Technical white paper

Digistor Citadel C series SSD Cigent PBA Guide and Technical Support paper

HP Digistor Citadel C Series SSD with Cigent preboot authentication (PBA)

Table of contents

Introduction....2
Initial installation....2
- Initial installation overview....2
- Citadel C Series PBA Installer and Manual....3
- Drive installation....3
- BIOS installation....3
- NVMe installation (required)....3
- Block SID authentication (required)....3
- Secure Boot....3
- System BIOS settings....4
- Create a bootable USB PBA installer flash drive....4

Known technical limitations....4
- Citadel FIPS Device Self-Test command....4
- Indicator light function....4
- Power management recommendations....4

Troubleshooting....5
- Replacing or recovering from a drive failure....5
- Drive lock error during boot symptoms....5
- Replacing or recovering from a failed secondary drive....5
- Replacing or recovering from a failed primary drive....5
- DriveLock passwords....5

Introduction

The Digistor Citadel C Series solid-state drive (SSD) represents a high-end security solution developed collaboratively by HP and Digistor. This self-encrypting drive (SED) is FIPS-certified, ensuring compliance with stringent security standards. When used in conjunction with Cigent® preboot authentication (PBA), this SSD effectively protects systems from unauthorized access.

Before starting any operating system or virtual machine stored on the drive, you must authenticate yourself using a username/password, Smart Card, or a combination of both. This authentication persists until the drive is turned off, ensuring that data remains secure at all times.

This document serves as a guide for installing the Digistor Citadel C Series SSD and the Cigent PBA software. For more information about how to configure user settings and options within the PBA administrative console, see Cignet's documentation.

With the Citadel C Series PBA implementation, you must provide trusted credentials directly to the SSD before the computer can recognize its presence. This security measure effectively prevents unauthorized access to the encrypted drive and its data, even if the SSD is physically removed from the system.

Implementing a zero-trust architecture by securing Data at Rest (DAR) is crucial in preventing cyberattacks and safeguarding sensitive information. The Citadel C Series SEDs—powered by Cigent—are specifically designed to protect sensitive data across various endpoint devices, including laptops and desktops.

Initial installation

Initial installation overview

The HP Citadel C SSD, part of the DIGISTOR Citadel C Series, comes with the Cigent PBA software preinstalled, but initially disabled. This allows you to set up and configure your operating system immediately upon unboxing. After the operating system installation is completed, you must enable the PBA to ensure full protection of your systems.

For the latest software and documentation, you can see the insert provided with your purchase, which contains the necessary links and passwords for accessing these resources. The DIGISTOR Citadel C Series Advanced SSD not only incorporates preboot authentication capabilities, but also offers enhanced security features accessible via Windows client software. Each configuration option is password protected to maintain security integrity.

To activate the preboot authentication feature and secure your drive, scan the following QR code, and then enter the password. You can find the password on the DIGISTOR card included in the box with your SSD.

For further support, contact support@cdsg.com.

Citadel C Series PBA Installer and Manual

Installer download: DIGISTOR_PBA_v1.0.6.43.zip (401.4 MB)

User Manual: Citadel_CSeries_Manual_A9-4500-01_Rev2.pdf (1.6 MB)

This technical white paper serves as a resource for understanding the features, known issues, and installation processes related to the Digistor Citadel C Series SSD and its PBA capabilities, aimed at ensuring the highest level of data security for end-users.

Drive installation

Install the DIGISTOR Citadel C Series SSD(s) using the HP system platform M.2 SSD installation instructions.

BIOS installation

Before installing the PBA software, make sure that the BIOS settings are configured correctly. Incorrect configuration might prevent the software from installing or disable certain features within the PBA. The BIOS is supported on computers with Citadel/FIPS Drives.

- HP Z6 G5A requires BIOS 1.1.24 or later
- HP Z8 G5/HP Z8 Fury G5/HP Z6 G5/HP Z4 G5 requires BIOS 1.2.17 or later
- HP Z2 G9 requires BIOS 03.03.15 or later

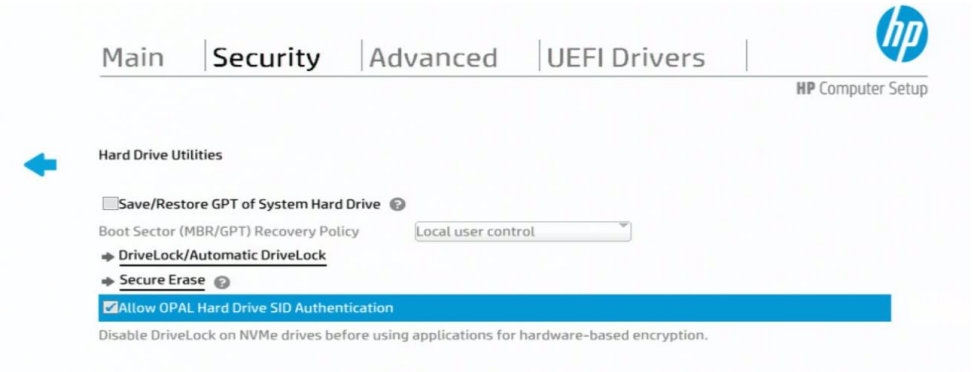
CAUTION: Downgrading a BIOS version is not supported on computers with a Citadel/FIPS drive. Older BIOS revisions lack compatibility fixes for S3 sleep and drive stability. This can cause data loss or reboot failures.

NVMe installation (required)

NVMe Operation sets the operating mode of the integrated storage device controller with a choice between Advanced Host Controller Interface (AHCI) and Redundant Array of Independent Disks (RAID). This configuration is located in the Storage section of the BIOS. This must be set to AHCI for the PBA software to recognize the SED.

Block SID authentication (required)

TCG storage devices, like self-encrypting drives, will block all attempts to authenticate the SID authority. Make sure that Allow OPAL Hard Drive SID Authentication is enabled.



Secure Boot

Secure Boot prevents unauthorized operating systems from running at boot time. Setting Secure Boot to ON is a best practice, but it is not required for installation of the PBA. If you plan to use the TPM authentication option with Tool Cigent_PBA_v1.0.6.43, you must enable Secure Boot.

System BIOS settings

BIOS setting	Required state
Configure Storage Controller for RAID or VMD	Disabled
Allow OPAL Hard Drive SID Authentication	Enabled

Create a bootable USB PBA installer flash drive

Before using the Citadel C Series SSD, you must activate the PBA. Follow these steps to create a bootable USB flash drive with the software you need to activate the PBA. For more information, see the CigentPBAInstallationandUserManual1.0.6.43.pdf.

CAUTION: This procedure erases all data on the drive.

1. Download the PBA installation software, or scan the QR code provided and enter the password located on your DIGISTOR service information card.

2. See the CigentPBAInstallationandUserManual1.0.6.43.pdf to start the PBA installation and pre-install PBA boot.

NOTE: HP recommends that you immediately change the default password or add a second administrator user and remove the original administrator user that came pre-installed with the PBA.

Known technical limitations

Citadel FIPS Device Self-Test command

The Citadel FIPS-certified SSD does not support the Device Self-Test command. This limitation might affect diagnostic capabilities, because the necessary BIOS presence is not available.

Indicator light function

You might observe that the Caps Lock and Num Lock indicator lights do not turn on when these keys are active. Despite this visual issue, the function of the keys remains intact, allowing normal operations.

Power management recommendations

The Preboot Authentication (PBA) function supports the Sleep (S3) mode in power management settings. However, for optimal security, HP recommends that you configure the computer to use Hibernate (S4) mode. To maximize security efficacy, avoid using Sleep (S3) mode.

Troubleshooting

Replacing or recovering from a drive failure

If the PBA is protecting more than one drive, the recovery procedure depends on whether the drive you are replacing is a primary or secondary drive. A failure of the primary drive results in a computer that is unable to boot to the PBA. A computer with a failed secondary drive can still boot to the PBA. Use one of the following procedures, depending on whether the primary drive or secondary drive is being replaced or has failed.

Drive lock error during boot symptoms

1. Turn off the computer and remove all Citadel/FIPS drives.
2. Turn on the computer and boot into BIOS, and then enable **Allow OPAL Hard Drive SID Authentication**.
3. Reinstall the drives and restart the computer.

NOTE: Upgrade to latest BIOS version. Make sure that the BIOS setting **Allow OPAL Hard Drive SID Authentication** is enabled.

Replacing or recovering from a failed secondary drive

1. Turn off the computer.
2. Install the replacement SSD.
3. Turn on the computer.
4. Log in to the PBA administrative console, and then select the **Maintenance** page.
5. Add the new secondary drive.
6. Restart the computer.

Replacing or recovering from a failed primary drive

1. Turn off the computer.
2. Create a bootable USB flash drive with the same version of PBA software that was previously installed.
3. Turn on the computer and boot to the USB flash drive.
4. Install the PBA to the primary drive. The secondary drive is not listed for selection as it already contains a PBA environment.
5. Restart the computer.
6. The login page indicates secondary drive(s) found.
7. Log in to the PBA administrative console, and then select the **Maintenance** page.
8. Import each of the secondary drives one at a time.

DriveLock passwords

If you see a message asking for a password before booting into the Cigent Installer or the Cigent PBA, review your BIOS settings and make sure that the SID authentication is **enabled**.

First Edition: April 2025