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

Cigent PBA Installation Guide and User Manual

Mar 2024
Build 20
PBA Version 1.0.6

1 Table of Contents

Known Issues

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

2 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.

3 Initial Installation

3.1 Initial installation overview

You can obtain a copy of the PBA software from:

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

3.2 Drive installation

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

3.3 Configure UEFI and BIOS Settings

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

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

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

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

Secure Boot – ON (RECOMMENDED)

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

3.4 Operating System installation

Install any operating system or virtual machines.

3.5 Create a bootable USB 3.0 thumb drive

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

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

1. Extract the file from the provided zip and ensure all files remain in the same directory.
2. Insert a USB 3.0 thumb drive into your computer.
3. Start an Administrator command window and change directory to the location of loader software.
4. Run PBALoader.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.

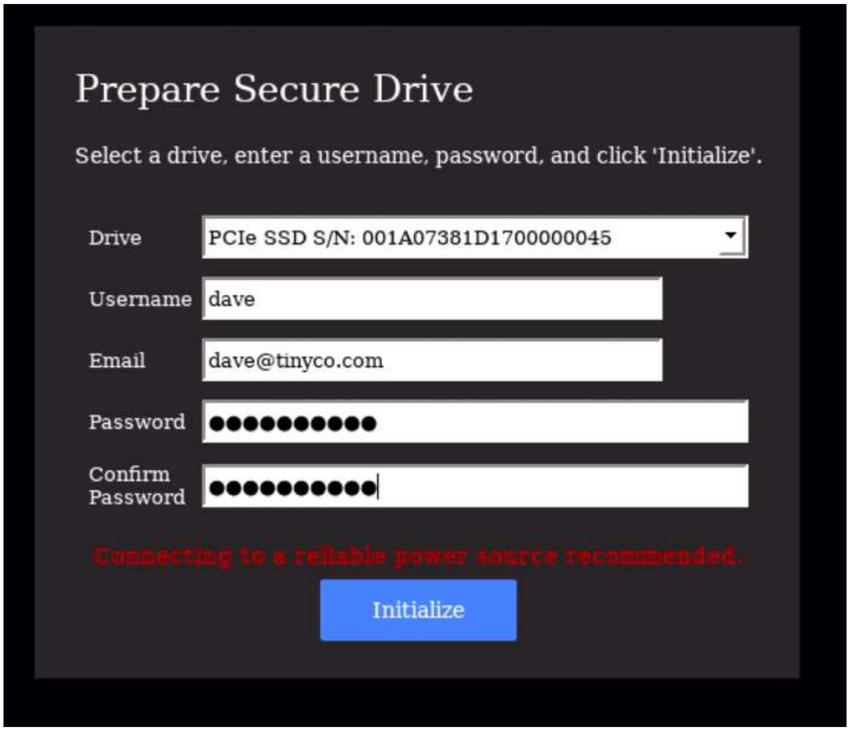
The process can take several minutes to complete. Once successful you may remove the USB thumb drive and proceed to the next step.

3.6 Boot to the USB thumb drive

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

3.7 Install the 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.



Prepare Secure Drive

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

Drive: PCIe SSD S/N: 001A07381D1700000045

Username: dave

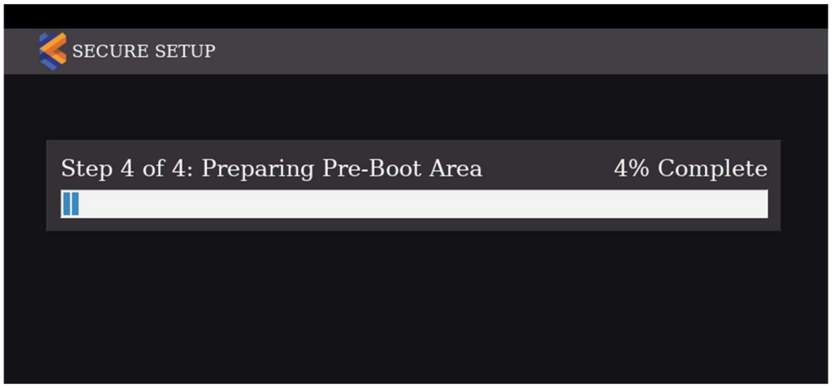
Email: dave@tinyco.com

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.



Step 4 of 4: Preparing Pre-Boot Area 4% Complete

Once complete, power off the computer.

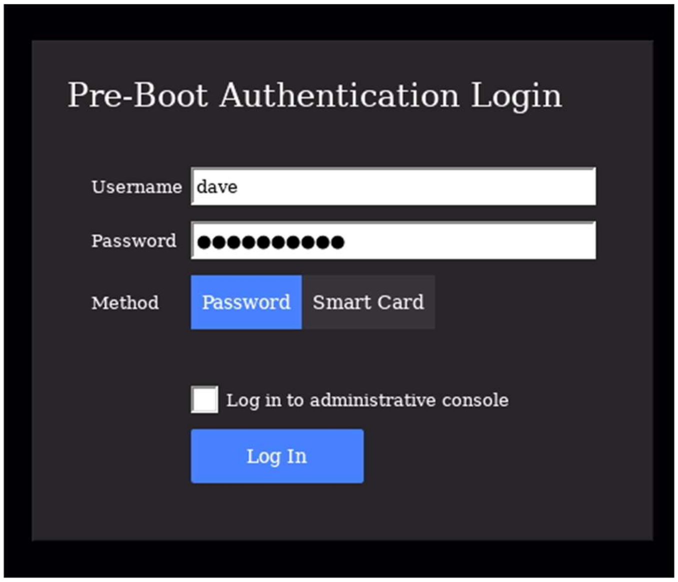
Your Cigent PBA is now installed and ready for use.

Remove the USB thumb drive and power up the system.

3.8 Initial login

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

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



Pre-Boot Authentication Login

Username: dave

Password: ●●●●●●●●●●●

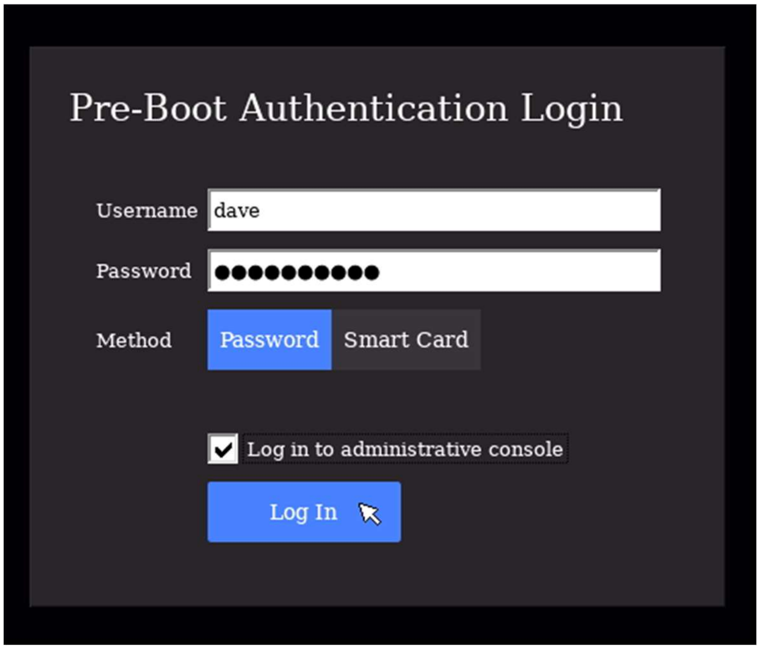
Method: Password | Smart Card

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

4 Using the Administrative Console

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

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



Pre-Boot Authentication Login

Username: dave

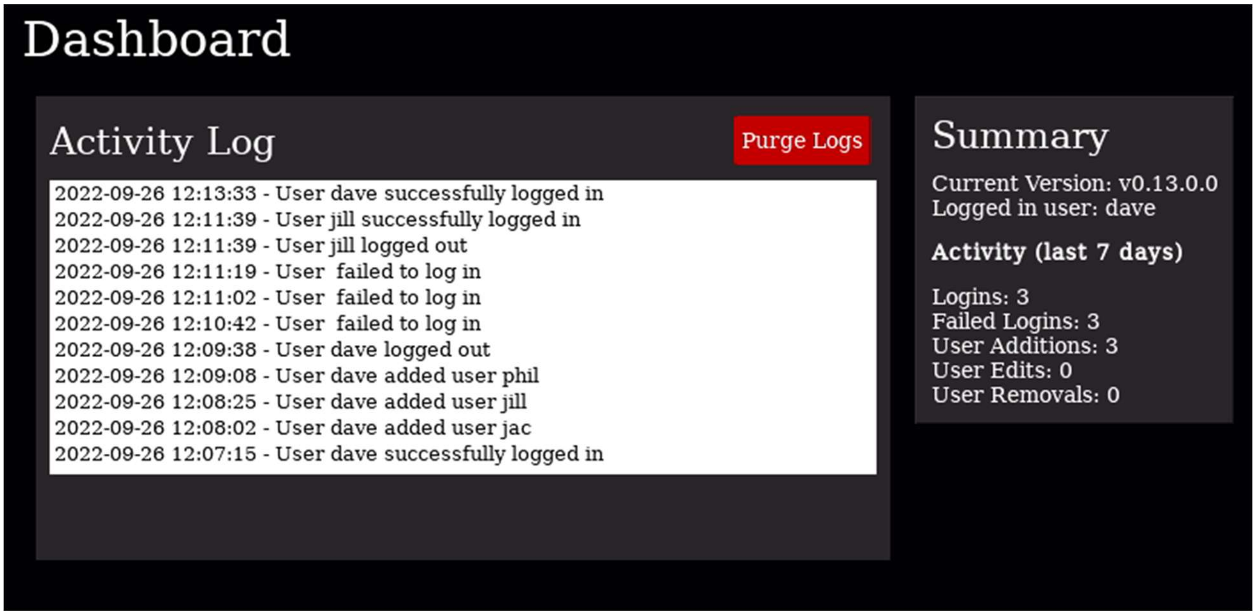
Password: ●●●●●●●●●●●

Method: Password

☑ Log in to administrative console

4.1 Dashboard

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



```
2022-09-26 12:13:33 - User dave successfully logged in
2022-09-26 12:11:39 - User jill successfully logged in
2022-09-26 12:11:39 - User jill logged out
2022-09-26 12:11:19 - User  failed to log in
2022-09-26 12:11:02 - User  failed to log in
2022-09-26 12:10:42 - User  failed to log in
2022-09-26 12:09:38 - User dave logged out
2022-09-26 12:09:08 - User dave added user phil
2022-09-26 12:08:25 - User dave added user jill
2022-09-26 12:08:02 - User dave added user jac
2022-09-26 12:07:15 - User dave successfully logged in
```

Current Version: v0.13.0.0
Logged in user: dave

Activity (last 7 days)

Logins: 3
Failed Logins: 3
User Additions: 3
User Edits: 0
User Removals: 0

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

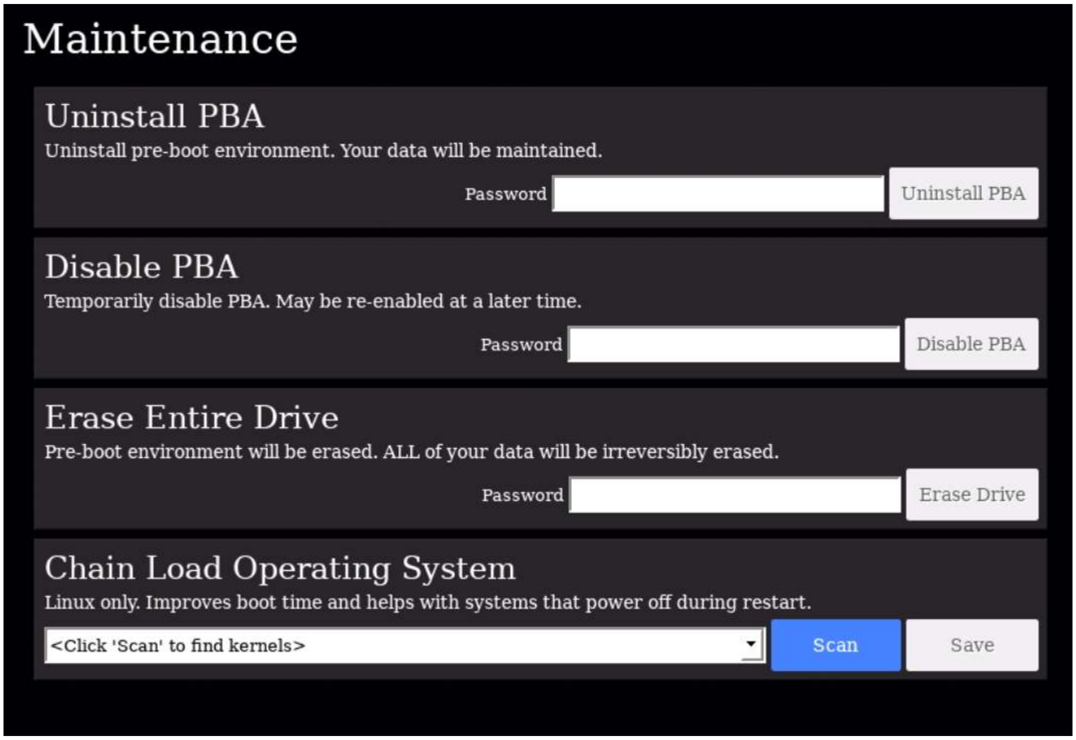
The following activities are recorded:

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

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

4.2 Maintenance

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



Maintenance

Uninstall PBA

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

Disable PBA

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

Erase Entire Drive

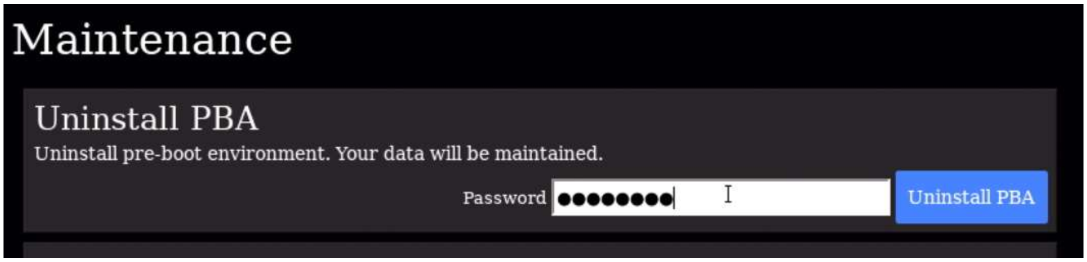
Pre-boot environment will be erased. ALL of your data will be irreversibly erased.

Chain Load Operating System

Linux only. Improves boot time and helps with systems that power off during restart.

4.2.1 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.



Maintenance

Uninstall PBA

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

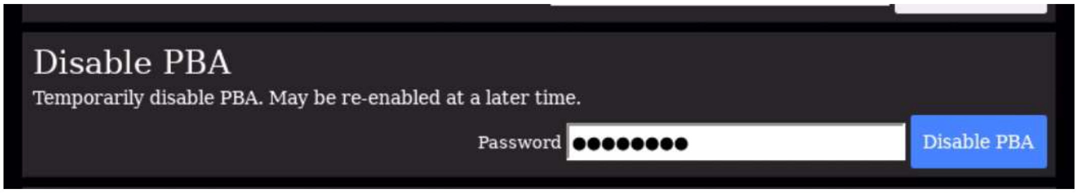
Password ●●●●●●●●●

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.

4.2.2 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.



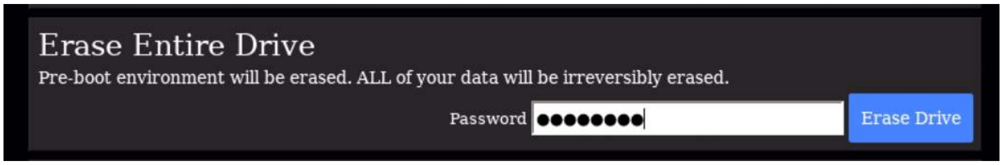
Disable PBA

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

Password ●●●●●●●●●

4.2.3 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.



Erase Entire Drive

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

Password ●●●●●●●●

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.

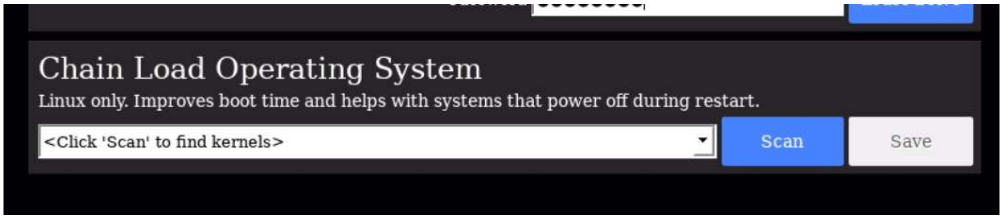
1. Enter your administrator password in the Erase Entire Drive section
2. Click Erase Drive.

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

Once complete, power off the system.

4.2.4 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.



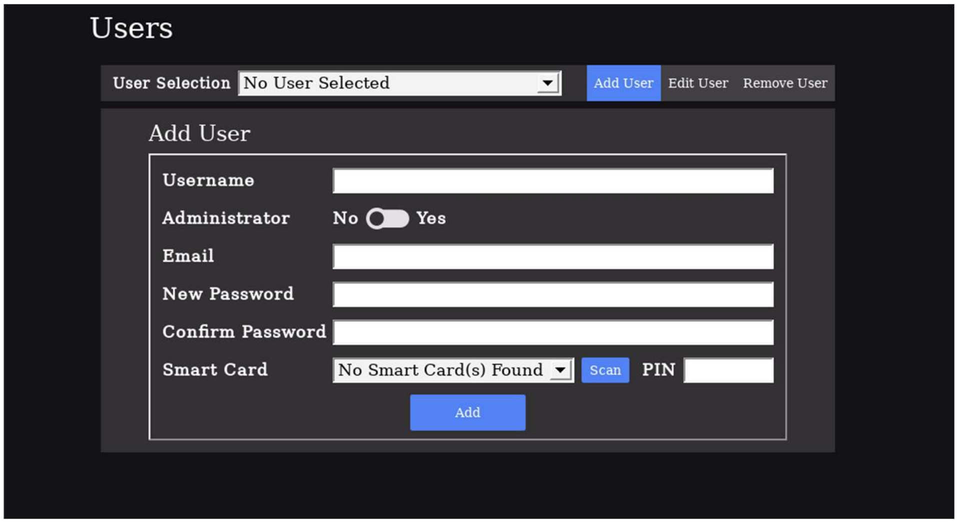
Chain Load Operating System

Linux only. Improves boot time and helps with systems that power off during restart.

<Click 'Scan' to find kernels>

4.3 Users

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



Users

User Selection: No User Selected

Add User

Username

Administrator: No ○ Yes

Email

New Password

Confirm Password

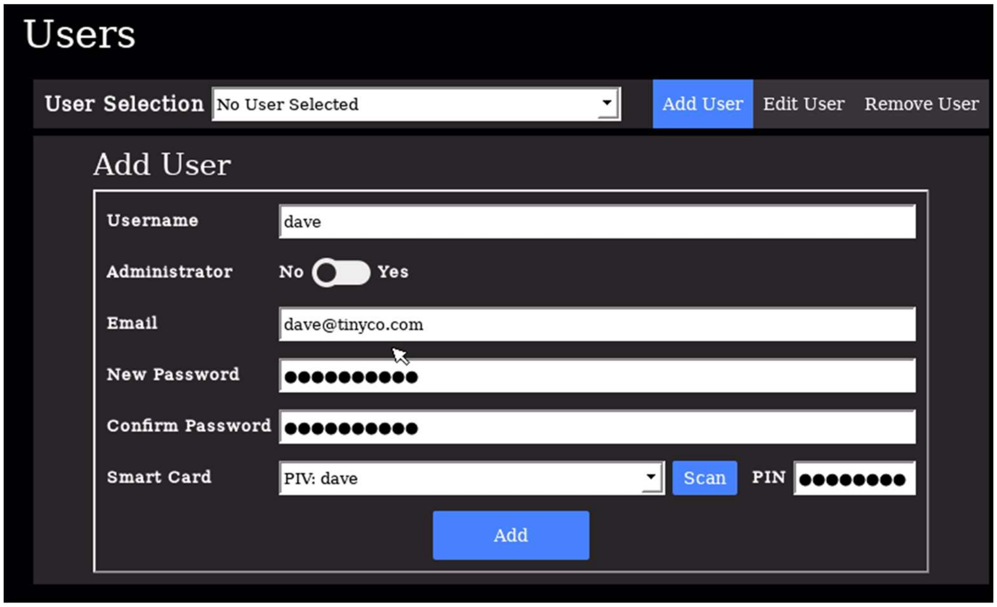
Smart Card: No Smart Card(s) Found PIN

Roles and Capabilities

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

4.3.1 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.



User Selection	No User Selected
Username	dave
Administrator	No ○ Yes
Email	dave@tinyco.com
New Password	●●●●●●●●●●
Confirm Password	●●●●●●●●●●
Smart Card	PIV: dave
PIN	●●●●●●●●

4.3.2 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.

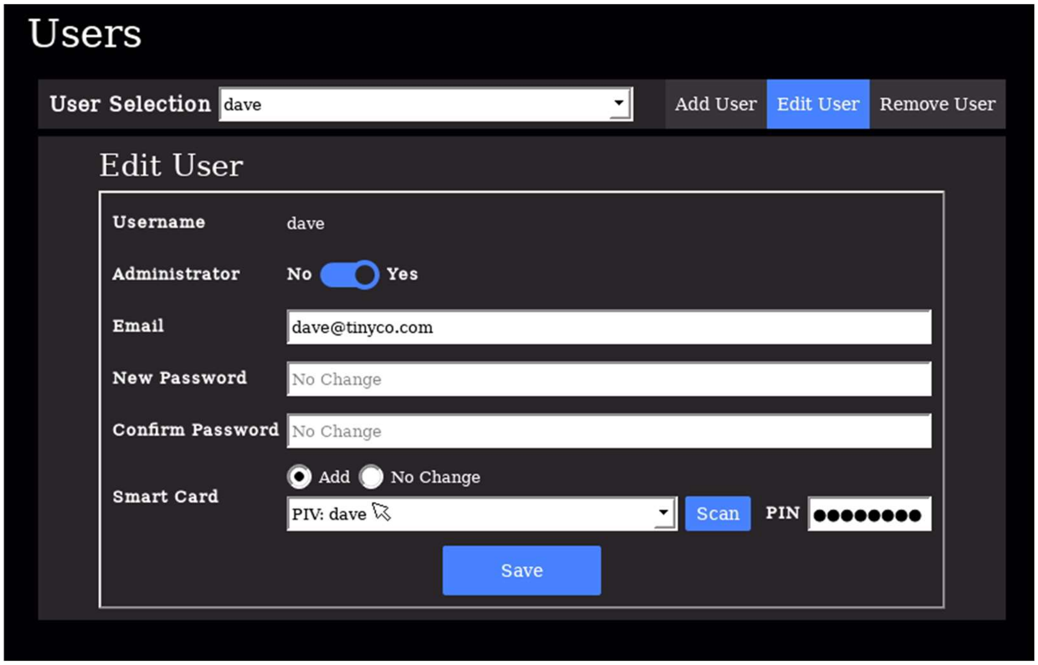
Note that to Add a Smart Card to a user, the smart card must be inserted and the PIN correctly entered. If you do not see the smart card listed after inserting it, click the Scan button then open the selection list to find your card. Once the card shows in the selection list, enter the PIN before clicking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

4.3.3 Edit User

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

Administrators can change the following user attributes:

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



Users

User Selection: dave

Edit User

Username: dave

Administrator: No ● Yes

Email: dave@tinyco.com

New Password: No Change

Confirm Password: No Change

Smart Card: ● Add ○ No Change

PIV: dave

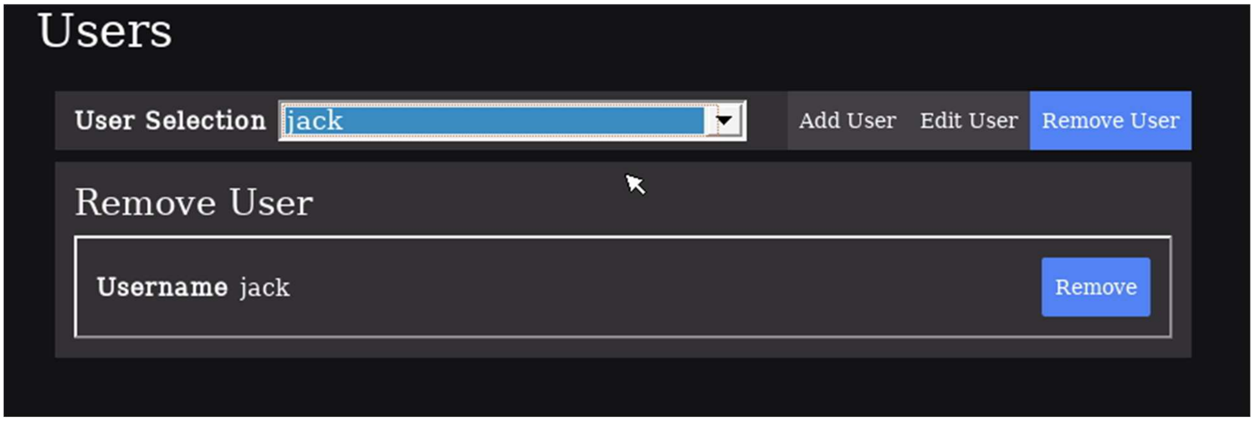
PIN ●●●●●●●●

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.

4.3.4 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.



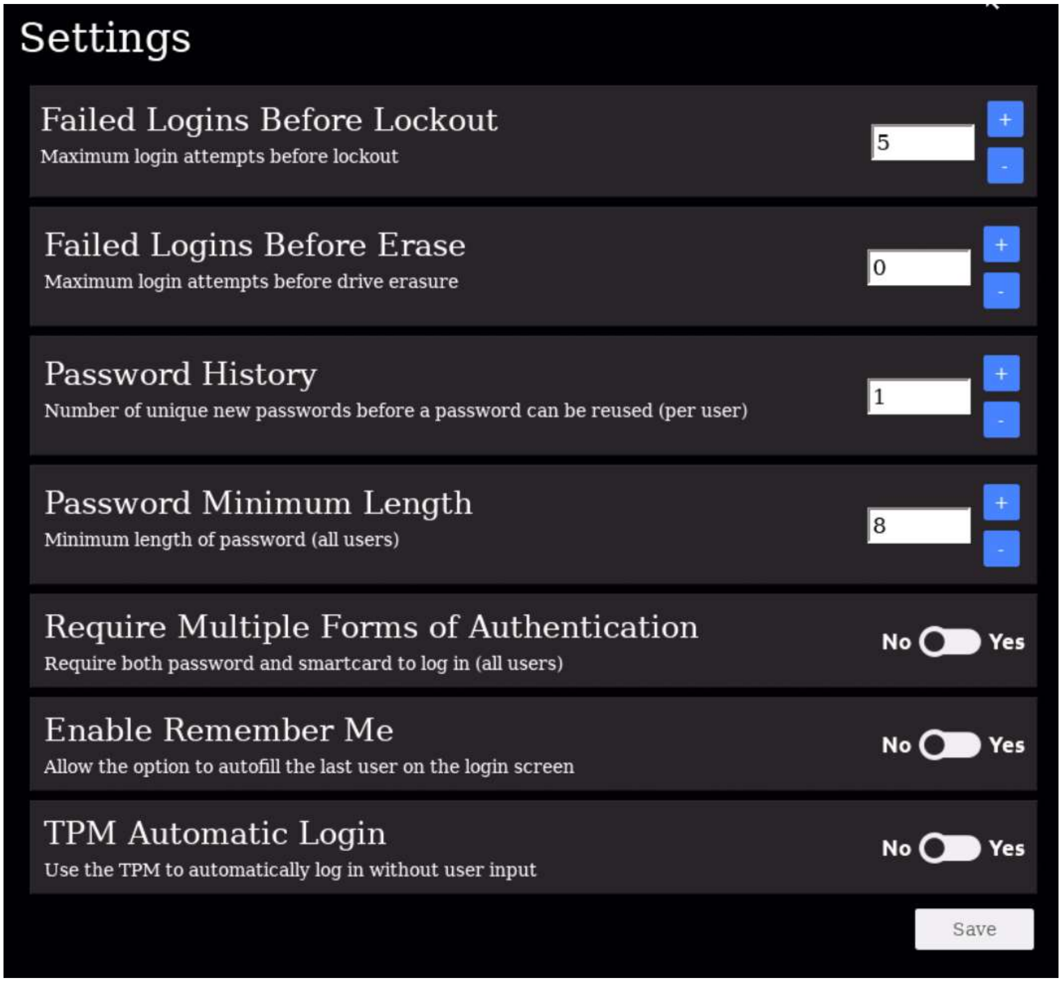
User Selection jack

Username jack

1. Select an existing user from the User Selection list.
2. Click Remove next to the username.

4.4 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.



Settings

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 Yes

Enable Remember Me
Allow the option to autofill the last user on the login screen
No Yes

TPM Automatic Login
Use the TPM to automatically log in without user input
No Yes

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

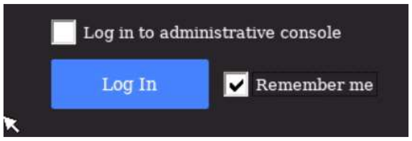
Password History

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.

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.



☐ Log in to administrative console

☑ Remember me

TPM Automatic Login
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.

5 Reinstallation of the Cigent PBA

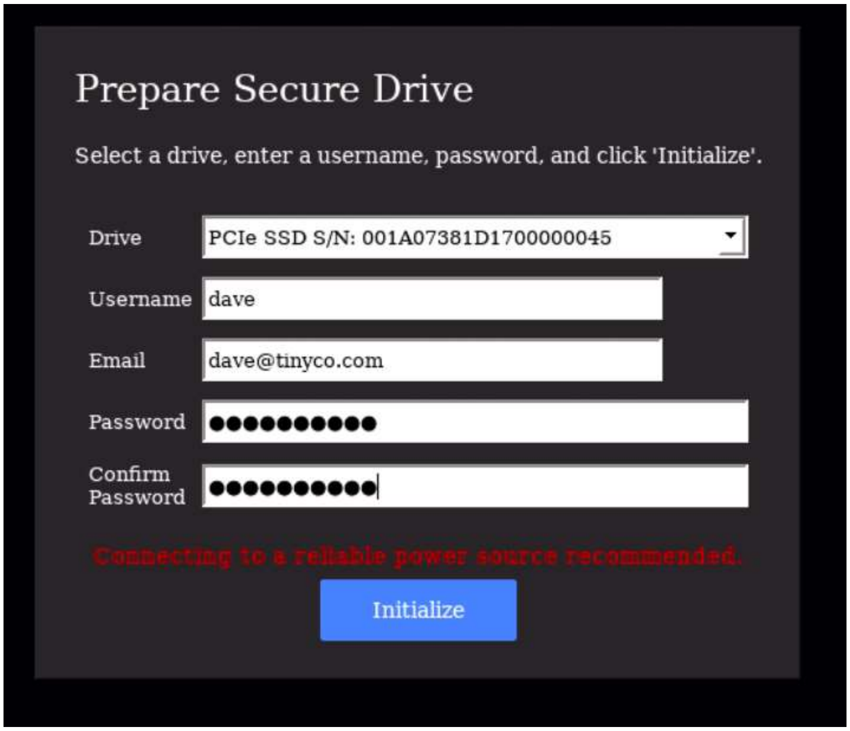
Reinstallation of the Cigent PBA software will be necessary if you used the **Erase Entire Drive** or **Uninstall PBA** features from the maintenance page or erased the drive using another utility.

The reinstallation process is 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: PCIe SSD S/N: 001A07381D1700000045

Username: dave

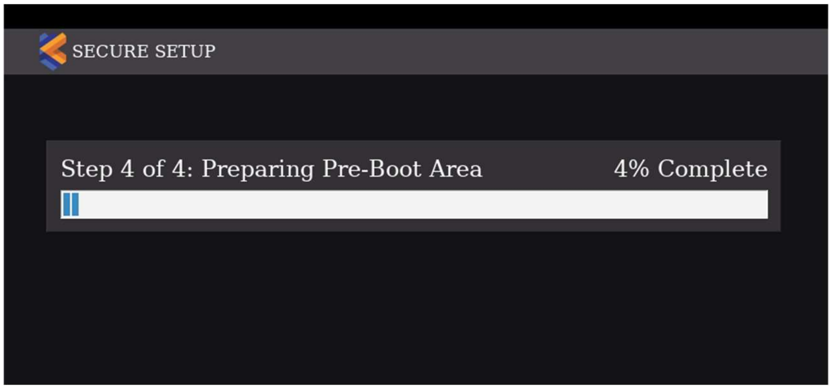
Email: dave@tinyco.com

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.



Step 4 of 4: Preparing Pre-Boot Area 4% Complete

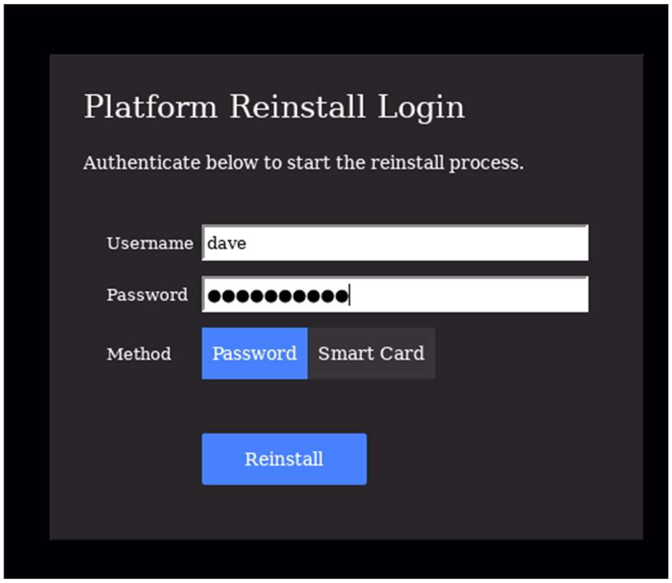
Once complete, power off the computer.
Remove the USB thumb drive from the computer.

6 Re-enabling the Cigent PBA

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

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

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



Platform Reinstall Login

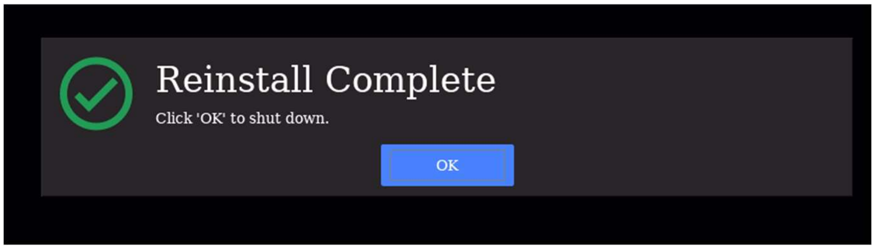
Authenticate below to start the reinstall process.

Username: dave

Password: ●●●●●●●●●●●

Method: Password

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



Reinstall Complete

Click 'OK' to shut down.

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

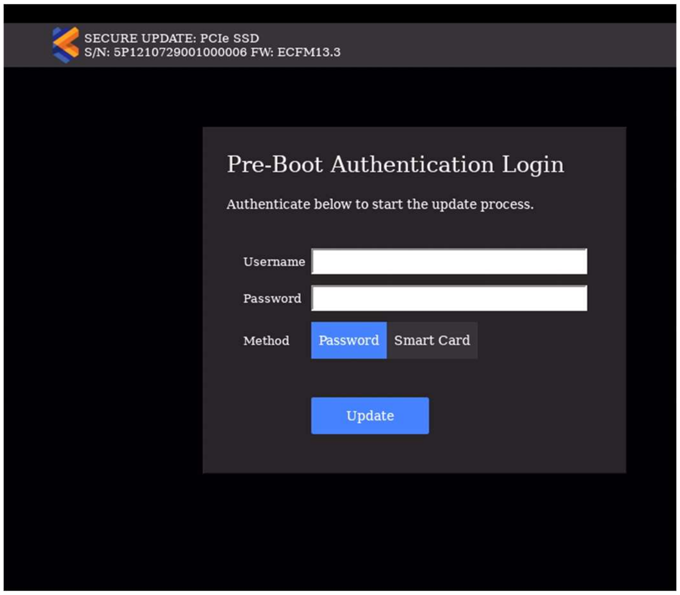
7 Updating the Cigent PBA software

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

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

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

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



SECURE UPDATE: PCIe SSD
S/N: 5P1210729001000006 FW: ECFM13.3

Pre-Boot Authentication Login

Authenticate below to start the update process.

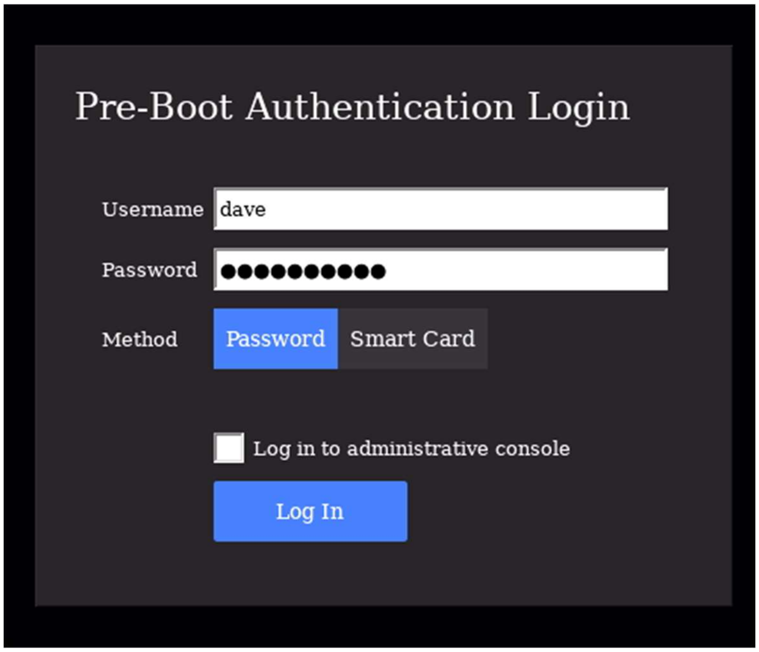
Enter valid administrator credentials and click Update. The process will take about 10 minutes to complete. Once complete shutdown the system and remove the USB drive.

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

8 Logging in and Logging Out

8.1 Logging in with a username and password

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



Pre-Boot Authentication Login

Username dave

Password ●●●●●●●●●●●

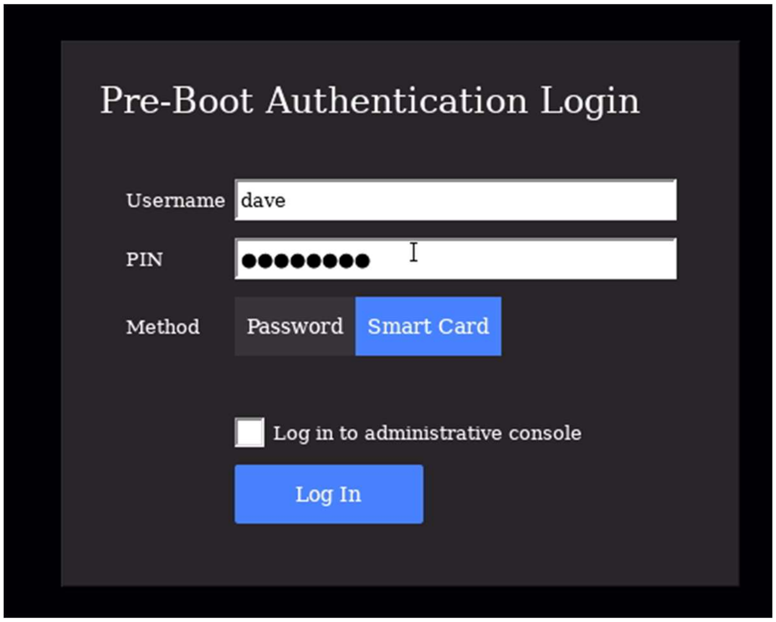
Method Password

□ Log in to administrative console

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.



Pre-Boot Authentication Login

Username dave

PIN ●●●●●●●●

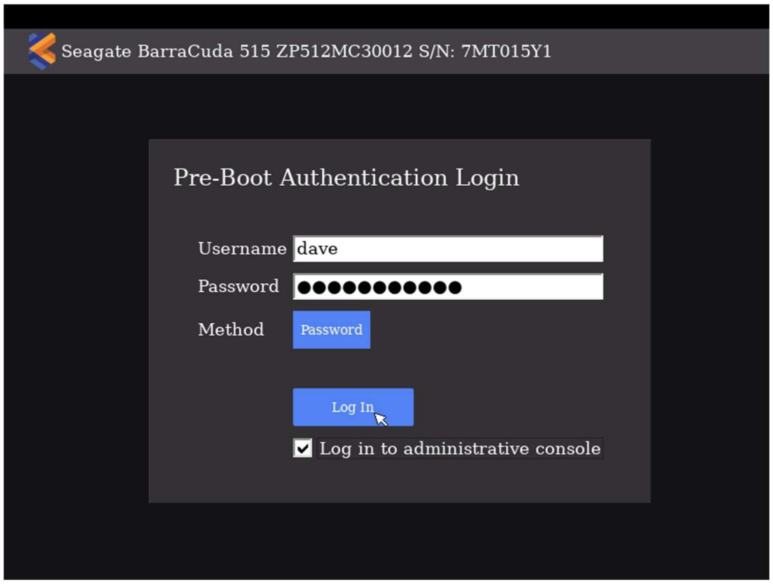
Method Password **Smart Card**

□ Log in to administrative console

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

8.3 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.



Seagate BarraCuda 515 ZP512MC30012 S/N: 7MT015Y1

Pre-Boot Authentication Login

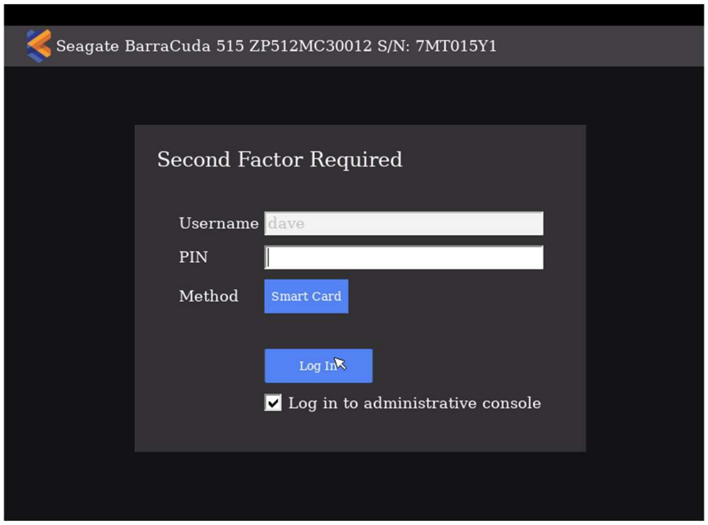
Username: dave

Password: ●●●●●●●●●●●

Method: Password

☑ Log in to administrative console

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



Seagate BarraCuda 515 ZP512MC30012 S/N: 7MT015Y1

Second Factor Required

Username: dave

PIN:

Method: Smart Card

☑ Log in to administrative console

4. Insert your smartcard.

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

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

8.4 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