Shift5 – Full Disk Encryption (FDE) Administrator Guidance Document

August 19, 2025

Table of Contents

1. Introduction

1.1. Document Purpose and Audience

This document provides installation, configuration, and administration instructions for the Shift5 Full Disk Encryption (FDE) solution, hereafter referred to as the Target of Evaluation (TOE). This guide is intended for System Administrators responsible for the setup, management, and secure operation of the TOE in its NIAP-evaluated configuration.

This operational guidance is distributed to administrators as part of the TOE delivery to ensure they are aware of its role in establishing and maintaining the evaluated configuration.

1.2. TOE Identification and Overview

The TOE is a software Full Drive Encryption (FDE) solution integrated into the Shift5 Manifold. It provides data-at-rest protection for removable USB storage drives.

- **TOE Name:** Shift5 Full Disk Encryption (FDE)
- **Operational Environment:** SUSE Linux Enterprise Micro 6.0 on a Shift5 Manifold.

The FDE functionality is managed through the Data At Rest Protection (DARP) service, which is accessible via a web-based User Interface (UI). The TOE utilizes Linux Unified Key Setup (LUKS) to perform block-level encryption on the entire data partition of a removable drive.

1.3. Scope of Evaluation

The NIAP evaluation covers the FDE functionality for **removable USB data drives only**. The encryption of the Manifold's internal system boot drive is explicitly **out of scope** for this evaluation.

The evaluated security functions are:

- Cryptographic Erase (Zeroization)
- Changing/Updating the Data Encryption Key (DEK)
- Changing the Authorization Factor (Passphrase)
- Trusted Software/Firmware Updates
- Protection of data on removable media

Any other security functionality provided by the Shift5 Manifold is not covered by the Evaluation Activities.

1.4. Cryptographic Services

The TOE operates in a FIPS 140-2 compliant mode, leveraging cryptographic modules provided by the underlying SUSE Linux Enterprise Micro operating system, including OpenSSL and the Linux kernel cryptographic libraries.

All evaluated cryptographic engines and algorithms are configured by default following the installation procedures in this document and require no additional administrator action. Only

evaluated cryptographic engines are supported; do not modify or replace them. Use of other cryptographic engines was not evaluated or tested.

2. Preparative Procedures (AGD_PRE.1)

2.1. Secure Acceptance and Installation

The Shift5 Manifold is shipped with the TOE software pre-installed. Administrators must:

1. Verify the physical integrity of the received hardware, ensuring there are no signs of tampering (OE.PHYSICAL).
2. Install the provided ISO image according to the standard Shift5 provisioning procedures.

2.2. System and Operational Environment (OE) Requirements

The TOE is designed to operate on the Shift5 Manifold hardware platform running SUSE Linux Enterprise Micro 6.0. The administrator must ensure:

- The removable USB drive to be encrypted is new or has been sanitized to ensure no residual data exists (OE.INITIAL_DRIVE_STATE).
- The Shift5 Manifold is physically secured in its operational environment.
- The administrator possesses the necessary credentials, provided securely during provisioning:
  - Root user credentials for console access.
  - DARP service default user credentials.
  - TLS key decryption password.

2.3. Initial System Startup and Configuration

1. After installing the ISO, power on the Shift5 Manifold and wait for the initial configuration to complete. The system is ready when all four LEDs on the Manifold display green, red, and blue indicators.
2. Access the Manifold console via SSH using the root credentials: ssh root@<manifold-ip>
3. Start the DARP service (See Section 4.1).

3. Administrator Roles and Responsibilities (FMT_SMR.1)

The TOE defines a single administrative role, the **Administrator**. The Administrator is responsible for all security-relevant functions of the TOE, including:

- Starting and stopping the FDE service.
- Initializing encryption on new drives.
- Managing authorization factors (passphrases).
- Managing Data Encryption Keys (DEKs) via re-encryption and zeroization.
- Installing trusted updates.

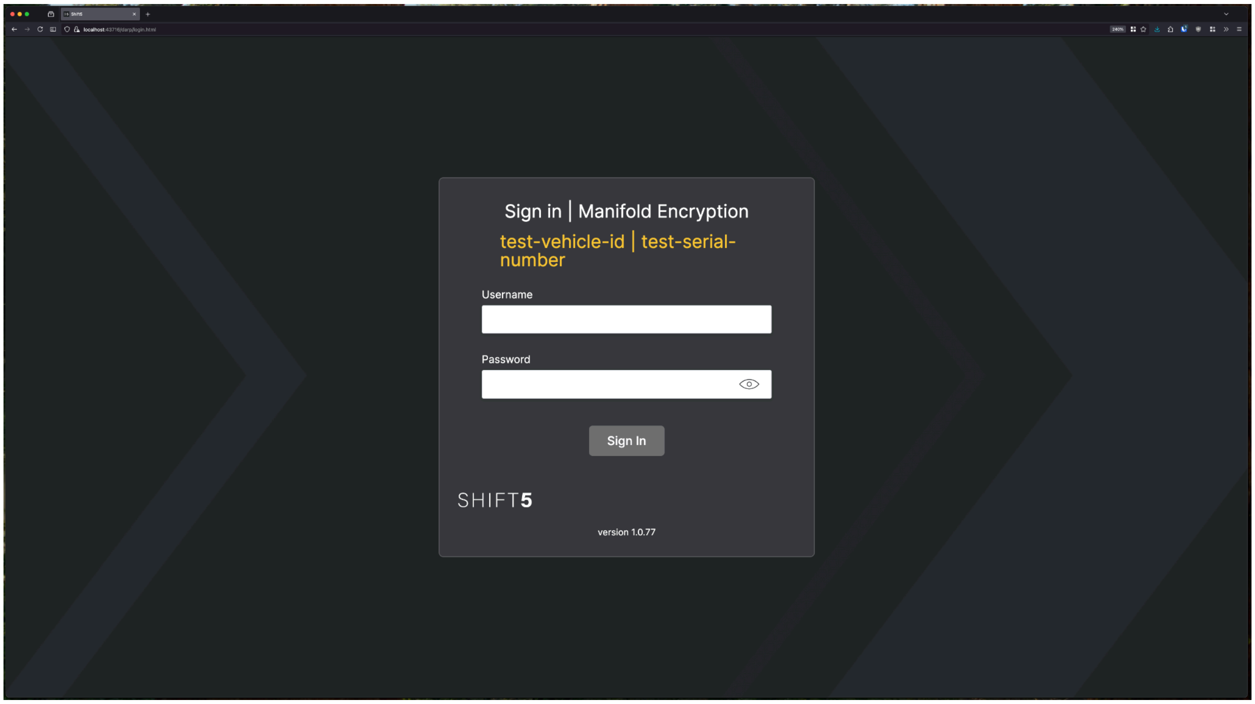
All management functions are performed by this single role.

4. TOE Administration and Management

4.1. Activating the FDE Service (DARP)

The DARP service must be running to perform any encryption-related operations. This service does not persist through power cycles and must be reactivated after every system restart.

1. Log into the Manifold console as the root user. The root password is programmatically set upon the provisioning of the Manifold to a 16+ characters that must contain special characters, numbers and letters. That password is then securely shared.
2. Start disk encryption: `/opt/shift5/bin/start_fde` and enter the Full Disk Encryption passphrase
3. Execute the start script: /opt/shift5/bin/start
4. When prompted, enter the TLS key decryption password.
    - The TLS private key is encrypted by Shift5. When starting DARP with /opt/shift5/bin/start, the user must enter a passphrase to decrypt the TLS private key and enable the DARP service to start. The TLS passphrase is programmatically set upon the provisioning of the Manifold and is then securely shared.
5. Verify the service is running by checking the pod status: kubectl get pods -A. Ensure the DARP pod shows a Running status.
6. Access the DARP management UI via a web browser at https://<manifold-ip>:32713/darp.
7. Log in with the default credentials and **change the password immediately** upon first login to the DARP UI. Default credentials are: `shift5 / Shift5!`



Sign in | Manifold Encryption

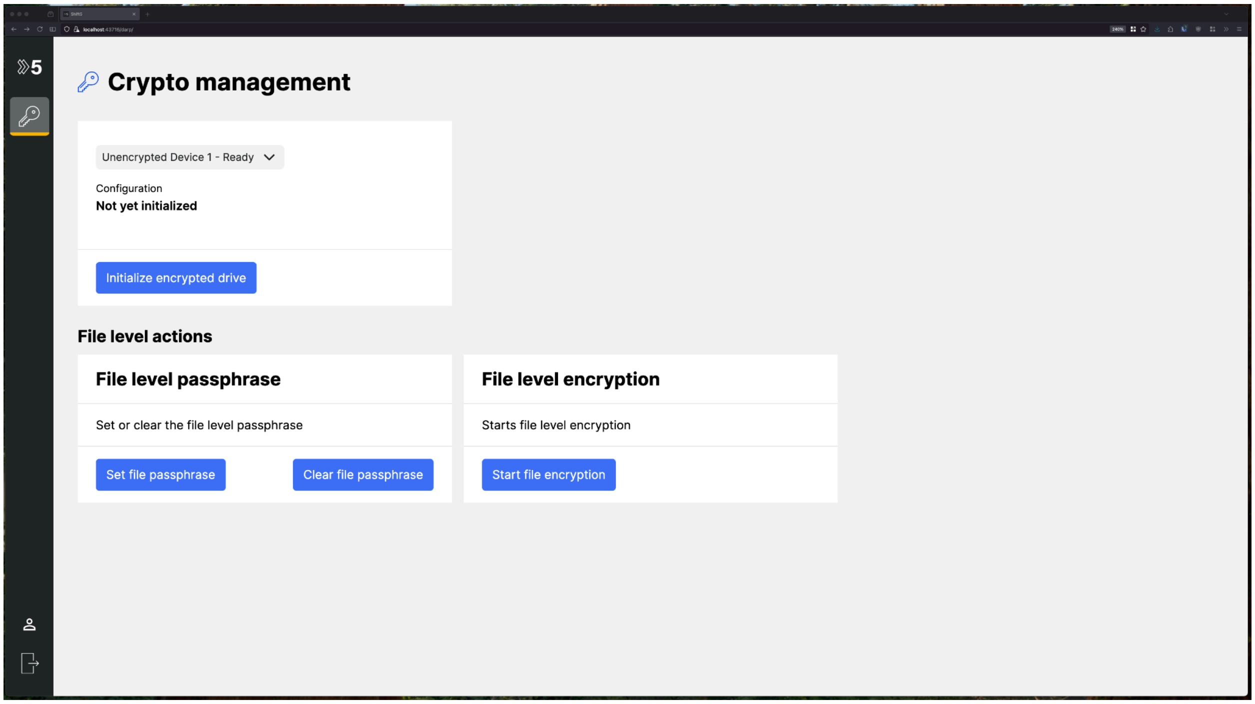
test-vehicle-id | test-serial-number

Exhibit 1: DARP Management UI Login Page

4.2. initializing Drive Encryption (FDP_DSK_EXT.1)

This procedure prepares a new or sanitized removable drive for secure use.

1. Ensure the target USB drive is physically connected to the Shift5 Manifold.
2. Log into the DARP UI.
3. From the "Crypto management" panel, click **Initialize encrypted drive**.



Crypto management

Configuration
Not yet initialized

File level actions

File level passphrase

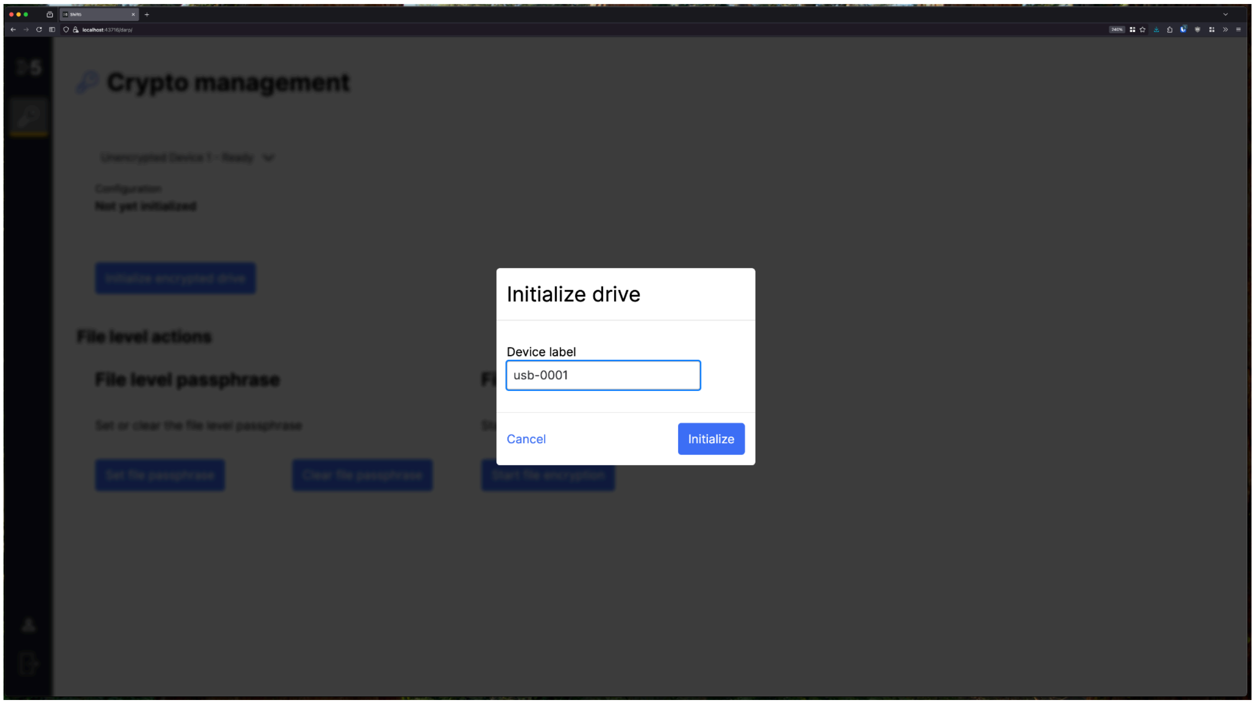
Set or clear the file level passphrase

File level encryption

Starts file level encryption

Exhibit 2: Crypto Management page to Initialize drive

4. In the dialog box:
   - ○ Select the target removable drive from the dropdown list.
   - ○ Enter a descriptive **Device label**.



Initialize drive

Device label: usb-0001

Exhibit 3: Entering device label before initializing drive

5. Click **Initialize**. A success notification will appear, and the drive status will update to show it is encrypted and unlocked.

4.3. Management of Authorization Factors (FMT_SMF.1)

The primary authorization factor for accessing encrypted data is the user-defined passphrase.

4.3.1. Changing the Data Encryption Passphrase

1. Log into the DARP UI (IAW Section 4.1 Steps 6 & 7).
2. Zeroize the drive
3. Set a new passphrase using /opt/shift5/bin/start_fde
4. Restart the DARP service to have it reload the new passphrase file

4.3.2. Password Validation (FCS_VAL_EXT.1.3)

If an incorrect passphrase is entered, the user will need to wait 2 seconds between each subsequent authentication attempt.

4.4. Management of Encryption Keys (FMT_SMF.1)

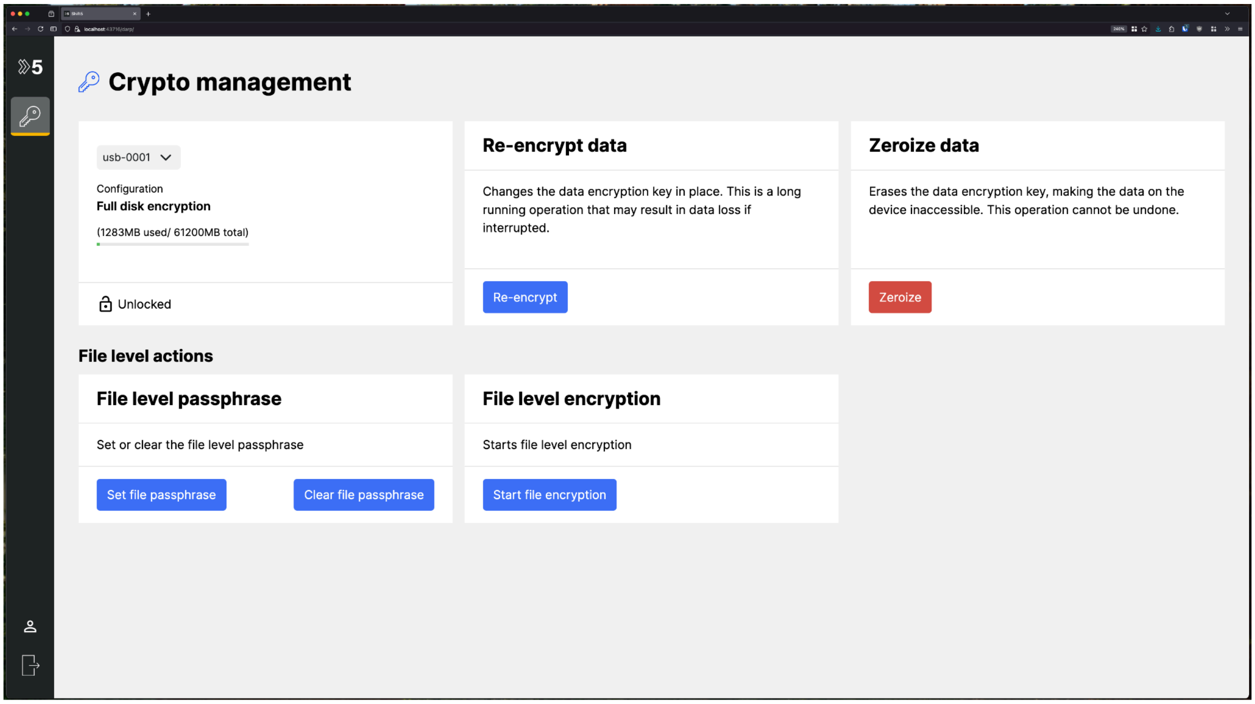
The TOE provides functions to manage the lifecycle of the Data Encryption Key (DEK).

4.4.1. Re-encrypting the Drive (Generating a New DEK)

This process generates a new DEK and re-encrypts the data on the drive with the new key. This does not change the user passphrase.

1. Log into the DARP UI (IAW Section 4.1 Steps 6 & 7).

2. Select the encrypted drive from the dropdown menu.



Crypto management

usb-0001

Configuration

Full disk encryption

(1283MB used/ 61200MB total)

Unlocked

Re-encrypt data

Changes the data encryption key in place. This is a long running operation that may result in data loss if interrupted.

Zeroize data

Erases the data encryption key, making the data on the device inaccessible. This operation cannot be undone.

File level actions

File level passphrase

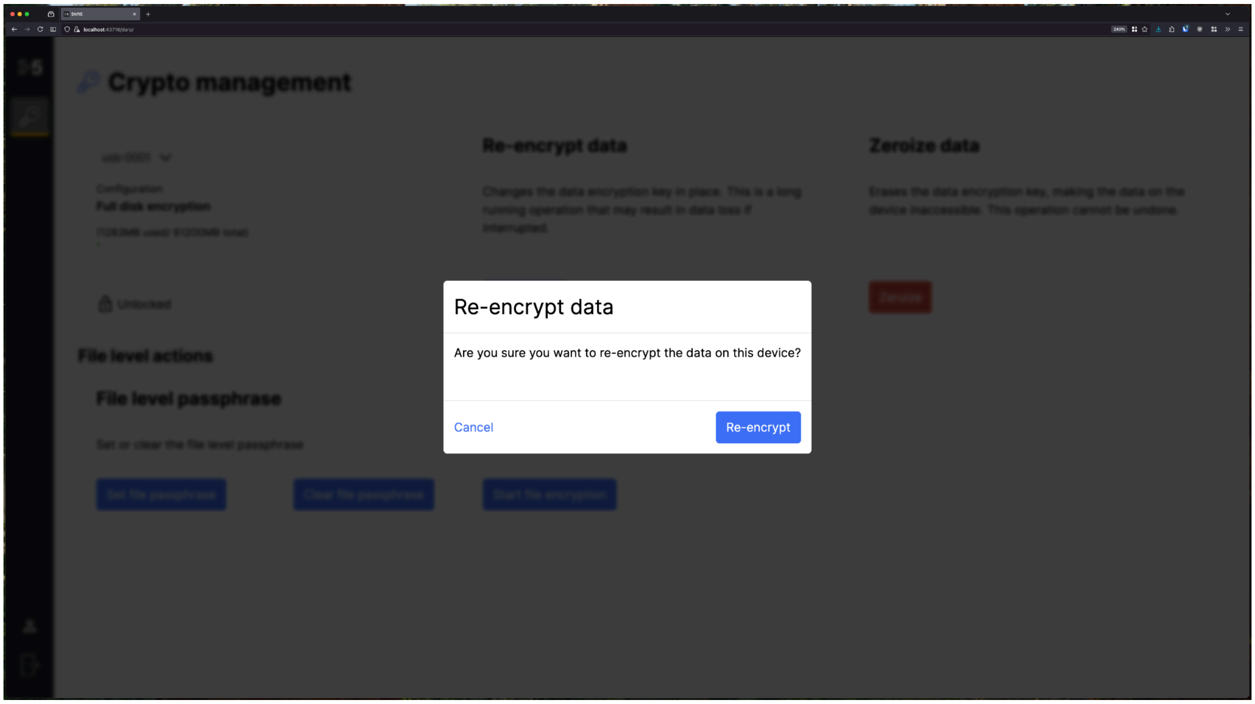
Set or clear the file level passphrase

File level encryption

Starts file level encryption

Exhibit 4: DARP Management UI landing page before Re-Encrypt

3. In the "Re-encrypt data" panel, click the **Re-encrypt** button.



Re-encrypt data

Are you sure you want to re-encrypt the data on this device?

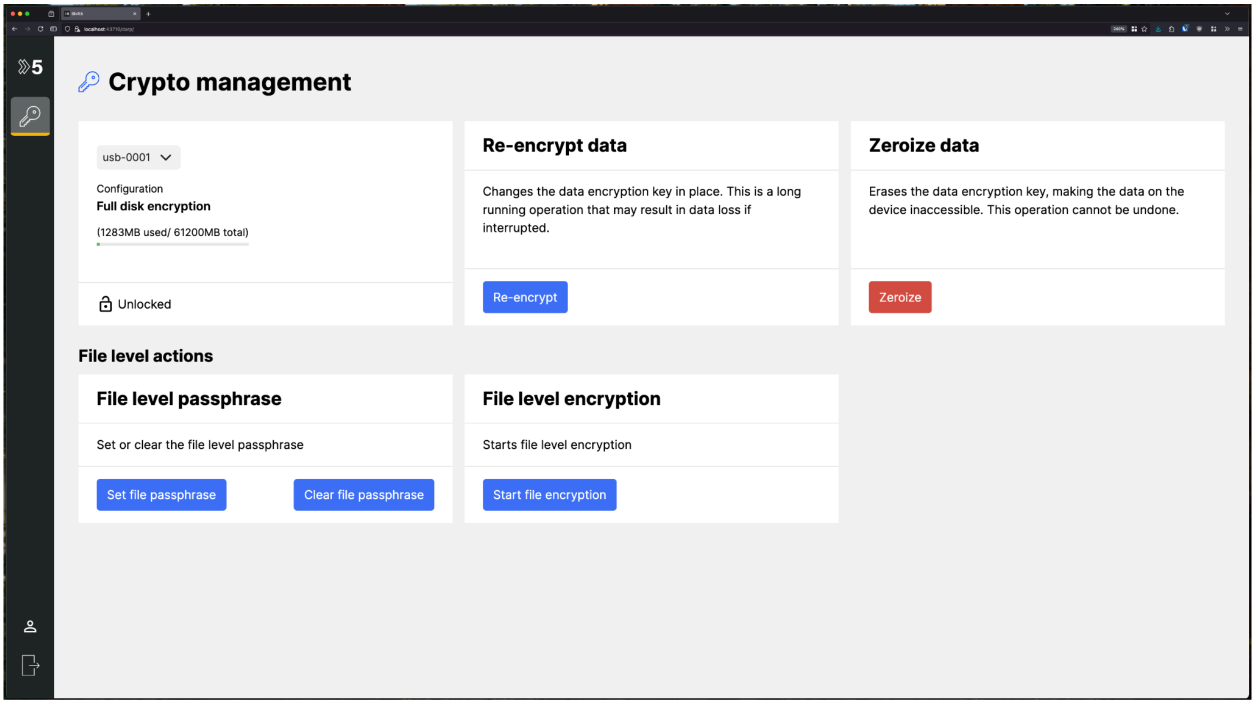
Exhibit 5: DARP Management UI Confirmation of Re-Encrypt

4. The process will begin in the background. This is a long-running operation; do not interrupt it or power down the device.

4.4.2. Cryptographic Erase (Zeroize)

This function securely erases the DEK, rendering all data on the drive permanently inaccessible.

1. Log into the DARP UI.
2. Select the encrypted drive.



Crypto management

usb-0001

Configuration
Full disk encryption
(1283MB used/ 61200MB total)

Unlocked

Re-encrypt data

Changes the data encryption key in place. This is a long running operation that may result in data loss if interrupted.

Zeroize data

Erases the data encryption key, making the data on the device inaccessible. This operation cannot be undone.

File level actions

File level passphrase

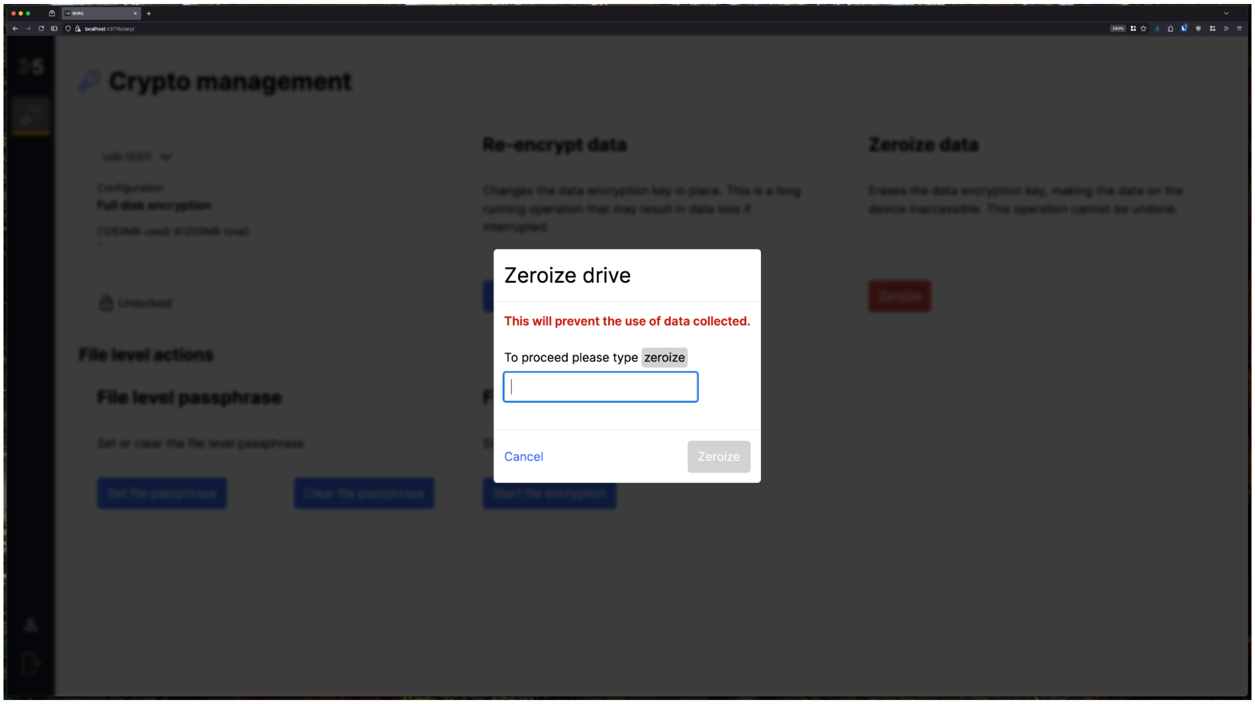
Set or clear the file level passphrase

File level encryption

Starts file level encryption

Exhibit 6: DARP Management UI landing page before Zeroize

3. In the "Zeroize data" panel, click the **Zeroize** button.
4. A confirmation dialog will appear. To proceed, you must type the word zeroize into the text field and confirm the action.



Re-encrypt data

Changes the data encryption key in place. This is a long running operation that may result in data loss if interrupted.

Zeroize data

Erases the data encryption key, making the data on the device inaccessible. This operation cannot be undone.

File level actions

File level passphrase

Set or clear the file level passphrase

Zeroize drive

This will prevent the use of data collected.

To proceed please type zeroize

Cancel

Zeroize

Exhibit 7: DARP Management UI to Zeroize drive

5. Upon confirmation, the DEK is destroyed, and the drive returns to an uninitialized state. **This action is irreversible.**

4.5. Trusted Updates (FPT_TUD_EXT.1)

The TOE software can be securely updated to a new version provided by Shift5. The update mechanism includes digital signature verification to ensure authenticity and integrity.

1. Obtain the signed update package from Shift5.
2. Log into the Manifold UI at https://<manifold-ip>:443.
3. Navigate to the system or update section of the UI.
4. Upload the update package using the provided function.
5. The TOE will automatically verify the digital signature of the update before proceeding.
    - **Successful Verification:** The update will be installed. The user must run opt/shift5/bin/start_fde to set the LUKS passphrase and /opt/shift5/bin/start to start DARP after the update
    - **Failed Verification:** The update will be rejected, and an error message will be displayed. The existing TOE software will remain unchanged. Do not attempt to re-install a package that has failed verification and reach out to your Shift5 Field Engineer for support.

4.6. Shutdown

The Manifold can be shutdown via the console with the following command: `reboot -h now`

5. Security Functionality and Guidance (AGD_OPE.1)

5.1. Authorization Factor Acquisition (FCS_AFA_EXT.1)

The TOE uses a **passphrase** as its authorization factor.

- **Characteristics:** The passphrase must be between 32 and 128 ASCII printable characters. The administrator is responsible for ensuring the passphrase has sufficient complexity and entropy to protect the data.
- **Acquisition:** The passphrase is required to unlock an encrypted drive after it has been locked or after a system power cycle (which requires the DARP service to be restarted and the drive to be subsequently unlocked).

5.2. Cryptographic Support (FCS)

- **Key Generation (FCS_CKM.1):** The TOE uses a FIPS-validated deterministic random bit generator (DRBG) from the underlying Linux kernel to generate cryptographic keys (DEKs). The DEK is generated using AES-256. These parameters are set by default and cannot be configured by the administrator.
- **Data Encryption (FCS_COP.1(f)):** Data encryption is performed using AES-XTS mode with 256-bit keys. This mode is configured by default and is the only mode supported.
- **Key Derivation (FCS_COP.1(b)):** The passphrase is used to unlock the DEK via a key derivation function using PBKDF2 and SHA-384. This hash algorithm is configured by default.
- **Random Bit Generation (FCS_RBG_EXT.1):** The TOE uses the operating environment's FIPS-validated DRBG for all entropy needs. This is not configurable.

5.3. Protection of the TSF (FPT)

5.3.1. Power Saving States (FPT_PWR_EXT.1)

The TOE supports only one Compliant power saving state:

- **G3 (Mechanical Off):** A complete power-off of the Shift5 Manifold.

Any other power saving states (e.g., sleep (S3), hibernate (S4)) are considered non-compliant. The evaluated configuration requires that these non-compliant states are disabled in the operating environment. Upon resuming from a G3 state, the Shift5 Manifold must be powered on, the DARP service must be started (Section 4.1), and the drive must be unlocked using its passphrase.

5.3.2. Timing of Power Saving States (FPT_PWR_EXT.2)

The TOE enters the G3 state when the administrator shuts down the system or when an unexpected power loss occurs. In either case, all cryptographic keys are cleared from volatile memory, ensuring the data remains secure. An unexpected power loss results in a secure state equivalent to a controlled shutdown.

5.4. Key Destruction (FCS_CKM.4)

- **Power Management (FCS_CKM.4(a)):** All cryptographic keys (DEKs) are stored in volatile system memory (RAM) during operation. When the TOE enters the G3 (Mechanical Off) state, power is cut to the RAM, which immediately and effectively destroys all stored keys.
- **Zeroization (FCS_CKM.4(d)):** The "Zeroize" function (Section 4.4.2) actively destroys the DEK

stored in the LUKS header on the removable drive. For solid-state drives (SSDs), the TOE relies on the operating system and file system to issue TRIM commands to the underlying hardware. This instructs the drive's garbage collection mechanisms to erase the physical blocks where the old key was stored. It is assumed that the drive is healthy and supports TRIM to ensure timely destruction of logically inaccessible key copies created by wear-leveling.

6. Troubleshooting

- **DARP UI Not Accessible:** Verify the DARP service is running with kubectl get pods -A. If not, restart it using the procedure in Section 4.1.
- **TLS Key Decryption Failure:** The incorrect password was likely entered. Re-run /opt/shift5/bin/start and carefully re-enter the password. If the disk initialization or unlock fails to run /opt/shift5/bin/start_fde with passphrase and restart DARP service
- **Drive Not Detected in UI:** Check the physical USB connection. Ensure the drive is properly seated in the USB port.

7. Acronyms and Definitions

- **AGD:** Administrator Guidance Document
- **DARP:** Data At Rest Protection
- **DEK:** Data Encryption Key
- **FDE:** Full Disk Encryption
- **ISO:** ISO 9660 Filesystem Image
- **LUKS:** Linux Unified Key Setup
- **NIAP:** National Information Assurance Partnership
- **OE:** Operational Environment
- **TOE:** Target of Evaluation
- **UI:** User Interface

8. Appendix A: NIAP Requirements Mapping

The following table maps the assurance activity requirements from the Protection Profile to the corresponding sections within this Administrator Guidance Document.

Requirement Identifier	**Requirement Description**	**Corresponding AGD Section(s)**
AGD_OPE.1	Operational User Guidance	Section 1.1, Section 1.3, Section 5
AGD_PRE.1	Preparative Procedures	Section 2
FCS_AFA_EXT.1	Authorization Factor Acquisition	Section 5.1

FCS_AFA_EXT.2	Timing of Authorization Factor Acquisition	Section 5.1, Section 5.3.1
FCS_CKM.1(b)	Cryptographic key generation (Symmetric)	Section 5.2
FCS_CKM.4(a)	Key Destruction (Power Management)	Section 5.4
FCS_CKM.4(d)	Key Destruction (Software TOE)	Section 5.4
FCS_CKM_EXT.4(b)	Key/Material Destruction (Power Management)	Section 5.3.1, Section 5.3.2
FCS_COP.1(b)	Cryptographic Operation (Hash Algorithm)	Section 5.2
FCS_COP.1(f)	Cryptographic Operation (AES Data Encryption)	Section 5.2
FCS_RBG_EXT.1	Random Bit Generation	Section 5.2
FCS_VAL_EXT.1	Validation	Section 4.3, Section 5.1
FDP_DSK_EXT.1	Protection of Data on Disk	Section 4.2
FMT_MOF.1	Management of Functions Behavior	Section 5.3.1
FMT_SMF.1	Specification of Management Functions	Section 4.3, Section 4.4, Section 4.5
FMT_SMR.1	Security Roles	Section 3
FPT_PWR_EXT.1	Power Saving States	Section 5.3.1
FPT_PWR_EXT.2	Timing of Power Saving States	Section 5.3.2
FPT_TUD_EXT.1	Trusted Update	Section 4.5