Cigent® Full Drive Encryption (FDE) Installation Guide and User Manual

Feb 2026

FDE Version 1.2.1

Build 5

_____

1   Contents

_____

_____

1 Introduction

Cigent Full Drive Encryption (FDE) is a high-assurance data protection solution designed to secure sensitive information at rest through robust, full-drive encryption. Built with security and compliance in mind, Cigent FDE offers seamless integration with endpoint systems while maintaining strong safeguards against unauthorized access, physical theft, and advanced cyber threats.

This document provides comprehensive technical and operational guidance for deploying and managing Cigent Full Drive Encryption in environments requiring compliance with internationally recognized security standards. In particular, it outlines how Cigent FDE meets the requirements of the Common Criteria for Information Technology Security Evaluation (CC), providing assurance that the product has been rigorously designed, implemented, and tested to meet stringent security objectives.

Cigent FDE is suited for use in enterprises, government agencies, and critical infrastructure environments where protecting data integrity and confidentiality is paramount. With built-in support for pre-boot authentication, secure key management, and policy-driven access controls, Cigent FDE helps organizations enforce consistent encryption practices while minimizing impact on system performance and user productivity.

Whether you are preparing for a Common Criteria evaluation, managing secure deployments, or simply ensuring your organization aligns with industry best practices, this documentation serves as your authoritative guide to understanding, configuring, and operating Cigent Full Drive Encryption.

_____

2 System Overview

Cigent Full Drive Encryption (FDE) is an endpoint data protection solution that provides **transparent, full-drive encryption** to safeguard sensitive information stored on client devices. It ensures that all data on a system's storage device is encrypted at rest, making it inaccessible to unauthorized users, even in the event of physical loss or theft of the device.

The system is composed of a tightly integrated set of software components that operate at the lowest levels of the operating system and boot process, ensuring robust security from startup through runtime. Cigent FDE encrypts the entire contents of the storage drive, including the operating system, applications, and user data, using strong cryptographic algorithms and secure key management mechanisms.

The product is designed to conform to the **Common Criteria** evaluation process, providing assurances that the system has been developed according to rigorous international security standards. It implements controls to protect the **confidentiality, integrity, and availability** of user and system data against a range of threats, including unauthorized access, tampering, and brute-force attacks.

Key Features:
- **Pre-Boot Authentication (PBA):** Ensures only authorized users can boot and access the operating system.
- **Full-Drive AES Encryption:** Encrypts all sectors of the Windows OS volume using AES-256 XTS encryption.
- **Secure Key Storage:** Cryptographic keys are stored in an encrypted database using AES-256 encryption making them inaccessible and unreadable outside of the FDE environment.
- **Policy-Based Management:** Administrators can define and enforce encryption and access policies based on organizational requirements.
- **Tamper Detection and Response:** Includes capabilities to detect and respond to unauthorized attempts to bypass security controls.
- **Centralized Management Integration:** Supports remote deployment and updating using management systems including Microsoft SCCM, SolarWinds, etc.

Intended Deployment Environment:
Cigent FDE is designed for deployment on endpoint systems, including laptops, desktops, and workstations, in environments requiring elevated levels of data protection, such as:
- Government and defense agencies
- Regulated industries (finance, healthcare, energy)
- Enterprises with sensitive intellectual property

_____

- Organizations pursuing Common Criteria or similar compliance frameworks

2.1 Transition to Compliant Power Saving State

The Cigent FDE software is designed to ensure that no sensitive information remains in volatile memory after it is no longer needed. This includes cryptographic keys, user credentials, and any authentication artifacts. Upon shutdown or transition into a low-power state, the FDE software performs an orderly cleanup of sensitive material. The system is considered to have fully transitioned into the Compliant power saving state when all volatile memory used by the FDE has been reliably cleared.

Expected Transition Time
Based on internal testing and implementation behavior, the transition time for the Target of Evaluation (TOE) to enter the Compliant power saving state—i.e., the time required for volatile memory to be cleared—is as follows:
- Time to complete memory sanitization: typically under 1 second after FDE exit is initiated.
- This process is triggered automatically as part of the normal shutdown or handoff sequence to the BIOS/Firmware/OS bootloader.

Additional Notes
Sanitization routines include zeroization of all sensitive memory buffers used during authentication.

_____

3   Initial Installation

3.1   Initial installation overview

You can obtain a copy of the FDE software:

- Visit https://support.cigent.com Here you will find instructions on how to request a trial or paid subscription.
- If you already have a Full Drive Encryption subscription, you can download the Cigent FDE software from the downloads page of the Cigent Management console.

3.2   Operating System installation

A supported operating system should be installed and fully patched prior to starting installation.

- Microsoft Windows 10 version 1809 x64 or greater
- Microsoft Windows 11 version 21H2 x64 or greater

> **It is highly recommended that you backup your system prior to installation.**

3.3   Expected Behavior after installation

Cigent Full Drive Encryption is compatible with Microsoft BitLocker and is designed to be installed before BitLocker is enabled. During installation, even if BitLocker is disabled, the system may briefly display a message indicating that BitLocker could not be enabled. This behavior is expected and typically occurs only during the first restart following installation.

During installation, the Cigent Full Drive Encryption software updates the system boot process. As a result, users who normally sign in with Windows Hello may be prompted to sign in once using their password or smartcard after the initial restart. After signing in, Windows Hello can be reset, after which the Windows Hello sign-in method will function normally again.

_____

3.4 Install Cigent FDE

Cigent FDE will only protect the Windows OS drive currently. Multiple drives will be supported in a subsequent release.

Note: Administrator privileges are required to install Cigent FDE.

1. Double click on the installer executable to start the installation.

2. Select the checkbox to agree to terms of use and then click Next.
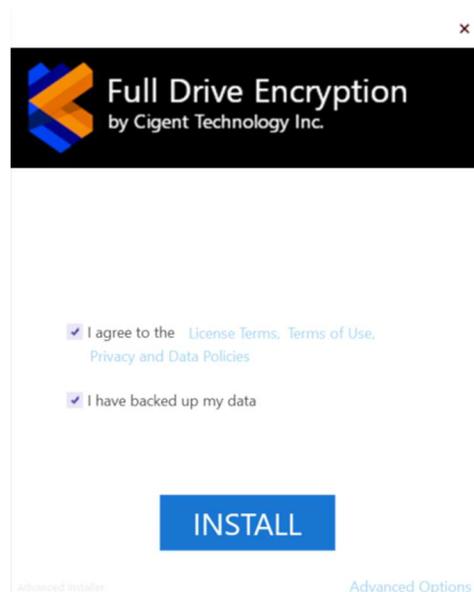
3. Setup Credentials. This is the password you will enter on the EFI setup page after restart. You can choose to use the default password (Admin6174!) or enter your own setup password by unchecking the Use Default Password checkbox. Then click Install.

The process may take a few minutes to complete.

4. Click Finish to complete the installation.

5. It is highly recommended that you restart immediately after installation.
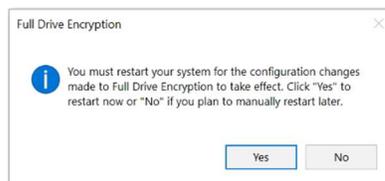
6. Upon restart, you will see the FDE authentication setup page. You may complete the setup now or click cancel to complete the setup at a future date.
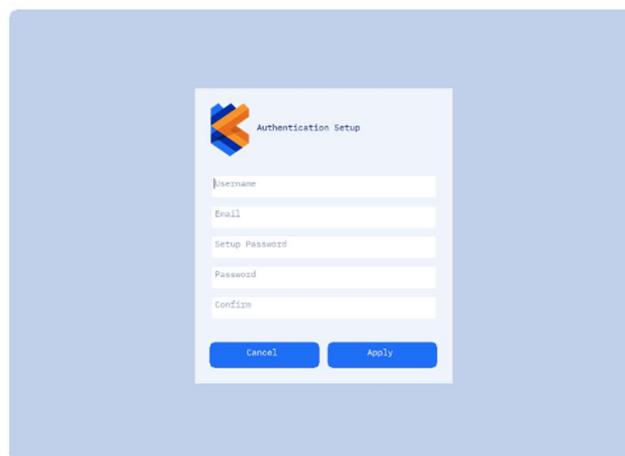
7. If you choose to complete setup now, enter a username and password twice. Enter the Setup Password used when installing in windows then click Apply.
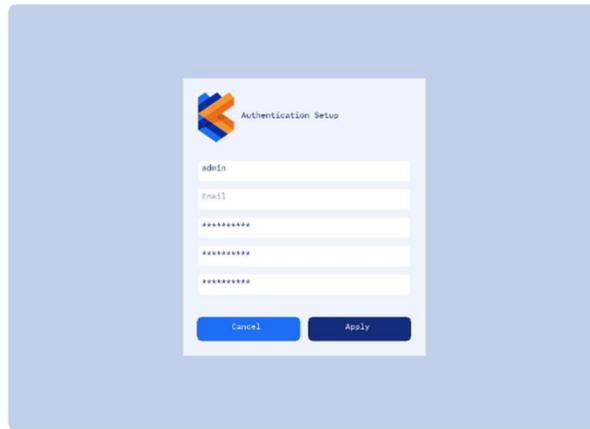
Windows will now start. Logging into Windows will initiate the full drive encryption.

_____

3.5 Installing Cigent FDE Using MSI

In addition to the executable installer, Cigent FDE can be deployed using an **MSI package**. This method is intended for administrators who need to automate deployments through scripts, Group Policy, or enterprise software management tools.

NOTE: After the execution of the MSI installation command a reboot is required to initiate the encryption of the drive.

Example Command

```
msiexec /i "FDE_Installer_v1.1.6.msi" /qn USER_NAME="cigent" USER_CRED="Cigent1!" USER_EMAIL="cigent@cigent.com"
ACCEPT_EULA=Y DATABACKEDUP=Y ENROLLCODE="Cigent123!" ENROLL_USAGE_LIMIT=10 /l*v "logfile.log"
```

Required Parameters
These parameters are required for running any MSI install.
- **ACCEPT_EULA**
  This parameter must be passed and set equal to Y, ensuring the user has accepted the end user license agreement.
- **DATABACKEDUP**
  This parameter must also be passed in and set equal to Y, making sure the user has backed up their data.

Mutually Exclusive Parameters
Each of these parameters are used mutually exclusive of each other and lead to a type of install. The first two use the original UI style install, requiring the creation of the admin user on restart. The last skips the EFI creation and automates creation of the initial admin user.
- **USER_PASSWORD**
  The **setup password** normally entered in the graphical UI. Follows the same password requirements as the UI.
- **USE_DEFAULT_PASSWORD**
  Install using the default password offered in the graphical UI.
- **USER_NAME**, **USER_CRED**, and **USER_EMAIL***(Optional)*
  Install and set up an admin user with the username and password described in the above parameters. An email can also be passed in but is not required.

Optional Parameters
- **APPDIR**
  The installation location of the FDE software.
  Default: C:\Program Files\Cigent\FDE.
- **ENROLLCODE**, **ENROLL_USAGE_LIMIT**, and **ENROLL_EXPIRES_UTC***(Optional)*
  These inputs create an enrollment code to be used for smart cards on install. The code is the code used to enroll. The usage limit is the number of users that can use the enroll code. The expiration date is the expiration time of the enrollment code. ENROLLCODE and ENROLL_USAGE_LIMIT both are required. ENROLLCODE follows

_____

the above password requirements but must be 10 to 128 characters in length. ENROLL_USAGE_LIMIT must be a nonnegative integer. Setting it to 0 allows unlimited usage.

Notes
- The /qn switch enables a **silent installation** with no user interaction.
- Ensure that the system meets all prerequisites (Windows 10 or 11, fully patched, with backups performed) before running the MSI.
- After installation, restart the system to complete setup and enable pre-boot authentication.

3.6 Initial login

The user credential entered during installation has an administrative role by default. It is recommended to 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 FDE login page will automatically load.
2. On the login screen, enter the credentials you used during the FDE installation process.
3. Click Log In.
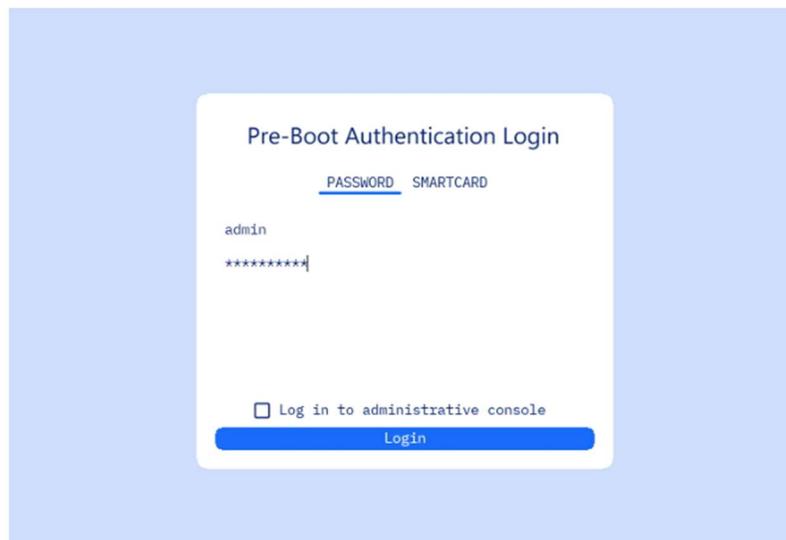
For details on how to log in to the administrative console, see section Using the Administrative Console.

_____

4   Using the Windows application

After signing into windows, you will see a Cigent FDE icon in the tray. When the icon is green, a drive is being encrypted or decrypted otherwise it is the normal Cigent icon.

1. Right click on the tray icon to open the menu. Select Status to open the Dashboard.
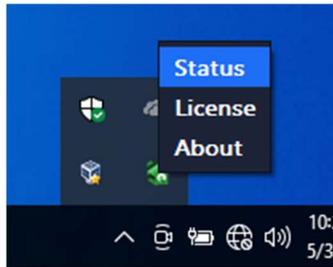
4.1   Status Page

During encryption, the dashboard will show encryption progress updating every few seconds or so.

Once encryption has completed, the dashboard will display Encrypted next to each drive.

_____
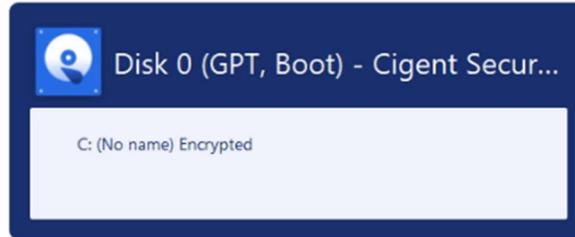
4.2 License page

A 30 day trial license is automatically generated during installation. A full license will need to be obtained using the Request Code. (See Requesting a license key.)
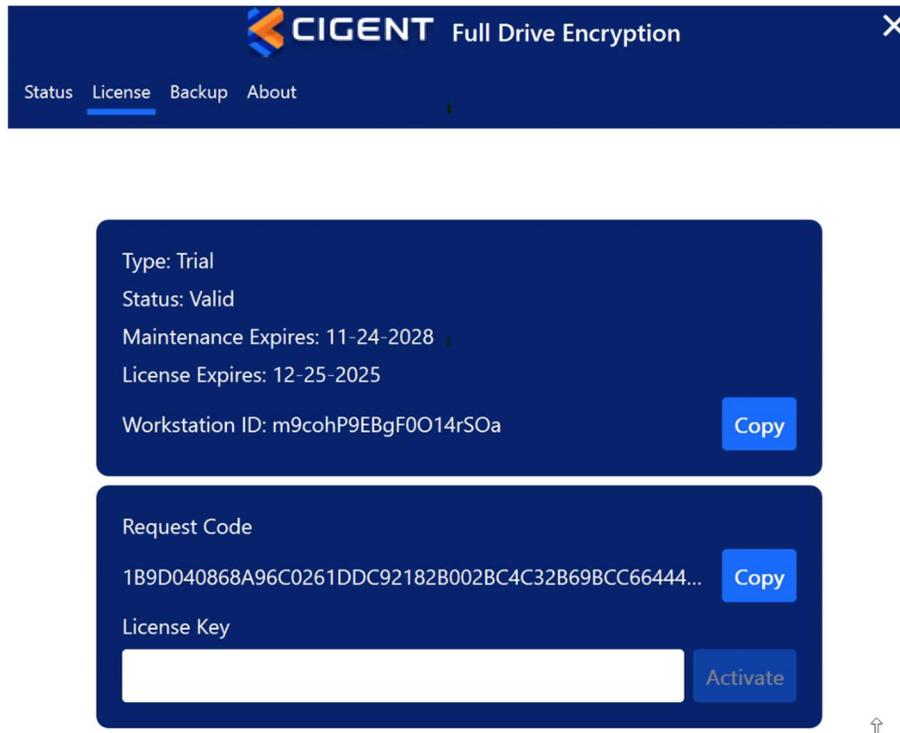
4.3 Backup page

See Backup and Recovery section for details.

_____

4.4 About page

The About page displays details about the application version, contact information for Cigent and user policy links.

_____

4.5 Requesting a License Key

During the installation process a 30 day trial license is automatically generated along with a unique Workstation ID. If you have an Cigent FDE subscription, a permanent license key can be self-generated by uploading the Request Code to the Full Drive Encryption page in the Cigent Management console (https://central.cigent.com) This key can then be used to activate the application permanently.

1. Open the Cigent FDE application and navigate to the License page.
2. Click Copy to place the license Request Code into your clipboard.
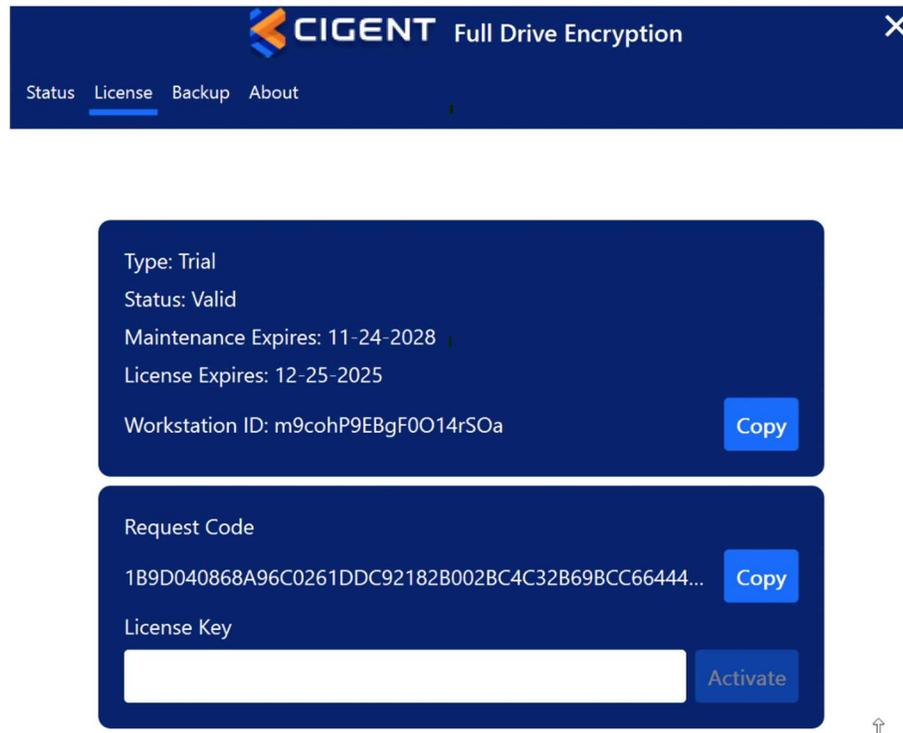
3. In the console, navigate to the Your Products page and select the Full Drive Encryption product link under the Full Drive Encryption subscription.

_____
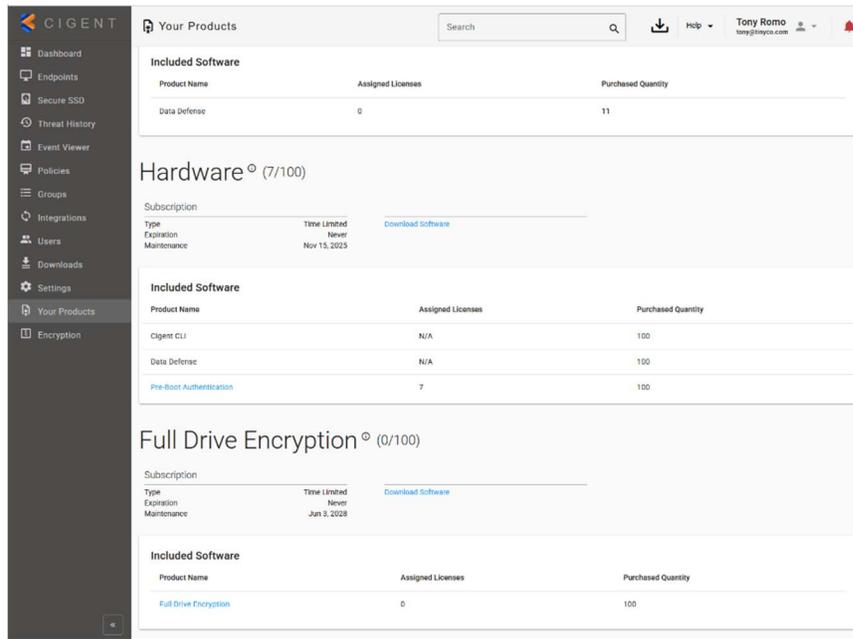
4. Click in the Request Code input box and paste the code into it. Click Generate License.
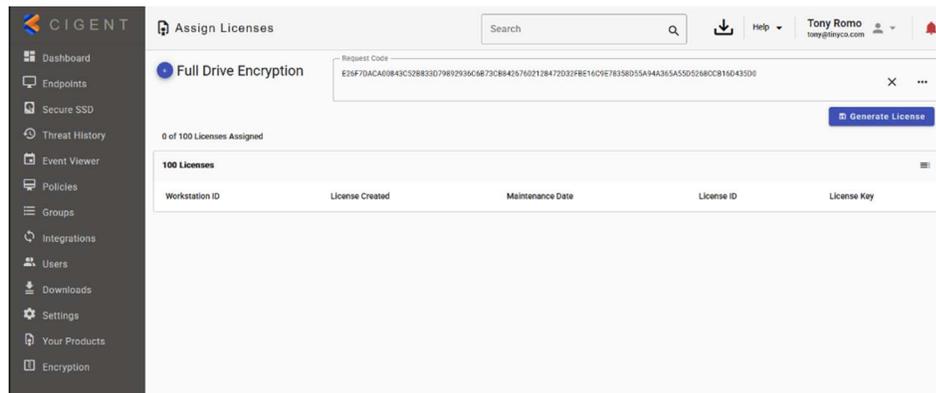
5. Click the Copy License icon to place the license key into your clipboard.
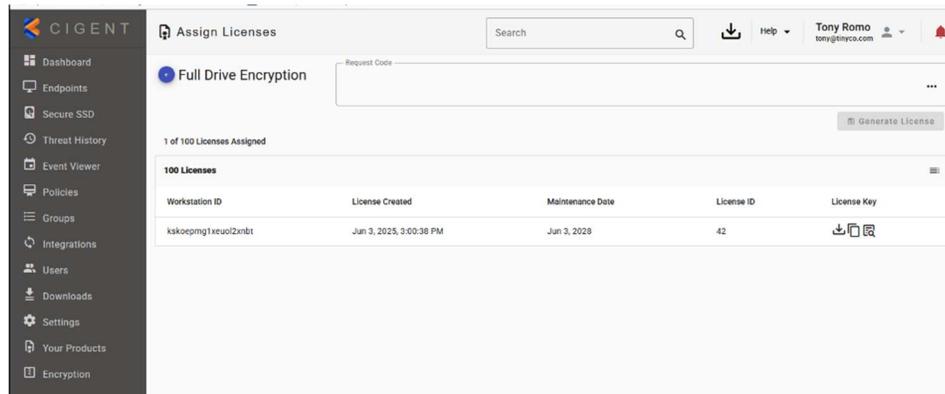
6. Paste the License Key into the License Key input box then click Activate.

7. Your Cigent FDE is now fully licensed.

_____

5 Using the Administrative Console

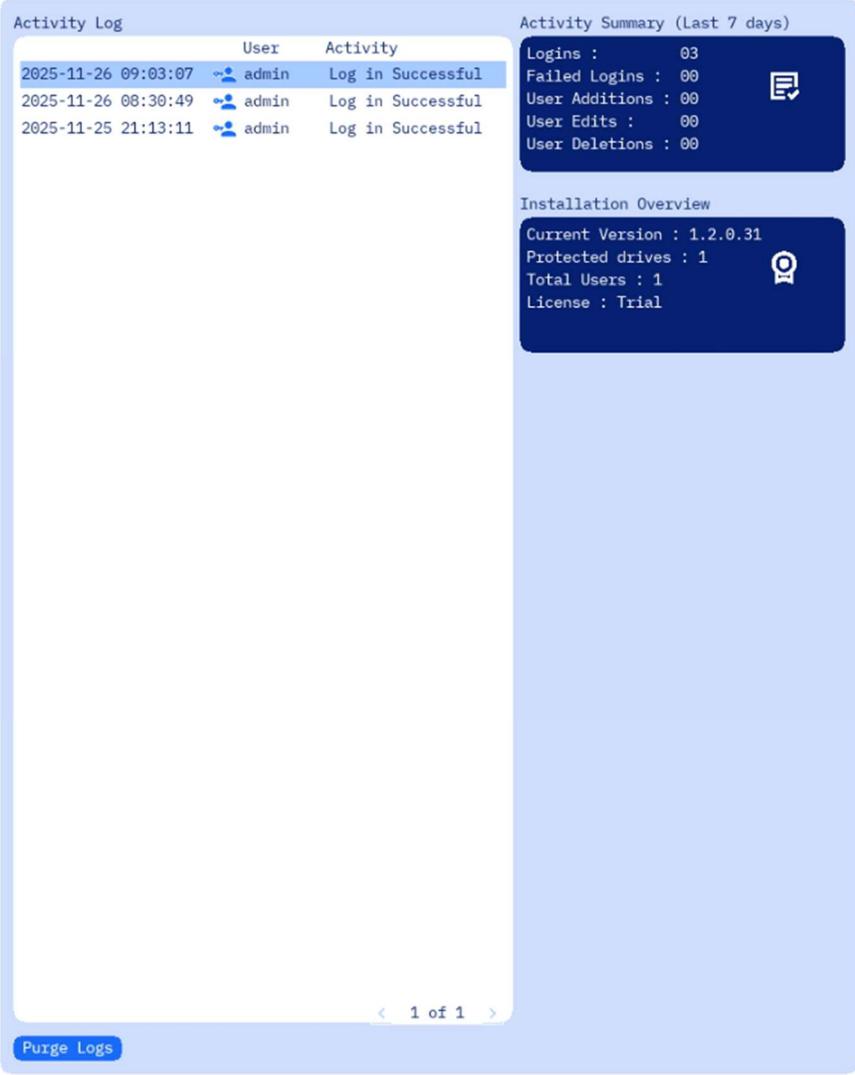The administrative console allows administrators to manage users, perform maintenance tasks, and view activity logs pertaining to the FDE environment.

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

PASSWORD   SMARTCARD

admin

****

☑ Log in to administrative console

Login

_____
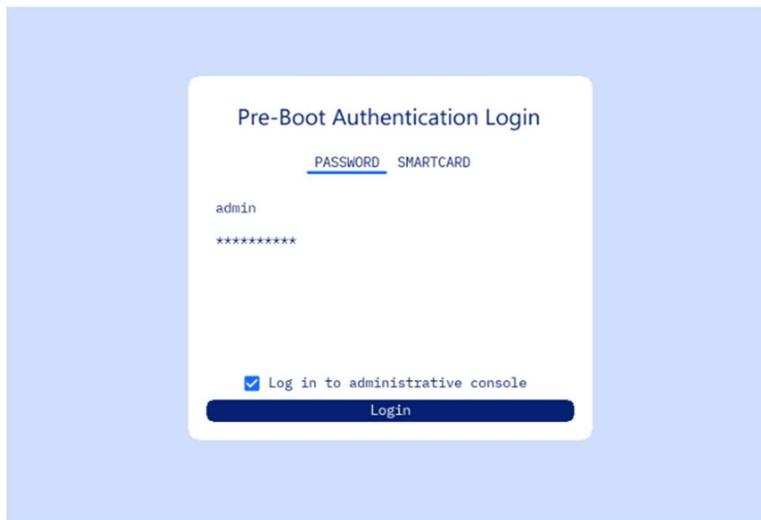
5.1 Dashboard

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

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.

5.2 Maintenance

The maintenance page allows administrators to uninstall the FDE PBA environment, disable the FDE PBA, and erase the drive by changing the encryption key.
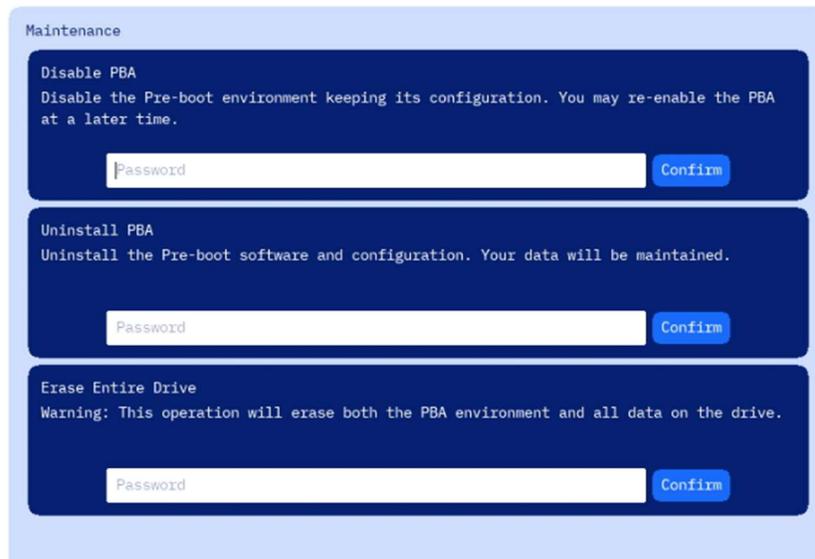
5.2.1 Disable PBA

Disabling the FDE 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 FDE will require interrupting the automatic login and authenticating as an existing administrative user. See Re-enable FDE for details.

5.2.2 Uninstall PBA

FDE PBA uninstallation should be initiated from the EFI application. Once you click Confirm, the application will close and proceed to windows. Decryption will automatically start. Once

_____

decryption is complete, you can uninstall the application using Windows Add/Remove programs.

5.2.3   Erase Entire Drive

The Erase Entire Drive feature allows administrators to cryptographically erase the protected data by erasing the encryption metadata which ensures all data on the drive is unrecoverable. Note that the protected volume is not deleted but its contents are no longer useable.

Once complete, power off the system.

_____

5.3 Users

The Users page allows administrators to add, modify, and delete user accounts from the PBA environment. Non-administrative users can use this page to change their password and modify other forms of authentication.
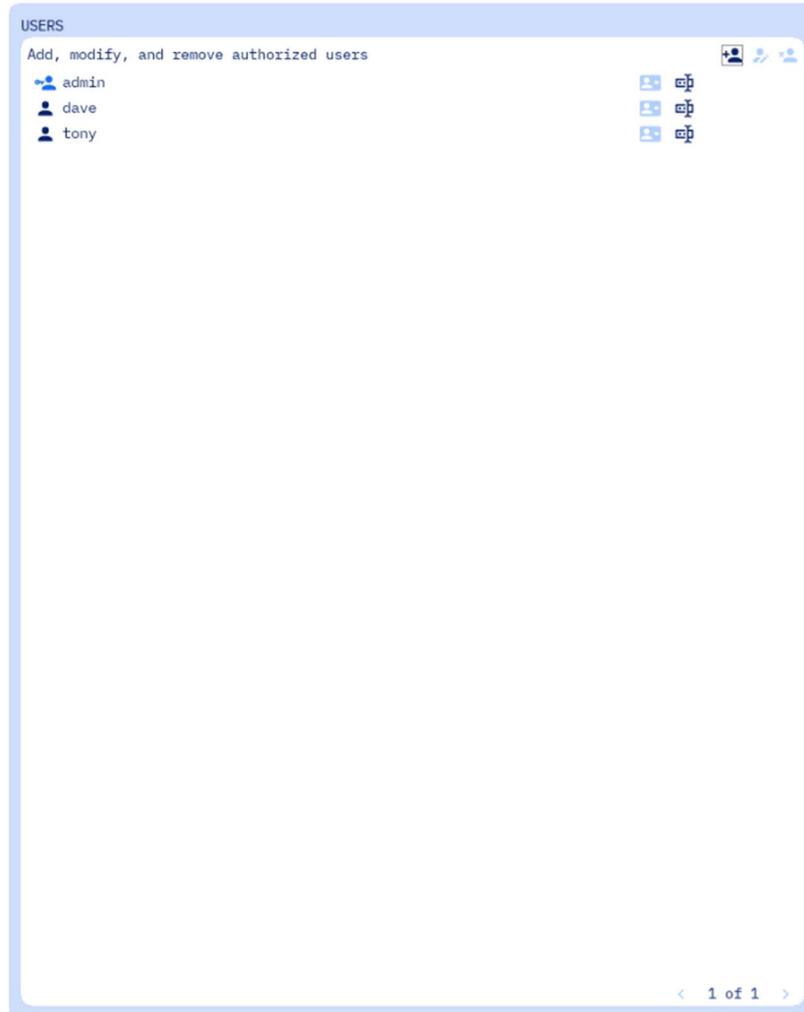
Roles and Capabilities

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

_____

5.3.1   Authentication options and requirements

Each FDE user can be configured with two different authentication options: password or smartcard. When adding users, password is required while Smartcard is optional.

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

Smartcard

Any smartcard or device supporting NIST SP 800-73-4 – *Interfaces for Personal Identity Verification* are supported. This includes Common Access Cards (CACs), SIPR tokens and multiprotocol security keys that support the PIV interface (for example Swissbit iShield and Yubikey 5 series.) Authentication requires the presence of the device as well as a PIN. The PIN is setup separately from FDE.

To add a smartcard to a user, ensure the smart card is inserted and click *Scan*. The dropdown will show supported certificates on the card. Enter the already configured PIN before saving the changes.

5.3.2   Add User

The Add User page is used to add a new user using password and optionally a smartcard.

www.cigent.com
_____

```
Add User
   Username         todd
   Administrator    ☐
   Email            todd@tinyco.com
   Password         **********
   Confirm          **********
   Smart card       None                                    ⌄  [Scan]
                    PIN




                        [Cancel]  [Add]
```

1. Enter a unique username.
2. Set the Administrator role as desired.
3. Enter an email address. (Optional)
4. Enter and confirm a password.
5. (Optional) Select the smart card certificate from the menu and enter the PIN.
6. Click *Add*.

Click the Scan button next to Smartcard if your device is not listed after inserting the card.

5.3.3   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

1. Select an existing user from the table and click the edit user icon.
2. Change one or more user attributes.
3. Click Save.

Note that to Add a Smart Card to an existing user, the device should be inserted before entering the page. If you do not see the device listed after inserting it, click Scan.
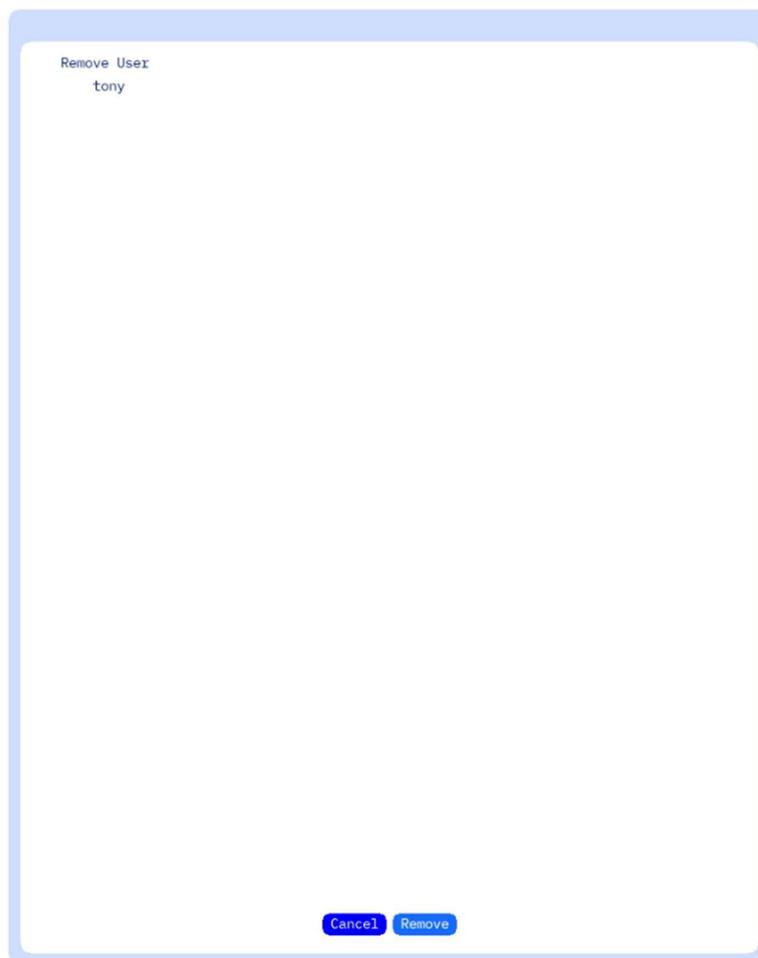
_____

5.3.4   Remove User

Removing a user will permanently delete a user from the FDE environment. Users will no longer be able to authenticate to the FDE to access the protected operating system nor the FDE administrative console.

1. Select an existing user or users from the table and click the remove user icon.
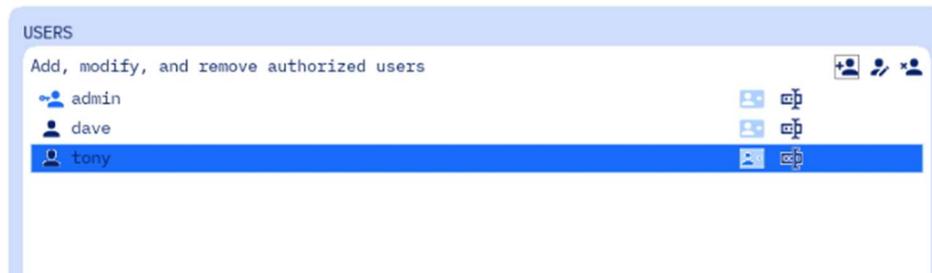
2. Click Remove.

_____

5.4 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.

5.4.1 Settings - Login

Failed logins before lockout

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

Min: 1 *Max*: 10

Failed logins before erase

The number of consecutive failed login attempts before the drive is automatically erased.
Only attempts with valid usernames are considered towards failures.
Min: 0 (Disabled) *Max*: 999

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.

_____

5.4.2   Settings - Password

SETTINGS
LOGIN   PASSWORD

Password History
Number of unique passwords before reuse allowed (per user)(1-20) |1

Password Length
Minimum length of password (8-128)   8

Cancel   Save

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.
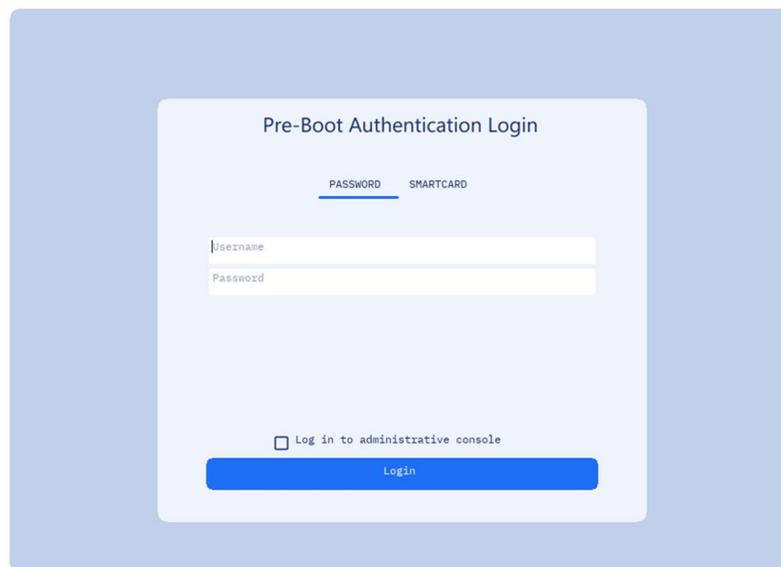
Min: 1 *Max*: 128

6 Re-enabling the Cigent FDE

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

1. Interrupt the automatic login countdown by pressing any key before the timer expires.
2. Login as an administrator
3. On the Maintenance page, enter your password in Enable PBA and click Confirm.

Maintenance

Enable PBA

Enable the Pre-boot environment keeping its configuration.

**********   Confirm

4. The system will restart and present the normal login screen.

Pre-Boot Authentication Login

PASSWORD   SMARTCARD

Username

Password

☐ Log in to administrative console

Login

_____

7   User Self Enrollment

In some situations, it may be necessary to allow users to self-enroll as a user of the FDE. This could be if the recipient of the device is in a remote location or no administrator is located at a remote site. To support this scenario, administrators can enable user self enrollment using a smart card. The self enrollment capability and UI are enabled using the FDE MSI install or with command line options. Administrators can specify an enrollment password with a usage quantity and expiration timestamp. See the MSI install for additional information.

7.1   User Self Enrollment using Smart card

If an enrollment password is configured the login page will display a self registration option.
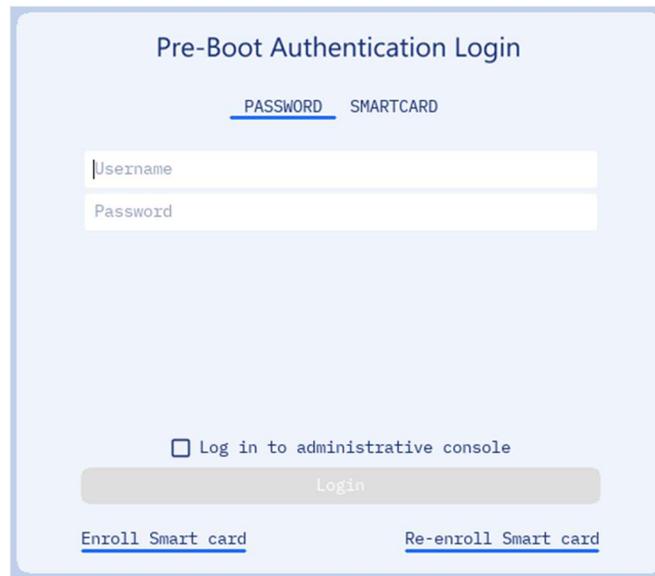
1. From the EFI, log in page, click Enroll Smart card.
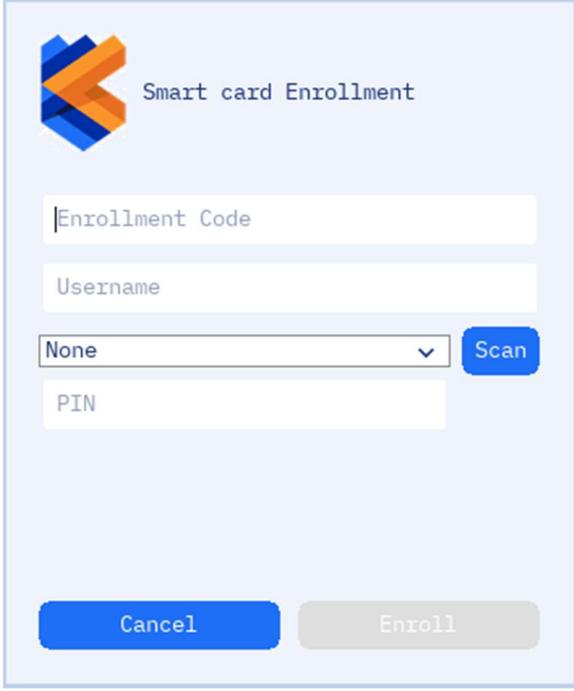
_____

2. Enter the provided enrollment code, a unique username and your smart card PIN, then click Enroll.
3. Click Ok to return to the login page.
4. The user can immediately login to the FDE using their smart card.

7.2 User Self Re-enrollment using Smart card

If a smart card only user receives a replacement smart card, they will need to use the Re-enroll page to update their smart card in the FDE.
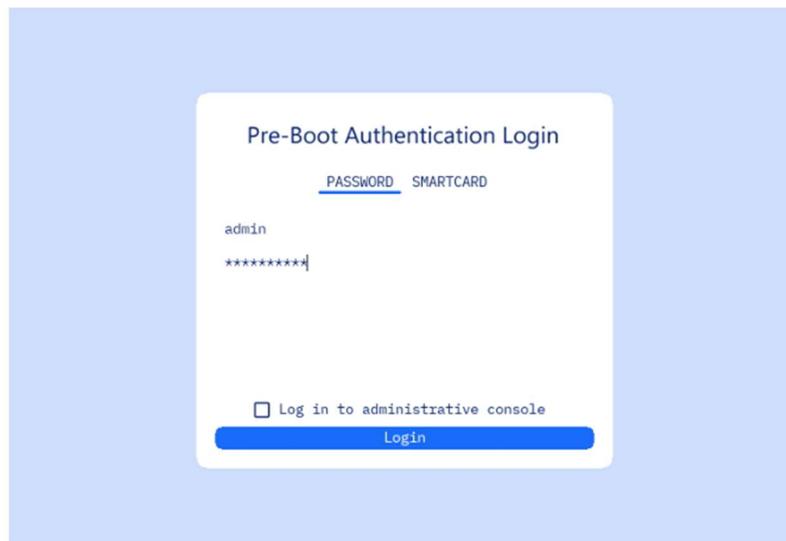
1. Click Re-enroll Smart card
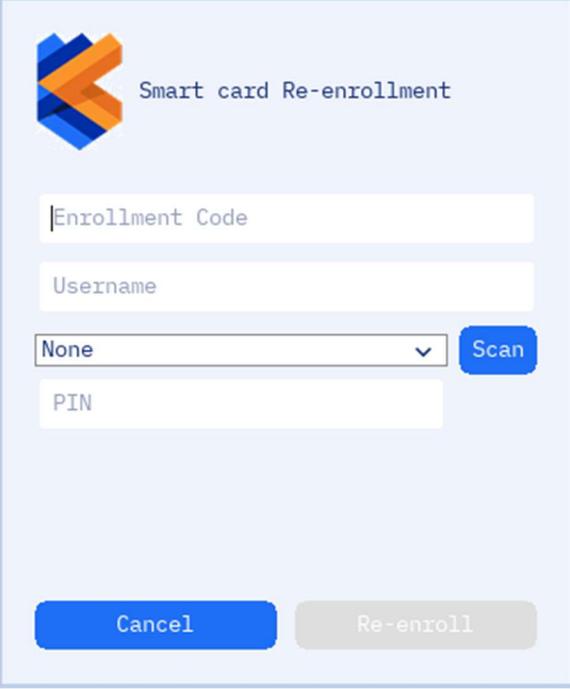
2. Enter the provided enrollment code, your existing username and your new smart card PIN, then click Enroll Smart Card.

_____

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.

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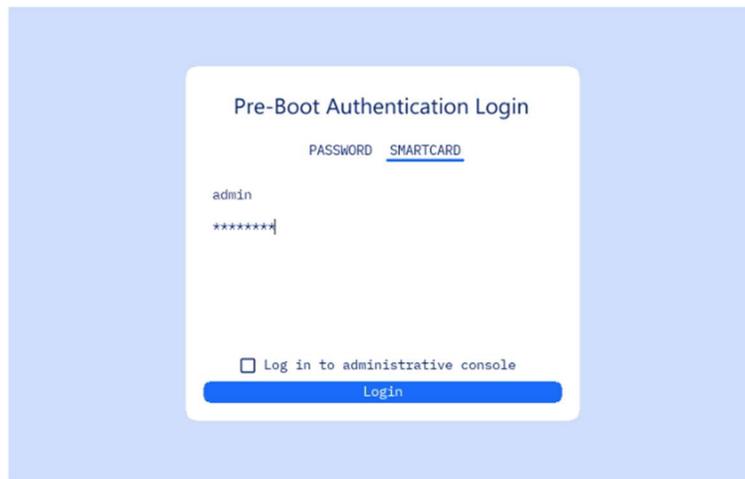
If the authentication is successful, your system will reboot and automatically start your operating system.

8.3 Logging out of the FDE 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.

_____

9 Backup and Recovery

It is strongly recommended that you create a backup of your Cigent FDE configuration files immediately after installation and after any configuration changes. Store these backup files in a secure location separate from the system being encrypted.

The recovery process involves:
1. Downloading the Cigent FDE recovery image from the Cigent Support site.
2. Creating a bootable USB drive using that image.
3. Copying your previously created backup file to the USB drive.
4. Booting the affected system from the USB drive and restoring the configuration files.

9.1 Create bootable OS device

1. Obtain latest Bootable FDE Recovery OS binary file from support.cigent.com.

2. Open Full Drive Encryption dashboard and navigate to the Backup page.
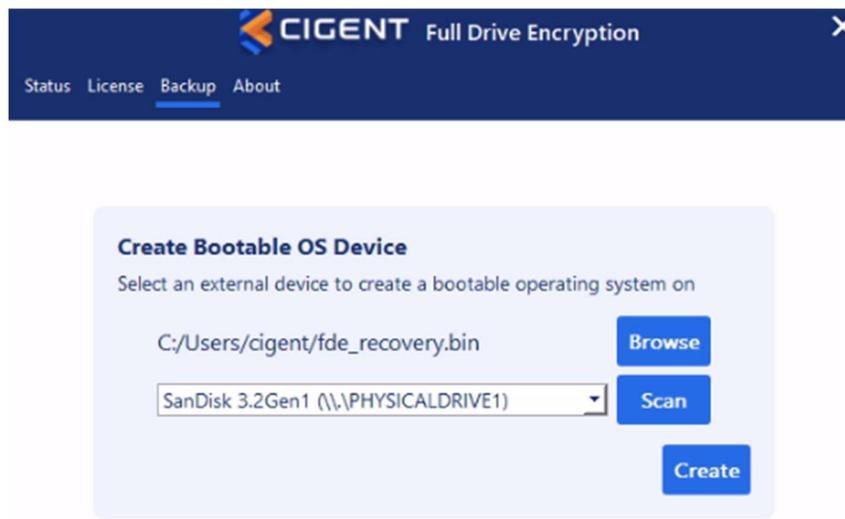
3. Click Browse and select the newest Bootable FDE recovery binary file (fde_recovery.bin)
4. Click Scan and select the desired USB device to make bootable.
   WARNING: The USB device will be overwritten, any data on this device will be lost
5. Click Create to start creating the bootable device.

_____
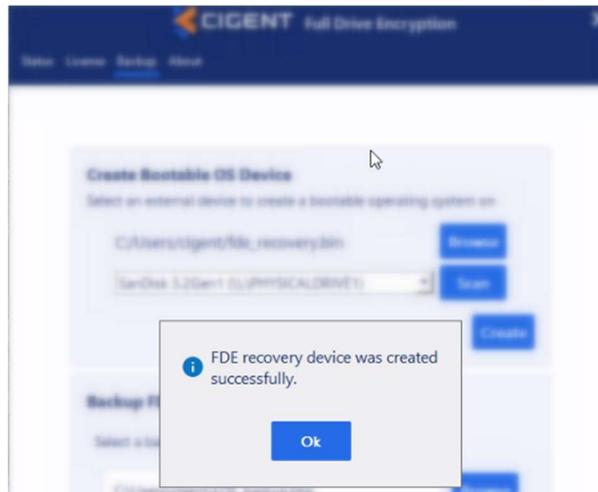
6. Once complete, click OK.

   Note: During the creation of the bootable USB drive, an additional DATA partition is automatically created. Place the recovery file created while following the steps in **Create FDE backup file** in this location.
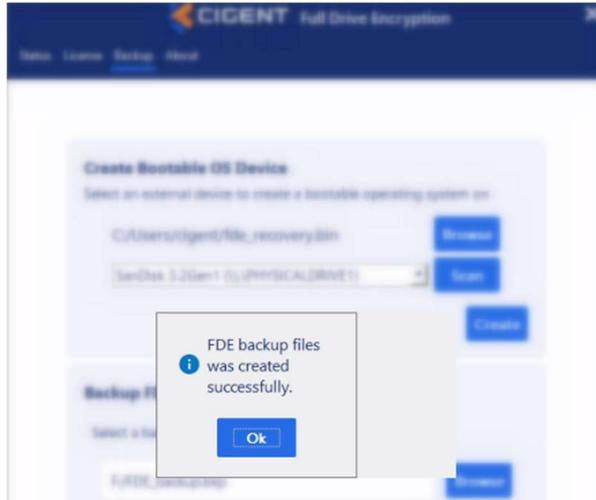
9.2 Create FDE backup file

1. Open FDE Dashboard and navigate to the Backup page.
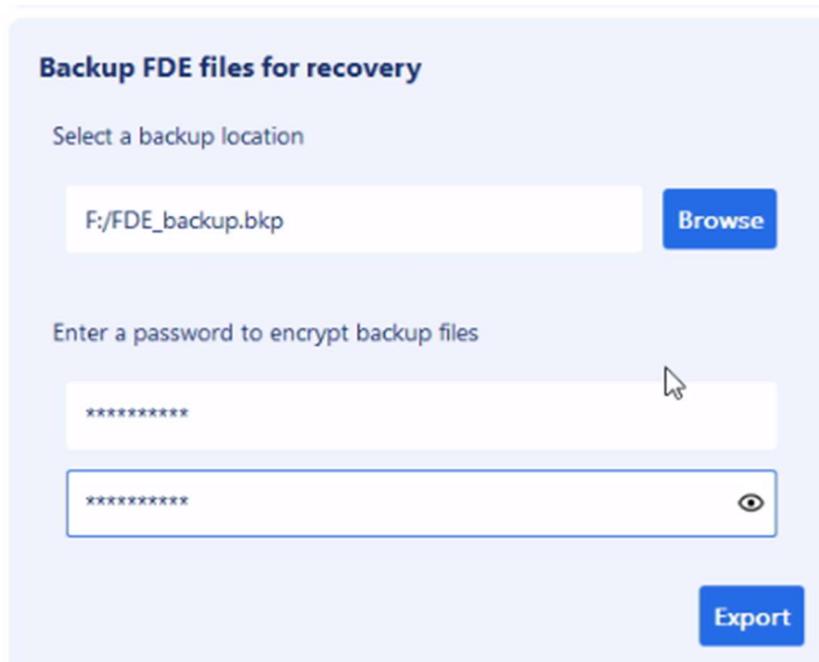
2. Select the destination for the backup file.
   Note: If you have previously created the USB recovery drive, please place the backup file on the DATA partition of that drive.

_____

3. Enter a password to encrypt the backup file.
   This password is separate from the FDE login password.
4. Re-enter the password to confirm.
5. Click Export to generate the encrypted backup file.

9.3 Restore FDE backup file

1. Insert and boot from the FDE recovery drive.
2. Once booted, the FDE Recovery will automatically mount and detect all available backups. Select the desired backup file from the drop down.
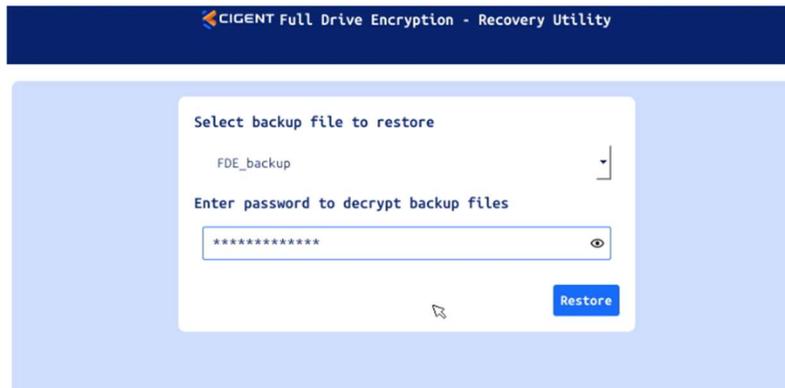

3. Enter the password to decrypt the back file. This is not the FDE admin/user login password.
4. Click Restore to start the restore process.
5. Once complete, you will be prompted to restart the system.
6. It is highly recommended to log into FDE to review/update all authorized users

_____

10 Updating Cigent FDE

For information on obtaining the newest version of Cigent FDE see section Initial Installation. When you are ready to update the Cigent FDE software, initiate the update by double clicking the EXE from Windows explorer.

It is strongly recommended that you create a backup of your Cigent FDE configuration files prior to updating. See Backup and Recovery for instructions on creating a backup.

The first part of the update process performs a digital signature verification to ensure integrity and authenticity of the Cigent FDE software. Failure of the signature verification will result in an error message. If you receive this message, redownload the Cigent FDE or contact support.
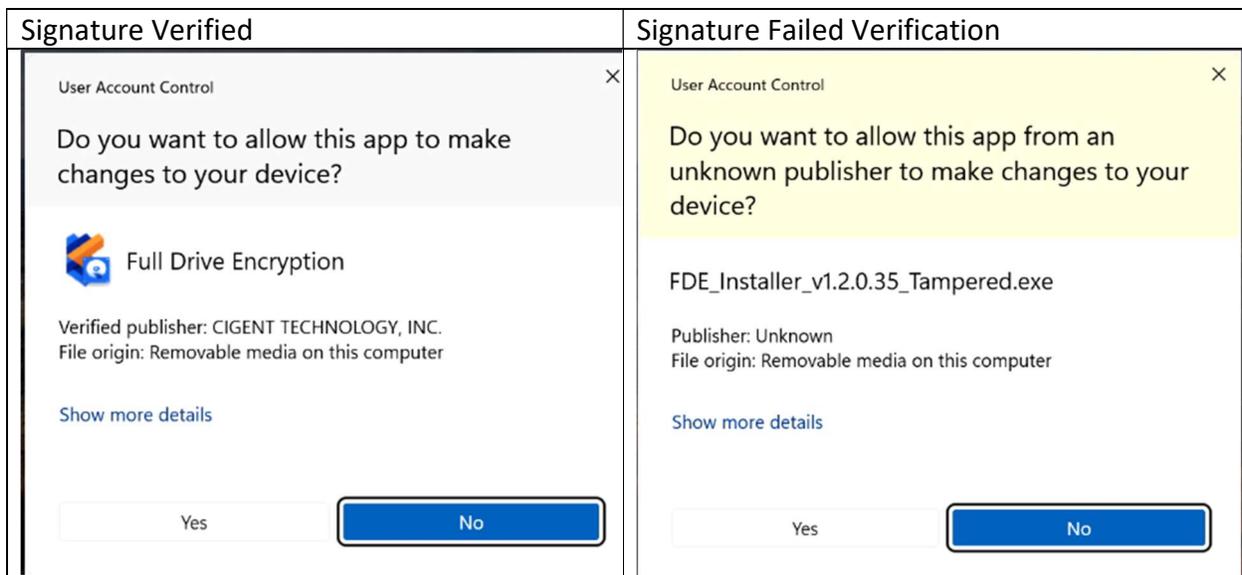
Signature Verified	Signature Failed Verification

It is strongly recommended that you create a backup of your Cigent FDE configuration files immediately after installation and after any configuration changes. Store these backup files in a secure location separate from the system being encrypted.

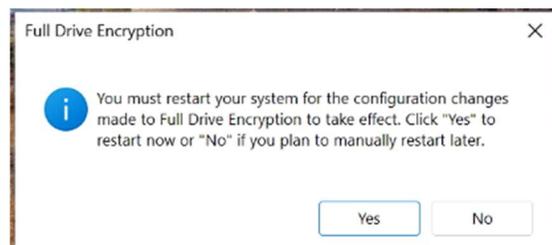1. Click Update to start the update process.

_____
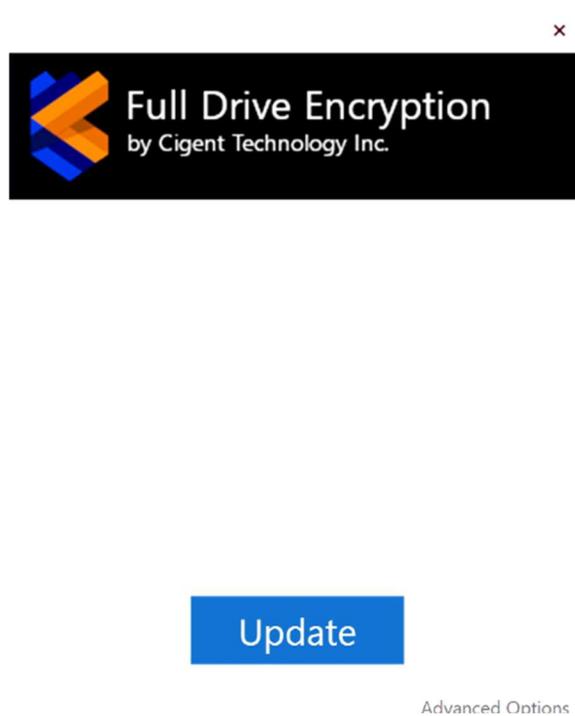
2. If you receive a message to close the running FDE applications, choose to Automatically close the applications and click OK.

3. Once complete, click Ok.

_____

4. Restart the system to complete the update.

5. Verify the version was successfully updated by reviewing the version indicated at the bottom of the FDE login page.