



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

Cigent Single and Multidrive PBA Installation Guide and User Manual

Aug 2025
Build 64
PBA Version 1.0.6

1 Table of Contents

2 Introduction	3
1 Initial Installation	4
1.1 Initial installation overview	4
1.2 Drive installation	4
1.3 Configure UEFI and BIOS Settings	4
1.4 Operating System installation	5
1.5	5
1.6 Create a bootable USB 3.0 thumb drive	5
1.7 Boot to the USB thumb drive	6
1.8 Install the PBA	7
1.8.1 Primary and Secondary drive overview	7
1.9 Initial login	10
2 Using the Administrative Console	11
2.1 Dashboard	12
2.2 Maintenance	13
2.2.1 Disable PBA	13
2.2.2 Uninstall PBA	14
2.2.3 Erase Entire Disk	15
2.2.4 Reactivate/Activate	16
2.3 Users	18
2.3.1 Authentication options and requirements	19
2.3.2 Add User	20
2.3.3 Edit User	21
2.3.4 Remove User	21
2.4 Drives	22
2.4.1 View protected drives	23
2.4.2 Remove Secondary drive(s)	23
2.4.3 Add Secondary drive(s)	25
2.4.4 Import Secondary drive(s)	26
2.5 Settings	30
2.5.1 Settings - Login	30
2.5.2 Settings - Password	32
2.5.3 Settings - Other	32
3 Reinstallation of the Cigent PBA	34
4 Re-enabling the Cigent PBA	37
5 Updating the Cigent PBA software	37
6 User Self Enrollment	38

6.1 User Self Enrollment using Smart card	39
6.2 User Self Re-enrollment using Smart card	40
7 Logging in and Logging Out	42
7.1 Logging in with a username and password	42
7.2 Logging in with a Smart card	43
7.3 Logging in with a Security Key	43
7.4 Logging in with Two Factor Authentication	45
7.5 Logging out of the PBA Administrative console	46
8 Troubleshooting	47
8.1 Replacing or recovering from a drive failure	47
8.1.1 Replacing or recovering from a failed secondary drive.	47
8.1.2 Replacing or recovering from a failed primary drive.	47

Known Issues

1. 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.

1 Initial Installation

1.1 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.

1.2 Drive installation

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

1.3 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.

1.4 Operating System installation

Install any operating system or virtual machines.

1.5

1.6 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.exe -l` (This will list available drives. Note the physical drive number.)
5. Run `PBALoader.exe -d \\.\PHYSICALDRIVE1 -load pba_v1.0.6.55.bin`

Optional Parameters

- a. `-alt` (Enables access to additional authentication methods of security key and TPM)
- b. `-raid` (Add this option if the host has more than 5 drives to be protected or some of the drives are connected to a supported RAID controller)
- c. `-open` (Forces the PBA to be loaded on a drive without provisioning the drive (the MBR data is just written to the beginning of the drive). This is used for systems that won't boot a locked drive (even if the MBR shadow is showing and it should be able to boot it).

Notes using -open parameter:

- The drive will NOT be protected in any way, but it will also not contain any critical data as the database will still be stored on one of the secondaries.
- Only drives without partitions will be allowed as open primaries.

- The install process will overwrite the first 256MiB of the drive.
- Open primaries that are erased will not fully erase, only the first 256MiB will be overwritten.

EXAMPLE USAGE with -open parameter:

1. Install 2 drives in the system
2. Install an OS on one of the drives
3. Create installer USB
 - a. `pbaloader.exe -d \\.\PHYSICALDRIVE1 -load pba_v1.0.6.64.bin -open -raid`
4. Boot to PBA installer drive
5. Load PBA
 - a. Select the non-OS drive as the open primary (beginning of drive must be erased or no partitions must be present)
 - b. Select the OS as a secondary
 - c. Complete the install
6. Reboot into uefi
7. Set boot order: put OS before open primary

Note: This is important because the open primary will ALWAYS boot (unlike the normal shadow MBR which hides its boot data after login)
8. Follow steps in Section 3.8

Note: The custom_pba_v1.0.6.53.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.

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

1.7 Boot to the USB thumb drive

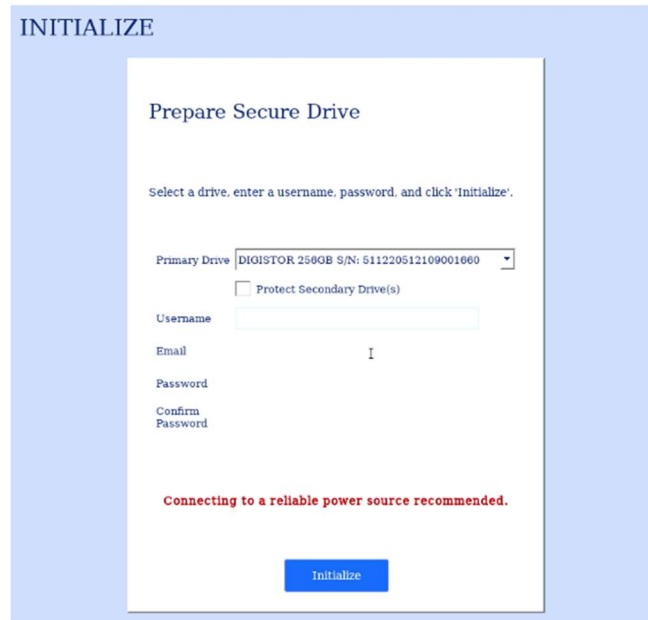
1. Ensure the power is turned off.
2. Insert the bootable USB thumb drive into the computer with the Cigent Secure SSD.
3. Turn on the computer and press the appropriate key for your computer to display the boot menu. The typical keys are F1, F2, F10, F12 or Esc.
4. Choose the USB thumb drive from the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

1.8 Install the PBA

1.8.1 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.



The screenshot shows a web-based interface titled "INITIALIZE" with a sub-header "Prepare Secure Drive". Below the sub-header, there is a instruction: "Select a drive, enter a username, password, and click 'Initialize'." The form includes a "Primary Drive" dropdown menu currently showing "DIGISTOR 250GB S/N: 511220512109001060". There is a checkbox labeled "Protect Secondary Drive(s)" which is currently unchecked. Below these are input fields for "Username", "Email", "Password", and "Confirm Password". A red warning message at the bottom states "Connecting to a reliable power source recommended." and a blue "Initialize" button is at the very bottom.

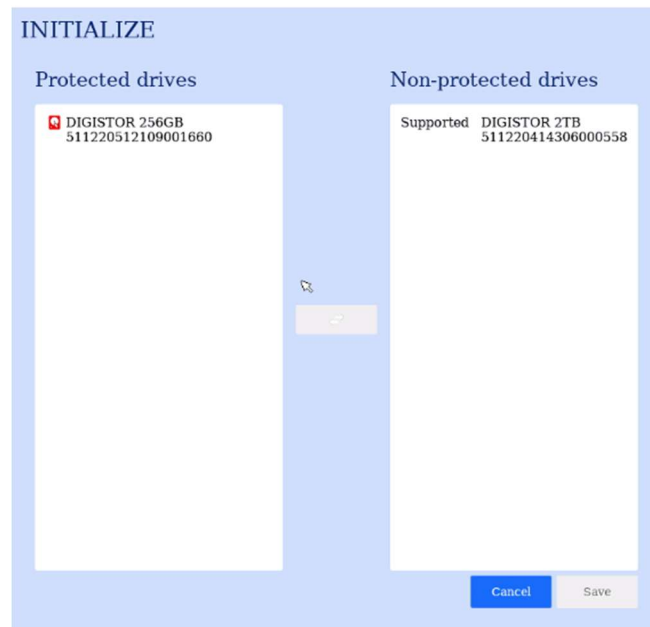
2. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will boot.
3. On a system with more than one drive:
 - a. Select a primary drive. The primary drive is the location the PBA software will be installed and from which the system will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

NOTE:

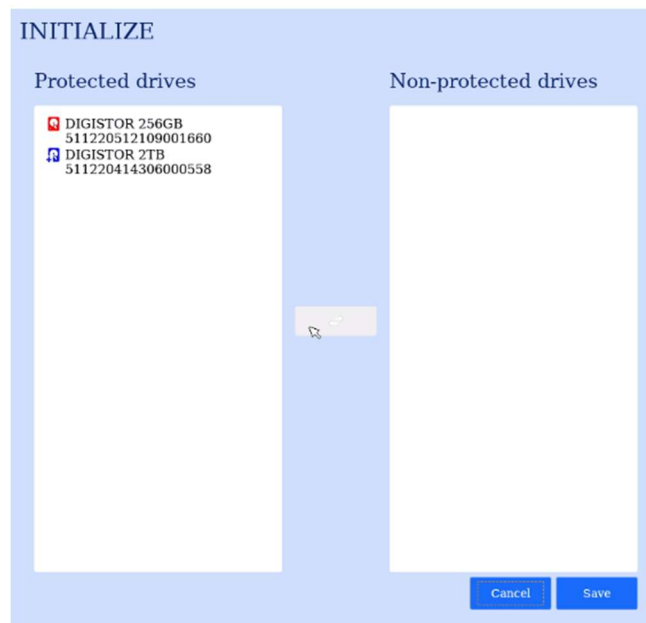
- When loading the PBA using a loader created with the -open flag, select the desired open primary as the main drive and select the other drives to protect as secondaries. Note that the first secondary in the list is the one that will hold the database.

- 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.

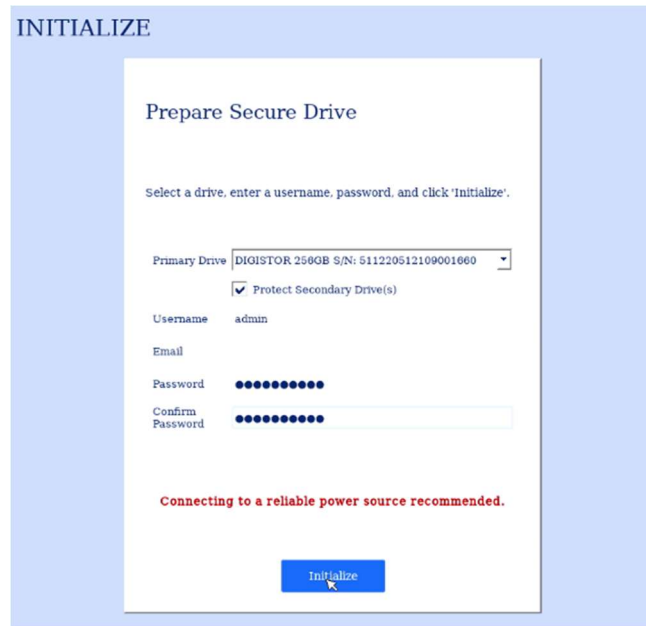


- c. Select drives from the Non-protected drives list and click the double arrow button to move them to Protected drives.



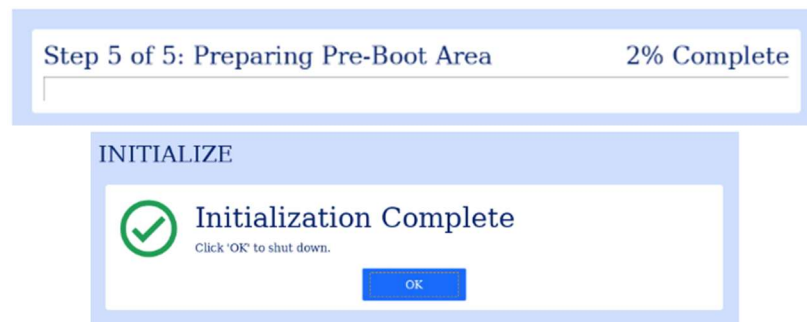
- d. Select the secondary drives to protect and click Save.

4. Enter a username, email (optional) and password. (See Username and Password Requirements in Add User section for details.)
5. Then click Initialize/Update (NOTE: Update is applicable when upgrading during activation.)



The screenshot shows a window titled "INITIALIZE" with a sub-header "Prepare Secure Drive". Below this, it says "Select a drive, enter a username, password, and click 'Initialize'." There is a dropdown menu for "Primary Drive" showing "DIGISTOR 250GB S/N: 511220512109001060". A checkbox labeled "Protect Secondary Drive(s)" is checked. Below these are input fields for "Username" (containing "admin"), "Email", "Password" (masked with dots), and "Confirm Password" (also masked with dots). A red message at the bottom states "Connecting to a reliable power source recommended." and a blue "Initialize" button is at the bottom right.

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



The top part of the screenshot shows a progress bar labeled "Step 5 of 5: Preparing Pre-Boot Area" with "2% Complete" on the right. Below this is another window titled "INITIALIZE" with a green checkmark icon and the text "Initialization Complete". It also says "Click 'OK' to shut down." and has a blue "OK" button at the bottom.

Once complete, power off the computer.

Your PBA is now installed and ready for use.

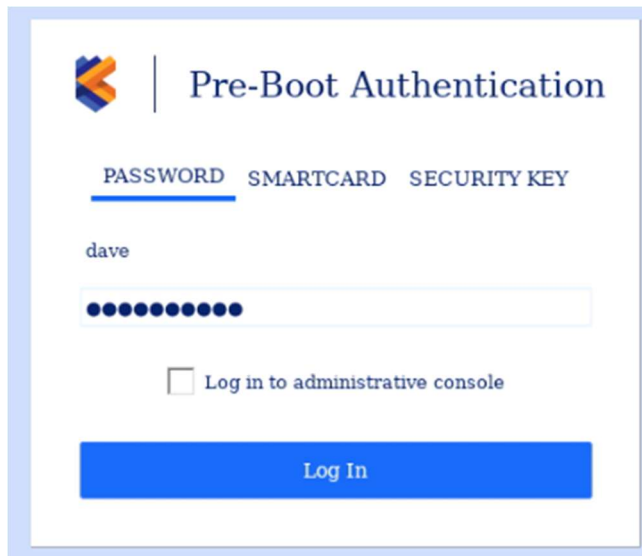
Remove the USB thumb drive and power up the system.

NOTE:

1.9 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.

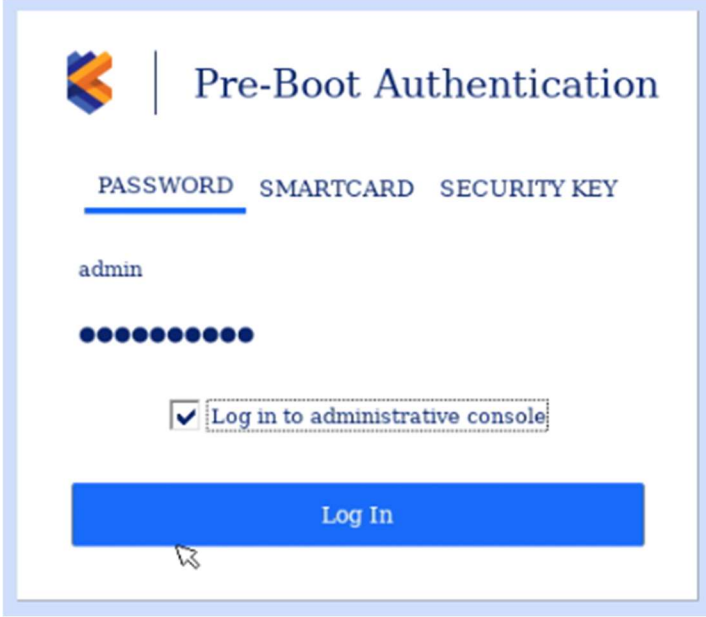
The image shows a Pre-Boot Authentication (PBA) login screen. At the top left is a logo consisting of three interlocking geometric shapes in blue, orange, and yellow. To the right of the logo is the title "Pre-Boot Authentication". Below the title are three tabs: "PASSWORD", "SMARTCARD", and "SECURITY KEY". The "PASSWORD" tab is selected and underlined. Below the tabs, the username "dave" is entered in a text field. Below the username is a password field represented by a series of black dots. Below the password field is a checkbox labeled "Log in to administrative console". At the bottom of the screen is a large blue button labeled "Log In".

For details on how to log in to the administrative console, see section [Using the Administrative Console](#).

2 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.



The image shows a Pre-Boot Authentication (PBA) login screen. At the top left is a logo consisting of three stylized 'C' shapes in blue, orange, and yellow. To the right of the logo is the text "Pre-Boot Authentication". Below this, there are three tabs: "PASSWORD", "SMARTCARD", and "SECURITY KEY". The "PASSWORD" tab is selected and underlined. Under the "PASSWORD" tab, the username "admin" is entered. Below the username is a password field represented by ten black dots. Below the password field is a checkbox that is checked, with the text "Log in to administrative console" next to it. At the bottom of the form is a large blue button labeled "Log In". A mouse cursor is pointing at the bottom left corner of the "Log In" button.

2.1 Dashboard

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

The screenshot displays the PBA administrative dashboard with a dark blue header containing navigation links: DASHBOARD, MAINTENANCE, USERS, DRIVES, SETTINGS, and HELP. The main content area is divided into three sections:

- Activity Log:** A table listing recent activities in descending time order. Each entry includes a timestamp, a user icon, the user name, and the action performed.

Timestamp	User	Action
08-09 10:26	admin	Log in successful
08-08 17:28	admin	Logged out
08-08 15:45	admin	Log in successful
08-08 15:38	admin	Logged out
08-08 15:38	admin	Modified user admin
08-08 15:37	admin	Deleted user user2
08-08 15:37	admin	Deleted user user1
08-08 15:37	admin	Log in successful
08-08 15:21	admin	Logged out
08-08 13:56	admin	Log in successful
08-07 20:23	admin	Logged out
08-07 17:06	admin	Added user user2
08-07 17:05	admin	Added user user1
08-07 14:26	admin	Log in successful
08-07 14:25	admin	Logged out
08-07 14:25	admin	Log in successful
08-07 13:42	admin	Logged out
08-07 13:41	admin	Log in successful
- Activity Summary (Last 7 days):** A summary box showing statistics for the last 7 days: Logins: 7, Failed Logins: 0, User Additions: 2, User Edits: 1, and User Deletions: 2. It includes a document icon with a checkmark.
- Installation Overview:** A box showing system information: Current version: v1.0.6.26, Protected drives: 2, Total Users: 1, and License: Perpetual. It includes a shield icon.

A "Purge Logs" button is located at the bottom of the Activity Log section.

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.

2.2 Maintenance

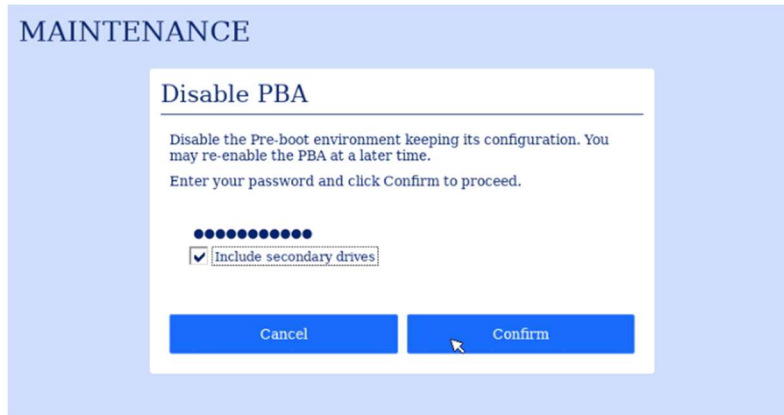
The maintenance page allows administrators to uninstall the PBA environment, disable the PBA, and completely erase the drive.



2.2.1 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.

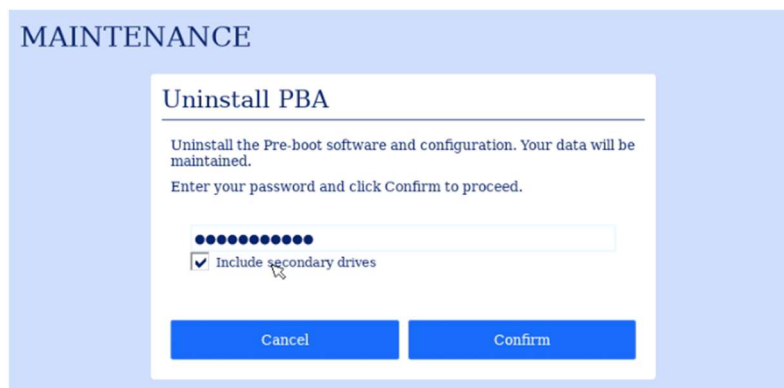


1. Click *Disable PBA*.
2. Enter your administrator password.
3. Click *Confirm*.

2.2.2 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.



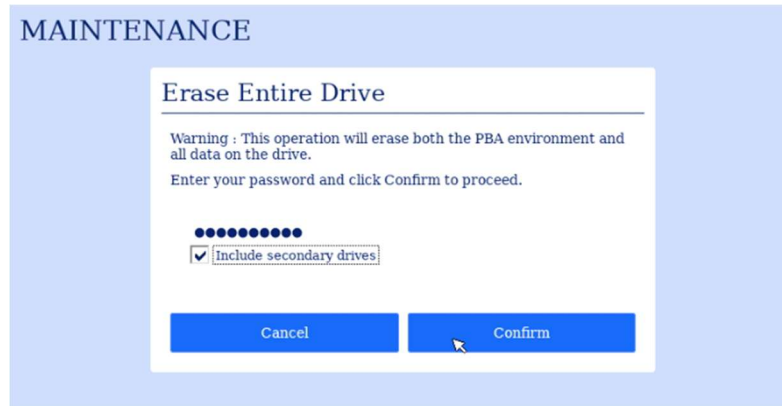
1. Click *Uninstall PBA*.
2. Enter your administrator password.
3. Click *Confirm*.

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

2.2.3 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.

2.2.4 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 being supported, however the PBA will continue to function normally.



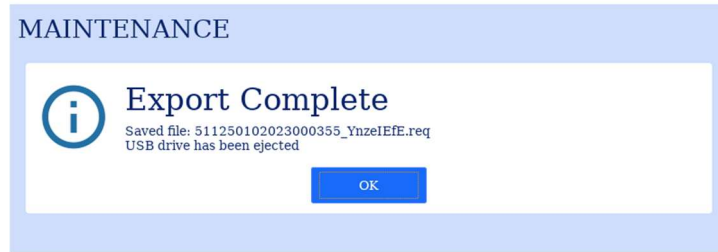
If additional secondary drives or RAID support is required a license key will need to be requested using the license activation process.

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.

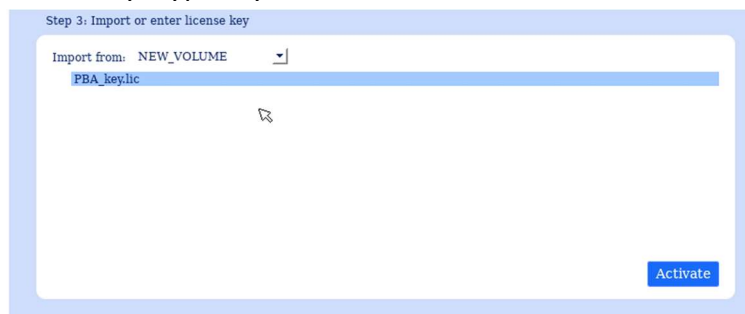
1. Insert the USB drive.
2. Click Reactivate

A light blue dialog box titled "MAINTENANCE". It contains three steps for license activation. Step 1, "Copy or Save request code to USB storage", shows the "Drive Serial: 511250102023000355" and a "Request Code" (a long alphanumeric string). Below the request code is a "Save to:" field with "NEW_VOLUME" selected and a "Save" button. Step 2, "Use request code in the license key request (contact supplier)", is empty. Step 3, "Import or enter license key", has an "Import from:" dropdown menu with "<Select a Device>" selected and an "Activate" button. At the bottom right is a "Cancel" button.

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.

2.3 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

2.3.1 Authentication options and requirements

Each PBA user can be configured with three different authentication options including password, smart card and security key. Password is always required. Smart card and security key authentication are optional. As of this release, only Smart card can be used for a two-factor authentication setup (requiring both a password and smart card 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

Smart card

Any smart card or device supporting NIST SP 800-73-4 – *Interfaces for Personal Identity Verification* or ISO/IEC 7816 are supported. This includes Common Access Cards (CACs), SIPR tokens 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 a PIN. The PIN is setup separately from the PBA.

To add a smart card 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.

2.3.2 Add User

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

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 Smart card or Security Key if your device is not listed after inserting the card or key.

2.3.3 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

USERS

Edit User

Username: user1

Administrator: No ☐ Yes ☐

Email:

New Password: No Change

Confirm Password: No Change

Smart Card: ☐ Add ☒ No Change

Security Key: ☒ Add ☐ No Change

Security Key: Swissbit iShield Key Pro

☒ Auto ☐ Touch ☐ PIN

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.

2.3.4 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.

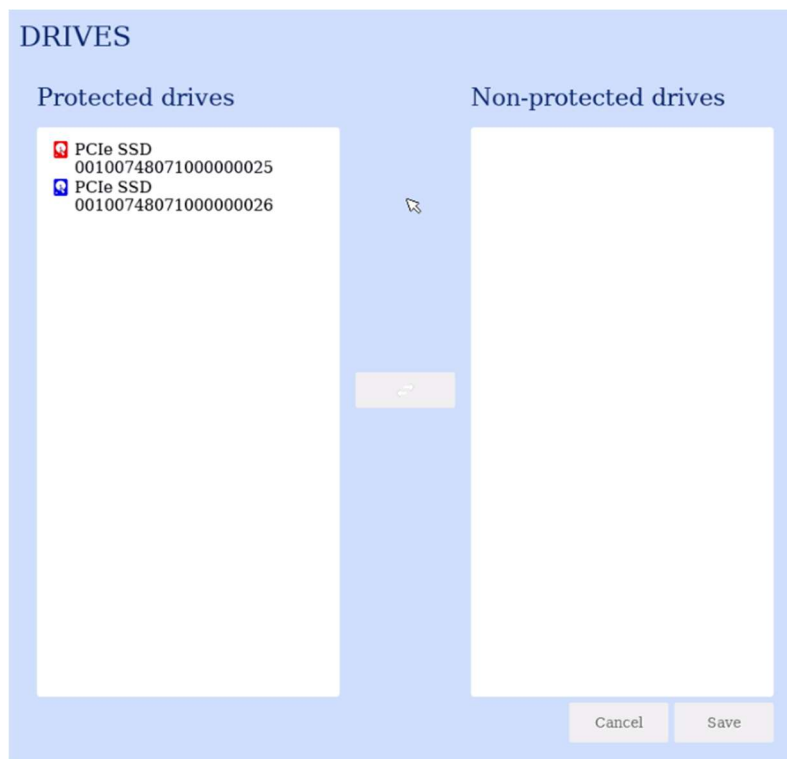


2.4 Drives

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.

2.4.1 View protected drives

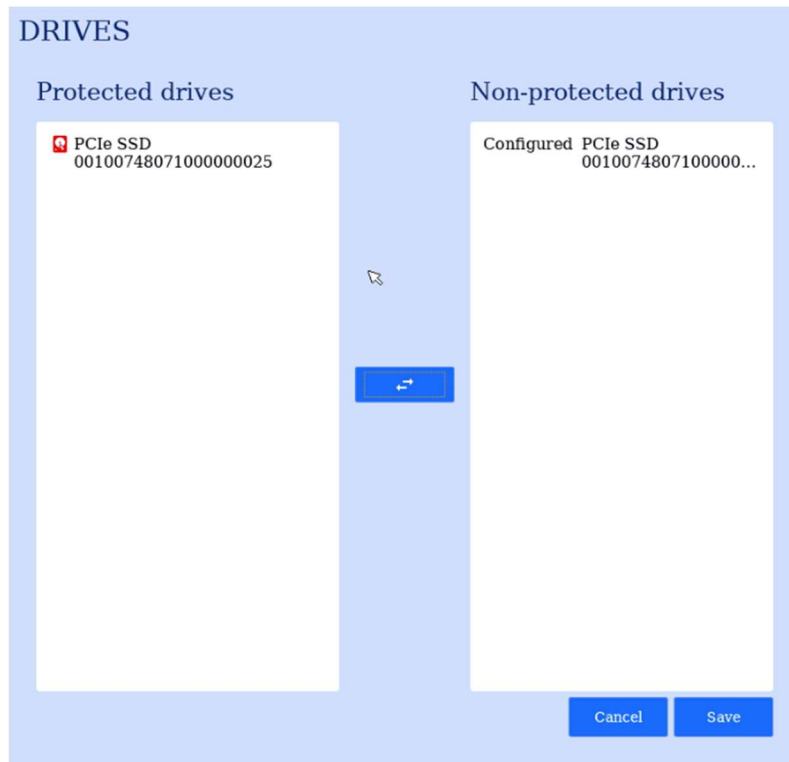
The *Protected drives* column shows details of the drives under the protection of PBA including model number and serial number. The primary drive is indicated with a red icon and all secondaries, if present, are blue. The *Non-protected drives* column shows drives recently removed from protection or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



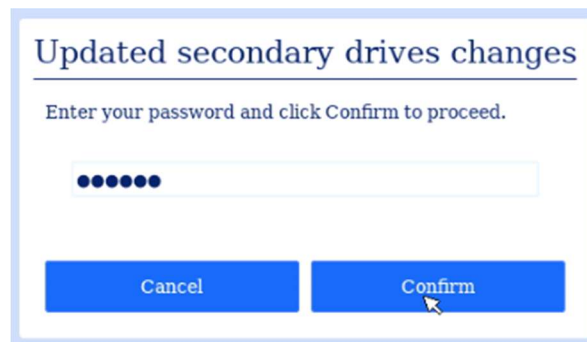
2.4.2 Remove Secondary drive(s)

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.



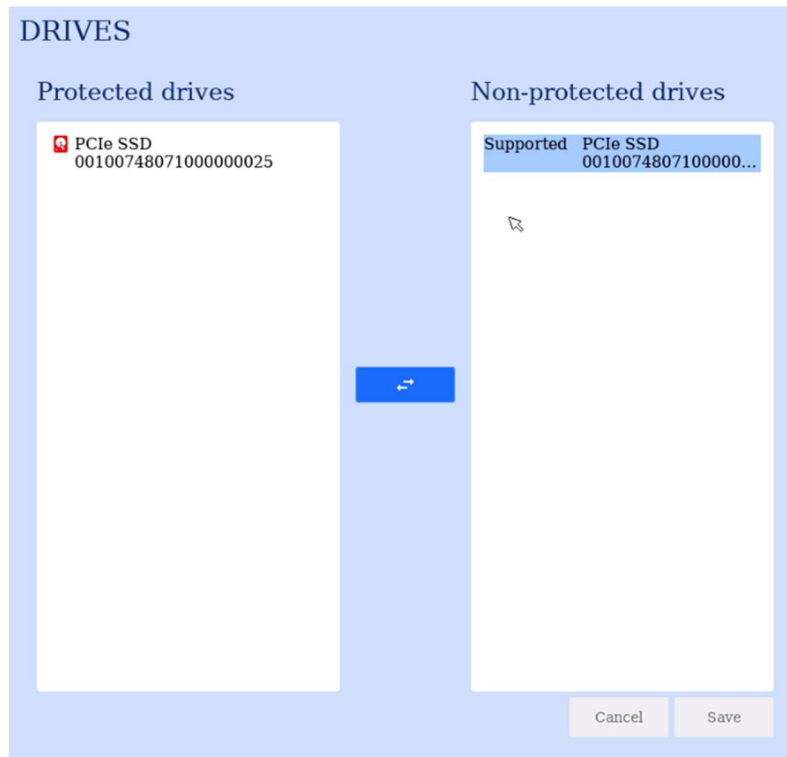
The drive will now show as Supported indicating it is no longer protected but could be added to the protected drives list.



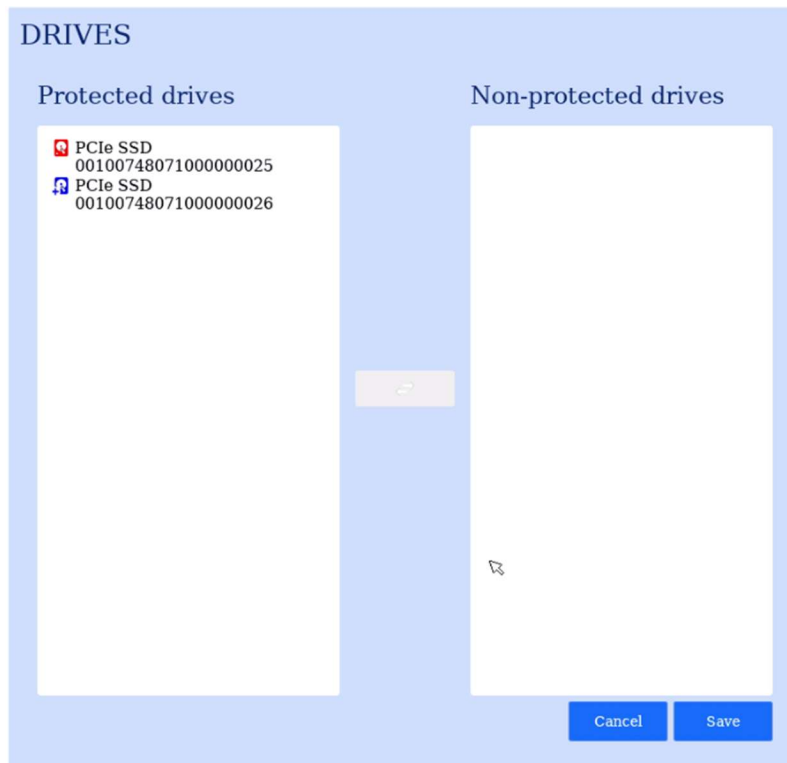
2.4.3 Add Secondary drive(s)

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

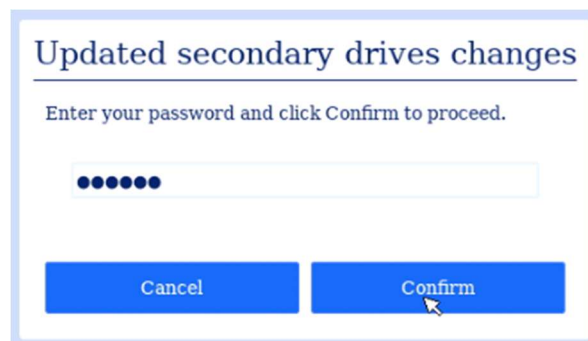
1. Select one or more drives shown as Supported from the Non-Protected column.



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



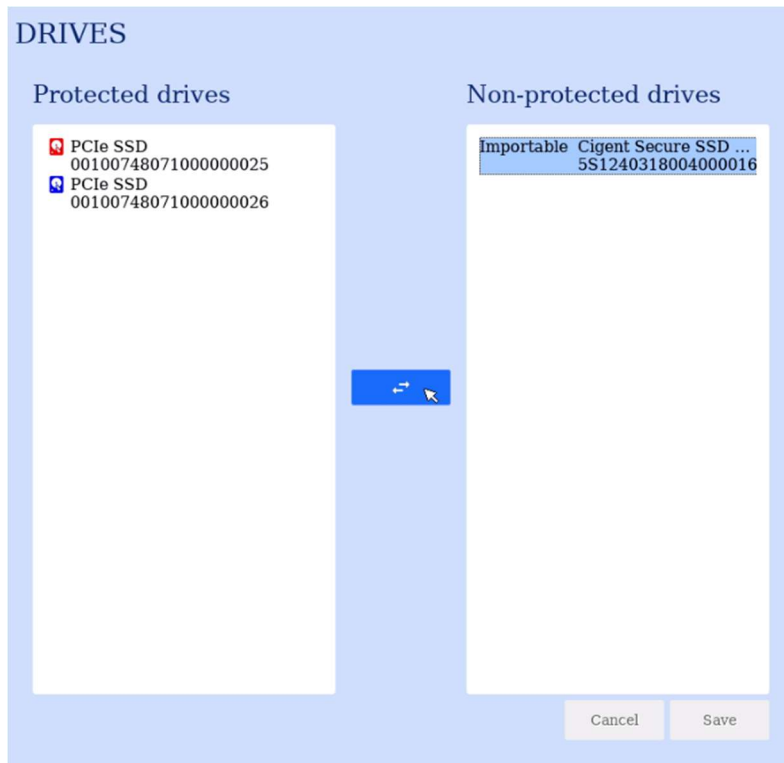
3. Click Save.
4. Enter your password and click Confirm.



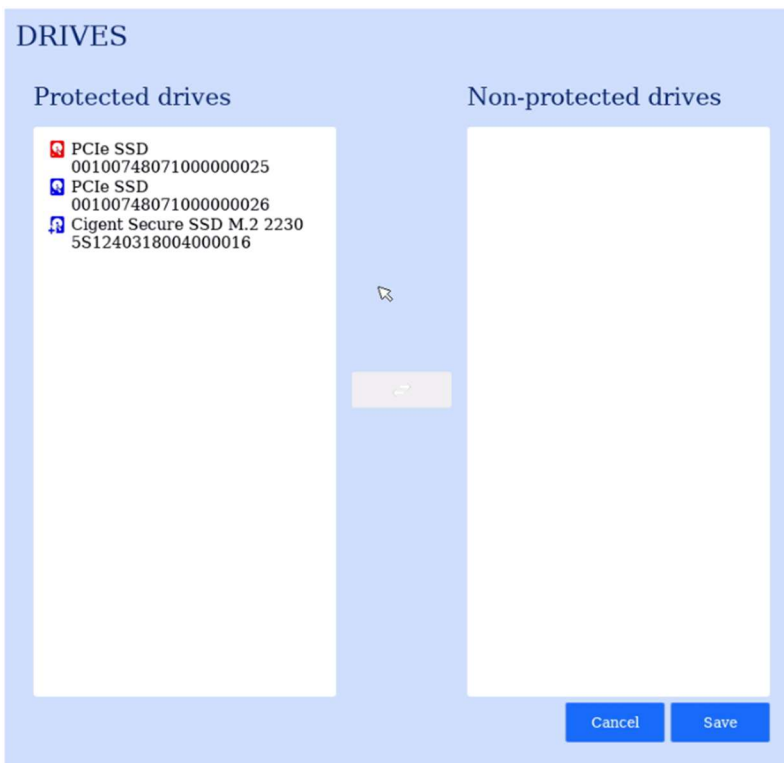
2.4.4 Import Secondary drive(s)

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.)

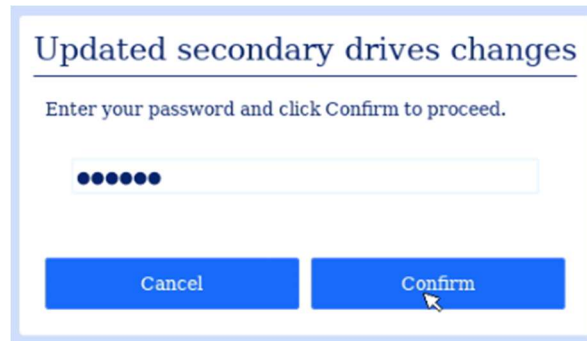
1. Select one or more drives labeled Importable from the Non-protected drive list.



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.



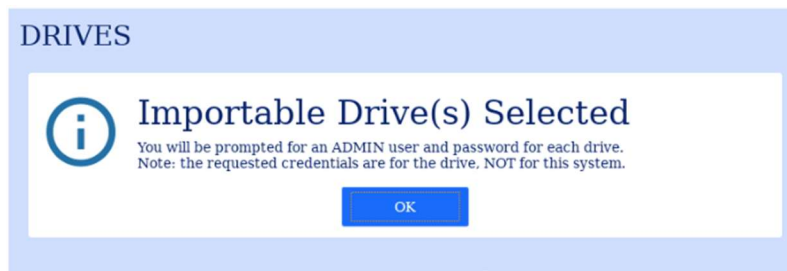
Updated secondary drives changes

Enter your password and click Confirm to proceed.

•••••

Cancel Confirm

5. Click Ok.



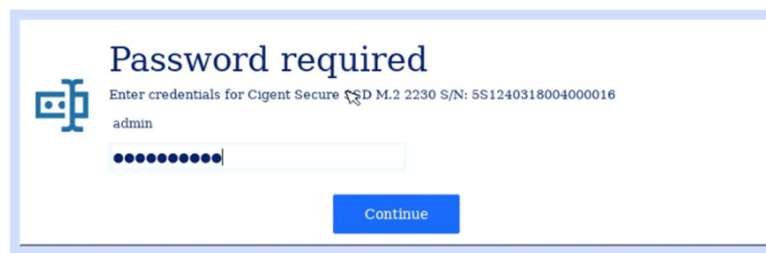
DRIVES

 **Importable Drive(s) Selected**

You will be prompted for an ADMIN user and password for each drive.
Note: the requested credentials are for the drive, NOT for this system.

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.)



 **Password required**

Enter credentials for Cigent Secure SSD M.2 2230 S/N: 5S1240318004000016

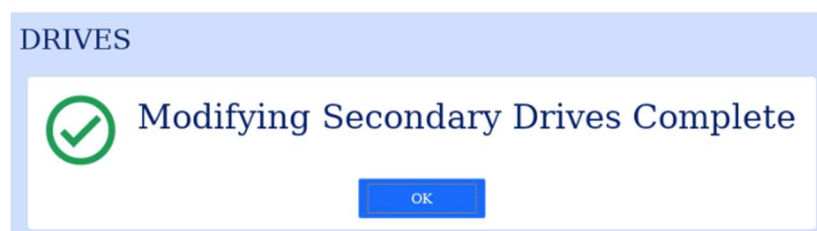
admin

•••••

Continue

7. Click Continue. Repeat for each drive selected.

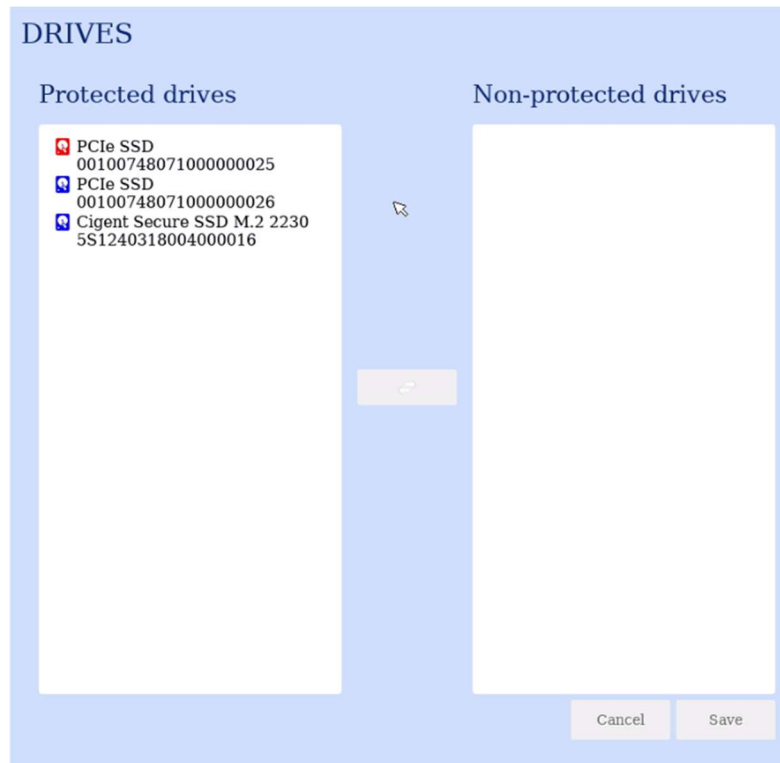
8. Click Ok.



DRIVES

 **Modifying Secondary Drives Complete**

OK



2.5 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.

2.5.1 Settings - Login

SETTINGS

LOGIN PASSWORD OTHER

Failed logins before logout
Maximum login attempts before logout (1-9) 5

Failed logins before erase
Maximum login attempts before drive erasure (0 = disable ; 0-999) 0

Available Authentication Modes

Choose which additional authentication modes can be configured for log in TPM ☐ Security Key ☐ Smart Card ☒

Require multiple forms of authentication
Require both password and additional factor to log in (all users) Disabled

Enable remember me
Allow option on log in screen to remember last user signed in ☐

Failed logins before logout

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: 9

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

Available Authentication Modes

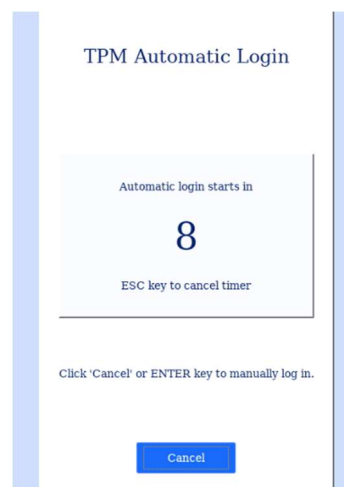
Enable or disable authentication modes that can be used to log in. Password authentication cannot be disabled. Note that access to TPM and Security Key modes is enabled during the

installation or activation processes. Password, smart card and multifactor(password+smart card) are the only common criteria certified modes of authentication.

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.



Security Key

Enable authentication using a FIDO2 U2F device such as Swissbit iShield and Yubikey 5 series.

Smart card

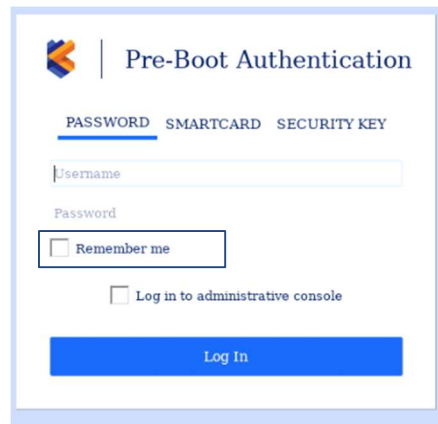
Enable authentication using a smart card.

Require multiple forms of authentication

Require both password and smart card 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 smart card or delete the user first.

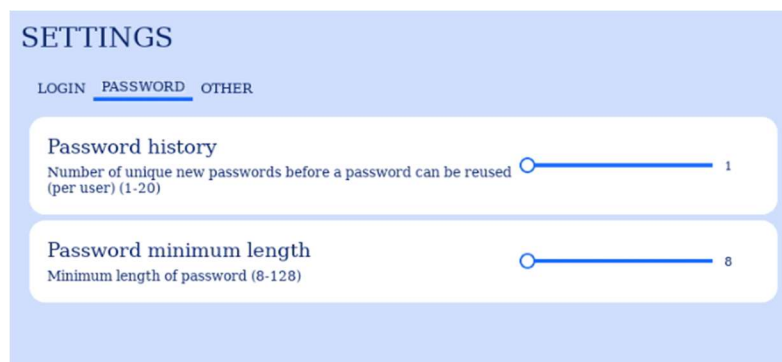
Enable remember me

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.



The image shows the Pre-Boot Authentication (PBA) login screen. It features a logo on the left and the title 'Pre-Boot Authentication' on the right. Below the title are three tabs: 'PASSWORD' (selected), 'SMARTCARD', and 'SECURITY KEY'. The 'PASSWORD' tab contains a 'Username' input field, a 'Password' input field, a 'Remember me' checkbox, and a 'Log in to administrative console' checkbox. A blue 'Log In' button is at the bottom.

2.5.2 Settings - Password



The image shows the 'SETTINGS' screen with the 'PASSWORD' tab selected. It contains two settings:

- Password history**: Number of unique new passwords before a password can be reused (per user) (1-20). The slider is set to 1.
- Password minimum length**: Minimum length of password (8-128). The slider is set to 8.

Password history

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

Min: 1 Max: 20

Password minimum length

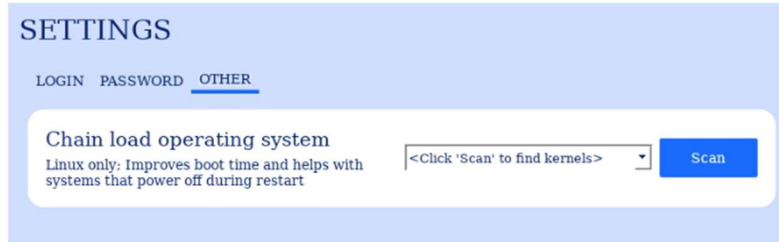
The minimum password length required for each user. The requirement will be enforced the next time an existing user changes their password or a new user is added.

Min: 1 Max: 128

2.5.3 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.



The screenshot shows a web-based settings interface with a light blue background. At the top, the word "SETTINGS" is displayed in a dark blue, serif font. Below it, there are three tabs: "LOGIN", "PASSWORD", and "OTHER", with "OTHER" being the active tab and underlined. The main content area is a white rounded rectangle. It features the title "Chain load operating system" in a bold, dark blue font. Below the title is a smaller line of text: "Linux only: Improves boot time and helps with systems that power off during restart". To the right of this text is a dropdown menu with the placeholder text "<Click 'Scan' to find kernels>". Further to the right is a blue button with the word "Scan" in white text.

3 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.

INITIALIZE

Prepare Secure Drive

Select a drive, enter a username, password, and click 'Initialize'.

Primary Drive: DIGISTOR 256GB S/N: 511220512109001060

☐ Protect Secondary Drive(s)

Username:

Email:

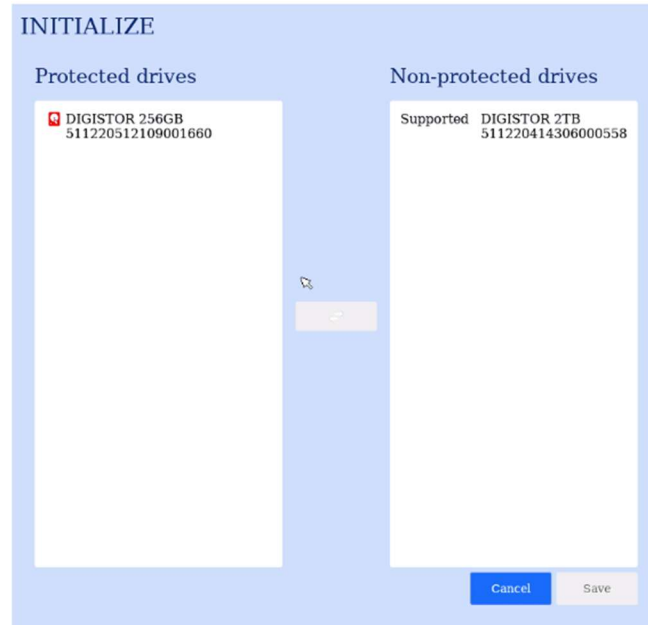
Password:

Confirm Password:

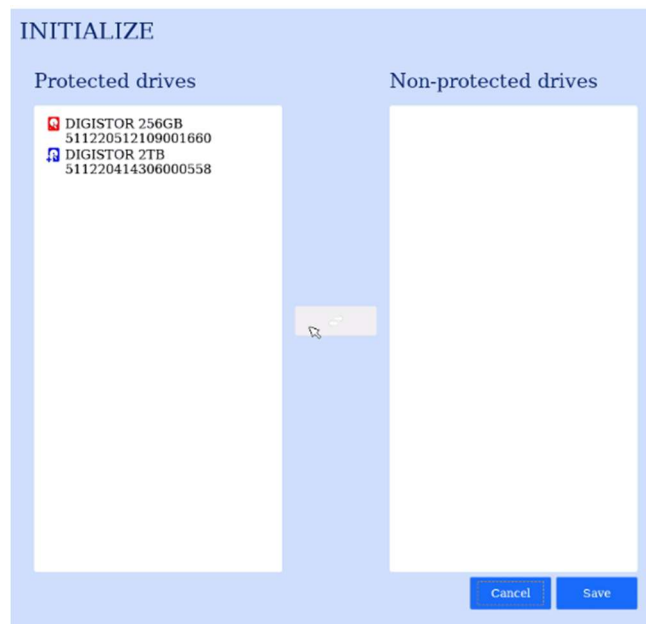
Connecting to a reliable power source recommended.

Initialize

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.

INITIALIZE

Prepare Secure Drive

Select a drive, enter a username, password, and click 'Initialize'.

Primary Drive: DIGISTOR 256GB S/N: 511220512109001660

☒ Protect Secondary Drive(s)

Username: admin

Email:

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Connecting to a reliable power source recommended.

Initialize

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

Step 5 of 5: Preparing Pre-Boot Area 2% Complete

INITIALIZE

 Initialization Complete

Click 'OK' to shut down.

OK

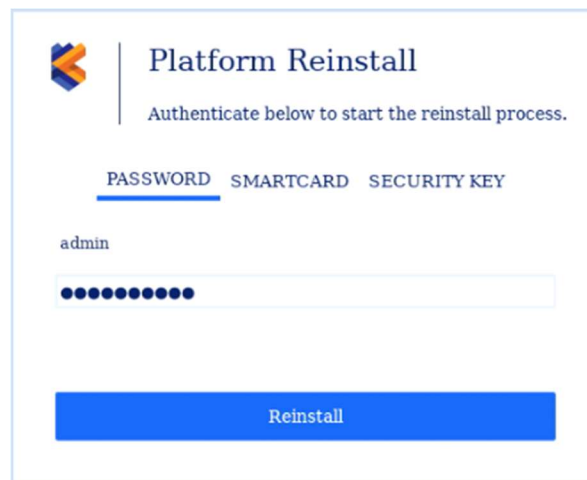
Once complete, power off the computer.
Remove the USB thumb drive from the computer.

4 Re-enabling the Cigent PBA

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

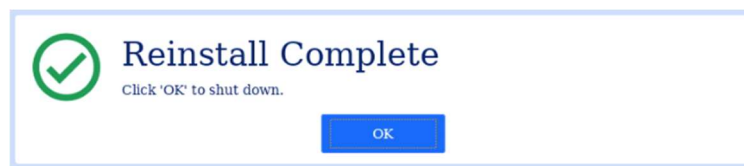
1. An installation USB drive of the same version of Cigent PBA installed on the device
(See section [Create a bootable USB 3.0 thumb drive](#))
2. Administrator credentials to the disabled PBA environment

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.



The screenshot shows a 'Platform Reinstall' window. At the top left is a logo with three colored squares (blue, orange, green). To the right of the logo, the text 'Platform Reinstall' is displayed in a large font, followed by 'Authenticate below to start the reinstall process.' in a smaller font. Below this, there are three tabs: 'PASSWORD', 'SMARTCARD', and 'SECURITY KEY'. The 'PASSWORD' tab is selected and underlined. Under the 'PASSWORD' tab, the username 'admin' is entered, and the password field is masked with 12 black dots. At the bottom of the window is a large blue button labeled 'Reinstall'.

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



The screenshot shows a 'Reinstall Complete' message box. On the left is a green circular icon with a white checkmark. To the right of the icon, the text 'Reinstall Complete' is displayed in a large font, followed by 'Click 'OK' to shut down.' in a smaller font. At the bottom right of the box is a blue button labeled 'OK'.

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

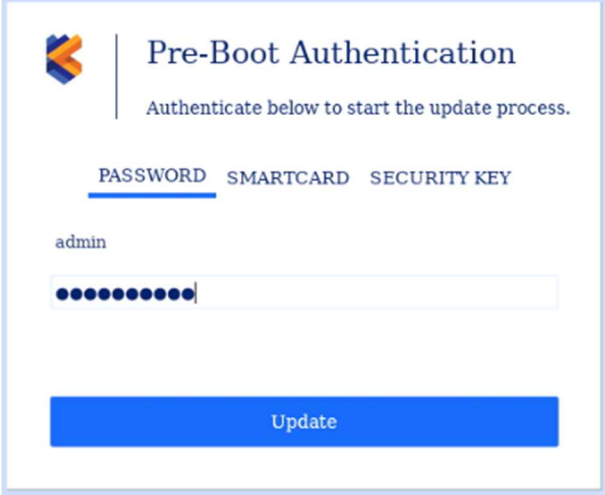
5 Updating the Cigent PBA software

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.

The image shows a 'Pre-Boot Authentication' window. At the top left is a logo consisting of three stylized 'K' shapes in blue, orange, and yellow. To the right of the logo, the title 'Pre-Boot Authentication' is displayed in a large, dark blue font. Below the title, a subtitle reads 'Authenticate below to start the update process.' in a smaller, dark blue font. Underneath the subtitle, there are three tabs: 'PASSWORD', 'SMARTCARD', and 'SECURITY KEY'. The 'PASSWORD' tab is selected and underlined. Below the tabs, the username 'admin' is entered. A password field, represented by a series of black dots, is positioned below the username. At the bottom of the window is a large blue button with the word 'Update' in white text.

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.

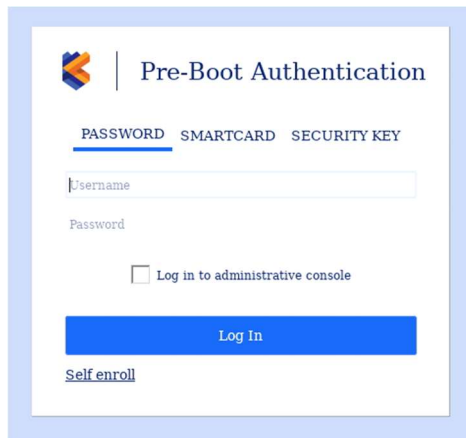
6 User Self Enrollment

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 a enrollment password with a usage quantity and expiration timestamp. See the command line utility help for additional information.

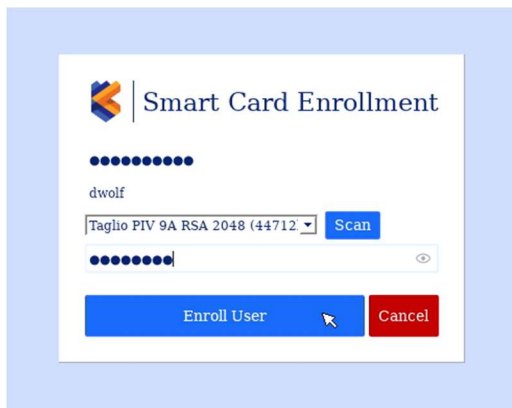
6.1 User Self Enrollment using Smart card

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

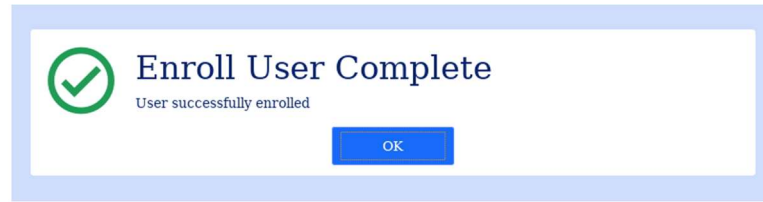
1. Click Self enroll

The image shows the 'Pre-Boot Authentication' login screen. It features a logo on the top left and three tabs: 'PASSWORD', 'SMARTCARD', and 'SECURITY KEY'. The 'PASSWORD' tab is selected. Below the tabs are input fields for 'Username' and 'Password'. There is a checkbox labeled 'Log in to administrative console' and a blue 'Log In' button. At the bottom, there is a link labeled 'Self enroll'.

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

The image shows the 'Smart Card Enrollment' screen. It features a logo on the top left. Below the logo is a series of dots representing a password. There is a text input field containing 'dwolf'. Below that is a dropdown menu showing 'Taglio PIV 9A RSA 2048 (44712)' and a blue 'Scan' button. Below the dropdown is another series of dots representing a PIN. At the bottom, there are two buttons: a blue 'Enroll User' button and a red 'Cancel' button.

3. Click Ok to return to the login page.

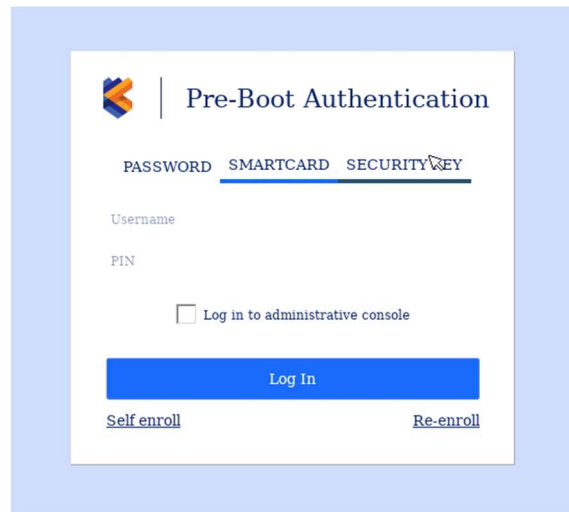


4. The user can immediately login to the PBA using their smart card.

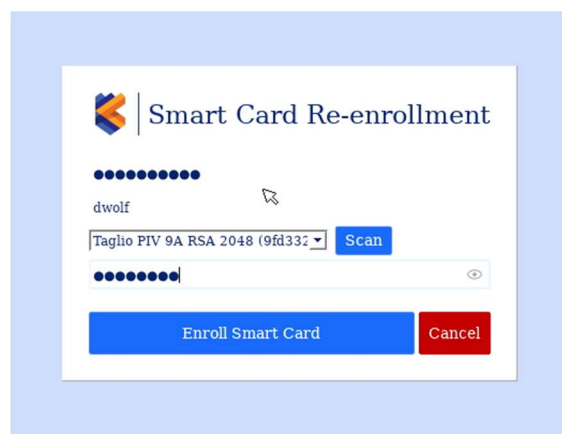
6.2 User Self Re-enrollment using Smart card

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



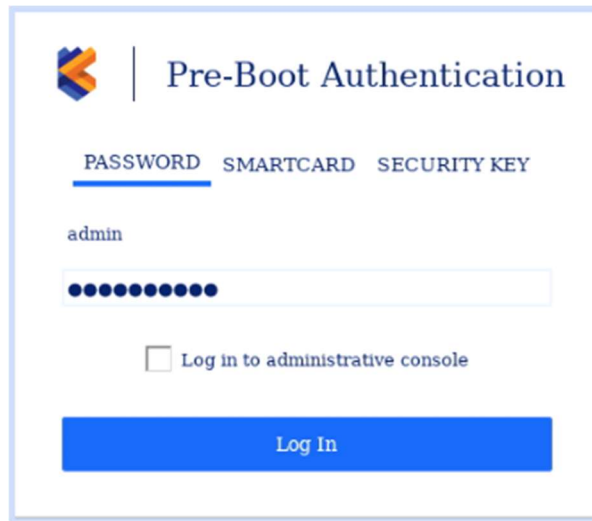
2. Enter the provided enrollment password, your existing username and your new smart card PIN, then click Enroll Smart Card.



7 Logging in and Logging Out

7.1 Logging in with a username and password

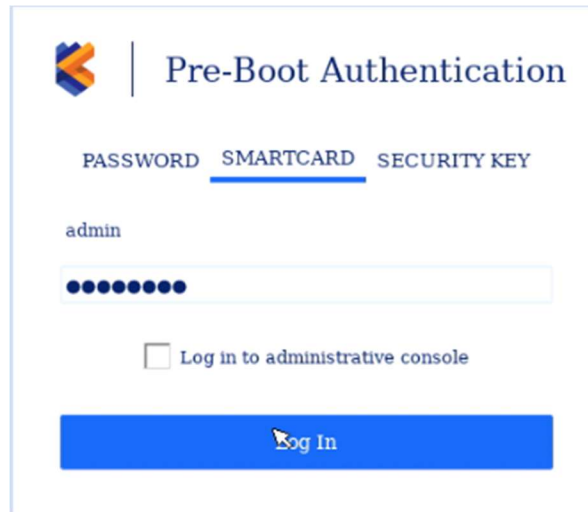
3. Power on the computer and wait for the PBA authentication screen to appear.
4. Enter your username and password.
5. Click Log in.

The image shows a Pre-Boot Authentication (PBA) screen. At the top left is a logo consisting of three stylized, overlapping geometric shapes in blue, orange, and yellow. To the right of the logo is the text "Pre-Boot Authentication". Below this, there are three tabs: "PASSWORD", "SMARTCARD", and "SECURITY KEY". The "PASSWORD" tab is selected and underlined. Under the "PASSWORD" tab, the username "admin" is entered. Below the username is a password field represented by a series of black dots. Below the password field is a checkbox labeled "Log in to administrative console". At the bottom of the screen is a large blue button with the text "Log In" in white.

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

7.2 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.



The image shows a 'Pre-Boot Authentication' window. At the top left is a logo consisting of two overlapping triangles, one blue and one orange. To the right of the logo is the title 'Pre-Boot Authentication'. Below the title are three tabs: 'PASSWORD', 'SMARTCARD' (which is selected and underlined with a blue line), and 'SECURITY KEY'. Under the 'SMARTCARD' tab, the username 'admin' is entered in a text field. Below the text field is a PIN field represented by ten black dots. Below the PIN field is a checkbox labeled 'Log in to administrative console'. At the bottom of the window is a large blue button with a mouse cursor icon and the text 'Log In'.

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

7.3 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

●●●●●●●●

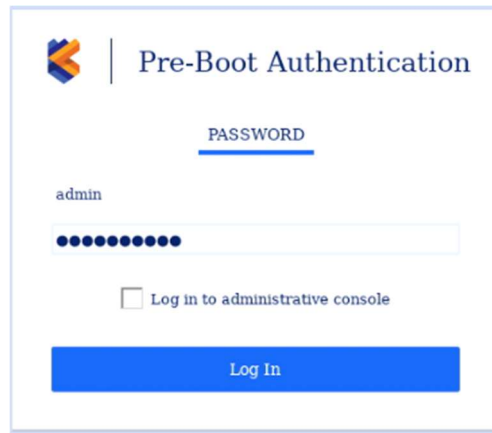
I

☐ Log in to administrative console

Log In

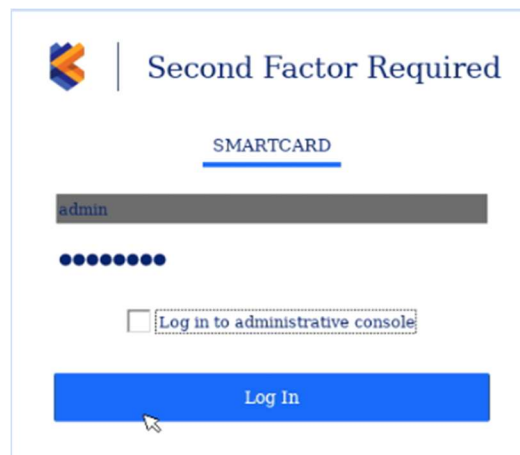
7.4 Logging in with Two Factor Authentication

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



The image shows a 'Pre-Boot Authentication' screen. At the top left is a logo consisting of two overlapping triangles, one blue and one orange. To the right of the logo is the text 'Pre-Boot Authentication'. Below this, the word 'PASSWORD' is underlined. There is a text input field containing the username 'admin'. Below the username field is a password field represented by a series of black dots. Below the password field is a checkbox labeled 'Log in to administrative console'. At the bottom of the screen is a large blue button labeled 'Log In'.

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



The image shows a 'Second Factor Required' screen. At the top left is the same logo as the previous screen. To the right of the logo is the text 'Second Factor Required'. Below this, the word 'SMARTCARD' is underlined. There is a text input field containing the username 'admin'. Below the username field is a PIN field represented by a series of black dots. Below the PIN field is a checkbox labeled 'Log in to administrative console'. At the bottom of the screen is a large blue button labeled 'Log In'. A mouse cursor is pointing at the 'Log In' button.

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

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

7.5 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.

8 Troubleshooting

8.1 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.

8.1.1 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.

8.1.2 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.