



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

Cigent PBA Installation Guide and User Manual

Aug 2023
V21
PBA Version 1.0.6

Table of Contents

1	Introduction	3
2	Initial Installation	4
2.1	Initial installation overview	4
2.2	Drive installation	4
2.3	Configure UEFI and BIOS Settings	4
2.4	Operating System installation	4
2.5	Create a bootable USB 3.0 thumb drive	5
2.6	Boot to the USB thumb drive	5
2.7	Install the Cigent PBA	5
2.8	Initial login	7
3	Using the Administrative Console	8
3.1	Dashboard	9
3.2	Maintenance	10
3.2.1	Uninstall PBA	11
3.2.2	Disable PBA	11
3.2.3	Erase Entire Disk	12
3.3	Users	14
3.3.1	Add User	15
3.3.2	Username and Password Requirements	15
3.3.3	Edit User	16
3.3.4	Remove User	17
3.4	Settings	18
4	Reinstallation of the Cigent PBA	20
5	Re-enabling the Cigent PBA	22
6	Updating the Cigent PBA software	23
7	Logging in and Logging Out	24
7.1	Logging in with a username and password	24
7.2	Logging in with a Smart Card	25
7.3	Logging in with Two Factor Authentication	26
7.4	Logging out of the PBA Administrative console	27

Known Issues

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

1 Introduction

The Cigent Secure SSD is a FIPS-certified, self-encrypting drive (SED). When combined with Cigent's pre-boot authentication (PBA) protects systems 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 both. Users remain authenticated until the drive is powered off.

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

2 Initial Installation

2.1 Initial installation overview

Cigent Secure SSDs contain a small FAT32 partition containing a copy of the Cigent PBA and Cigent Windows software and associated user manuals for your convenience. You can safely delete this partition once you no longer need it. You can always find the latest Cigent PBA software on the Licenses page of the Cigent management console and documentation can be found at <https://www.cigent.com/support>.

2.2 Drive installation

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

2.3 Configure UEFI and BIOS Settings

The following settings need to be set according to the required state prior to installation of the the Cigent PBA software. Each manufacturer and model have unique locations and names for settings.

PC Manufacturer	Bios Setting	Required State
Dell	SATA Operation	AHCI
Lenovo	Block SID Authentication	Disable

2.4 Operating System installation

Install any operating system or virtual machines.

2.5 Create a bootable USB 3.0 thumb drive

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

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

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

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

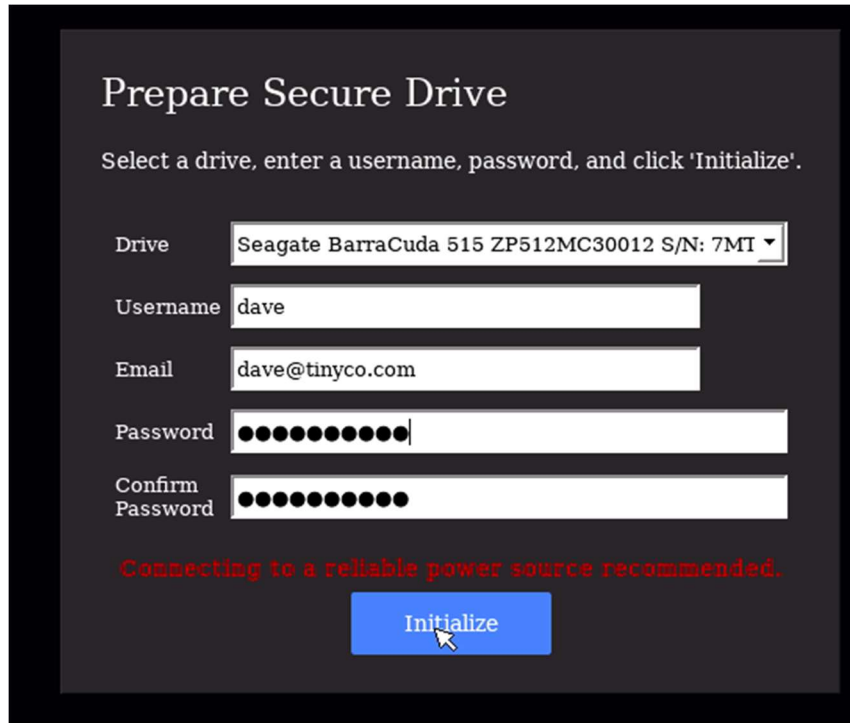
2.6 Boot to the USB thumb drive

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.

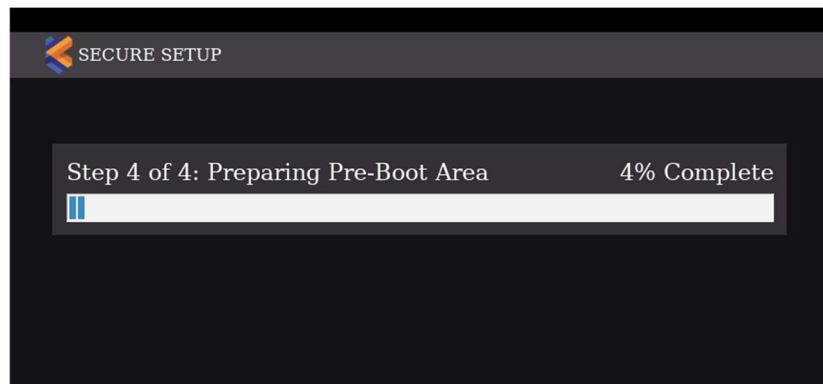
2.7 Install the Cigent PBA

1. The Secure Setup screen will be displayed.
2. If you have more than one internal drive, be sure the Cigent Secure SSD is selected.
3. Enter a username, email (optional) and password. (See Username and Password Requirements in Add User section for details.)

4. Then click Initialize.



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



Once complete, power off the computer.

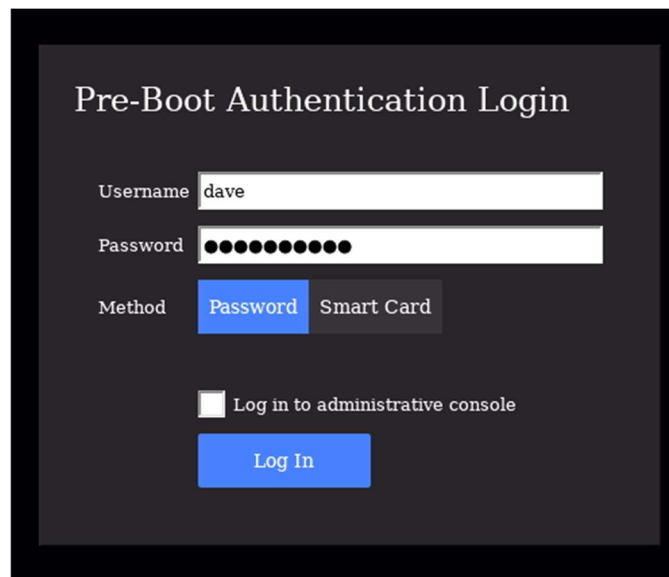
Your Cigent PBA is now installed and ready for use.

Remove the USB thumb drive and power up the system.

2.8 Initial login

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

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



Pre-Boot Authentication Login

Username

Password

Method

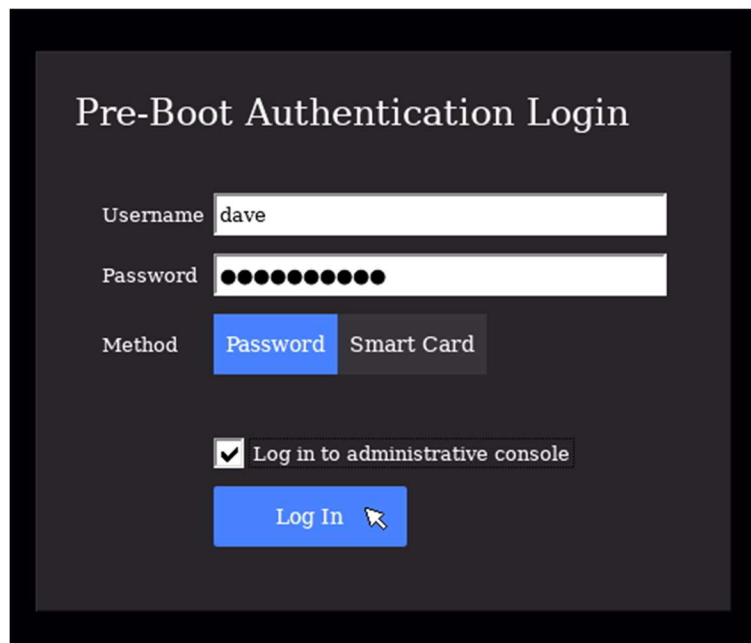
Log in to administrative console

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.

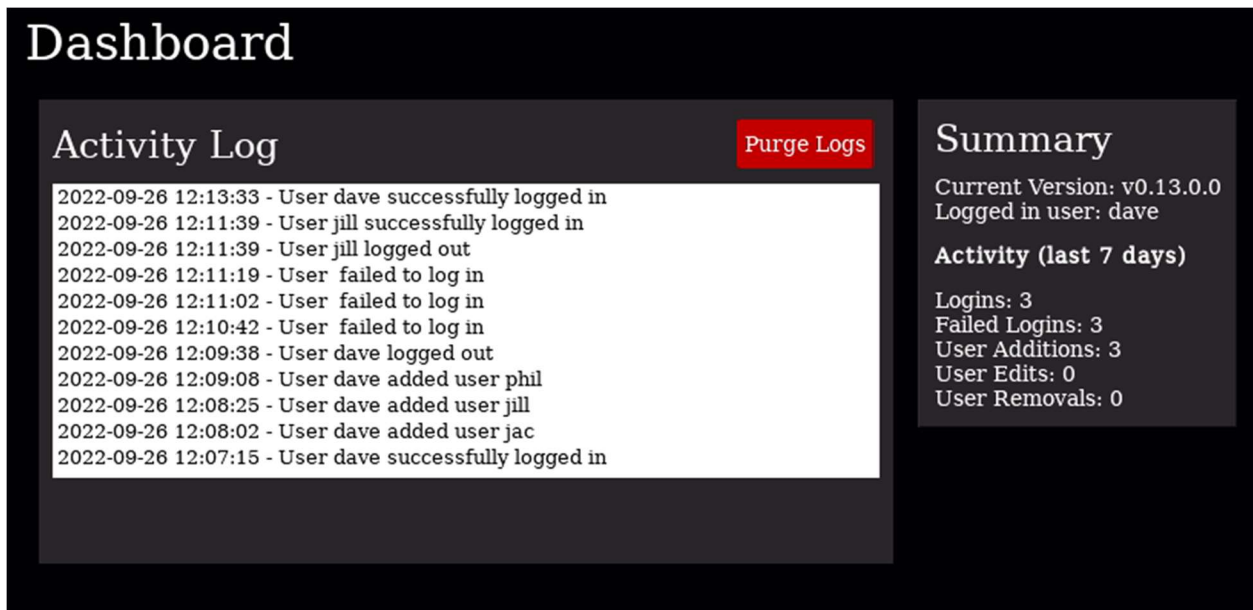
You can enter the administrative console from the login page by checking the “Log in to administrative console” checkbox before clicking Log In.



The screenshot shows a login interface titled "Pre-Boot Authentication Login". It features a dark background with white text and input fields. The "Username" field contains the text "dave". The "Password" field is filled with black dots. Below the password field, there are two buttons for the authentication method: "Password" (highlighted in blue) and "Smart Card" (greyed out). A checkbox labeled "Log in to administrative console" is checked. At the bottom, there is a blue "Log In" button with a mouse cursor pointing to it.

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.

Maintenance

Uninstall PBA
Uninstall pre-boot environment. Your data will be maintained.

Password

Disable PBA
Temporarily disable PBA. May be re-enabled at a later time.

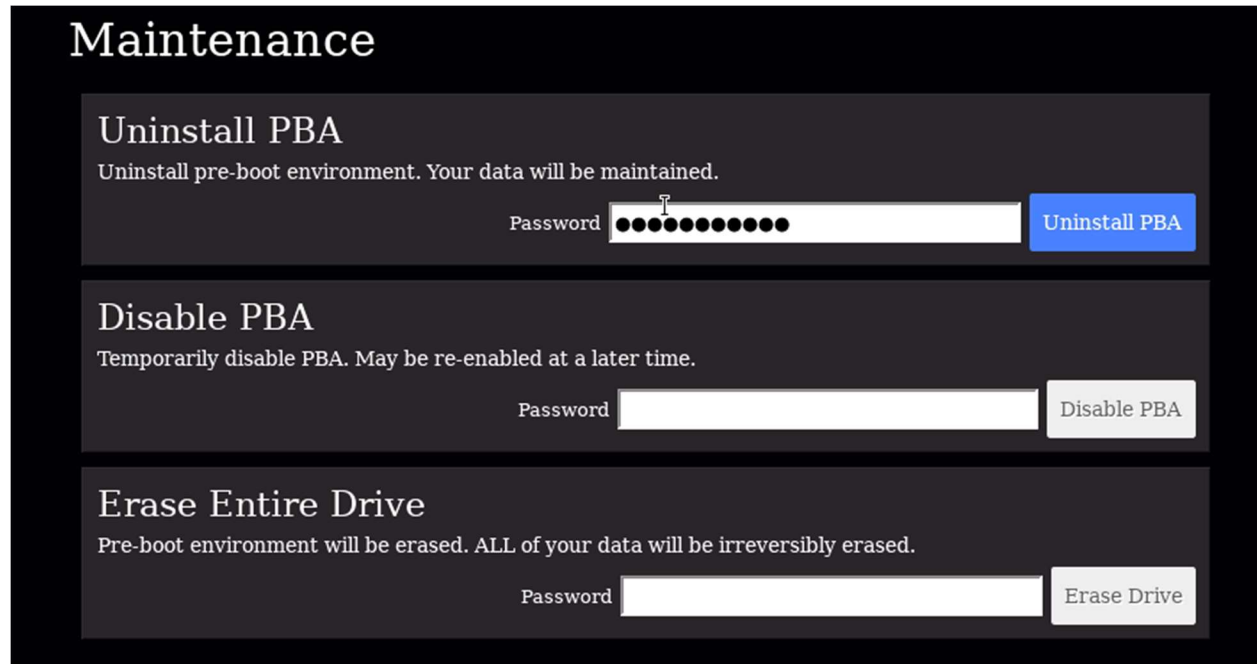
Password

Erase Entire Drive
Pre-boot environment will be erased. ALL of your data will be irreversibly erased.

Password

3.2.1 Uninstall PBA

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

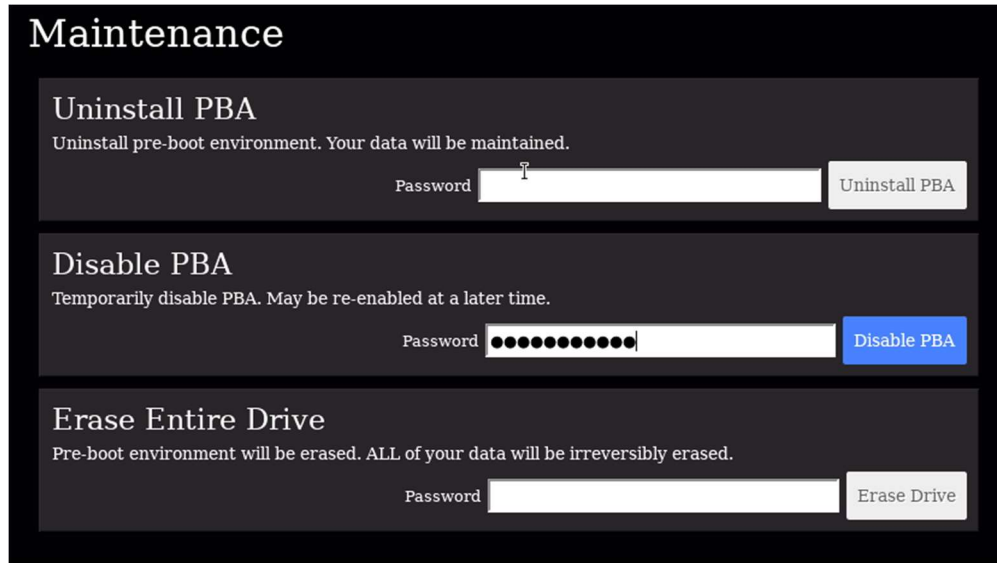


1. Enter your administrator password into the Password field in the Uninstall PBA section.
2. Click Uninstall PBA.

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

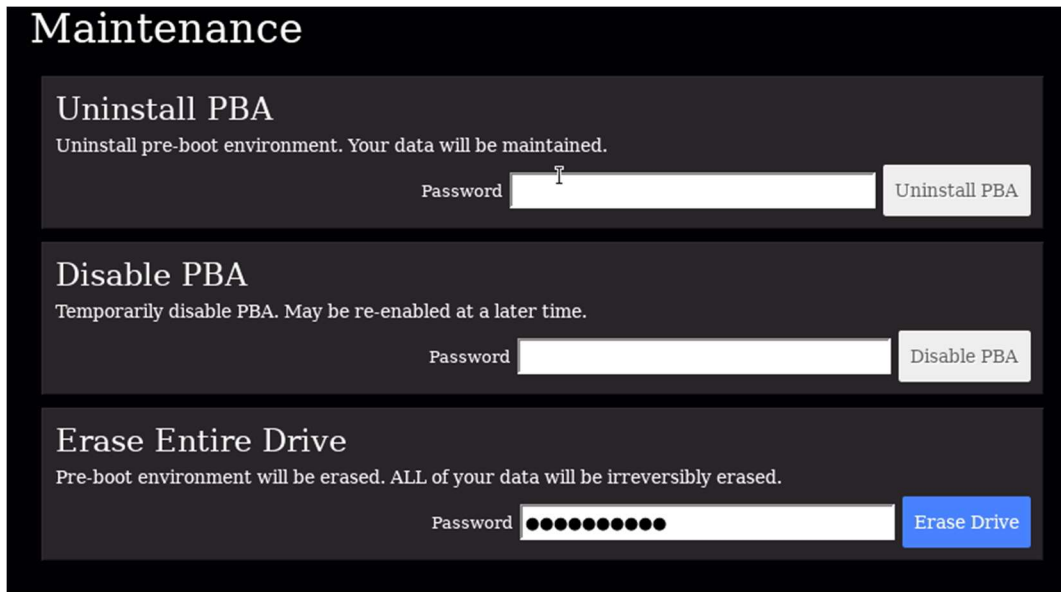
3.2.2 Disable PBA

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.



3.2.3 Erase Entire Disk

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



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.

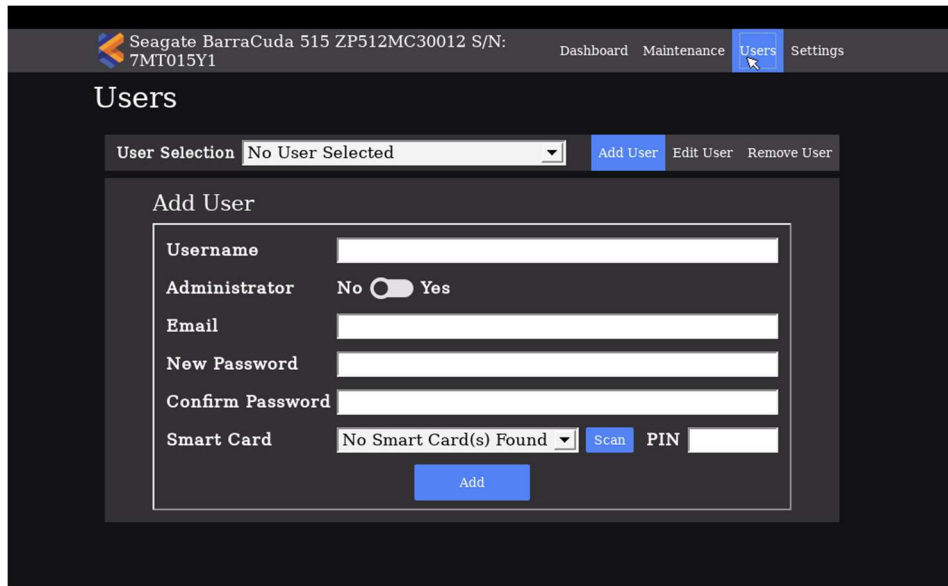
- The Erase Verification firmware feature is used to ensure all mapped and unmapped blocks have been erased.
1. Enter your administrator password in the Erase Entire Drive section
 2. Click Erase Drive.

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

Once complete, power off the system.

3.3 Users

The Users page allows administrators to add, modify, and delete user accounts from the PBA environment.



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

3.3.1 Add User

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

The screenshot shows a web interface titled "Users". At the top, there is a "User Selection" dropdown menu currently showing "No User Selected". To the right of this menu are three buttons: "Add User" (highlighted in blue), "Edit User", and "Remove User". Below this is a section titled "Add User" which contains a form with the following fields:

- Username:** A text input field containing "dave".
- Administrator:** A toggle switch currently set to "No".
- Email:** A text input field containing "dave@tinyco.com".
- New Password:** A password input field with 12 black dots.
- Confirm Password:** A password input field with 12 black dots.
- Smart Card:** A dropdown menu showing "PIV: dave", a blue "Scan" button, and a PIN input field with 12 black dots.

At the bottom center of the form is a blue "Add" button.

3.3.2 Username and 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

1. Enter a unique username.
2. Set the Administrator role as desired.
3. Enter an email address.
4. Enter and confirm a password.
5. Select the smart card from the selection and enter the correct PIN.
6. Click Add.

Note that to Add a Smart Card to a user, the smart card must be inserted and the PIN correctly entered. If you do not see the smart card listed after inserting it, click the Scan button then open the selection list to find your card. Once the card shows in the selection list, enter the PIN before clicking Save.

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

The screenshot shows the 'Users' application interface. At the top, there is a 'User Selection' dropdown menu with 'dave' selected. To the right of the dropdown are three buttons: 'Add User', 'Edit User' (highlighted in blue), and 'Remove User'. Below this is the 'Edit User' form. The form contains the following fields and controls:

- Username:** dave
- Administrator:** A toggle switch set to 'Yes'.
- Email:** dave@tinyco.com
- New Password:** No Change
- Confirm Password:** No Change
- Smart Card:** Radio buttons for 'Add' (selected) and 'No Change'. Below this is a dropdown menu showing 'PIV: dave' and a 'Scan' button.
- PIN:** A field with 10 black dots for entering the PIN.
- Save:** A blue button at the bottom of the form.

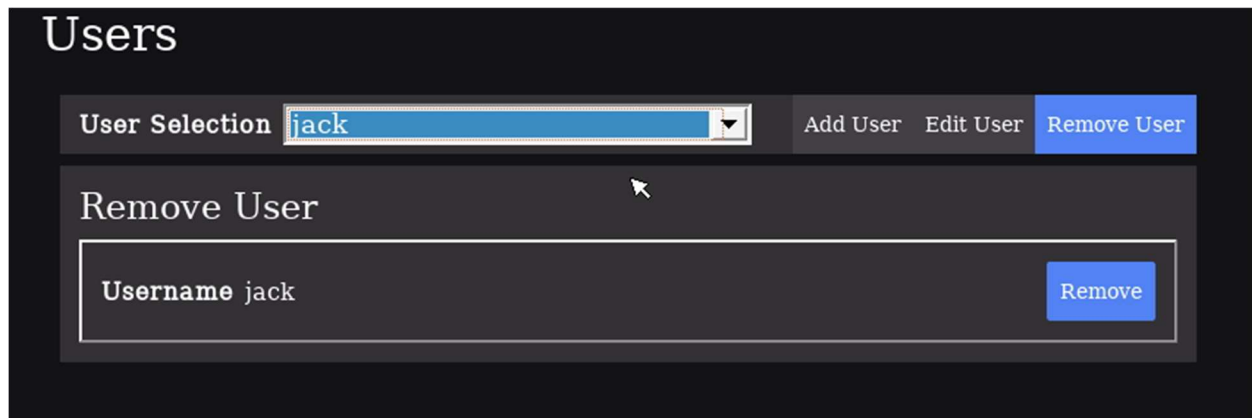
1. Select an existing user from the User Selection list.
2. Change one or more user attributes.
3. Click Save.

Note that to Add a Smart Card to an existing user, the smart card must be inserted and the PIN correctly entered. If you do not see the smart card listed after inserting it, click the Scan button

then open the selection list to find your card. Once the card shows in the selection list, enter the PIN before clicking Save.

3.3.4 Remove User

The Remove User page is used to permanently remove 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 from the User Selection list.
2. Click Remove next to the username.

3.4 Settings

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

The screenshot shows a settings interface with a dark background. At the top left, the word "Settings" is written in white. Below it are five rows of settings, each with a title, a description, a value field, and control buttons. The first row is "Failed Logins Before Lockout" with a value of 5. The second is "Failed Logins Before Erase" with a value of 0. The third is "Password History" with a value of 1. The fourth is "Password Minimum Length" with a value of 8. The fifth is "Require Multiple Forms of Authentication" with a toggle switch set to "No". A "Save" button is located at the bottom right of the settings area.

Setting Name	Description	Value	Control
Failed Logins Before Lockout	Maximum login attempts before lockout	5	+ / -
Failed Logins Before Erase	Maximum login attempts before drive erasure	0	+ / -
Password History	Number of unique new passwords before a password can be reused (per user)	1	+ / -
Password Minimum Length	Minimum length of password (all users)	8	+ / -
Require Multiple Forms of Authentication	Require both password and smartcard to log in (all users)	No	Toggle (Yes/No)

Failed Logins Before Lockout

The number of consecutive failed login attempts (across all users) before a restart is required. Only valid user names are considered towards failures.

Min: 1 Max: 10

Failed Logins Before Erase

The number of consecutive failed login attempts before the disk is automatically erased. Only valid user names are considered towards failures.

Min: 0 (Disabled) Max: 999

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

Require Two-Factor Authentication

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

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

5. 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.

6. Boot from the USB thumb drive.
7. The Secure Setup screen will be displayed.
8. If you have more than one internal drive, be sure the Cigent Secure SSD is selected.
9. Enter a username, email (optional) and password. (See Username and Password Requirements in Add User section for details.)
10. Then click Initialize.

Prepare Secure Drive

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

Drive

Username

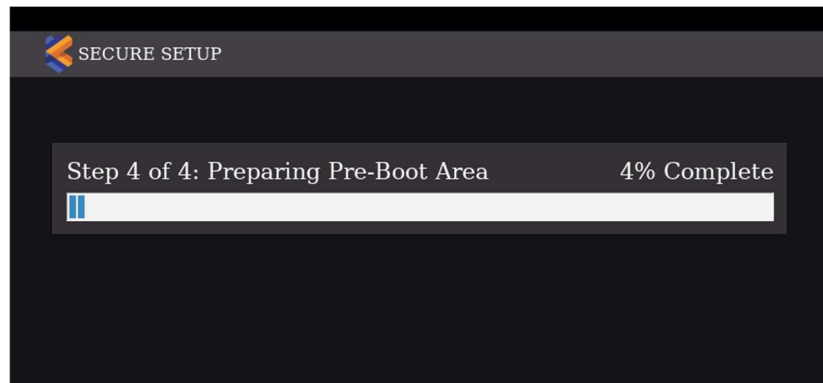
Email

Password

Confirm Password

Connecting to a reliable power source recommended.

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



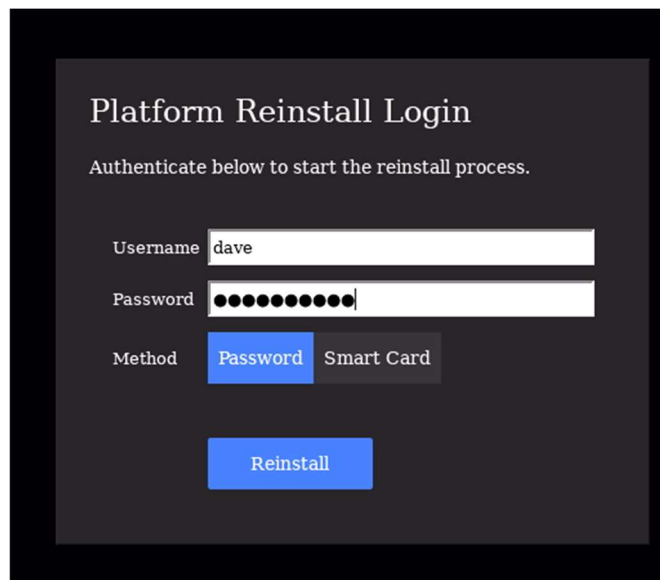
Once complete, power off the computer.
Remove the USB thumb drive from the computer.

5 Re-enabling the Cigent PBA

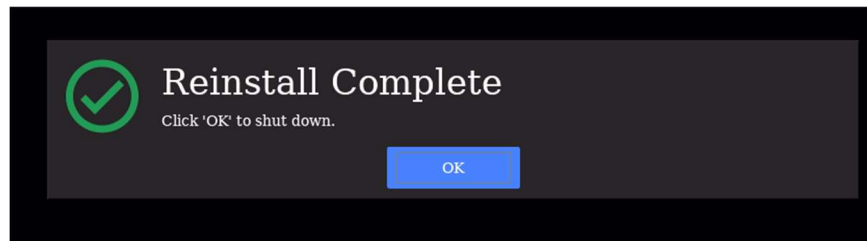
To re-enable PBA after temporarily disabling it from the maintenance page you will need the following:

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.



After shutting down restart the system. The PBA environment should once more present the normal login screen.

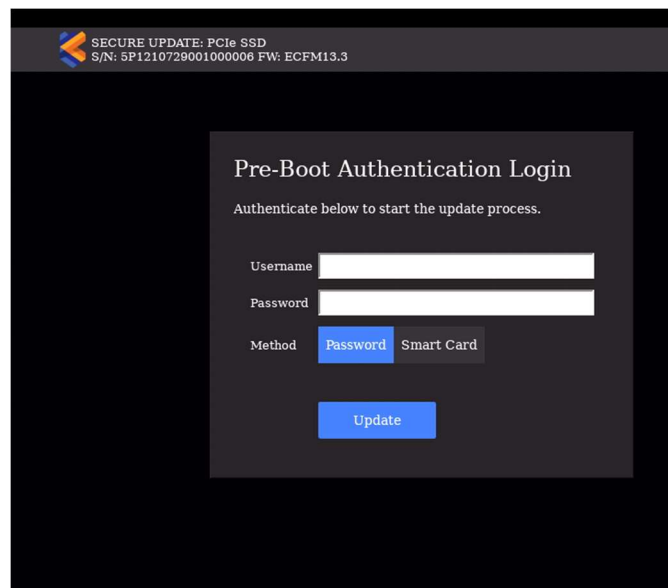
6 Updating the Cigent PBA software

For information on obtaining the newest version of the Cigent PBA software see section [Initial installation overview](#).

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

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

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



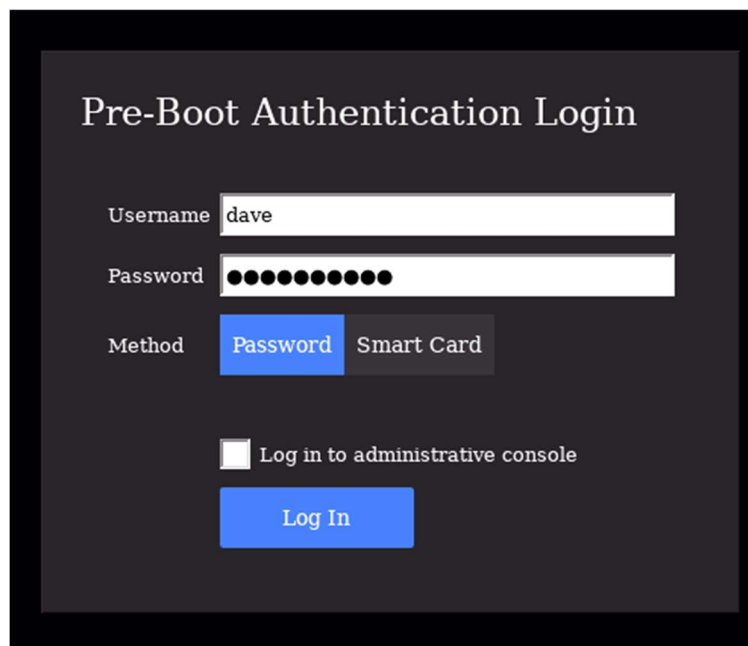
Enter valid administrator credentials and click Update. The process will take about 10 minutes to complete. Once complete shutdown the system and remove the USB drive.

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

7 Logging in and Logging Out

7.1 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.

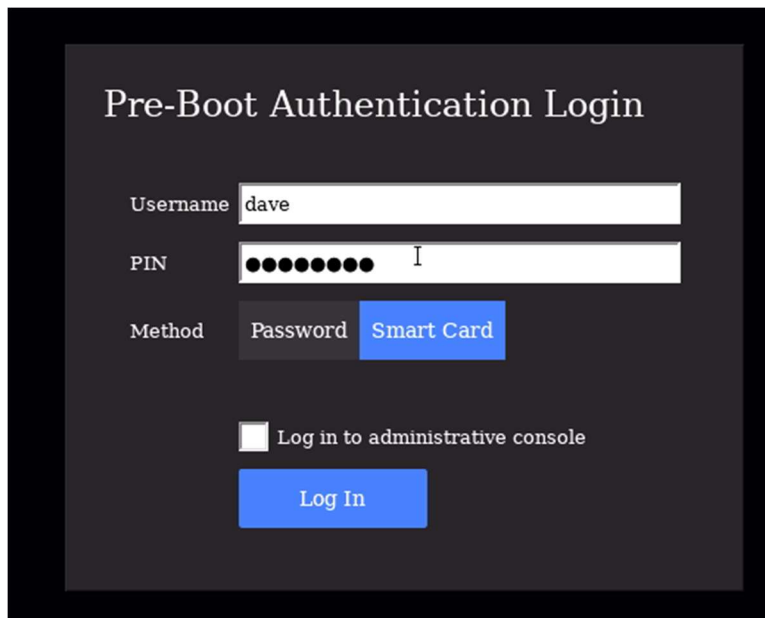


The image shows a 'Pre-Boot Authentication Login' screen with a dark background. It features a title at the top, followed by three input fields: 'Username' containing 'dave', 'Password' with masked characters, and 'Method' with 'Password' selected. Below these is a checkbox for 'Log in to administrative console' and a blue 'Log In' button.

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.



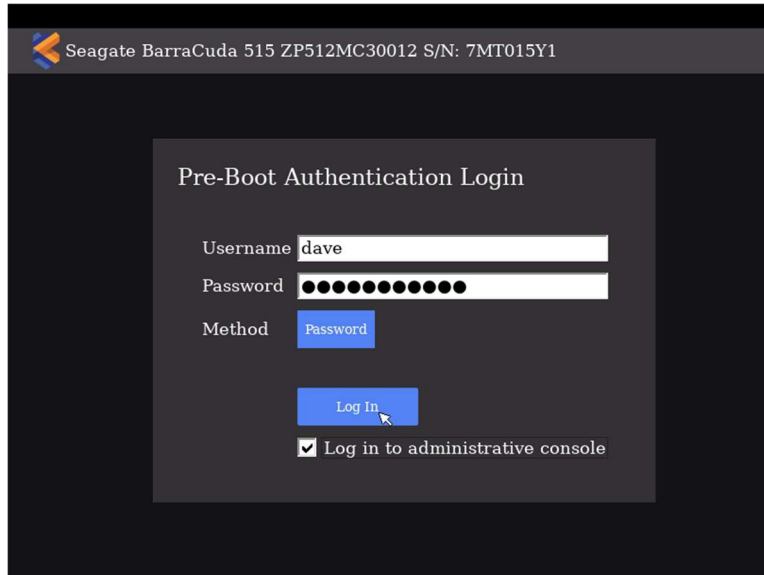
The image shows a 'Pre-Boot Authentication Login' screen with a dark background. It features the following elements:

- Title:** Pre-Boot Authentication Login
- Username:** A text input field containing 'dave'.
- PIN:** A text input field with ten black dots and a cursor, representing a masked PIN.
- Method:** Two buttons: 'Password' (grey) and 'Smart Card' (blue and highlighted).
- Checkboxes:** An unchecked checkbox labeled 'Log in to administrative console'.
- Log In:** A blue button at the bottom.

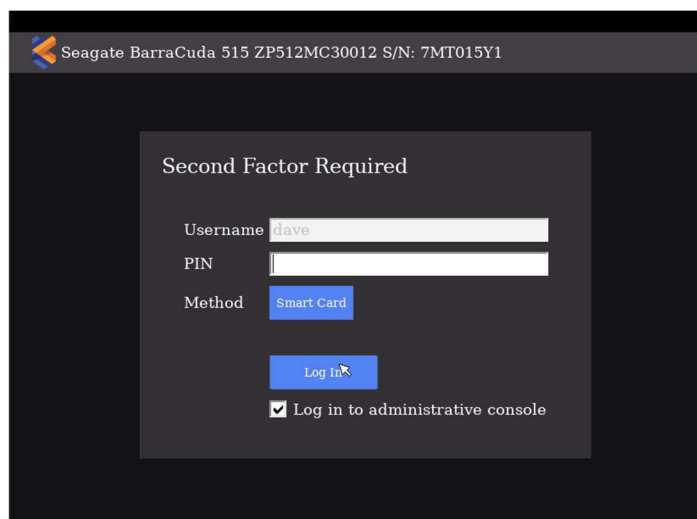
If the authentication is successful, your system will reboot and automatically start your operating system.

7.3 Logging in with Two Factor Authentication

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



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



4. Insert your smartcard.

5. Enter the PIN.
6. Click Log In.

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

7.4 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.

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.