



Citadel C Series SSD Installation User Manual

Models Covered:

Citadel C-SEL

Citadel C-ADV

1 Table of Contents

1. Introduction	4
2 Initial Installation.....	5
2.1 Initial installation overview	5
2.2 Drive installation	5
2.3 Configure UEFI and BIOS Settings	5
2.4 Operating System installation	6
2.5 Create a bootable USB PBA Installer thumb drive.....	6
2.6 Boot to the USB thumb drive	7
2.7 Enable the Pre-Installed PBA	8
3 Using the Administrative Console.....	10
3.1 Dashboard	11
3.2 Maintenance	12
3.2.1 Uninstall PBA.....	13
3.2.2 Disable PBA.....	14
3.2.3 Erase Entire Disk	15
3.3 Users	16
3.3.1 Add User	17
3.3.2 Username and Password Requirements	18
3.3.3 Edit User	19
3.3.4 Remove User	20
3.4 Settings.....	21
4 Reinstallation of the Cigent PBA	23

4.1 Initial login.....	25
5 Re-enabling the PBA.....	26
6 Logging in and Logging Out.....	28
6.1 Logging in with a username and password	28
6.2 Logging in with a Smart Card	28
6.3 Logging in with Two Factor Authentication.....	30
6.4 Logging out of the PBA Administrative console.....	31

Known Issues

1. Capslock and Numlock do not light up when active, however they are working properly.

1. Introduction

The Citadel C Series SSD is a FIPS-certified, self-encrypting drive (SED) protects systems against unauthorized access with pre-boot authentication (PBA), powered by Cigent.

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 Citadel C Series SSD and PBA software. It also details how to configure users and options in the PBA administrative console.

2 Initial Installation

2.1 Initial installation overview

Citadel C Series SSDs have been pre-installed with the Cigent PBA software which has been disabled. After you have installed and configured your operating system you must enable the PBA to fully protect your system.

You can always find the latest software and documentation at digistor.com/c-series-software. It is password protected, so be sure to use the password **douglas-fir25**.

In the future should the Citadel C Series SSD be erased, follow the steps in the [Reinstallation of the PBA](#) section.

2.2 Drive installation

Install the Citadel C Series SSD into your system following your computer manufacturer's instructions.

2.3 Configure UEFI and BIOS Settings

Each manufacturer and model have unique locations and names for settings.

PC Manufacturer	Bios Setting	Require State
Dell	SATA Operation	AHCI
Dell	UEFI Boot Path Security	Never
Dell, Lenovo	Secure Boot	Off
Lenovo	Block SID Authentication	Disable

2.4 Operating System installation

Install any operating system or virtual machines.

2.5 Create a bootable USB PBA Installer thumb drive

Before using the Citadel C Series SSD, you will first need to activate the PBA. Follow the steps below to create a bootable thumb drive with the software you need to activate the PBA or use a Citadel Activator Device (sold separately), which is a thumb drive that has the software pre-loaded.

WARNING: All data on the USB thumb drive will be erased.

Note: You can use the same USB thumb drive to activate multiple Citadel C Series drives in other systems, which means you only have to create the USB drive once.

1. Download the PBA installation software from digistor.com/c-series-software. The password to access the website is **douglas-fir25**.
2. Extract the file from the provided ZIP and ensure all files remain in the same directory.
3. Insert a USB thumb drive into your computer. (Remove any other thumb drives to avoid errors.)
4. Start an Administrator command window and change directory to the location of loader software.
(e.g. `cd C:\Downloads\Cigent_PBA_v1.0.4`)
5. Run **PBALoader_v1.2.exe -i**
6. Choose the number next to the correct USB thumb drive (if more than 1).
7. Select **1** for Load operation.
8. Select the **PBA_v1.0.4.bin file** (or the version you have).
9. Confirm your selection by typing '**YES**' and then press **Enter**.

```
Select Administrator: Command Prompt
C:\Cigent>PBAloader_v1.2.exe -i

-----
Cigent PBA Loader v1.2
-----
This software is protected from copying under U.S. and
international copyright laws and treaties. Any unauthorized
copying, alteration, distribution, transmission, performance,
display or other use of this software is prohibited without
the expressed written consent of Cigent Technology Inc.
-----
WARNING! This utility will destroy the data on the selected
USB drive. DO NOT USE IT IF YOU ARE UNSURE HOW IT WORKS
-----

Available USB drives
-----
1) \\.\PHYSICALDRIVE1 Model: 'Kingston DataTraveler G3 USB Device' SN: '001372982BA9EAB1750F001B' [1 partition(s)]
-----
Select a drive (-1 to quit)
1
-----
Select an operation (-1 to quit)
-----
1) Load (initialize the selected drive)
2) Clear (clear the setup data from the selected drive)
1
-----
Select an pba file (-1 to quit)
-----
1) PBA_v0.3.bin
2) PBA_v0.3.bin_sha256.txt
1
-----
WARNING! This operation will destroy the data on the
selected drive!
-----
Enter YES to continue or NO to cancel
YES
Loading PBA data
Using "\\.\PHYSICALDRIVE1"
Writing PBA data: 100%
PBA file written
```

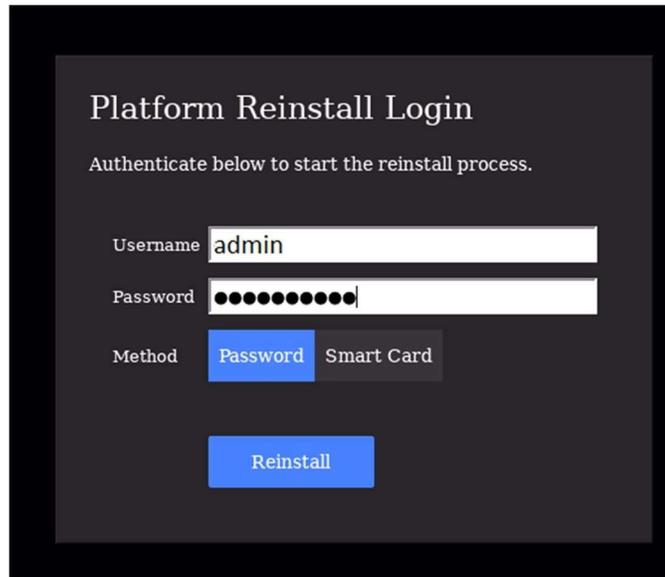
The process can take several minutes to complete. Once successful, you may remove the USB thumb drive and proceed to the next step.

2.6 Boot to the USB thumb drive

1. Ensure the power is turned off.
2. Insert the bootable USB thumb drive or Citadel Activator Device into the computer with the Citadel C Series 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 Enable the Pre-Installed PBA

The PBA software will boot from the USB thumb drive. Once running, it will detect the disabled installation and prompt for administrator credentials.



1. Enter the following default credentials then press **Reinstall**:
Username: **Administrator**
Password: **Administrator_1**
2. Once the process is complete, press **OK** to shut down the computer.

Your PBA is now enabled and ready for use.

3. Remove the USB thumb drive and power up the system.
4. Once the PBA starts, use the same default credentials to log into the administrative console to begin your customizations.

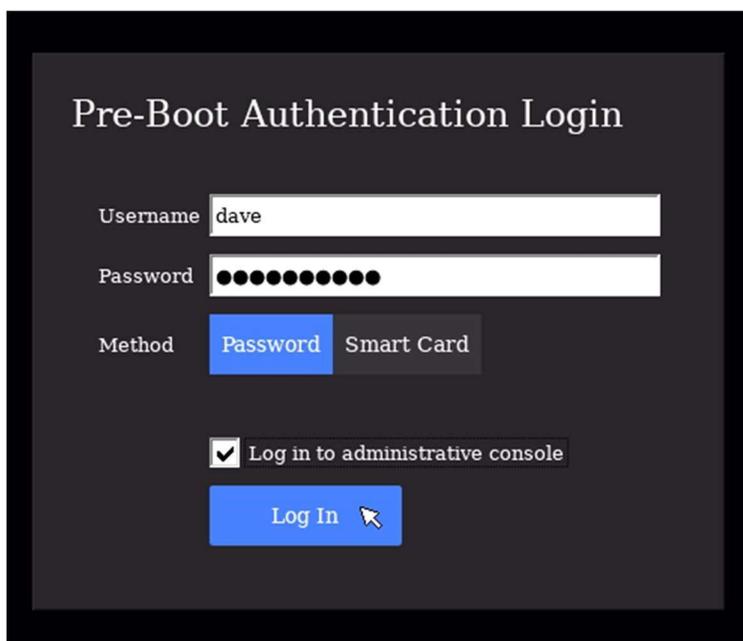
For details on how to log in to the administrative console, see section [Using the Administrative Console](#).

Note: It is strongly recommended that you immediately either change the default password or add a second admin user and remove the original admin user that came pre-installed with the PBA.

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**.

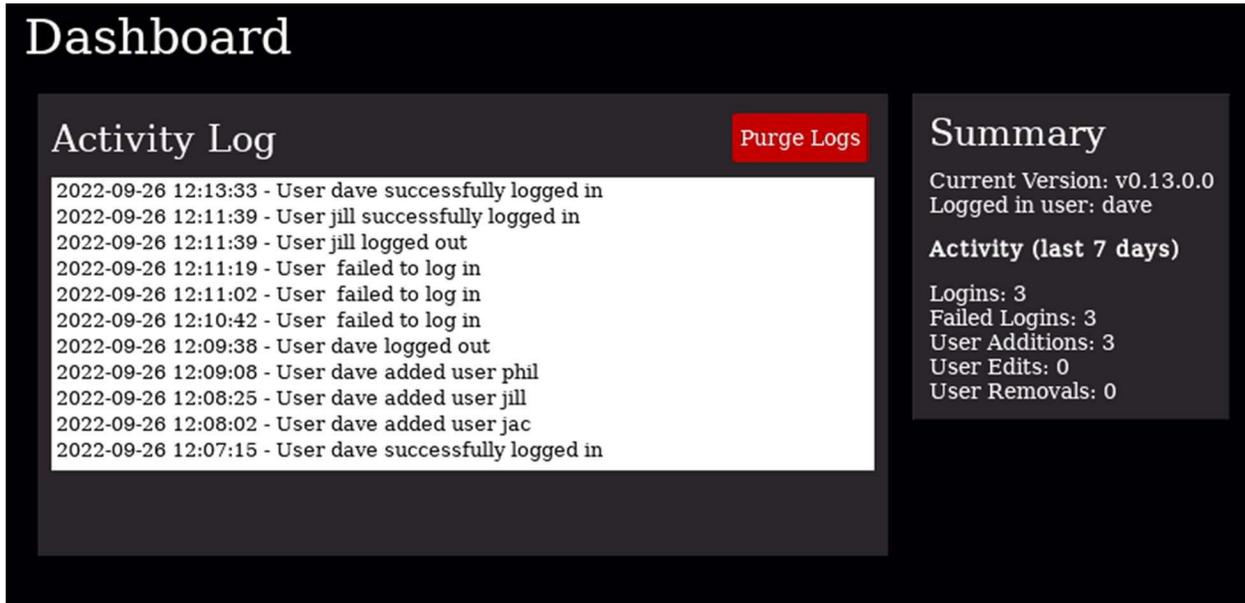


The screenshot shows a dark-themed login interface titled "Pre-Boot Authentication Login". It features the following elements:

- Username:** A text input field containing the name "dave".
- Password:** A text input field where the password is masked with black dots.
- Method:** A selection area with two buttons: "Password" (highlighted in blue) and "Smart Card" (greyed out).
- Administrative Console Access:** A checkbox labeled "Log in to administrative console" which is checked.
- Log In Button:** A blue button with the text "Log In" and a mouse cursor icon 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 screenshot shows a dashboard with a dark background. At the top left, the word "Dashboard" is written in a large, white, serif font. Below this, there are two main sections. The left section is titled "Activity Log" in a white, serif font. To its right is a red button with the text "Purge Logs" in white. Below the "Activity Log" title is a white box containing a list of activity log entries in a small, black, sans-serif font. The right section is titled "Summary" in a white, serif font. Below this title, there is a list of summary statistics in a small, black, sans-serif font.

Activity Log Purge Logs

- 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

Summary

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

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.

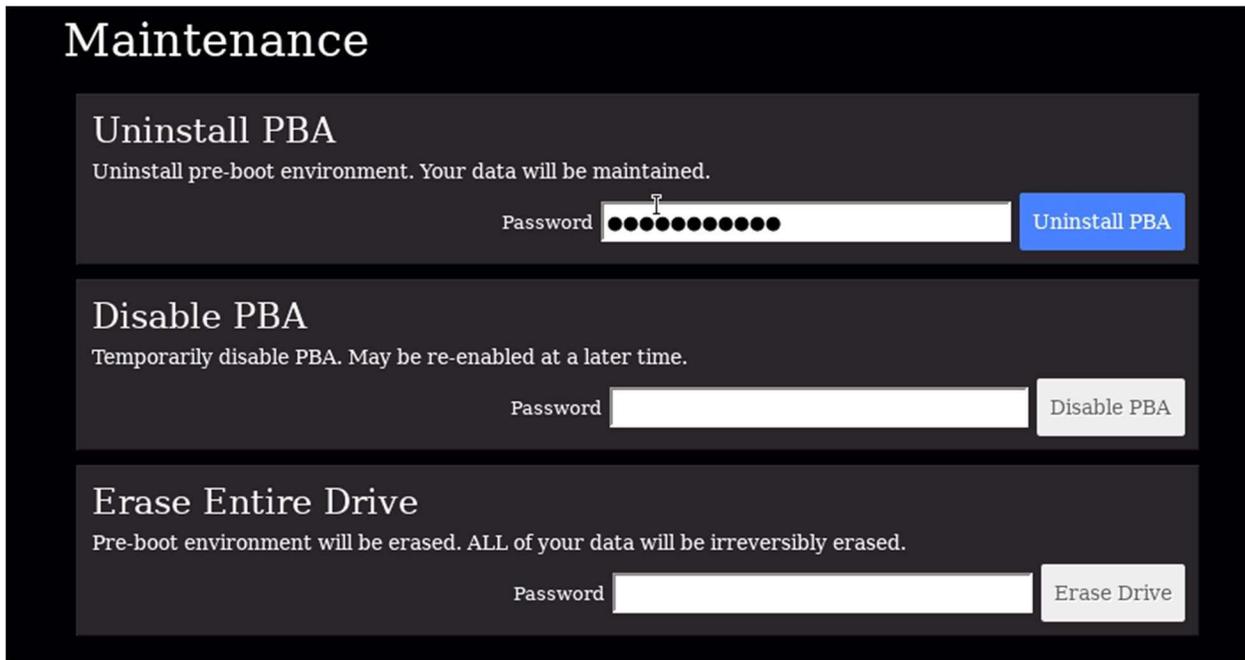
Password

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 PBA software which will remove all files, configuration and user information. Your operating system environment will be preserved and boot as normal.

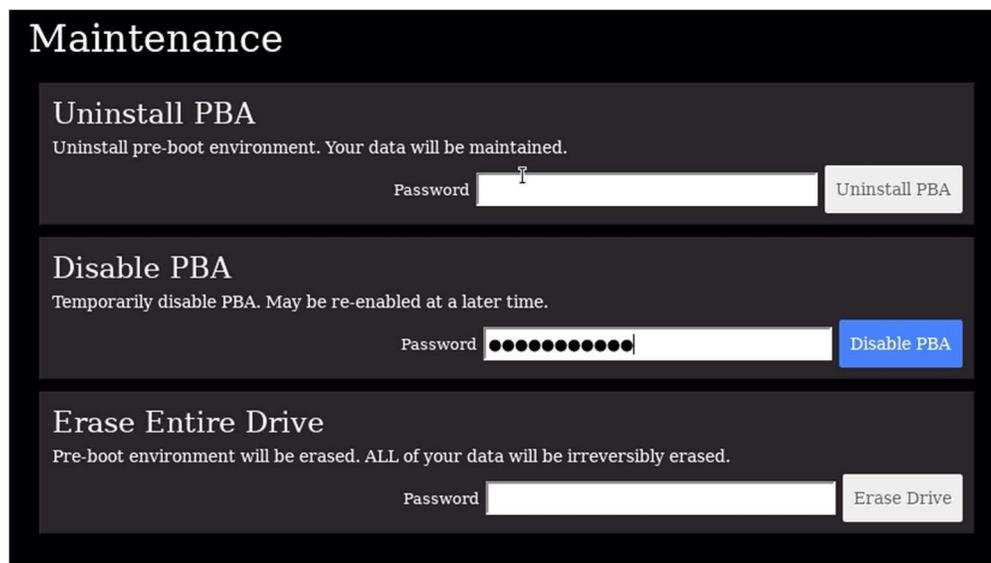


1. Enter your administrator password into the Password field in the Uninstall PBA section.
2. Click **Uninstall PBA**.

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

3.2.2 Disable PBA

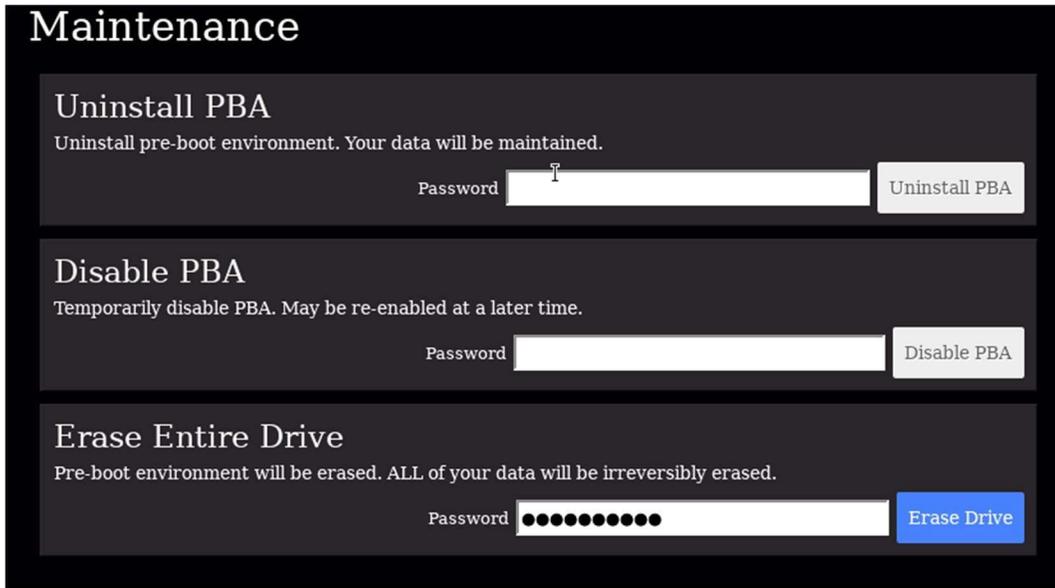
Disabling the PBA temporarily allows the system to boot directly to the operating system without the need to authenticate. This can be useful for administrators during update operations that require repeated restarts of the system. All settings and configuration will be preserved while disabled. Re-enabling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



WARNING: The authentication key change proceeds immediately after clicking Disable PBA.

3.2.3 Erase Entire Drive

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 Disk procedure:

- The Data Encryption Key (DEK) of the Citadel C Series SSD is changed. This is also known as Crypto Erase.
- The PBA executes a Format NVM with the sanitize option that will sanitize every block on the drive.
- The Erase Verification firmware feature is used to ensure all mapped and unmapped blocks have been erased.

Steps to Erase

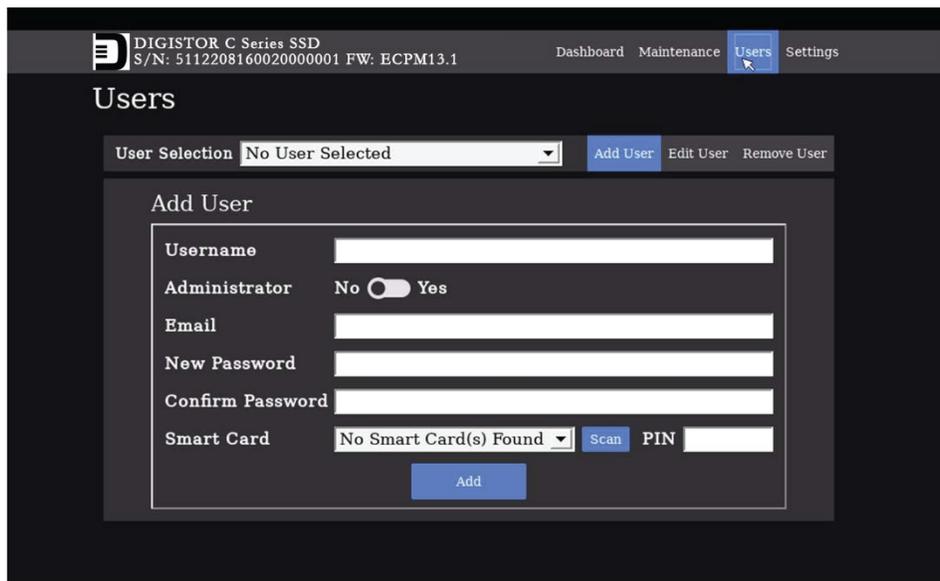
1. Enter your administrator password in the Erase Entire Drive section
2. Click **Erase Drive**.

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

3. 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

Disable PBA	Yes	No
Reactivate (Re-enabling) PBA	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 the 'Users' management interface. At the top, there is a 'User Selection' dropdown menu with 'No User Selected' and buttons for 'Add User', 'Edit User', and 'Remove User'. Below this is the 'Add User' form, which includes the following fields:

- Username:** Text input field containing 'dave'.
- Administrator:** Toggle switch set to 'No'.
- Email:** Text input field containing 'dave@tinyco.com'.
- New Password:** Password input field with 10 dots.
- Confirm Password:** Password input field with 10 dots.
- Smart Card:** Dropdown menu showing 'PIV: dave', a 'Scan' button, and a 'PIN' input field with 10 dots.

An 'Add' button is located at the bottom of the form.

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: 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 a web interface titled "Users". 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" (which is highlighted in blue), and "Remove User". Below this is the "Edit User" form. The form contains the following fields and controls:

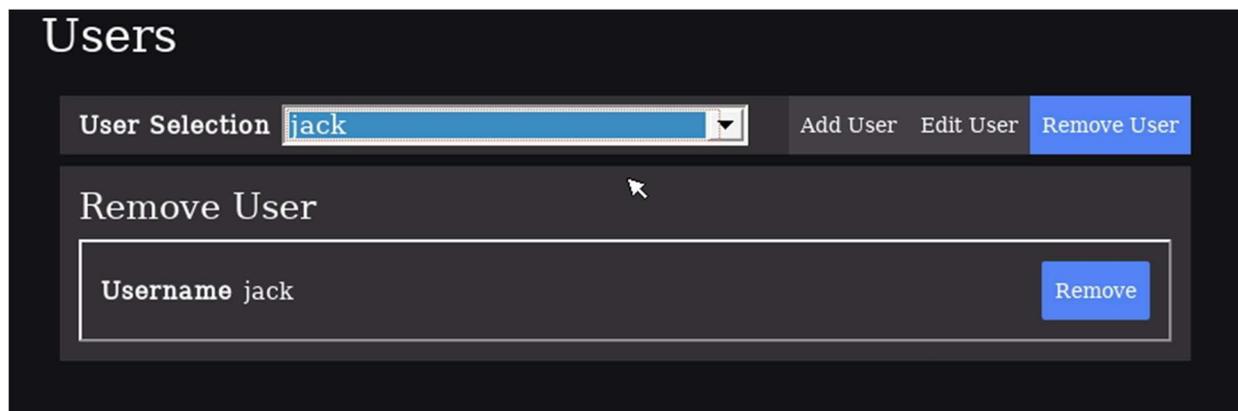
- Username:** dave
- Administrator:** A toggle switch set to "Yes".
- Email:** dave@tinyco.com
- New Password:** No Change
- Confirm Password:** No Change
- Smart Card:** Radio buttons for "Add" (selected) and "No Change". Below this is a dropdown menu showing "PIV: dave" and a "Scan" button. To the right of the dropdown is a "PIN" field with a masked input (dots).
- 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: 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**.

3.3.4 Remove User

Use the Remove User page 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.

Settings

Failed Logins Before Lockout
Maximum login attempts before lockout +
-

Failed Logins Before Erase
Maximum login attempts before drive erasure +
-

Password History
Number of unique new passwords before a password can be reused (per user) +
-

Password Minimum Length
Minimum length of password (all users) +
-

Require Multiple Forms of Authentication
Require both password and smartcard to log in (all users) No Yes

Save

Failed Logins Before Lockout

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

Min: 1

Max: 10

Failed Logins Before Erase

The number of consecutive failed login attempts before the disk is automatically erased. Only valid usernames 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: 8

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 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 like the process you followed initially to enable the preinstalled and disabled PBA.

1. Create a bootable USB thumb drive containing the PBA software. (See section [Create a bootable USB PBA Installer thumb drive](#))

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

2. Boot from the USB thumb drive.
3. The Secure Setup screen will be displayed.
4. If you have more than one internal drive, be sure the Citadel C Series SSD is selected.
5. Enter a username, email (optional) and password. (See Username and Password Requirements in [Add User section](#) for details.)
6. Then click **Initialize**.

Prepare Secure Drive

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

Drive DIGISTOR C Series SSD S/N: 511220816002000000

Username dave

Email dave@tinyco.com

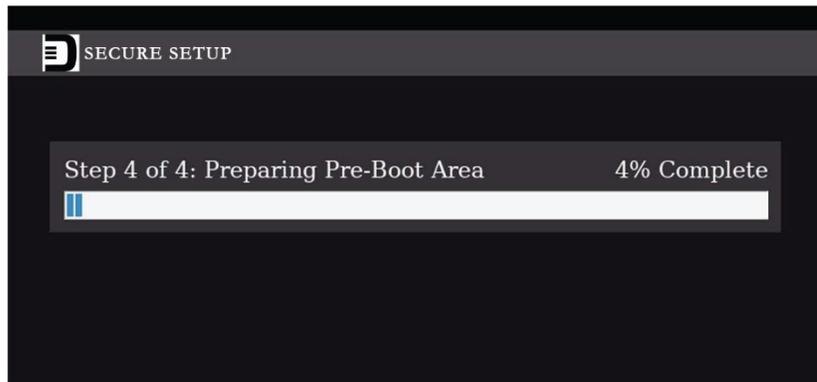
Password ●●●●●●●●

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.

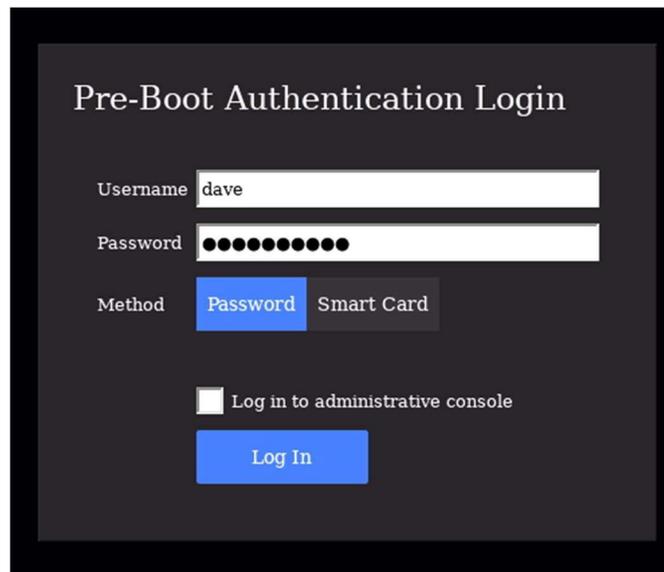


7. Once complete, power off the computer.
8. Remove the USB thumb drive from the computer.

4.1 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 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 Password Smart Card

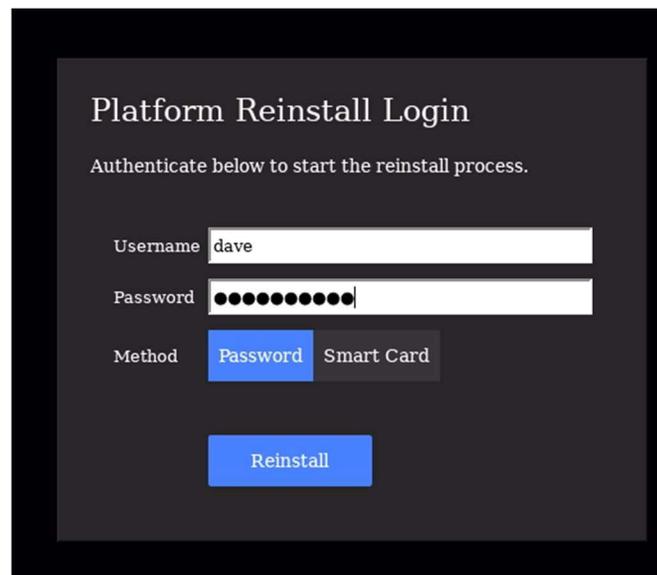
Log in to administrative console

5 Re-enabling the PBA

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

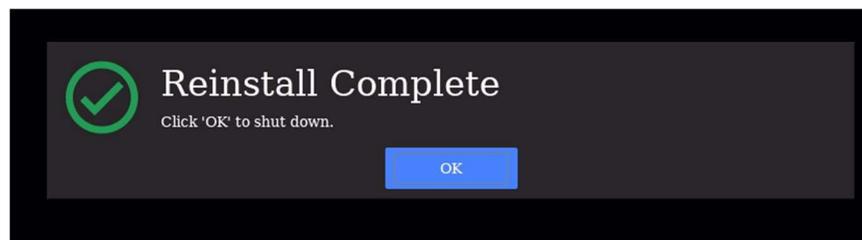
1. An installation USB drive of the same version of PBA software installed on the device. See section [Create a bootable USB PBA Installer thumb drive](#))
2. Administrator credentials to the disabled PBA environment

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 image shows a 'Platform Reinstall Login' screen. At the top, it says 'Platform Reinstall Login' and 'Authenticate below to start the reinstall process.' Below this, there are three input fields: 'Username' with the text 'dave', 'Password' with ten black dots, and 'Method' with two buttons: 'Password' (highlighted in blue) and 'Smart Card' (greyed out). At the bottom, there 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.

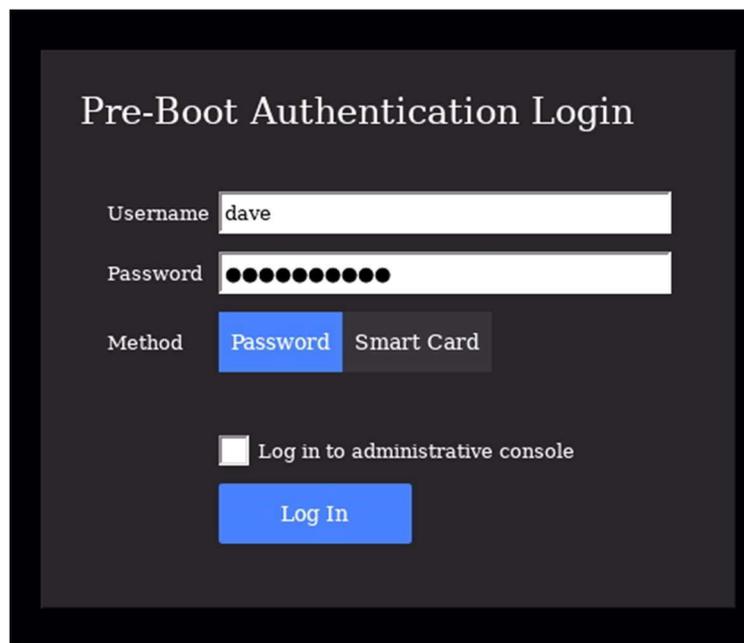


After shutting down restart the system. The PBA environment should once more present the normal login screen.

6 Logging in and Logging Out

6.1 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**.



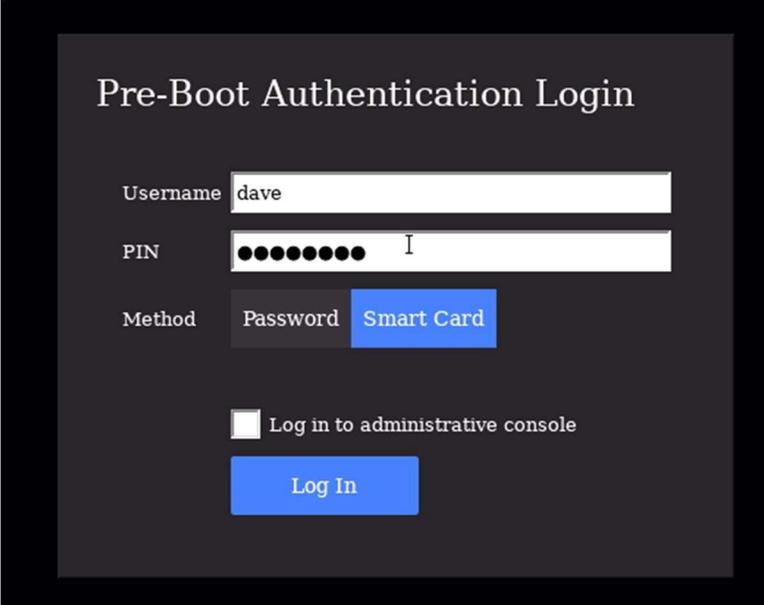
The image shows a 'Pre-Boot Authentication Login' screen with a dark background. At the top, the title 'Pre-Boot Authentication Login' is displayed in white. Below the title, there are three input fields: 'Username' containing the text 'dave', 'Password' containing ten black dots, and 'Method' with two buttons: 'Password' (highlighted in blue) and 'Smart Card' (greyed out). Below the input fields, there is a checkbox labeled 'Log in to administrative console' which is currently unchecked. At the bottom of the screen is a blue button labeled 'Log In'.

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

6.2 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**.



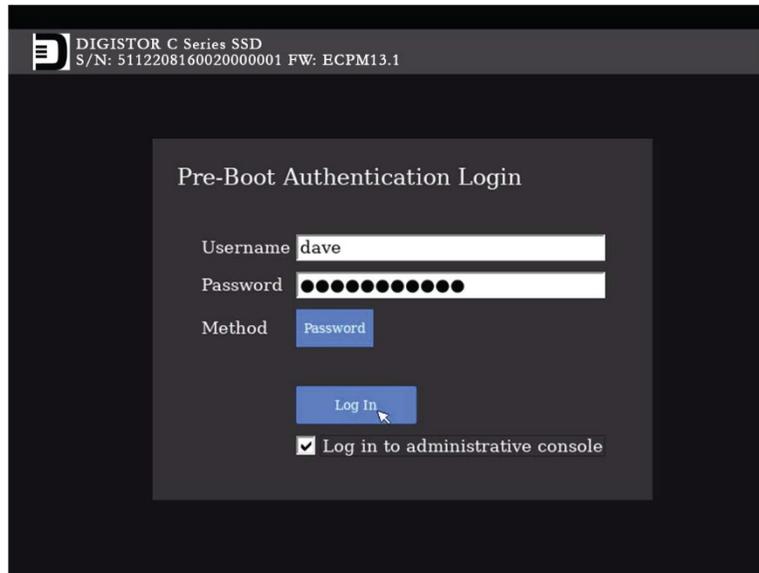
The image shows a 'Pre-Boot Authentication Login' screen with a dark background. It features the following elements:

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

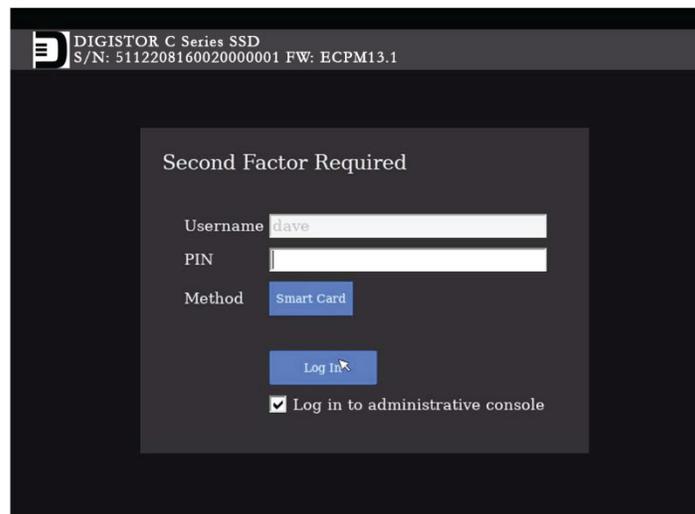
If the authentication is successful, your system will reboot and automatically start your operating system.

6.3 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.

6.4 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, first power off, then power on.

For more information about Citadel C Series SSDs please visit

<http://www.digistor.com/citadel/c-series>

©2022 CRU Data Security Group, LLC. ALL RIGHTS RESERVED.

This User Manual contains proprietary content of CRU Data Security Group, LLC ("CDSG") which is protected by copyright, trademark, and other intellectual property rights.

Use of this User Manual is governed by a license granted exclusively by CDSG (the "License"). Thus, except as otherwise expressly permitted by that License, no part of this User Manual may be reproduced (by photocopying or otherwise), transmitted, stored (in a database, retrieval system, or otherwise), or otherwise used through any means without the prior express written permission of CDSG. Use of the full Product Variables: Product Name (Short) product including, without limitation, its user interfaces, is subject to all of the terms and conditions of this User Manual and the above referenced License.

DIGISTOR is a trademark owned by CDSG and are protected under trademark law. This User Manual does not grant any user of this document any right to use any of the Trademarks.

Cigent is a registered trademark of Cigent Technology, Inc. and is used with permission.

Product Warranty

CDSG warrants this product to be free of significant defects in material and workmanship for a period of three (3) years from the original date of purchase. CDSG's warranty is nontransferable and is limited to the original purchaser.

Limitation of Liability

The warranties set forth in this agreement replace all other warranties. CDSG expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CDSG dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CDSG or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CDSG product or service, even if CDSG has been advised of the possibility of such damages. In no case shall CDSG's liability exceed the actual money paid for the products at issue. CDSG reserves the right to make modifications and additions to this product without notice or taking on additional liability.

A9-4500-01 Rev. 2.0