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

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 comprehensive guide for installing the Digistor Citadel C Series SSD and configuring the Cigent PBA software. It also outlines the necessary steps to configure user settings and options within the PBA administrative console.

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 systems 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 refer to 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.

For further support, contact support@cdsg.com.

Citadel C Series PBA Installer and Manual

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.

Known technical limitations

Citadel FIPS Device Self-Test command

The Citadel FIPS-certified SSD currently 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 illuminate 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 advises that you configure the system to use Hibernate (S4) mode instead. You are encouraged to avoid using Sleep (S3) mode altogether to maximize security efficacy.

First Edition: March 2025