



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

Cigent Single and Multidrive PBA Quick Start Guide

Sep 2026

PBA Version 2.0.1.25

1 Quick Start Overview

This Quick Start Guide provides the standard workflow for preparing a system, installing Cigent PBA, and completing the initial sign in. The recommended installation method uses the Cigent CLI directly from a supported Windows or Linux operating system. A bootable USB installation method is included as an alternative for systems where CLI installation is not appropriate.

Recommended installation method: Cigent CLI. This method installs PBA directly from the operating system and does not require creating or booting from USB installation media.

Advanced configurations and complete CLI installation options are documented in the Cigent CLI Reference Guide and the full Cigent PBA Installation Guide and User Manual.

2 Before You Begin

2.1 What You Need

- A supported self-encrypting drive (SED), such as a Cigent Secure SSD, installed in the target system.
- The operating system installed and booting normally.
- The Cigent CLI and the PBA installation package available on the target system.
- Administrator or equivalent elevated access to run the Cigent CLI.
- An initial PBA administrator username and password.
- A reliable power source. Do not interrupt power while PBA is being installed or initialized.
- For the alternative bootable-media method only: a USB 3.0 or later flash drive and the extracted PBA Loader package.

2.2 Initial Administrator Credentials

The credentials specified during installation become the initial PBA administrator account. Choose the credentials before beginning installation.

Requirement	Value
Username	1-40 characters
Password length	8-128 characters

Requirement	Value
Password complexity	At least one uppercase letter, one lowercase letter, one number, and one supported special character

3 Prepare the Target System

3.1 Install the SSD and Operating System

Install the supported Cigent Secure SSD or other supported SED according to the computer manufacturer's instructions. Install and verify the operating system before installing PBA.

3.2 Configure UEFI/BIOS Settings

Verify the following firmware settings before installing PBA. Incorrect settings can prevent PBA from detecting the drive or can disable PBA features.

Setting	Required Value	Notes
SATA/NVMe Operation	AHCI	Required. PBA requires AHCI to recognize the SED.
Block SID Authentication	Off	Required. After disabling, proceed with PBA installation on the next restart because some systems may re-enable it automatically.
Secure Boot	On	Recommended. Required if TPM automatic authentication will be used.
Microsoft UEFI CA	Enabled	Required when Secure Boot is enabled. The standard PBA package is Microsoft-signed.

Note: Not every firmware setting is exposed by every system manufacturer. If a listed option is not available in the firmware interface, it can be ignored.

4 Install PBA Using the Cigent CLI (Recommended)

The Cigent CLI can install PBA directly from a supported Windows or Linux operating system. This method avoids the need to create a bootable USB installer and is the recommended path for a standard installation.

4.1 Prepare for CLI Installation

1. Ensure the Cigent CLI and the PBA installation package are available on the target system.
2. Open an elevated command prompt or terminal appropriate for the operating system.
3. Identify the physical drive that will be used as the PBA target.
4. Have the username and password for the initial PBA administrator account available.

4.2 Run the PBA Install Command

The following example from the PBA Installation Guide installs PBA to the specified target drive, creates the initial administrator account, enables the PBA, and returns JSON output. The example uses Windows command syntax.

Example:

```
.\\CigentCLI.exe install --target pba --target_user test_pba_admin -  
target_password DemoPBAUser345! --drive \\.\PHYSICALDRIVE0 --allow_os -  
pba_bin_file .\\pba_v2.0.1.25.pkg --enable --json
```

WARNING: The installation process can take 10 minutes or more. Do not interrupt the installation or power off the computer while PBA is being initialized.

Replace the example administrator credentials, physical drive, and PBA package path with the values for the target system. Refer to the Cigent CLI Reference Guide, Section 6.1 Installation & Updates, for the complete install command syntax and additional installation options.

For multidrive, RAID, alternate licensing, controller-based locks or other advanced installation requirements, use the applicable CLI options documented in the Cigent CLI Reference Guide.

4.3 Restart and Continue to Initial Sign In

After the CLI installation completes successfully, restart the target system. PBA authentication occurs before the operating system starts. Continue to Section 6, Initial Sign In, to verify the installation.

5 Alternative Method: Install PBA Using Bootable USB

Use the bootable USB method when installation from the operating system is not available or when the environment requires booting into the PBA installation environment.

5.1 Create the PBA Installation USB

WARNING: Creating the installer erases all data on the selected USB flash drive.

1. Extract all files from the provided PBA ZIP archive and keep them in the same directory.
2. Insert the USB flash drive.
3. Open an Administrator Command Prompt and change to the directory containing PBAloader.exe.
4. Run PBAloader.exe -i to start Interactive Mode.
5. Select the USB flash drive from the discovered drives.
6. Select Load as the operation.
7. Select the Microsoft-signed PBA package, for example pba_v2.0.1.25.bin.
8. Enter YES when prompted and wait for the utility to report that the PBA file has been written successfully.

```

Cigent PBA Loader v3.1.9
-----
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: 'SanDisk 3.2Gen1' SN: '0901479d8ff811521359' [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 a PBA file (-1 to quit)
-----
1) pba_v2.0.1.15.bin
2) custom_pba_v2.0.1.15.bin
1

-----
WARNING! This operation will destroy the data on the
selected drive!
-----
Operation: Load pba_v2.0.1.15.bin on SanDisk 3.2Gen1 [S/N: 0901479d8ff811521359]
Enter YES to continue or NO to cancel
YES

Loading PBA data
Writing PBA data: 100%
Validating PBA data: 100%
PBA file written

```

PBAloader Interactive Mode

5.2 Boot the Target System from USB

1. Power off the target computer.
2. Insert the PBA installation USB.
3. Power on the computer and open the system boot menu. Common boot menu keys include F1, F2, F10, F12, or Esc.
4. Select the USB flash drive and boot from it.

5.3 Select the Primary Drive

When the Secure Setup screen appears, select the primary drive. The primary drive is the drive on which PBA is installed and from which the PBA environment boots.

INITIALIZE

Prepare Secure Drive

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

Primary Drive Cigent Secure SSD M.2 2230 Alpha S/N: 51125010

☐ Protect Secondary Drive(s)

Username

Email

Password

Confirm Password

Connecting to a reliable power source recommended.

Initialize

Help

Secure Setup - select the primary drive

5.4 Optional: Protect Secondary Drives

If the system contains additional supported drives that should be protected during the initial installation:

1. Select Protect Secondary Drives.
2. Select one or more drives from the Non-protected drives list.
3. Use the double-arrow button to move the drives to the Protected drives list.
4. Click Save.

Selecting secondary drives

INITIALIZE

Protected drives

Non-protected drives

Supported Cigent Secure SSD ...
511250102023000358

Cancel Save Help

Secondary drive selected for protection

INITIALIZE

Protected drives

Non-protected drives

Cigent Secure SSD M.2 2230 ...
511250102023000358
Cigent Secure SSD M.2 2230 ...
511250102023000355

Cancel Save Help

5.5 Create the Initial Administrator and Initialize PBA

On the Secure Setup screen, enter the username, optional email address, password, and password confirmation for the initial administrator account. Verify the selected drives, then click Initialize.

INITIALIZE

Prepare Secure Drive

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

Primary Drive Cigent Secure SSD M.2 2230 Alpha S/N: 51125010

☒ Protect Secondary Drive(s)

Username admin

Email

Password

Confirm Password

Connecting to a reliable power source recommended.

Initialize

Help

Initial administrator credentials entered

WARNING: The installation process can take 10 minutes or more. Do not interrupt the installation or power off the computer while PBA is being initialized.



PBA initialization progress

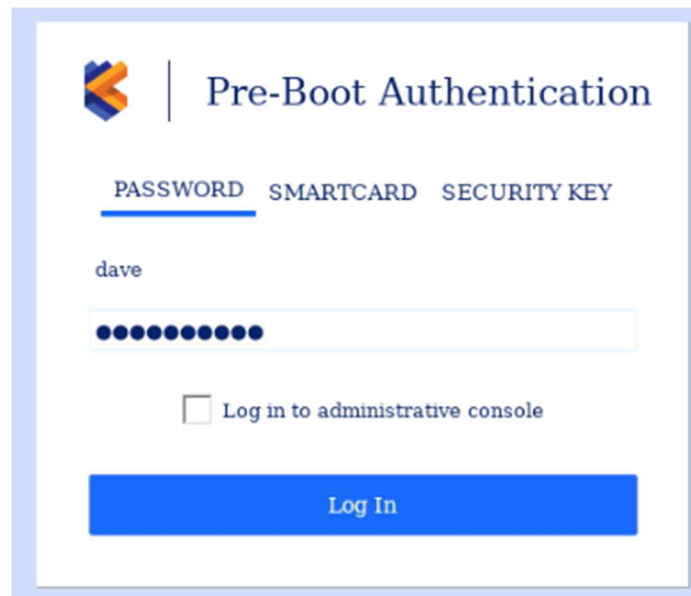
When initialization completes, the PBA login page is displayed. Remove the installation USB before continuing.

6 Initial Sign In

6.1 Verify the First Login

The initial credentials specified during installation have the Administrator role by default. Perform a normal login at least once before entering the administrative console so you can verify that the system successfully starts the operating system.

1. At the PBA login screen, enter the administrator username and password created during installation.
2. Leave Log in to administrative console unchecked.
3. Click Log In.
4. Verify that the system starts the installed operating system successfully.



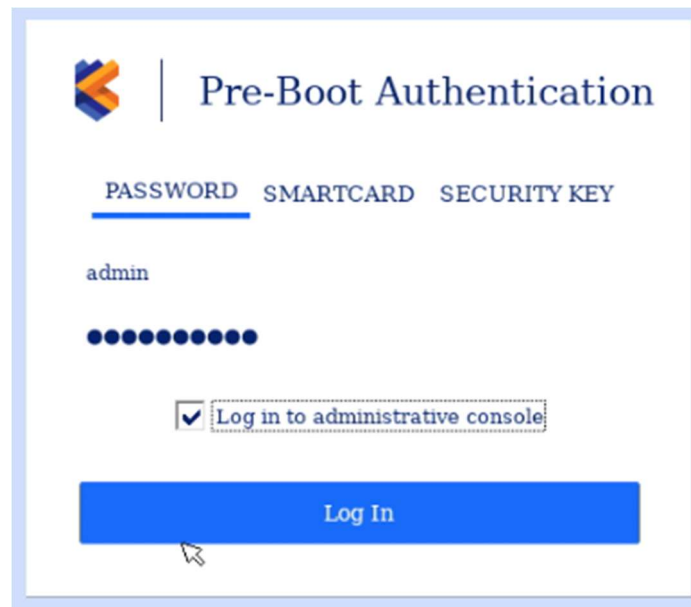
Initial PBA login

Note: After successful authentication, the protected drive is unlocked and the system starts the operating system. This confirms that the basic PBA installation is operational.

7 Optional: Access the Administrative Console

After confirming a successful normal login, administrators can enter the PBA Administrative Console to manage users, drives, settings, maintenance functions, and activity logs.

1. Restart or power on the system to return to the PBA login screen.
2. Enter the administrator username and password.
3. Select Log in to administrative console.
4. Click Log In.



Logging in to the PBA Administrative Console

8 Installation Complete

Your PBA is now installed and ready for use.

Use the full Cigent PBA Installation Guide and User Manual for additional configuration and administration, including:

- Adding, editing, and removing PBA users.
- Configuring smart cards, security keys, USB tokens, and two-factor authentication.
- Adding, removing, or importing secondary drives.
- Configuring login, password, chainload, and PIN Erase settings.
- Disabling, re-enabling, updating, reinstalling, or uninstalling PBA.
- Troubleshooting, system reports, PSID revert, and drive failure recovery.

9 Support

For PBA software downloads and support resources, visit <https://support.cigent.com>. For installation issues, the Help option on the PBA initialization page can be used to export a system report to a FAT32-formatted USB device for support review.

©2026 Cigent Technology Inc. All rights reserved. Cigent is a registered trademark of Cigent Technology Inc. in the United States and other jurisdictions.