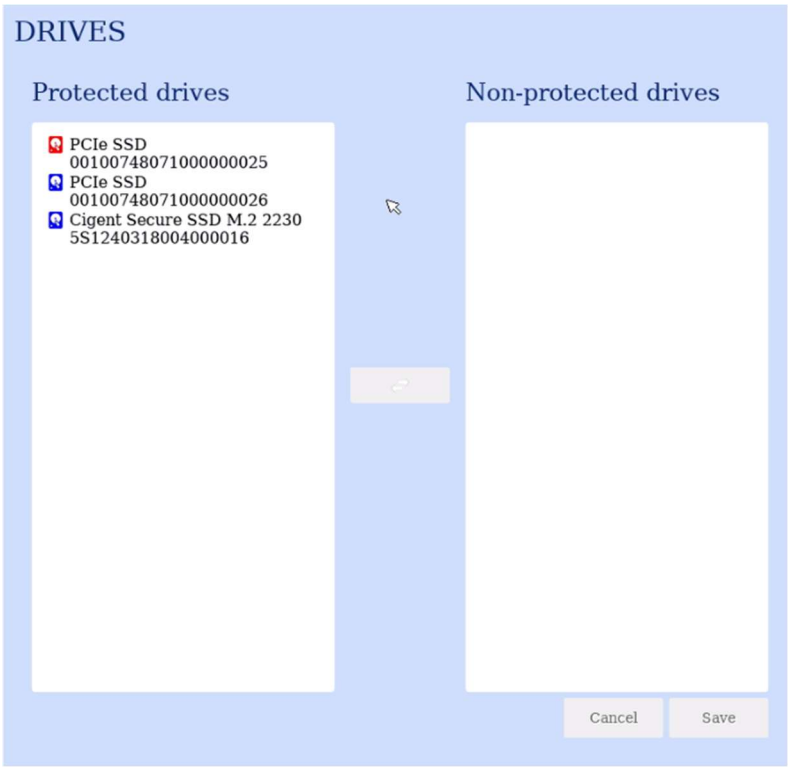


6. Enter administrator credentials from the source PBA then click Continue. (NOTE: These are the credentials from the PBA installation where this drive was originally configured, not the credentials for the running PBA.)

7. Click Continue. Repeat for each drive selected.

8. Click Ok.

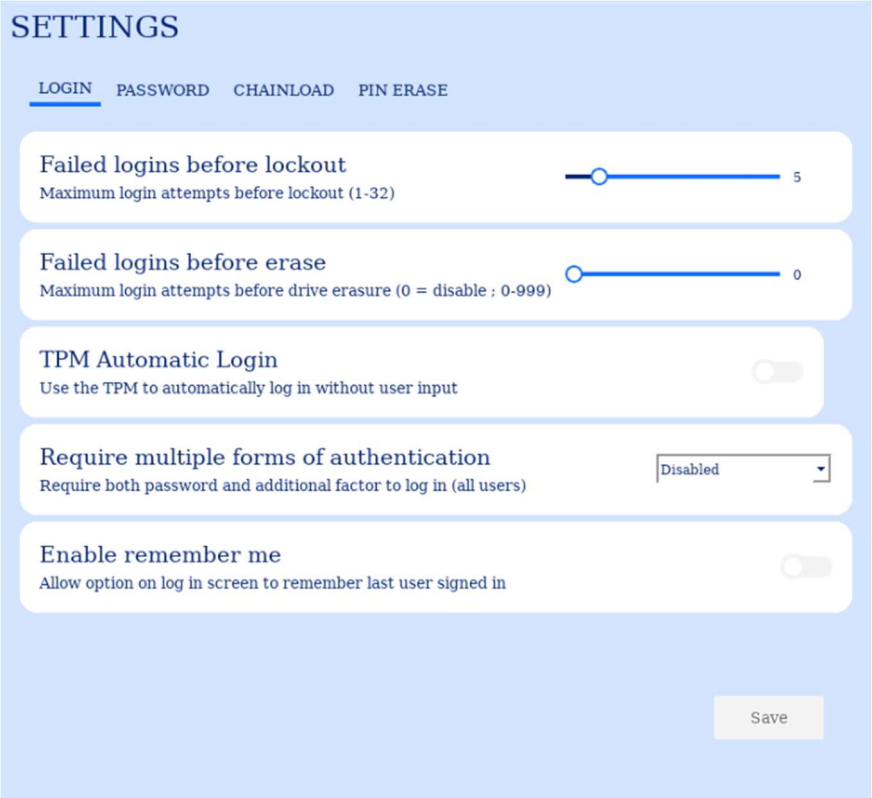



DRIVES
Protected drives
Non-protected drives
PCIe SSD
00100748071000000025
PCIe SSD
00100748071000000026
Cigent Secure SSD M.2 2230
5S1240318004000016
Cancel
Save

3.5 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.

3.5.1 Settings - Login



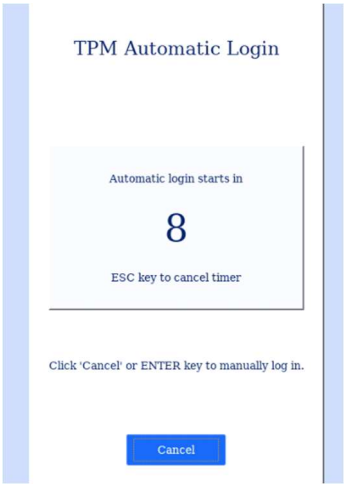
Failed logins before lockout
The number of consecutive failed login attempts (across all users) before a restart is required. Only attempts with valid usernames are considered towards failures.
Min: 1 *Max*: 32

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: TPM automatic authentication was not part of the Common Criteria evaluation.



Require multiple forms of authentication

Enforces the use of two distinct authentication factors during login.

The **first factor** is always the user's password.

The **second factor** can be one of the following:

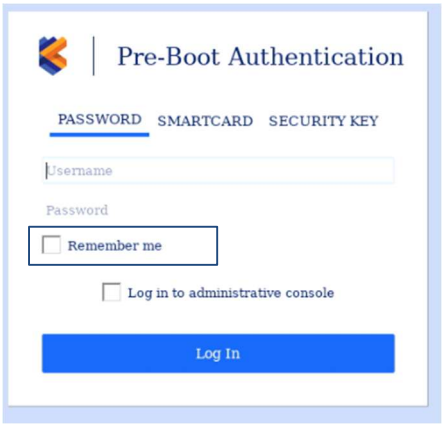
- Smart card
- Security key (touch)
- Security key (PIN)

When this setting is enabled, users will first be prompted to enter their username and password. Upon successful password verification, they will be prompted to complete the configured second authentication factor.

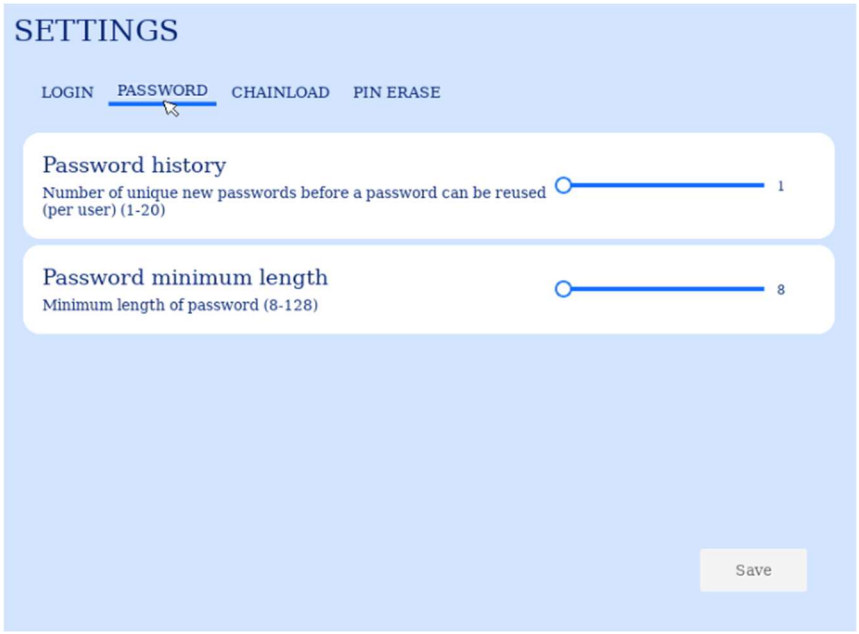
If a user is not configured for a second factor at the time this setting is enabled, they will be required to enroll a supported second factor during their next login attempt. Until enrollment is completed, the user will not be permitted to access the system.

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.



3.5.2 Settings - Password



Password history

The number of unique passwords per user before a password can be reused.

Min: 1 *Max*: 20

Password minimum length

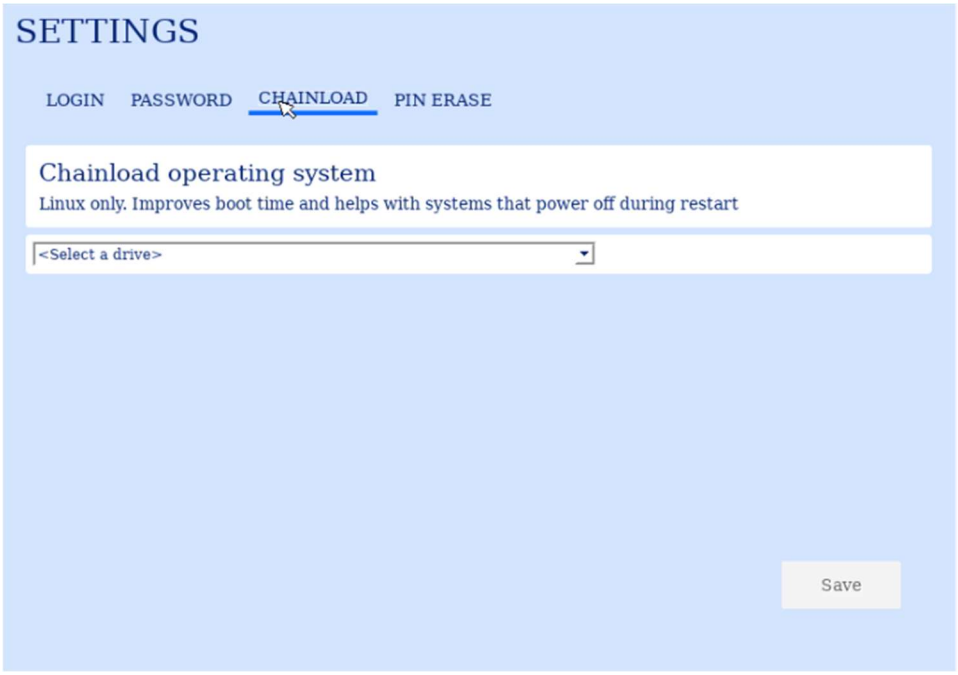
The minimum password length required for each user. The requirement will be enforced the next time an existing user changes their password or a new user is added.

Min: 1 *Max*: 128

3.5.3 Settings - Chainload

Chain load operating system

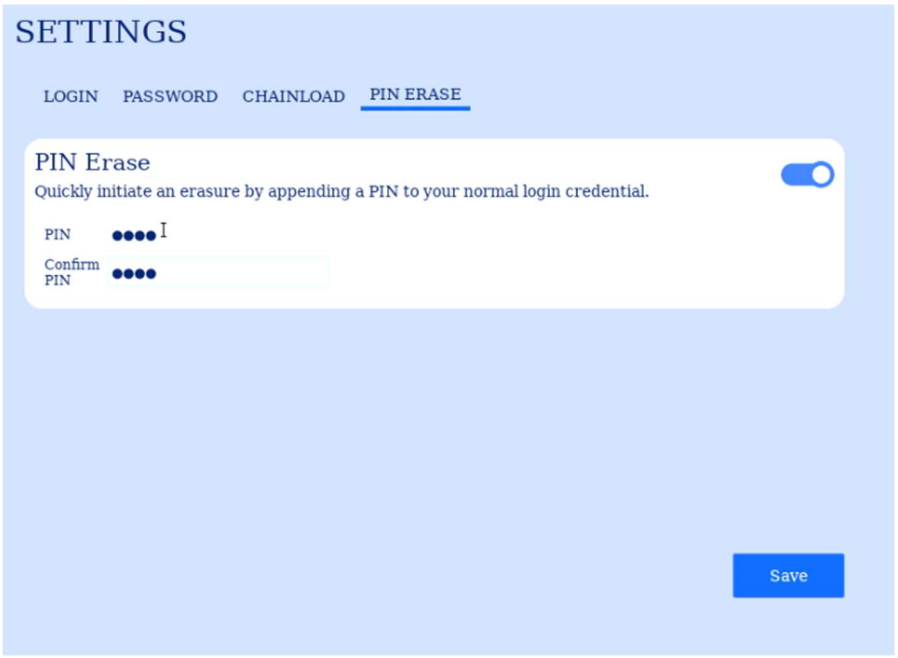
Chain loading is when a boot loader loads another boot loader to begin the boot process. This process greatly reduces the time needed to start the target operating system. Currently, Cigent PBA supports chain loading to Linux only. Click Scan to initiate a search for available kernels on the boot drive.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



3.5.4 Settings – Pin Erase

PIN Erase

Enable and define a special code (4-15 characters -numbers, upper and lower case) that when appended to the users normal password or smartcard PIN, will initiate a complete disk erasure. The erase PIN is available for all users defined in the PBA.


SETTINGS
LOGIN
PASSWORD
CHAINLOAD
PIN ERASE
PIN Erase
Quickly initiate an erasure by appending a PIN to your normal login credential.
PIN
Confirm PIN
Save

4 Reinstallation of the Cigent PBA

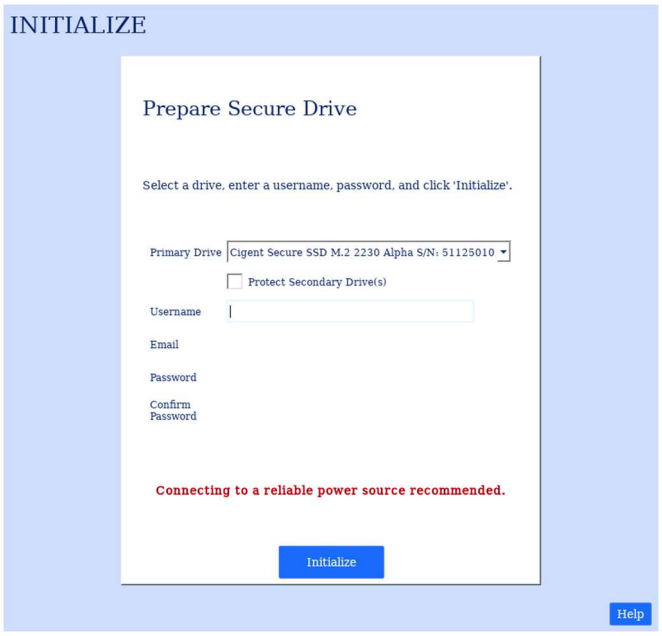
Reinstallation of the Cigent PBA software will be necessary if you used the **Erase Entire Drive** or **Uninstall PBA** features from the maintenance page or erased the drive using another utility.

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

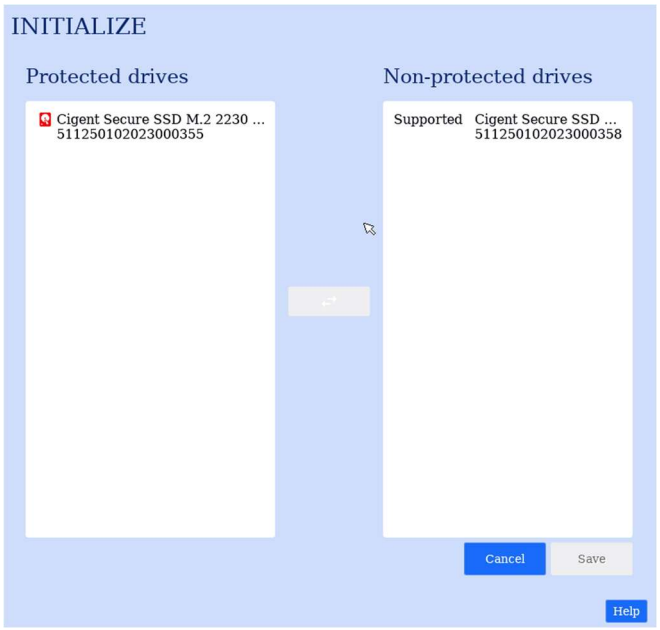
1. Create a bootable USB thumb drive containing the Cigent PBA software. (See section Create a bootable USB 3.0 thumb drive **)**

> **Note:** The same bootable USB drive that was used to enable the Cigent PBA can be used if available.

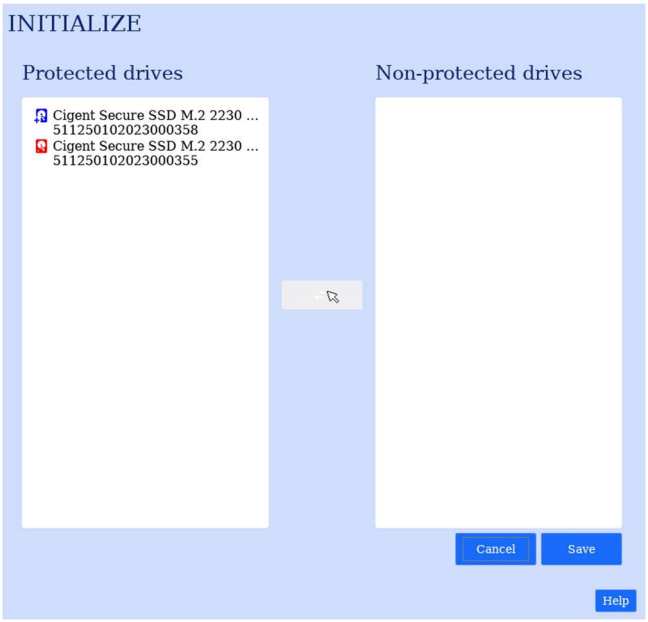
2. Boot from the USB thumb drive.
3. The Prepare Secure Drive screen will be displayed.



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.

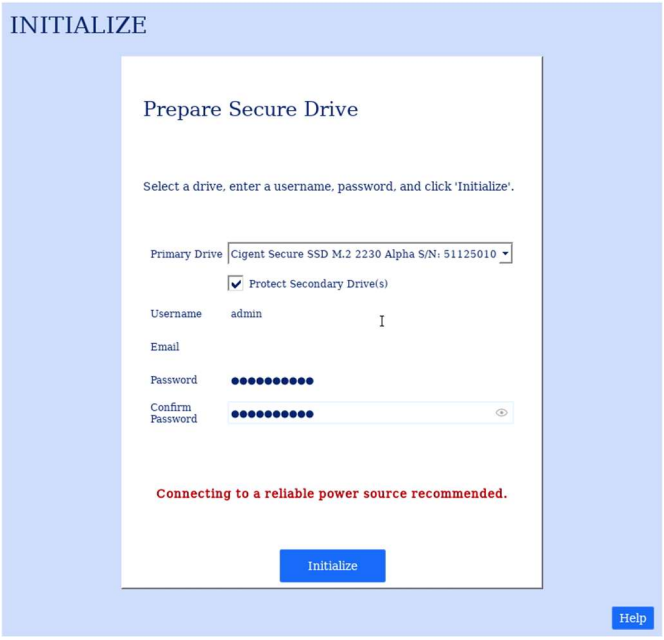


c. Select some or all of the drives from the Non-protected drives list and click the double arrow button to move them to Protected drives.

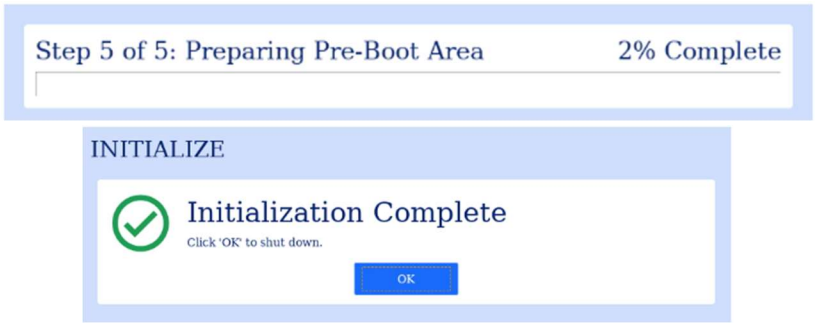


d. Select the secondary drives to protect and click Save.

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.



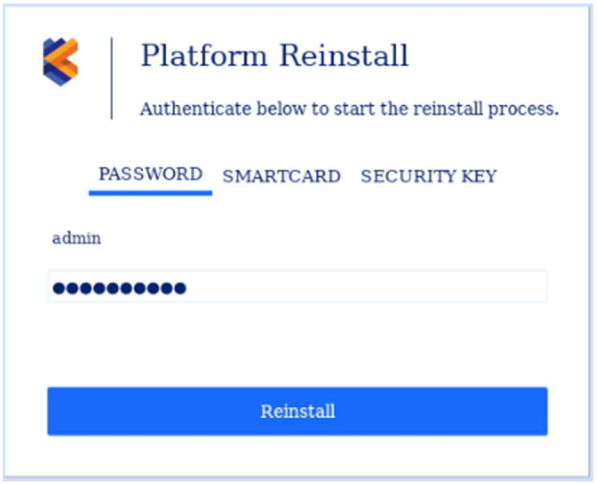
Once complete, power off the computer.
Remove the USB thumb drive from the computer.

5 Re-enabling the Cigent PBA

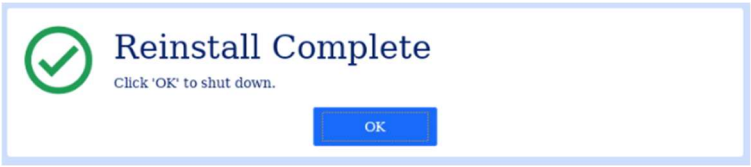
To re-enable PBA after temporarily disabling it from the maintenance page you will need the following:

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.

6 Updating the Cigent PBA software

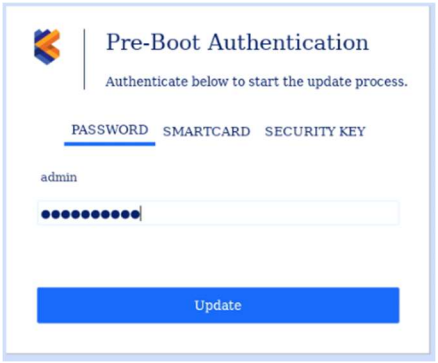
For information on obtaining the newest version of the Cigent PBA software see section Initial installation overview.

Note: Upgrade from 1.0.6.53 and greater to version 2.0.1.15 is supported.

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

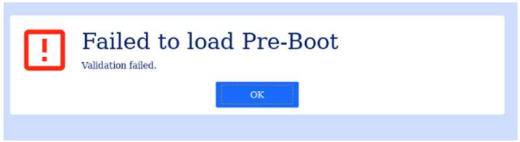
1. An installation USB drive of the newer version of Cigent PBA installed on the device (See section Create a bootable USB 3.0 thumb drive)
2. Administrator credentials to the PBA environment

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 update login screen.



Enter valid administrator credentials and click Update. The process will take about 10 minutes to complete.

The first part of the update process performs a digital signature verification to ensure integrity and authenticity of the Cigent PBA. Failure of the signature verification will result in an error message and prevent update of the PBA. If you receive this message, redownload the Cigent PBA or contact support.



If the update is successful, shutdown the system and remove the USB drive. On the next boot, the PBA environment should once more present the normal login screen and indicate the updated version.

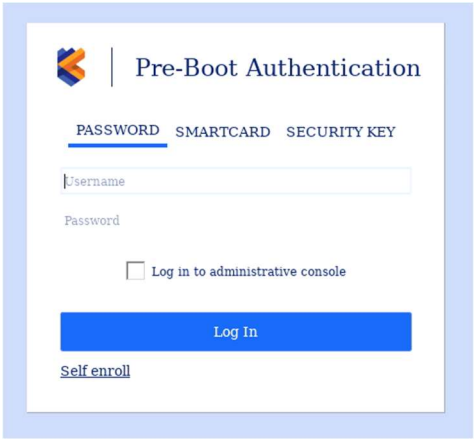
7 User Self Enrollment

In some situations, it may be necessary to allow users to self-enroll as a user of the PBA. This could be if the recipient of the device is in a remote location or no administrator is located at a remote site. To support this scenario, administrators can enable user self enrollment using a smart card. The self enrollment capability and UI are enabled using the PBA command line utility with the -enrollcode option. Administrators can specify an enrollment password with a usage quantity and expiration timestamp. See the command line utility help for additional information.

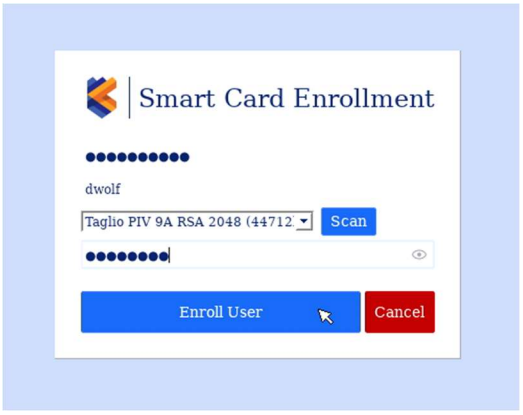
7.1 User Self Enrollment using Smart card

If an enrollment password is configured the login page will display self registration option.

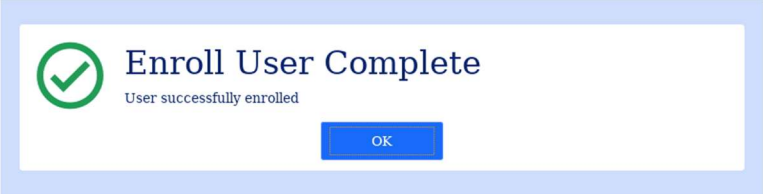
1. Click Self enroll



2. Enter the provided enrollment password, a unique username and your smart card PIN, then click Enroll User.



3. Click Ok to return to the login page.

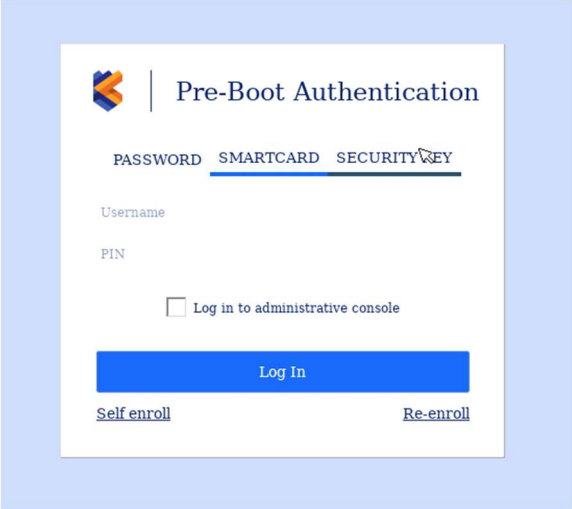


4. The user can immediately login to the PBA using their smart card.

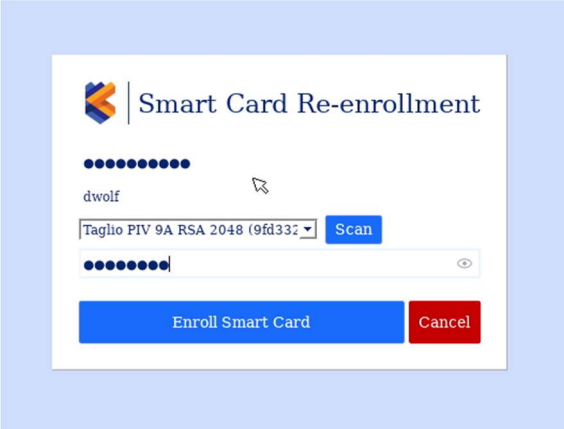
7.2 User Self Re-enrollment using Smart card

If a smart card only user receives a replacement smart card, they will need to use the Re-enroll page to update their smart card in the PBA.

1. Click Re-enroll



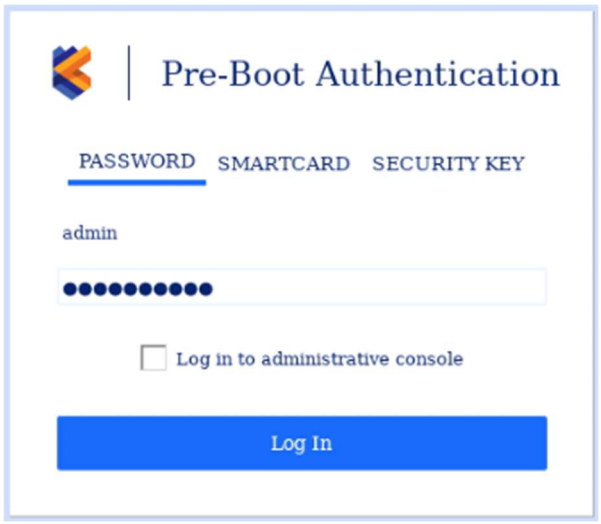
2. Enter the provided enrollment password, your existing username and your new smart card PIN, then click Enroll Smart Card.



8 Logging in and Logging Out

8.1 Logging in with a username and password

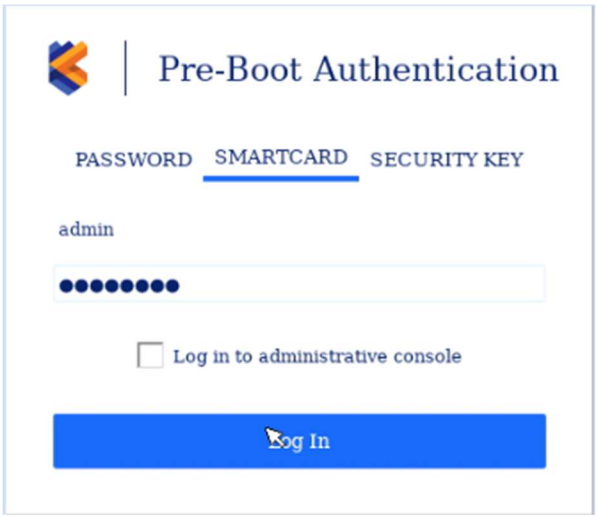
1. Power on the computer and wait for the PBA authentication screen to appear.
2. Enter your username and password.
3. Click Log in.



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

8.2 Logging in with a Smart Card

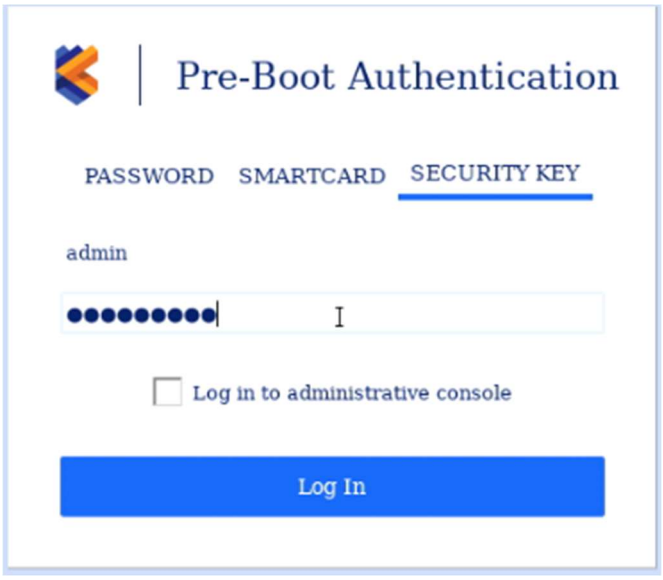
1. Power on the computer and wait for the PBA authentication screen to appear.
2. Click Smart Card.
3. Enter your Username and PIN.
4. Click Log In.



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

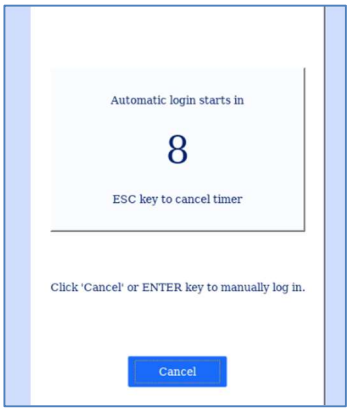
8.3 Logging in with a Security Key

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.



8.4 Logging in with a USB token

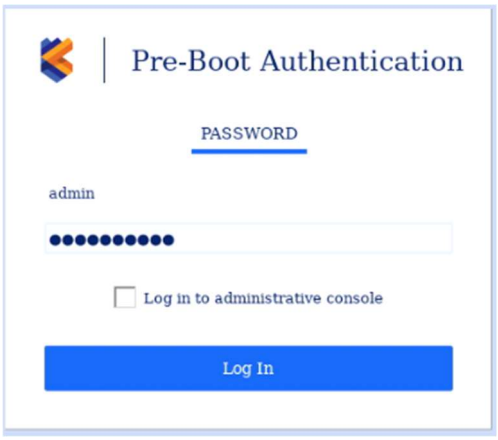
1. Insert the USB token.
2. Power on the computer.
3. The PBA will automatically initiate a countdown to login using USB token authentication. You can interupt the countdown to login using other authentication methods by clicking Cancel.



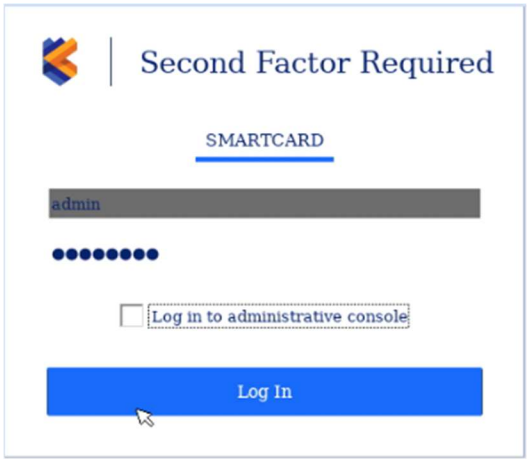
4. If authentication is successful, the system will unlock and perform a restart.
5. The USB token can now be removed.

8.5 Logging in with Two Factor Authentication

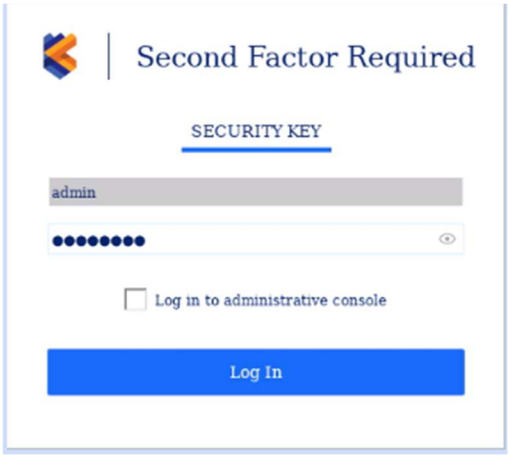
When the “Require Two-Factor Authentication” setting is enabled, all users must authenticate with a password and either a smartcard or security key. The Login page will first ask for the password then the second factor. If both factors are verified, the login will be successful.



1. Insert your smartcard or security key.
2. Power on the computer and wait for the PBA authentication screen to appear.
3. Enter the username and password.
4. Click Log In.



OR



5. For Smartcard, enter your PIN. For security key, touch or enter your PIN.
6. Click Log In.

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

8.6 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 Help

Additional diagnostic information and utilities are available from the Initialization page during installation by clicking Help.

9.1.1 System Report.

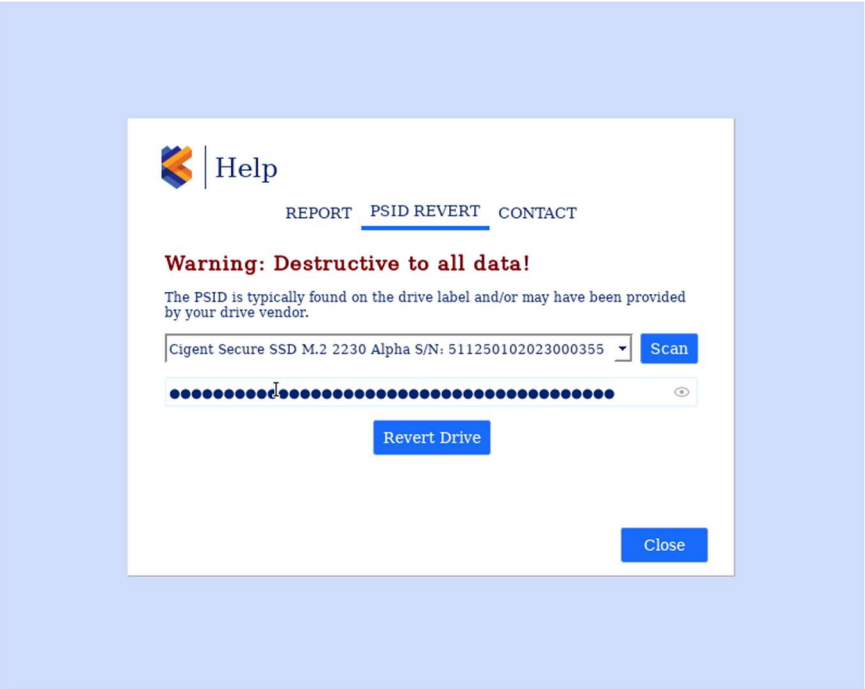
The report tab contains important information about the platform and drives which can be useful to support in helping with installation issues. The report can be exported to a FAT32 formatted usb device.

9.1.2 Resetting drive to factory

A PSID (Physical Security ID) revert returns the SSD to factory state if the drive has been configured with PBA. (Note that drives that do not already have PBA installed or disabled will not be restored to factory.)

To perform a PSID revert, you will need the PSID typically printed on the label and may also be in a QR code. Note that some drives' labels will display both a serial and PSID number. May sure to copy the correct one. The PSID is typically much longer than the serial number.

1. Choose the drive you wish to reset.
2. Enter the PSID.



3. Click Save

9.2 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.

9.2.1 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.

9.2.2 Replacing or recovering from a failed primary drive.

4. Shutdown the system.

5. 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**)
6. Boot to the USB thumb drive.
7. 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.**
8. Boot the system.
9. The Login page should indicate Secondary drive(s) found.
10. Log into the PBA administrative console and navigate to the Drives page.
11. 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