Shift5 File – Based Encryption (FBE) Administrator Guidance Document (AGD)
April 2026
Version: 1.3

Table of Contents

1. Introduction

1.1 Document Purpose and Scope of Evaluation (AGD_OPE.1)

Document Purpose and Intended Audience: This document provides installation, configuration, and administration instructions for the Shift5 Software File-Based Encryption (FBE) 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.

Scope of Evaluation: The NIAP evaluation covers the file-based encryption (FBE) functionality provided by the Shift5 Data At Rest Protection (DARP) service on the Shift5 Manifold.

Included in the evaluation boundaries: The evaluated security functions and management capabilities are strictly limited to:

- Configuring the WebUI webserver credential password.
- Configuring and changing the file-encryption password authentication factor.
- Changing the WebUI access password authentication factor.
- Enabling the encryption service.
- Decrypting selected files.

- Configuring the logging level.
- Destroying encrypted files (performing a cryptographic erase via the shred operation to destroy FEKs or KEKs).
- Performing trusted updates.
- Protection of DARP WebUI traffic through TLS as a server.

Excluded from the evaluation boundaries: Any other security functionality provided by the Shift5 Manifold is explicitly not covered by the Evaluation Activities. The Shift5 FBE Solution is designed to work in a two-layer Dual-DaR solution when combined with the Manifold Platform Full Disk Data-at-Rest Encryption. The full disk encryption scheme is covered by a separate evaluation and revisited here. This guide may make references to interoperability of both solutions since they are designed to work together, however this evaluation only covers the file-based application specifics.

1.2 TOE Identification (ALC_CMC.1, FPT_IDV_EXT.1)

- **Product Name:** Shift5 Software File-Based Encryption
- **Version:** 1.3
- **Version Query Instructions:** The TOE displays its current software version on the login screen of the DARP WebUI. To query the version:

1. Access the DARP WebUI via a web browser at: `https://<Manifold IP Address>:32713/darp`
2. View the current software version displayed in the version tag at the bottom of the login panel (e.g., "version 1.3.29").

1.3 Cryptographic and TLS Services

The TOE implements CAVP-certified cryptographic algorithms which are verified as a part of this evaluation. No configuration is needed for the cryptographic modules in order to be compliant. The use of any other cryptographic components beyond those that are identified are neither evaluated nor tested during the TOE's Common Criteria evaluation.

The TOE implements compliant TLS protocols which are verified as a part of this evaluation. No additional configuration is needed for the TLS protocol in order to be compliant.

2. Preparative Procedures (AGD_PRE.1)

2.1 Product and Functionality Overview

The Shift5 Software File-Based Encryption (FBE) is a containerized data-at-rest protection application integrated with and distributed as part of a container-hosting operating environment (such as the Shift5 operating system based on SUSE Linux Enterprise (SLE) Micro) on compatible hardware architectures. The FBE solution is designed to provide secure, file-level encryption for data collected and stored during the platform's operation.

Core Components and Functionality:

- **Data At Rest Protection (DARP) Service:** The core file encryption capabilities are managed by the DARP service, which operates as a Kubernetes pod within the Shift5 environment. The DARP service leverages CAVP-certified cryptographic algorithms to secure the system's files.
- **Cryptographic Key Architecture (FEK and KEK):** The FBE solution protects sensitive data by encrypting it with File Encryption Keys (FEK). To provide secure access control, these FEKs are subsequently wrapped and protected by Key Encrypting Keys (KEK). Access to the encryption service requires the administrator to establish a secure file encryption passphrase.
- **Secure File Decryption via Ramdisk:** Under normal operation, unencrypted files must include a .shift5 extension and are initially written to a volatile ramdisk. The DARP service reads these files from the ramdisk, encrypts them, and writes the newly encrypted files to non-volatile storage, appending a .s5e extension to the filename. When an administrator needs to access these files, they utilize a dedicated decryption script and the s5-decryptor utility. To prevent unauthorized data persistence during decryption on the manifold, the decryptor requires the user's passphrase and outputs the plaintext files directly back to a volatile ramdisk (/opt/shift5/data/ramdisk) rather than standard persistent storage.
- **Cryptographic Erase / File Shredding:** When encrypted data is no longer needed, the TOE provides a mechanism for secure cryptographic erasure. Administrators can use the Linux `shred` utility to securely overwrite and destroy the target encrypted files (e.g., `.s5e` files) and their associated FEKs/KEKs, rendering the data permanently inaccessible.
- **Administration and Management:** The FBE functionality is heavily managed via the command-line interface. Administrators use secure scripts executed over a serial connection (such as `/opt/shift5/bin/start_fe` and `/opt/shift5/bin/start`) to set passphrases, initialize keys, and activate the DARP service. Additionally, the DARP WebUI provides administrators with a Profile page to manage and update their WebUI user credentials.

The Shift5 FBE solutions provide multiple authentication factors to help secure sensitive data and further provide access controls for managing system resources. Through normal operation of the

FBE solution, the TOE interfaces with the following authorization factors:

- **Manifold Platform Credentials** – These credentials are set and utilized by the host platform. Consult your platform administrator guidance for further information on how to set and use these values. Since these credentials control the host platform, they are outside the boundary of this evaluation.
- **Manifold Platform WebUI Access Credentials** – this is a username and password used to access the Manifold-provided WebUI that is configured to run on port 443 by default. Similar to the platform credentials, these credentials are used to access platform resources and are also outside the boundary of this evaluation.
- **Manifold Platform Full-Drive Encryption Credentials** – this is a passphrase to control the full-drive layer of encryption that runs alongside the TOE's file-based solution. This full-drive encryption scheme is not covered by this evaluation and is separately evaluated.
- **Data at Rest Protection (DARP) Service WebUI Access Credentials** - this is a username and password used to access the TOE-specific WebUI. By default, the WebUI is accessed on port 32713 (which maps internally to the HTTPS service on port 43016). For container compatibility, the underlying Kubernetes cluster orchestration layer automatically exposes a secondary external port within the standard NodePort range (30000–32767), typically port 32700. This secondary port is for container compatibility only and maps directly to the exact same secure HTTPS service as the primary WebUI port. By default, the TOE ships with the following default credentials:

  Username/Password: shift5/shift5shift5

  Upon first log in to the DARP WebUI, the administrator will be asked to change the default password to something more secure. The TOE will not allow functionality until a new credential is set.
- **Data at Rest Protection (DARP) Service WebUI Webserver Certificate Passphrase** - The DARP WebUI utilizes an evaluated TLS interface. In order to provide secure authentication of the WebUI itself, the WebUI will create a new P-521 ECSDA Webserver certificate upon first startup. To ensure that the Webserver private key is stored in an encrypted manner, the TOE encrypts the webserver certificate with a Webserver passphrase-based encryption scheme. Upon creation of the webserver certificate at first startup, the administrator will configure a Webserver passphrase that must be re-entered in order to decrypt the certificate and start the DARP WebUI after each restart.
- **File-based Encryption (FBE) Passphrase** - a passphrase used to protect the key material that secures sensitive data. When File Encryption is started, the system establishes a random File Encryption Key (FEK) to encrypt the actual file bytes. The administrator-provided FBE Passphrase acts as a Key Encryption Key (KEK) to encrypt and protect this FEK. Both the encrypted file bytes and the encrypted FEK are then written together into the encrypted .s5e

file.

To configure and establish this KEK, the administrator must execute the /opt/shift5/bin/start_fe script from the command line prior to starting the DARP service. This script prompts the administrator to manually enter and set the passphrase; capturing and establishing this value is the only action the user must perform to initialize FBE protection. For detailed, step by step instructions on how to execute this script and input the passphrase, see Section 3.3 Enabling the Encryption Service

The system uses an ephemeral FBE passphrase, meaning a new passphrase must be entered each time File Encryption is started (e.g., via the WebUI), rather than just when the DARP service
boots up. In order to decrypt data through the decryption utility, the exact same passphrase must be provided to decrypt the FEK, which then decrypts the sensitive data. (Note: In the TOE's evaluated Attended Mode configuration, this authorization factor is a user-provided passphrase. In Unattended Mode, a public key is used as the KEK instead.)

The FBE passphrase is used directly in the sensitive data protection scheme to secure data at rest. Outside of this passphrase, the remaining passphrases are only used to control access to the platform or web interfaces. Although the DARP Service WebUI Webserver Certificate passphrase is used to derive a decryption key specific for the Webserver Certificate, this is separate from the sensitive data protection scheme and only used to provide an additional layer of access control to a WebUI management interface.

See Section 3 for further information on configuring new values for the authorization factors used by the TOE. See Section 4 for further information on password restrictions.

2.2 System Requirements and Platform Access (FDP_DEC_EXT.1)

- **Supported Platforms & Prerequisites:** The application is evaluated to run on SUSE Linux Micro 6 container-based environments and various hardware platforms manufactured by Shift5 (such as the evaluated Manifold platform). Shift5 distributes the application bundled with the OS image it provides for its supported platforms.
- **Platform Access Justification:** The TOE does not access any sensitive information repositories on the platform. The TOE requires access to a single hardware resource, "network connectivity," solely to host and expose its administrative WebUI on port 32713 (and the secondary compatibility port) to facilitate secure TLS-protected administrative sessions. The TOE utilizes no other hardware resources on the host platform.

2.3 Secure Acceptance and Installation of the DARP Software

The TOE software is integrated with the platform operating system and distributed pre-installed as part of the system image. Administrators must:

1. Verify the physical integrity of the received hardware, ensuring there are no signs of tampering (OE.PHYSICAL)
2. Install the provided operating system ISO image containing the pre-installed TOE software according to the standard Shift5 provisioning procedures. See the Shift5 platform provisioning materials and associated Common Criteria evaluation for details on how to complete this process.

2.4 Initial Provisioning

After installing the platform operating system (such as the Manifold OS) including the S5U container application, the DARP service requires some initial provisioning in order to configure credentials. See Section **3.3 Enabling the Encryption Service** of this guide for the procedure of starting up the Encryption Service. Upon starting up the Encryption Service for the first time, the TOE will create a new Webserver Certificate as well as require the administrator to configure a Webserver Certificate passphrase, change the default WebUI passphrase, and configure a new file-based encryption passphrase.

3. TOE Administration and Management (FMT_SMF.1)

3.1 Configuring the Logging Level

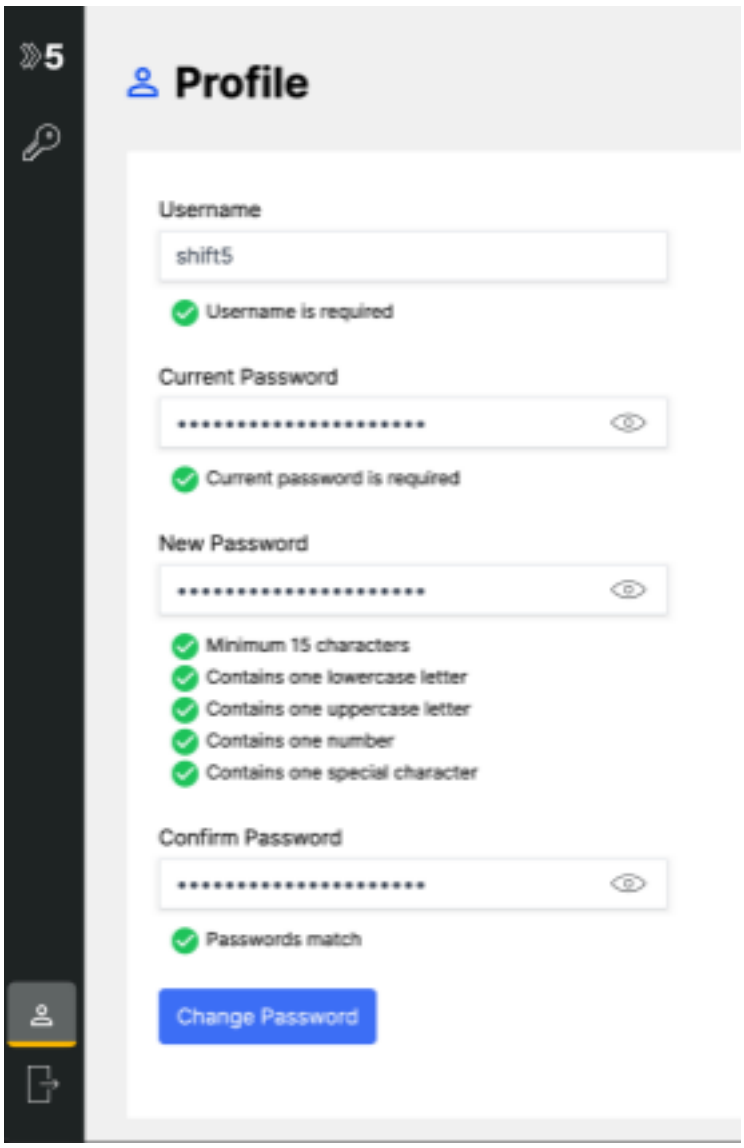
The TOE allows administrators to configure the system's logging level to capture necessary audit and diagnostic information. To configure the logging level, perform the following steps:

1. Edit the DARP configuration with the following command
    a. kubectl edit configmap -n shift5 darp-service-config
2. Edit the logLevel config value to one of the following values
    a. debug, info, warn, error
3. Restart the DARP pod with the following command
    a. kubectl delete pod -n shift5 <name of the DARP pod>

4. Execute the same DARP start scripts i.e. start_fde, start_fe, and start

3.2 WebUI Credential Management

1. Start the TOE WebUI service and log on to the DARP WebUI using the currently configured WebUI access username and password.
2. Navigate to the Profile Tab.
3. Enter in the previous password and new password to change the configured value. The previous password must match and the new password must meet the complexity rules (see Section 4.1 Authorization, Passphrase Conditioning, and Validation Limits for specific password constraints) in order to continue.



3.3 Enabling the Encryption Service

1. Log into the manifold unit console after image installation is complete
2. Initialize the encryption services:
    a. Initialize the external full-drive platform encryption service:
        Execute the /opt/shift5/bin/start_fde script file and enter an external full-drive encryption password
    b. Initialize the file-based encryption service:
        Execute the /opt/shift5/bin/start_fe script file and enter a secure file-based encryption passphrase. Running the start_fe script configures a new file-based encryption passphrase that will be used for this iteration of the encryption service

3. Activate the WebUI and DARP service

    Execute the /opt/shift5/bin/start script and provide the WebUI Webserver Certificate Passphrase

    On first run – the start script will require you to set the WebUI Webserver Certificate Passphrase that can later be reused to decrypt the webserver certificate

4. Log on to the DARP WebUI

    DARP WebUI can be accessed by browsing to https://<Manifold IP Address>:32713/darp

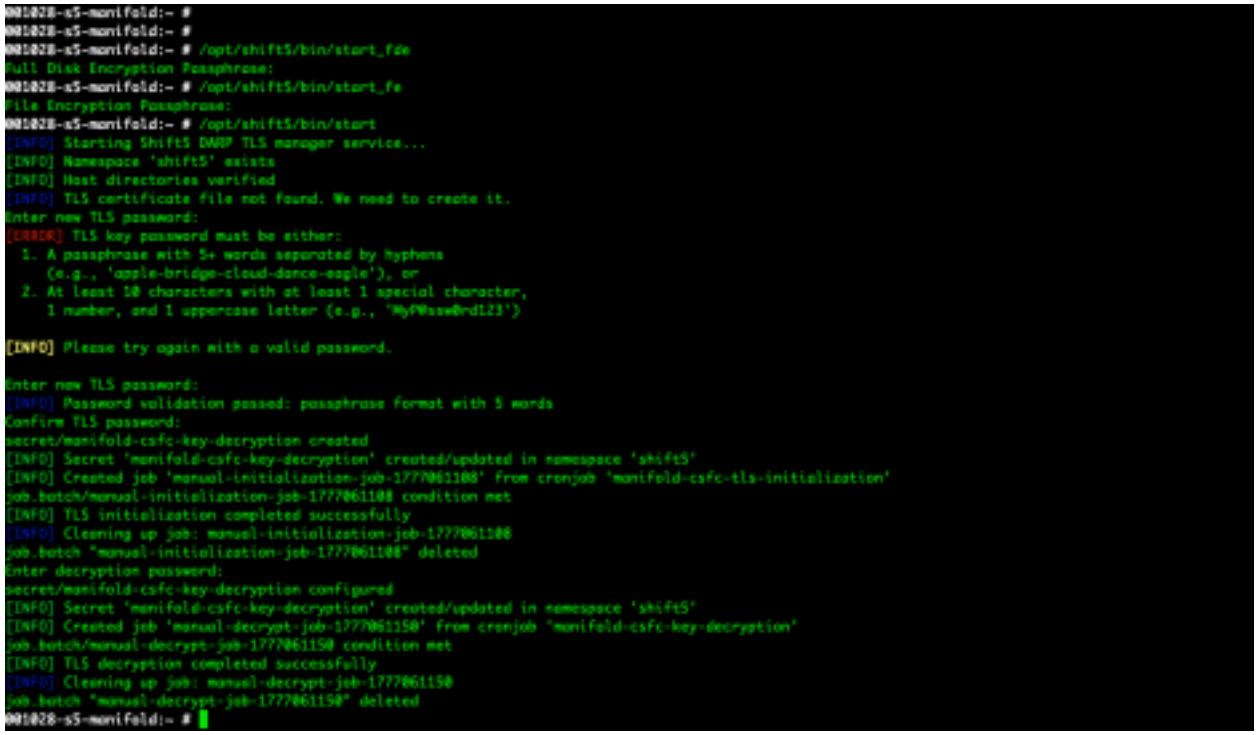
    Upon first login, the administrator can access the DARP WebUI with the default username and password. Immediately after logging in, the administrator will be required to change the default password before continuing

    Note on Secondary WebUI Port: Depending on the Kubernetes cluster configuration, a secondary port (typically port 32700) within the standard NodePort range (30000–32767) may also be active. This secondary port is strictly for container compatibility and maps to the exact same HTTPS service, utilizing the identical secure TLS interface as the primary port 32713.

5. Enable File Encryption through the WebUI

When the Manifold restarts the aforementioned scripts will need to be executed again before the Shift5 DARP Service is able to run. Also, when performing an update of the DARP service the

passwords will need to be entered again.



3.4 File Encryption Management (FCS_CKM_EXT.2 / EXT.3 / FMT_SMF.1(2))

3.4.1 Encrypting Selected Files

1. Start the File Encryption Service following Section 3.3 Enabling the Encryption Service 2. Create sensitive data to be encrypted

   The TOE service actively monitors the /opt/shift5/data/ramdisk directory for incoming files. Upon creation of a new file, the TOE FBE service will automatically encrypt the sensitive data using the random File Encryption Key (FEK) that was derived when DARP File Encryption was started. A new FEK is not derived for each file; instead, the FEK is recreated only when the DARP service restarts in any way, or when File Encryption is stopped and restarted. The encrypted data along with all meta-data needed to rederive the necessary keys from the password are saved in one file under the /opt/shift5/data/incoming directory

3. The administrator can confirm encryption is complete once the sensitive data is removed from the initial directory and the encrypted file appears.

3.4.2 Decrypting Selected Files

The Shift5 FBE includes a s5-decryptor tool to decrypt data on platform. While this script can be called more directly, the following procedure is provided to ensure that the decryption process properly clears up all associated values in accordance to the Common Criteria key destruction requirements and should

be used by any Common Criteria administrators:

1. Stop DARP file encryption
    a. Log into the DARP webUI at https://<manifold-ip>:32713/darp and Stop File Encryption in the UI.

2. Create decryption script:

```
#!/usr/bin/env bash
set -euo pipefail
INPUT=/opt/shift5/data/incoming
OUTPUT=/opt/shift5/data/ramdisk
KEY_FILE=/opt/shift5/data/ramdisk/fe/key.txt
KEY_DIR=$(dirname "${KEY_FILE}")
mkdir -p "${KEY_DIR}"
touch "${KEY_FILE}"
chmod 600 "${KEY_FILE}"
read -s -p "Enter FE passphrase: " passphrase
echo
echo -n "${passphrase}" > "${KEY_FILE}"
unset passphrase
kubectl exec -n shift5 "$(kubectl get pods -n shift5 | grep 'darp' | awk '{print
$1}')" -- /opt/shift5/app/s5-decryptor decrypt --input="${INPUT}"
--output="${OUTPUT}" --password-file="${KEY_FILE}"
```

3. Run decryption script to decrypt files from /opt/shift5/data/incoming to /opt/shift5/data/ramdisk

```
001067-s5-manifold:/home/shift5 # ./decrypt.sh
Enter FE passphrase:
Defaulted container "darp-service" out of: darp-service, darp-init-container (init)
sleeping for 10 seconds
done sleeping, starting decryption
Decrypting files in /opt/shift5/data/incoming to /opt/shift5/data/ramdisk
Skipping directory: /opt/shift5/data/incoming
001067-s5-manifold:/home/shift5 #
001067-s5-manifold:/home/shift5 # ls -l /opt/shift5/data/incoming/
total 0
001067-s5-manifold:/home/shift5 #
001067-s5-manifold:/home/shift5 # ls -l /opt/shift5/data/ramdisk/
total 4
drwxr-xr-x. 2 root root 60 Jun 23 16:05 fde
drwxr-xr-x. 2 root root 40 Jun 23 16:24 fe
-rw-r--r--. 1 root root 12 Jun 23 16:04 test.shift5
001067-s5-manifold:/home/shift5 #
```

Note, the TOE decryption utility is designed to decrypt files to a separate location as specified above. It is the responsibility of the user to actively erase any remnants of encrypted or decrypted data when no longer needed. See the later section 3.5 File Destruction / Shredding (FCS_CKM_EXT.4) for details on how to do this using the evaluated methods of data destruction

3.4.3 Configuring the File-Encryption Password

The file-encryption service uses a new passphrase each time the encryption process is started. This password is later verified and validated prior to decrypting sensitive data. Each instance of the FBE service will generate a new cryptographic salt, and use the password to derive a session key, used to protect individual file encryption keys. In order to rederive the cryptographic keys for decryption, the same password will be verified and validated prior to any decryption attempts. Further information about keys and their derivation are provided with the evaluation's security target.

Note: The file-encryption password resets each time the DARP service is stopped.

In order to configure a new file-encryption password, perform the following steps (for further details on this initialization process, reference Section 3.3 Enabling the Encryption Service):

1. Stop the DARP service by rebooting the manifold.
2. Execute the /opt/shift5/bin/start_fde script file to initialize the external full-drive encryption service.
3. Execute the /opt/shift5/bin/start_fe script file and enter a new password to recreate the appropriate keys.
4. Execute the /opt/shift5/bin/start script to activate the WebUI and start the DARP service.

3.5 File Destruction / Shredding (FCS_CKM_EXT.4)

Encrypted files created by the Shift5 FBE software contain all of the encrypted file contents and encrypted cryptographic keys needed to rederive the sensitive data from the user-provided file encryption password. By destroying the encrypted file, the administrator also destroys any associated cryptographic keys.

1. Run the shred tool to securely erase an encrypted file
    a. `shred -u /opt/shift5/data/incoming/secure.shift5.s5e`

```
001067-s5-manifold:/home/shift5 #
001067-s5-manifold:/home/shift5 # shred -u /opt/shift5/data/ramdisk/fe/key.txt
```

3.6 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 upload 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. Verification is performed on the image using the TOE's cryptographic library in conjunction with the vendor's internally stored signing key (ECDSA P-384 with SHA-384).

    - **Successful Verification:** The update will be installed. The DARP service container will need to be restarted 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. Security Functionality and Guidance (AGD_OPE.1)

This section details passive system behaviors, non-configurable limits, and security rules.

4.1 Authorization, Passphrase Conditioning, and Validation Limits (FIA_AUT_EXT.1, FCS_CKM_EXT.6, FCS_VAL_EXT.1)

- **Passphrase Requirements:**
    - DARP WebUI Webserver Certificate passphrases must be at least five hyphen-separated segments using only letters, digits, and hyphens or at least 10 characters with at least 1 special character, 1 number, and 1 uppercase letter. New passphrases must be entered twice to be accepted.
    - DARP WebUI password must be between 15 and 512 characters, containing at least one of lower case, upper case, number, and symbol characters.
    - DARP File Encryption Password must be between 32 and 128 characters, any printable ASCII characters from 0x20 to 0x7E are acceptable.
- **External Authorization Factors:**
    - Consult external guidance for configuring these values. Manifold user passwords are generally sixteen-character random strings from a defined alphanumeric and punctuation subset. Manifold WebUI passwords generally follow the same guidelines as the TOE WebUI password. Consult with external guidance for specifics on these values.

File-based Encryption Password Validation Limits: The FBE password validation limits are not configurable. Validations are strictly limited to a maximum of 8,640 attempts per 24-hour period due to constant-time validation comparisons.

4.2 Protection in Power Managed States (FDP_PM_EXT.1)

The manifold has only two power states: on and off. If the manifold is turned on and the OS login prompt is missing, turn the power off and then turn the power back on.

Warning on Non-Protected States: The TOE only protects new incoming data once the DARP service has been started in the WebUI. After any restart of the platform, the TOE is in a non-protected state and must once again be restarted and initialized before it can protect new incoming data.

Mitigation Instructions: Following any system reboot or power cycle, the administrator must log into the console, run the initialization scripts (`start_fde` and `start_fe`), supply the WebUI Webserver Certificate Passphrase via the `start` script, and re-enable file encryption through the DARP WebUI.

4.3 Protection of Temporary Resources (FDP_PRT_EXT.1)

Protection of Temporary Data: The TOE does not utilize any additional, temporary resources to perform its encryption. No special administrative measures are necessary to configure the protection of temporary files.

4.4 Key Destruction Mitigations (FCS_CKM_EXT.4)

Key Destruction Mitigations: To mitigate physical persistence of data, the underlying drive must support the TRIM command and implement garbage collection. The OS and file system must support TRIM over its connection channel (e.g., PCI-Express), and if a RAID array is utilized, it must support TRIM. The drive must be healthy and retired before significant damage occurs to minimize recoverable data in damaged sectors.

- The **fstrim** command is available on the Manifold giving access to the TRIM command
- The Manifold SSD performs garbage collection

```
001041-s5-manifold:/home/shift5 # fstrim -h

Usage:
 fstrim [options] <mount point>

Discard unused blocks on a mounted filesystem.

Options:
 -a, --all                trim mounted filesystems
 -A, --fstab              trim filesystems from /etc/fstab
 -I, --listed-in <list>   trim filesystems listed in specified files
 -o, --offset <num>       the offset in bytes to start discarding from
 -l, --length <num>       the number of bytes to discard
 -m, --minimum <num>      the minimum extent length to discard
 -t, --types <list>       limit the set of filesystem types
 -v, --verbose            print number of discarded bytes
     --quiet-unsupported  suppress error messages if trim unsupported
 -n, --dry-run            does everything, but trim

 -h, --help          display this help
 -V, --version       display version

Arguments:
 <num> arguments may be followed by the suffixes for
   GiB, TiB, PiB, EiB, ZiB, and YiB (the "iB" is optional)

For more details see fstrim(8).
001041-s5-manifold:/home/shift5 #
```

To further comply with the evaluated key destruction mechanisms, administrators should be aware of potential platform operations that could interfere with values being cleared from memory. This includes leveraging the platform clipboard and shell history. The Shift5 FBE application does everything in its power to sanitize and destroy its sensitive values when no longer needed and as documented in the Security Target, however end users should ensure that any additional operations outside of the TOE boundaries that may further interact with the TOE do not themselves retain any copy of passed in values.

5. Appendix A: Development Environment Guidance (ALC_CMS.1)

No explicit actions need to be taken to enable buffer overflow protection. Protections are already enabled by default.