NetApp Storage Encryption (NSE) Running ONTAP 9.10.1P14 Security Target

Version 1.3

21 September 2023

NetApp, Inc.

3060 Olsen Drive

San Jose, CA 95128

Contents

List of Tables

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is NetApp Storage Encryption (NSE) running ONTAP 9.10.1P14, an authorization acquisition product that obtains and manages authorization data used to access encrypted data stored on a full disk encryption product. The TOE provides the management and protection of keys that are used to protect the data encryption keys used by third-party self-encrypting drives (SEDs). The TOE supports third party SEDs that follow either the Trusted Computing Group's (TCG) Opal or Enterprise standards.

The ONTAP 9.10.1P14 component of the TOE is a proprietary operating system and data management software that is installed on the appliances listed below in Section 1.1 and that offers unified storage for applications that read and write data over block- or file- access protocols, in storage configurations that range from high-speed flash, to lower- priced spinning media, to cloud-based object storage.

ONTAP 9.10.1P14 implementations run on NetApp-engineered FAS (Fabric Attached Storage) or AFF (All Flash FAS) appliances and in private, public, or hybrid clouds (NetApp Private Storage or Cloud Volumes ONTAP).

The cloud-based storage is considered out of scope for the evaluation and has not been tested or evaluated.

The Security Target (ST) includes the following additional sections:

- TOE Description (Section 2)
- Documentation (Section 3)
- Security Problem Definition(Section 4)
- Security Objectives (Section 5)
- IT Security Requirements (Section 6)
- TOE Summary Specification (Section 7)
- Protection Profile Claims (Section 8)
- Rationale (Section 9)

1.1 Security Target, Target of Evaluation, and Common Criteria Identification

ST Title: NetApp Storage Encryption (NSE) running ONTAP 9.10.1P14 Security Target

ST Version: Version 1.3

ST Date: 22 August 2023

TOE Identification: NetApp Storage Encryption (NSE) running ONTAP 9.10.1P14

The non-TOE hardware required by and provisioned with the TOE is identified in the table below:

Storage Array	Disk Type	Controller Form Factor
FAS2620	HDD/SSD	2U/12 internal drives
FAS2650	HDD/SSD	2U/24 internal drives
FAS2720	HDD/SSD	2U/12 internal drives
FAS2750	HDD/SSD	2U/24 internal drives
FAS8200 Hybrid Flash	HDD/SSD	3U
AFF A200	SSD	2U
ASA AFF A220	NVMe Flash	2U/24 internal drives
AFF A300	SSD	3U
AFF C190	SSD	2U/24 internal drives
AFF A800	NVMe Flash	4U/48 internal drives
ASA AFF A800	NVMe Flash	4U with 48 SSD slots
AFF A320	SSD	2U
FAS9000	HDD	8U
AFF A700	SSD	8U
ASA AFF A700	SSD	8U
AFF A700s	SSD	4U/24 internal drives
FAS 8300	HDD	4U
FAS 8700	HDD	4U
AFF A400	SSD	4U
ASA AFF A400	SSD	4U
AFF A250	NVMe Flash	2U
ASA AFF A250	NVMe Flash	2U
FAS500f	NVMe Flash	2U

TOE Developer: NetApp, Inc.

Evaluation Sponsor: NetApp, Inc.

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
    - Part 3 Conformant
- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata, February 1, 2019* [CPP_FDE_AA_V2.0E] with the following optional and selection-based SFRs:
    - FCS_CKM.1(b)
    - FCS_COP.1(a)
    - FCS_COP.1(b)
    - FCS_COP.1(c)
    - FCS_COP.1(d)
    - FCS_KDF_EXT.1
    - FCS_PCC_EXT.1
    - FCS_RBG_EXT.1
    - FCS_VAL_EXT.1
    - FPT_TST_EXT.1

The following NIAP Technical Decision applies to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, all iterations (which are taken from [CPP_FDE_AA_V2.0E] are identified by a single lower alphabetic character in parentheses (e.g., FCS_COP.1(a)).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).

  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Terminology

Table 1: Terms and Definitions

Term	Definition
Authentication Key (AK)	Authentication key used to authenticate ONTAP to a SED. The 32-byte DRBG generated AK is used by the drive to protect the drive's DEK. For FDE-AA with NSE, the AK is the BEV. Note: AK is used generically in this document.
AK1	One of two authentication keys (AKs). AK1 (or AK2) can be used as the AK for the SED's data port, the SED's FIPS port, or both.
AK2	One of two authentication keys (AKs). AK2 (or AK1) can be used as the AK for the SED's data port, the SED's FIPS port, or both.
ALL-Flash FAS (AFF)	NetApp proprietary custom-build hardware appliances with only SSD drives and optimized ONTAP for low latency.
All-SAN Array (ASA)	NetApp proprietary custom-build hardware appliances with All SAN Array build on top of AFF platform, and provides only SAN-based data protocol connectivity.
Authorization Factor	A value that a user knows, has, or is (e.g. password, token, etc.) submitted to the TOE to establish that the user is in the community authorized to use the hard disk. This value is used in the derivation or decryption of the Border Encryption Value (BEV) and eventual decryption of the DEK. Note that these values may or may not be used to establish the particular identity of the user.
Border Encryption Value (BEV)	Value passed by the FDE Authorization Acquisition (FDE-AA) component to the FDE Encryption Engine (FDE-EE) component. For FDE-AA with NSE, the Authentication Key (AK) is the BEV.
Cluster Key Encryption Key (CKEK)	A 32-byte KEK that is generated via a DRBG. The CKEK is common to all nodes in the ONTAP cluster.
Cluster Passphrase	Cluster Passphrase is a 64 to 256-byte ASCII passphrase that is used as an authorization factor.
Cluster Pass-phrase Key Encryption Key (CP-KEK)	A 32-byte KEK that is derived from the cluster passphrase whose unwrapped value is derived using a passphrase based key derivation function. The CP-KEK is used to protect the CKEK.
Data Encryption Key (DEK)	A key used to encrypt data-at-rest.
Fabric-Attached Storage (FAS)	NetApp proprietary custom-build hardware appliances with HDD or SSD drives.
FC	Fibre Channel is the original networked block protocol. Instead of files, a block protocol presents an entire virtual disk to a client. The traditional FC protocol uses a dedicated FC network with specialized FC switches and requires a client computer to also have FC network interfaces. The virtual disk is represented by a LUN, with one or more LUNs being stored in an ONTAP volume.

Term	Definition
FCoE	FCoE is basically the same protocol as FC but uses datacenter-grade Ethernet network in place of the traditional FC transport. As with FC, the client requires an FCoE-specific network interface.
Intermediate Key	A key used in a point between the initial user authorization and the DEK.
iSCSI	iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port.
Key Chaining	The method of using multiple layers of encryption keys to protect data. A top layer key encrypts a lower layer key, which encrypts the data; this method can have any number of layers.
Key Encryption Key (KEK)	A key used to encrypt other keys, such as DEKs.
Key Material	Key material is commonly known as critical security parameter (CSP) data, and includes authorization data, nonces, and metadata.
Key Sanitization	A method of sanitizing encrypted data by securely overwriting or destroying the key that was encrypting the data.
Logical Interface	A LIF (logical interface) is an IP address or WWPN with associated characteristics, such as a role, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.
Logical Unit Number	A LUN (logical unit number) is an identifier for a device called a logical unit addressed by a SAN protocol.
Network Attached Storage (NAS)	A NAS is a single storage device that operates on data files. A NAS unit includes a dedicated hardware device that connects to a local area network, usually through an Ethernet connection. This NAS server authenticates clients and manages file operations in much the same manner as ordinary file servers, through well-established network protocols.
NetApp CryptoMod	This module provides NIST CAVP validated cryptographic operations for NSE and the onboard key manager (OKM).
NFS	NFS is the traditional file access protocol for UNIX and Linux systems. Clients can access files in ONTAP volumes using the NFSv3, NFSv4, NFSv4.1, and pNFS protocols. File access is controlled using UNIX-style permissions, NTFS-style permissions, or a combination of both.
Non-Volatile Memory	A type of computer memory that will retain information without power.
NVMe/FC	NVMe/FC, designed to work with flashed-based storage, offers scalable sessions, significantly reduced data latency, and higher throughput. NVMe/FC uses namespaces instead of LUNs. The NVMe namespaces, which are stored in an ONTAP volume, may only be accessed via the NVMe protocol.
OKM	Onboard Key Manager – local key-management without requiring an external key management server.
Protected Data	This refers to all data on the storage device with the exception of a small portion required for the TOE to function correctly. It is the space on the disk a user could write data to and includes the operating system, applications, and user data. Protected data does not include the Master Boot Record or Pre-authentication area of the drive – areas of the drive that are necessarily unencrypted.

Term	Definition
RDB	ONTAP's replicated database. RDB is a quorum-based synchronous transactional data replication service used by ONTAP components to persist configuration data. The RDB is available to a node only after the node joins the cluster.
Single-node cluster	A single-node cluster is a special implementation of a cluster running on a standalone node. The TOE can deploy a single-node cluster in a branch office, for example, assuming the workloads are small enough, and that storage availability is not a critical concern.
SMB/CIFS	SMB/CIFS is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. SMB/CIFS, like NFS, supports a mix of access permission styles.
Storage Array Networks (SAN)	A SAN is a local network of several devices. A SAN commonly uses Fibre Channel interconnects and connects a set of storage devices that share data with one another.
Submask	A submask is a bit string that can be generated and stored in a number of ways.
Storage Virtual Machine	Storage virtual machines (SVMs) serve data to clients and hosts. Like a virtual machine running on a hypervisor, an SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.
Target of Evaluation	A set of software, firmware, or hardware possibly accompanied by guidance. [CC1]
Volume Data Encryption Key (VDEK)	A symmetric key used to encrypt/decrypt the volume data. This may also be referred to as a Volume Encryption Key (VEK). The terms are used interchangeably in this document.
wAK	Wrapped (i.e. encrypted) version of AK. The wAK is formed by encrypting an AK with the CKEK. The term wAK is used as a generic reference to either wAK1 or wAK2 in this document.
wAK1	Wrapped version of AK1. The wAK1 is formed by encrypting AK1 with the CKEK.
wAK2	Wrapped version of AK2. The wAK2 is formed by encrypting AK2 with the CKEK.
wCKEK	The wrapped, or encrypted, version of the CKEK.
World Wide Port Name	A World Wide Port Name, (WWPN) is a World Wide Name assigned to a port in a Fibre Channel fabric. Used on storage area networks, it performs a function equivalent to the MAC address in Ethernet protocol, as it is supposed to be a unique identifier in the network.

1.3.2 Acronyms

Table 2: Acronyms

Acronym	Definition
AA	Authorization Acquisition
AK	Authentication Key
AES	Advanced Encryption Standard
AFF	All Flash FAS
ASA	All SAN Array

Acronym	Definition
BEV	Border Encryption Value
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CPP	Collaborative Protection Profile
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EE	Encryption Engine
FAS	Fabric Attached Storage
FC	Fibre Channel
FCoE	Fibre Channel Over Ethernet
FDE	Full Drive Encryption
FIPS	Federal Information Processing Standards
HDD	Hard Disk Drive
HMAC	Keyed-Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
iSCSI	Internet Small Computer Interface
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
IV	Initialization Vector
KEK	Key Encryption Key
LIF	Logical Interface
LUN	Logical Unit Number
MBR	Master Boot Record
NAS	Network Attached Storage
NFS	Network File System
NIST	National Institute of Standards and Technology
NSE	NetApp Storage Encryption
NVMe	Non-Volatile Memory Express
OS	Operating System
PRF	Pseudo Random Function

Acronym	Definition
RBG	Random Bit Generator
RDB	ONTAP's replicated database
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAN	Storage Array Networks
SAR	Security Assurance Requirements
SED	Self-Encrypting Drive
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SMB/CIFS	Server Message Block
SPD	Security Problem Definition
SPI	Serial Peripheral Interface
SSD	Solid State Drive
ST	Security Target
SVM	Storage Virtual Machine
SVM-KEK	Storage Virtual Machine Key Encryption Key
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functionality
TSS	TOE Summary Specification
USB	Universal Serial Bus
VDEK	Volume Data Encryption Key
wCKEK	Wrapped Cluster Key Encryption Key
wVDEK	Wrapped Volume Data Encryption Key
wSVM-KEK	Wrapped Storage Virtual Machine Key Encryption Key
WWPN	World Wide Port Name
XOR	Exclusive or
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

2 TOE Description

2.1 TOE Overview

The TOE is NetApp Storage Encryption (NSE) running ONTAP 9.10.1P14, an authorization acquisition product that obtains and manages authorization data used to access encrypted data stored on a full disk encryption product. The TOE provides authorization data to third party self-encrypting drives (SEDs).

2.2 TOE Description

The TOE is provided pre-installed on NetApp disk storage appliances consisting of storage controllers and one or more enclosures of SEDs. The NetApp appliances included in the evaluated configuration are listed below in Table 3.

NetApp Storage Encryption supports third party SEDs that follow either the Trusted Computing Group's (TCG) Opal or Enterprise standards. Both standards support the use of an authentication key (AK) and one or more data encryption keys (DEK) per drive. The AK is used by a client (client in this case indicating ONTAP, the NetApp operating system) to unlock a drive. Once the drive verifies that the AK is correct, it uses the AK to decrypt the drive's DEK(s).

NetApp Storage Encryption supports use of an external key management (KMIP) server or Onboard Key Manager (OKM) to manage the authentication key (AK) used by the array's SEDs. However, in the evaluated configuration, only OKM is supported, and OKM must be configured with CC mode enabled. When CC mode is enabled, OKM requires entry of the Cluster Passphrase every time the storage array is booted.

NetApp Storage Encryption may be configured via the appliance's RS-232 console port. NetApp Storage Encryption also supports various networking protocols including SSH, CIFS, NFS, HTTP, HTTPs, DHCP, SNMP, Fibre Channel, and iSCSI, among others. The Protection Profile ([CPP_FDE_AA_V2.0E]) associated with this product did not consider, nor did it include networking protocols as part of the security functional requirements and, as a result, did not include any requirements for addressing those protocols. Consequently, the protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOE's networking protocols.

It is suggested that a customer using the product consider the impact of using the product's SSH or HTTPs interfaces to administer the product as opposed to the product's RS-232 console interface. The customer should base their decision on the environment in which the TOE operates and the value of the data that needs to be protected.

2.3 TOE Architecture

Depending on the NetApp hardware controller model, node storage consists of flash disks, capacity HDD drives, or both. Network ports on the controller provide access to data. Physical storage and network connectivity resources are virtualized, visible to cluster administrators only, not to NAS clients or SAN hosts.

NetApp appliances typically are configured in cluster nodes in high-availability (HA) pairs for fault tolerance and non-disruptive operations. If a node fails or if a node needs to be brought down for routine

maintenance, its partner can take over its storage and continue to serve data from it. The partner gives back storage when the node is brought back on-line. HA pairs always consist of like controller models. The controllers typically reside in the same chassis with redundant power supplies. The HA functionality was not covered in the scope of the evaluation or testing.

Figure 1 TOE High-Availability Pair Configuration

ONTAP 9.10.1P14 supports all the major industry standard NAS and SAN based client protocols: NFS, SMB/CIFS, FC, FCoE, iSCSI, and NVMe/FC.

Customers use storage virtual machines (SVMs) to serve data to clients and hosts. An SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.

In addition to data volumes, ONTAP also uses the following special volumes (note: these volumes, like all volumes on an NSE system, are hosted on third party self-encrypting drives):

- A node root volume (typically “vol0”) contains node configuration information and logs.
- An SVM root volume serves as the entry point to the namespace provided by the SVM and contains namespace directory information.
- System volumes contain special metadata such as service audit logs.

ONTAP prevents customers from storing user data on these special volumes.

In addition to data SVMs, ONTAP deploys special SVMs for administration:

- An admin SVM is created when the cluster is set up.
- A node SVM is created when a node joins a new or existing cluster.
- A system SVM is automatically created for cluster-level communications in an IP space.

The administrative SVMs listed above cannot be used to serve data. All administration is performed via the CLI accessed using a console directly connected to the appliance’s RS-232 port.

NetApp Storage Encryption (NSE) provides the authentication key to “self-encrypting” drives (SEDs), also known as Full Disk Encryption, or FDE, drives, that encrypt data as it is written. The data cannot be read without an encryption key stored on the disk. The encryption key, in turn, is accessible only to an authenticated node.

On an I/O request, a node authenticates itself to an SED using one or more authentication keys (AKs) retrieved from the Onboard Key Manager. The authentication key used to authenticate ONTAP to a SED is used by the drive to protect the drive’s DEK. The authentication key, or AK, is a 32-byte value that is

generated by the TOE's DRBG. For the [CPP_FDE_AA_V2.0E] with NSE, the AK is the BEV. Note: AK is used generically in this document.

2.3.1 Physical Boundaries

The physical boundary of the TOE encompasses the NetApp ONTAP 9.10.1P14 software.

2.3.1.1 Hardware Requirements

The non-TOE hardware required by and provisioned with the TOE is identified in the table below:

Table 3 Non-TOE Hardware

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
Intel Xeon Processor D Family					
FAS2620	HDD/SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U/12 internal drives	Intel Xeon D-1528 (Broadwell) 2 x 64-bit 6-core 1.90 Ghz
FAS2650	HDD/SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U/24 internal drives	Intel Xeon D-1528 (Broadwell) 2 x 64-bit 6-core 1.90 Ghz
FAS2720	HDD/SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U/12 internal drives	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 Ghz
FAS2750	HDD/SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U/24 internal drives	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 Ghz)

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
FAS8200 Hybrid Flash	HDD/SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	480/480	3U	Intel Xeon D-1587 (Broadwell) 2 x 64-bit 16-core 1.70 Ghz
AFF A200	SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U	Intel Xeon D-1528 (Broadwell) 2 x 64-bit 6-core 1.90 Ghz
AFF A220	NVMe Flash	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U/24 internal drives	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 Ghz
ASA AFF A220	NVMe Flash	FC, FCoE, iSCSI	144	2U/24 internal drives	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 Ghz
AFF A300	SSD	NVMe/FC, FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	384	3U	Intel Xeon D-1587 (Broadwell) 2 x 64-bit 16-core 1.70 Ghz
AFF C190	SSD	CIFS, FCoE, iSCSI, NFS v3, NFS v4.0, NFS v4.1, NFS v4.2, NVMe/TCP, S3, SMB 2.0, SMB 2.1, SMB 2.x, SMB 3.0,	24	2U/24 internal drives	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 Ghz

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
		SMB 3.1, SMB 3.1.1			
Intel Xeon Scalable Processors (Skylake Server)					
AFF A800	NVMe Flash	IFS, FC, iSCSI, NFS v3, NFS v4.0, NFS v4.1, NFS v4.2, NFSv4/RDMA, NVMe/FC, NVMe/TCP, S3, SMB 2.0, SMB 2.1, SMB 2.x, SMB 3.0, SMB 3.1, SMB 3.1.1,	240	4U/48 internal drives	Intel Xeon Platinum 8160 (Skylake-SP) 4 x 64-bit 24-core 2.10 Ghz
ASA AFF A800	NVMe Flash	IFS, FC, iSCSI, NVMe/FC, NVMe/TCP, S3	240	4U/48 internal drives	Intel Xeon Platinum 8160 (Skylake-SP) 4 x 64-bit 24-core 2.10 Ghz
AFF A320	SSD	NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB	48	2U	Intel Xeon Silver 4114 (Skylake-SP) 4 x 64-bit 10-core 2.2 Ghz
Intel Xeon Processor E5 Family					
FAS9000	HDD	CIFS, FC, FCoE, iSCSI, NFS v3, NFS v4.0, NFS v4.1, NFS v4.2, S3, SMB 2.0, SMB 2.1, SMB	1,440/480	8U	Intel Xeon E5-2697v4 (Broadwell) 4 x 64-bit 18-core 2.30 Ghz

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
		2.x, SMB 3.0, SMB 3.1, SMB 3.1.1			
AFF A700	SSD	CIFS, FC, FCoE, iSCSI, NFS v3, NFS v4.0, NFS v4.1, NFS v4.2, NVMe/FC, NVMe/TCP, S3, SMB 2.0, SMB 2.1, SMB 2.x, SMB 3.0, SMB 3.1, SMB 3.1.1	470	8U	Intel Xeon E5-2697v4 (Broadwell) 4 x 64-bit 18-core 2.30 Ghz
ASA AFF A700	SSD	FC, FCoE, iSCSI, NVMe/FC, NVMe/TCP, S3	470	8U	Intel Xeon E5-2697v4 (Broadwell) 4 x 64-bit 18-core 2.30 Ghz
AFF A700s	SSD	NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB	216	4U/24 internal drives	Intel Xeon E5-2697v4 (Broadwell) 4 x 64-bit 18-core 2.30 Ghz
Cascade Lake Processor					
FAS8300	HDD	CIFS, FC, iSCSI, NFS v3, NFS v4.0, NFS v4.1, NFS v4.2, S3; SMB 2.0, SMB 2.1, SMB 2.x, SMB	720	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core 2.20 Ghz

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
		3.0, SMB 3.1, SMB 3.1.1			
FAS8700	HDD	CIFS, FC, iSCSI, NFS v3, NFS v4.0, NFS v4.1, NFS v4.2, S3; SMB 2.0, SMB 2.1, SMB 2.x, SMB 3.0, SMB 3.1, SMB 3.1.1	1440	4U	Intel Xeon Gold 5218 (Cascade Lake) 4 x 64-bit 16-core 2.3 Ghz
AFF A400	SSD	FC, iSCSI, NFS, pNFS, CIFS/SMB	480	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core 2.20 Ghz
ASA AFF A400	SSD	FC, iSCSI	480	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core 2.20 Ghz
Intel Xeon Processor (Skylake-D)					
AFF A250	NVMe Flash	NVMe/TCP, NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB,	576	2U; 24 internal SSD slots	Intel Xeon D-2164-IT (Skylake -D) 24 cores, 2.10 GHz
ASA AFF A250	NVMe Flash	NVMe/TCP, NVMe/FC, FC, iSCSI	576	2U; 24 internal SSD slots	Intel Xeon D-2164-IT (Skylake-D) 24 cores, 2.10 GHz

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
FAS500f	SSD	NVMe-oF, FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	48	2U	Intel Xeon D-2164-IT (Skylake-D) 24 cores, 2.10 GHz

The TOE is evaluated on an operational environment that comprises storage arrays equipped with the following Intel processors:

- Broadwell microarchitecture:
  - Intel Xeon D-1528
  - Intel Xeon D-1557
  - Intel Xeon D-1587
  - Intel Xeon E5-2697 v4
- Cascade Lake microarchitecture:
  - Intel Xeon Silver 4210
  - Intel Xeon Gold 5218
- Skylake-SP microarchitecture:
  - Intel Xeon Silver 4114
  - Intel Xeon Platinum 8160.
- Skylake-D
  - Intel Xeon D-2164-IT

The cryptographic modules included in the TOE have NIST Cryptographic Algorithm Validation Program (CAVP) certificates C1884, C1885, and A2157. The Operating Environments for these certificates include the following:

- Intel Xeon D-1528 (Broadwell microarchitecture), which covers the following storage arrays:
  - FAS2620, FAS2650, AFF A200: all include the Intel Xeon D-1528

  - FAS2720, FAS2750, AFF A220, ASA AFF A220, AFF C190: all include the Intel Xeon D-1557, which is equivalent at the microarchitecture level to the Intel Xeon D-1528
  - FAS8200 Hybrid Flash, AFF A300: includes the Intel Xeon D-1587, which is equivalent at the microarchitecture level to the Intel Xeon D-1528
  - AFF A700, AFF A700s, ASA AFF A700, FAS9000: include the Intel Xeon E5-2697 v4, which is equivalent at the microarchitecture level to the Intel Xeon D-1528
- Intel Xeon Platinum 8160 (Skylake-SP microarchitecture), which covers the following storage arrays:
  - AFF A800, ASA AFF A800 : includes the Intel Xeon Platinum 8160
  - AFF A320: includes the Intel Xeon Silver 4114, which is equivalent at the microarchitecture level to the Intel Xeon Platinum 8160
- Intel Xeon D-2164-IT (Skylake-D microarchitecture), which covers the following storage arrays:
  - AFF A250, ASA AFF A250, FAS500f, which is equivalent at the microarchitecture level to the Intel Xeon Platinum 8160
- Intel Xeon Silver 4210 (Cascade Lake microarchitecture), which covers the following storage arrays:
  - FAS8300, AFF A400, ASA AFF A400: includes the Intel Xeon Silver 4210
  - FAS8700: includes the Intel Xeon Gold 5218, which is equivalent at the microarchitecture level to the Intel Xeon Silver 4210.

Therefore, all storage arrays included in the evaluated configuration are covered by the A2157, C1884, and C1885 certificates, because they either include the same processor on which the certified algorithm testing was performed, or they include a processor that is equivalent at the microarchitecture level to a processor on which algorithm testing was performed.

2.3.2 Logical Boundaries

This section identifies the TOE's logical boundaries:

- Cryptographic Support
- Security Management
- Protection of the TSF

2.3.2.1 Cryptographic Support

The TOE includes NIST CAVP-validated cryptographic algorithms supporting cryptographic functions. The TOE provides Key Wrapping, Key Derivation, and BEV Validation.

2.3.2.2 Security Management

The TOE supports management functions for forwarding requests to change the DEK to the EE, forwarding requests to cryptographically erase the DEK to the EE, allowing authorized users to change authorization factors or set of authorization factors used, and initiate TOE software updates using a command line interface.

2.3.2.3 Protection of the TOE Security Functionality

The TOE provides trusted firmware updates, protects Key and Key Material; and supports power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

2.4 Excluded Functionality

The list below identifies features or protocols that are not evaluated or must be disabled, and the rationale why. Note that this does not mean the features cannot be used in the evaluated configuration (unless explicitly stated so). It means that the features were not evaluated and/or validated by an independent third party and the functional correctness of the implementation is vendor assertion. Evaluated functionality is scoped exclusively to the security functional requirements specified in this Security Target. The features below are out of scope.

Table 4 – Excluded Functionality

Feature	Description
SnapLock	NetApp SnapLock is the WORM (write once, read many) compliance replication solution from NetApp. It provides integrated data protection for workloads that need to adhere to regulatory guidelines such as HIPAA, SEC 17a-4(f) rule, FINRA, and CFTC as well as national requirements for German-speaking countries (DACH).
Trusted Platform Module (TPM)	The encryption keys for the onboard key manager (OKM) are not sealed by a physical TPM when running in Common Criteria mode.
MetroCluster	NetApp MetroCluster (MC) software is a solution that combines array-based clustering with synchronous replication to deliver continuous availability and zero data loss at the lowest cost. MetroCluster was not included in the evaluation and was not tested in the evaluated configuration.

Feature	Description
System Manager GUI	The System Manager GUI was modified with the intention of simplifying the way admins manage ONTAP basic operations, such as storage provisioning and day-to-day operations. The System Manager GUI is considered out of scope and all management is performed via the command line interface.
VMware Virtualization	VMware integration and supports a number of new features including FlexGroup datastore support. ONTAP 9.8 allows you to provision a FlexGroup volume as a VMware NFS datastore, simplifying datastore management with a single, scalable datastore that provides the power of a full ONTAP cluster. VMware Virtualization was not included in the evaluation and was not tested in the evaluated configuration.

3 Documentation

The following documents, part of the ONTAP 9.10.1P14 documentation set, are included in the TOE documentation:

- "ONTAP 9.10.1 commands"
- "Security and data encryption - ONTAP 9"
- "Cluster administration - ONTAP 9"
- "Set up, upgrade and revert ONTAP - ONTAP 9"
- "Volume administration - ONTAP 9"

These documents, as well as all others in the documentation set, are available via the following URLs:

- https://docs.netapp.com

4 Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the [CPP_FDE_AA_V2.0E].

In general, the [CPP_FDE_AA_V2.0E] has presented a Security Problem Definition appropriate for requirements for Data-at-Rest protection for a lost device that contains storage, and as such is applicable to the NetApp Storage Systems running ONTAP 9.10.1P14 TOE.

5 Security Objectives

The [cPP_FDE_AA_V2.0E] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [cPP_FDE_AA_V2.0E] has presented a Security Objectives statement appropriate for Data-at-Rest protection, and as such is applicable to the NetApp Storage Systems running ONTAP 9.10.1P14 TOE.

5.1 Security Objectives for the Operational Environment

Table 5: Security Objectives for Operational Environment

Objective	Description
OE.TRUSTED_CHANNEL	Communication among and between product components (i.e., AA and EE) is sufficiently protected to prevent information disclosure.
OE.INITIAL_DRIVE_STATE	The OE provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.
OE.PASSPHRASE_STRENGTH	An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE.
OE.POWER_DOWN	Volatile memory is cleared after power-off so memory remnant attacks are infeasible.
OE.SINGLE_USE_ET	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.
OE.STRONG_ENVIRONMENT_CRYPTO	The Operating Environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE and Appendix A.
OE.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.
OE.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
OE.PLATFORM_I&A	The Operational Environment will provide individual user identification and authentication mechanisms that operate independently of the authorization factors used by the TOE.
OE.PHYSICAL	The Operational Environment will provide a secure physical computing space such than an adversary is not able to make modifications to the environment or to the TOE itself.

6 IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the TOE and to scope the evaluation effort.

The SFRs have all been drawn from the [CPP_FDE_AA_V2.0E].

As a result, any selection, assignment, or refinement operations already performed by that Protection Profile (PP) on the claimed SFRs are not identified here (i.e., they are not formatted in accordance with the conventions specified in section 1.3 of this ST). Formatting conventions are only applied on SFR text that was chosen at the ST author's discretion.

6.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [CPP_FDE_AA_V2.0E]. This ST references the following extended SFRs.

- FCS_AFA_EXT.1 Authorization Factor Acquisition
- FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition
- FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)
- FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)
- FCS_KDF_EXT.1 Cryptographic Key Derivation
- FCS_KYC_EXT.1 Key Chaining (Initiator)
- FCS_KYC_EXT.2 Key Chaining (Recipient)
- FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning
- FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)
- FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
- FCS_VAL_EXT.1 Validation
- FPT_KYP_EXT.1 Protection of Key and Key Material
- FPT_PWR_EXT.1 Power Saving States
- FPT_PWR_EXT.2 Timing of Power Saving States
- FPT_TST_EXT.1 TSF Testing
- FPT_TUD_EXT.1 Trusted Update

6.2 TOE Security Functional Requirements

Table 6 identifies the SFRs satisfied by the TOE.

Table 6: TOE Security Functional Components

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_AFA_EXT.1 Authorization Factor Acquisition
	FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition
	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)
	FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)
	FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)
	FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)
	FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)
	FCS_KDF_EXT.1: Cryptographic Key Derivation
	FCS_KYC_EXT.1: Key Chaining (Initiator)
	FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning
	FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
	FCS_VAL_EXT.1: Validation
FMT: Security Management	FMT_MOF.1: Management of Functions Behavior
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Key and Key Material
	FPT_PWR_EXT.1: Power Saving States
	FPT_PWR_EXT.2: Timing of Power Saving States
	FPT_TST_EXT.1: TSF Testing

Requirement Class	Requirement Component
	FPT_TUD_EXT.1: Trusted Update

6.2.1 Cryptographic Support (FCS)

6.2.1.1 FCS_AFA_EXT.1 Authorization Factor Acquisition

FCS_AFA_EXT.1.1 The TSF shall accept the following authorization factors: [

- ***a submask derived from a password authorization factor conditioned as defined in FCS_PCC_EXT.1***

].

6.2.1.2 FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition

FCS_AFA_EXT.2.1 The TSF shall reacquire the authorization factor(s) specified in FCS_AFA_EXT.1 upon transition from any Compliant power saving state specified in FPT_PWR_EXT.1 prior to permitting access to plaintext data.

6.2.1.3 FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys)

FCS_CKM.1.1(b) The TSF shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [***256 bit***] that meet the following: [no standard].

6.2.1.4 FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)

FCS_CKM.4.1(a) The TSF shall [***erase***] cryptographic keys and key material from volatile memory when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1 that meets the following: [a key destruction method specified in FCS_CKM.4(d)].

6.2.1.5 FCS_CKM.4(d) Cryptographic Key Destruction (Software TOE, 3rd Party Storage)

FCS_CKM.4.1(d) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For volatile memory, the destruction shall be executed by a [***
  - ***single overwrite consisting of [***
    - ***a pseudo-random pattern using the TSF's RBG,***
    - ***zeroes,***
  - ***removal of power to the memory];***
- ***For non-volatile storage that consists of the invocation of an interface provided by the underlying platform that [***
  - ***logically addresses the storage location of the key and performs a [single] overwrite consisting of [***
    - ***a pseudo-random pattern using the TSF's RBG,***

- ***zeroes]***

]

that meets the following: [no standard].

6.2.1.6 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)

FCS_CKM_EXT.4.1(a) The TSF shall destroy all keys and key material when no longer needed.

6.2.1.7 FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)

FCS_CKM_EXT.4.1(b) The TSF shall destroy all key material, BEV, and authentication factors stored in plaintext when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1.

6.2.1.8 FCS_COP.1(a) Cryptographic Operation (Signature Verification)

FCS_COP.1.1(a) The TSF shall perform [cryptographic signature services (verification)] in accordance with a [

- ***RSA Digital Signature Algorithm with a key size (modulus) of [3072-bit***]

that meet the following: [

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes***

].

6.2.1.9 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1(b) The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [***SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].

6.2.1.10 FCS_COP.1(c) Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1(c) The TSF shall perform cryptographic [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [***HMAC-SHA-512***] and cryptographic key sizes [**L1 = 2,048, L2 = 512**] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**].

Application Note: *The key size [k] in the assignment falls into a range between L1 and L2 (defined in ISO/IEC 10118 for the appropriate hash function for example for SHA-256 L1 = 512, L2 =256) where L2 ≤ k ≤ L1.*

6.2.1.11 FCS_COP.1(d) Cryptographic Operation (Key Wrapping)

FCS_COP.1.1(d) The TSF shall perform [key wrapping] in accordance with a specified cryptographic algorithm [AES] in the following modes **[*KWP*]** and the cryptographic key size [***256 bits***] that meet the following: [AES as specified in ISO/IEC 18033-3, ***[NIST SP 800-38F]***].

6.2.1.12 FCS_KDF_EXT.1 Cryptographic Key Derivation

FCS_KDF_EXT.1.1 The TSF shall accept [***a conditioned password submask***] to derive an intermediate key, as defined in [

- ***NIST SP 800-132***]

using the keyed-hash functions specified in FCS_COP.1(c), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

6.2.1.13 FCS_KYC_EXT.1 Key Chaining (Initiator)

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [

- ***intermediate keys originating from one or more submask(s) to the BEV using the following method(s): [***
  - ***key derivation as specified in FCS_KDF_EXT.1,***
  - ***key wrapping as specified in FCS_COP.1(d),***

while maintaining an effective strength of [***256 bits***] for symmetric keys and an effective strength of [***not applicable***] for asymmetric keys.

FCS_KYC_EXT.1.2 The TSF shall provide at least a [***256 bit***] BEV to [**encryption engine**] [

- ***after the TSF has successfully performed the validation process as specified in FCS_VAL_EXT.1***].

6.2.1.14 FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning

FCS_PCC_EXT.1.1 A password used by the TSF to generate a password authorization factor shall enable up to [**256**] characters in the set of {upper case characters, lower case characters, numbers, and [**all printable ASCII characters**]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC-[***SHA-512***], with [**1024**] iterations, and output cryptographic key sizes [***256 bits***] that meet the following: [NIST SP 800-132].

6.2.1.15 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [***[NIST SP 800-90A]***] using [***CTR_DRBG (AES)***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- ***[2] software-based noise source(s),***
- ***[2] hardware-based noise source(s)***]

with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.2.1.16 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

FCS_SNI_EXT.1.1 The TSF shall [***use salts that are generated by a [DRBG as specified in FCS_RBG_EXT.1]***].

FCS_SNI_EXT.1.2 The TSF shall use [***no nonces***].

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner [

- ***CBC: IVs shall be non-repeating and unpredictable;***
- ***CCM: Nonce shall be non-repeating and unpredictable;***
- ***XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer;***
- ***GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key***].

6.2.1.17 FCS_VAL_EXT.1 Validation

FCS_VAL_EXT.1.1 The TSF shall perform validation of the [***submask***] using the following method(s): [

- ***key wrap as specified in FCS_COP.1(d)***].

FCS_VAL_EXT.1.2 The TSF shall require validation of the [BEV] prior to [forwarding the BEV to the EE].

FCS_VAL_EXT.1.3 The TSF shall [

- ***require power cycle/reset the TOE after [1] of consecutive failed validation attempts***].

Application Note: If an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives. Consequently, ONTAP will not see any drives and will panic, resulting in a system reboot.

While attempting to recover from a failure in the boot media, if an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives.

Consequently, ONTAP will not see any drives and will panic, resulting in a system reboot.

6.2.2 Security Management (FMT)

6.2.2.1 FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [use of Compliant power saving state] to [authorized users].

6.2.2.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) forwarding requests to change the DEK to the EE,
b) forwarding requests to cryptographically erase the DEK to the EE,
c) allowing authorized users to change authorization factors or set of authorization factors used,
d) initiate TOE firmware/software updates,
e) ***[no other functions]***].

6.2.2.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [authorized user].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.3 Protection of the TSF (FPT)

6.2.3.1 FPT_KYP_EXT.1 Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall [

- ***only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)].***

6.2.3.2 FPT_PWR_EXT.1 Power Saving States

FPT_PWR_EXT.1.1 The TSF shall define the following Compliant power saving states: [***G2(S5), G3***].

6.2.3.3 FPT_PWR_EXT.2 Timing of Power Saving States

FPT_PWR_EXT.2.1 For each Compliant power saving state defined in FPT_PWR_EXT.1.1, the TSF shall enter the Compliant power saving state when the following conditions occur: user-initiated request, [***shutdown***].

6.2.3.4 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), at the conditions [before the function is first invoked]***] to

demonstrate the correct operation of the TSF: [**cryptographic algorithm tests, software integrity test**].

6.2.3.5 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide [authorized users] the ability to query the current version of the TOE [***software***].

FPT_TUD_EXT.1.2 The TSF shall provide [authorized users] the ability to initiate updates to TOE [***software***].

FPT_TUD_EXT.1.3 The TSF shall verify updates to the TOE software using a [***digital signature as specified in FCS_COP.1(a)***] by the manufacturer prior to installing those updates.

6.3 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 1 augmented with the *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata, February 1, 2019. The assurance components are summarized in the following table:

Table 7: Assurance Components

Requirement Class	Requirement Component
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended Components Definition (ASE_ECD.1)
	ST Introduction (ASE_INT.1)
	Security Objectives for the Operational Environment (ASE_OBJ.1)
	Stated Security Requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE Summary Specification (ASE_TSS.1)
ADV: Development	Basic Functional Specification (ADV_FSP.1)
AGD: Guidance Documents	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
ALC: Life Cycle Support	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
ATE: Tests	Independent Testing – Sample (ATE_IND.1)
AVA: Vulnerability Assessment	Vulnerability Survey (AVA_VAN.1)

Requirement

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR**,** including a proprietary Key Management Description (Appendix E), and **[Entropy Essay, list of all of 3rd party**

software libraries (including version numbers), 3rd party hardware components (including model/version numbers)].

Table 8: Third Party Components

Component	Model/ Version Number
Third Party Hardware Components	
Solid State Drive (SSD)	FAS 2650: X440_PHM2800MCTO A800: X4010S172B1T9NTE FAS 8300: X440_PHM2800MCTO, X440_TPM3V800AMD
Hard Disk Drive	FAS 8020 : X417_HCBFE900A10, X417_SLTNG900A10
Third Party Software Components	
OpenSSL	OpenSSL 1.0.2zh-fips
Intel ISA-L Crypto Library	v2.22 Intel Intelligent Storage Acceleration Library Crypto

6.3.1 ADV_FSP.1 Basic functional specification

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.3.2 AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.3 AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.3.4 ALC_CMC.1 Labelling of the TOE

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

ALC_CMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5 ALC_CMS.1 TOE CM coverage

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.6 ATE_IND.1 Independent testing - conformance

ATE_IND.1.1D The developer shall provide the TOE for testing.

ATE_IND.1.1C The TOE shall be suitable for testing.

ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.3.7 AVA_VAN.1 Vulnerability survey

AVA_VAN.1.1D The developer shall provide the TOE for testing.

AVA_VAN.1.1C The TOE shall be suitable for testing.

AVA_VAN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

7 TOE Summary Specification

This Section describes the following security functions:

- Cryptographic Support
- Security Management
- Protection of the TSF

7.1 Cryptographic Support

All TOE cryptographic services are provided by the NetApp software modules CryptoMod version 2.2 and the NetApp Cryptographic Security Module (NCSM). NetApp's CryptoMod module is used to:

- Generate salts and keying material via a validate DRBG.
- Derive keys via PBKDFv2.
- Calculate cryptographic hashes.
- Encrypt/decrypt data using validated AES encryption/decryption modes.
- Calculate HMACs.
- Encrypt keys using KWP-AE.
- Decrypt keys using KWP-AD.
- Store volatile keys.
- Zeroize volatile keys.

The NetApp Cryptographic Security Module is used to validate the TOE's cryptographically signed images using approved cryptographic hash and digital signature validation algorithms. All cryptographic algorithms are NIST CAVP certified. The following table identifies the cryptographic algorithms used by the TSF, the associated standards to which they conform, and the NIST certificates that demonstrate that the claimed conformance has been met.

Table 9: CryptoMod version 2.2 Algorithm Certificates

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Hash Algorithm)			
FCS_COP.1.1(b)	SHA-256, SHA-512	ISO/IEC 10118-3:2004	C1884: SHA2-256 C1884: SHA2-512

SFR	Algorithm	Standard	Certificate
			C1885: SHA2-256 C1885: SHA2-512
Cryptographic Operation (Keyed Hash Algorithm)			
FCS_COP.1.1(c)	HMAC-512	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”	C1884: HMAC-SHA2-512 C1885: HMAC-SHA2-512
Cryptographic Operation (Key Wrapping)			
FCS_COP.1.1(d)	AES-KWP-256	NIST SP 800-38F	C1884: AES-KWP C1885: AES-KWP
Cryptographic Operation (Random Bit Generation)			
FCS_RBG_EXT.1	AES-256 (CTR_DRBG)	NIST SP 800-90A	C1884: Counter DRBG C1885: Counter DRBG

Table 10: NetApp Cryptographic Security Module (NCSM v2.0) Algorithm Certificates

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Signature Verification)			
FCS_COP.1.1(a)	RSA 3072	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes	A2157: RSA SigVer (FIPS 186-4)
Cryptographic Operation (Hash Algorithm)			

SFR	Algorithm	Standard	Certificate
FCS_COP.1.1(b)	SHA-256 SHA-384 SHA-512	ISO/IEC 10118-3:2004	A2157: SHA2-256, A2157: SHA2-384, A2157: SHA2-512

7.1.1 FCS_AFA_EXT.1: Authorization Factor Acquisition

The cluster passphrase serves as the password authorization factor. In CC mode, the cluster passphrase (64-256 bytes) must be entered at boot before ONTAP is allowed to boot. The Cluster Passphrase Key Encryption Key (CP-KEK) is derived from the Cluster Passphrase (CP) and the Cluster Salt using a NIST SP 800-132 approved password-based key derivation function (PBKDFv2).

There are three operations that require a user to enter the existing cluster passphrase:

1. Whenever the cluster passphrase is changed (security key-manager onboard update-passphrase).
2. When booting ONTAP (CC mode only).
3. When recovering from a failure in the boot media.

7.1.2 FCS_AFA_EXT.2: Timing of Authorization Factor Acquisition

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off). The Compliant power saving states require that the cluster passphrase be entered at boot before ONTAP is allowed to boot.

7.1.3 FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)

The TOE generates the Cluster Key Encryption Key (CKEK) which is a 256-bit AES key generated by the CryptoMod DRBG. The wCKEK is the encrypted (wrapped) form of CKEK using [NIST 800-38F] KWP-AE with CP-KEK used as the encrypting (wrapping) key. The CKEK key is used to wrap the Authentication Keys (AKs).

ONTAP creates two 32-byte DRBG generated authentication keys (collectively known as AKs) when the ONTAP Onboard Key Manager is configured. The two instances of authentication keys are called AK1 and AK2. Customers are free to assign AK1 (or AK2) to either the data or FIPS port of the controller's NSE drive. Best practices dictate that one AK be used for the drive's data port and the other for the drive's FIPS port.

Neither AK1 nor AK2 is persistently stored. The wrapped versions of the AKs (wAK1 and wAK2) are persistently stored in the OKM DB. For FDE-AA with NSE, the AK is a BEV.

7.1.4 FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

The keys in volatile memory are destroyed when entering the G3 or G2(S5) Compliant power saving state. In both states, power is removed from memory and all values drain to a zero state.

The G2(S5) Compliant power saving state is entered when an authorized user executes the `system node halt` command.

The G3 Compliant power saving state is entered when power to the appliance is removed, for example, by throwing the on/off switch or pulling the power plug.

Once either of the two Compliant power saving states is entered, the cluster passphrase must be entered in order for ONTAP to boot and resume operation.

7.1.5 FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)

Both AK1 and AK2 remain active as long as OKM is configured. New versions of AK1 and AK2 can be generated by first disabling OKM (`security key-manager onboard disable`) and then re-enabling OKM (`security key-manager onboard enable`). When OKM is disabled, all keys associated with OKM (CP-KEK, CKEK, AK1, and AK2) will be destroyed.

When a key is destroyed (or zeroized), it is destroyed in the following manner:

- Key stored in non-volatile memory:
  - Storage location overwritten with DRBG generated random data.
  - Storage location overwritten with zeroes.
  - Storage location read and compared with zero.
- Key stored in volatile memory:
  - Memory location overwritten with DRBG generated random data.
  - Memory location overwritten with zeroes.
  - Memory location read and compared with zero.

The CP, CP-KEK, CKEK, AK1, and AK2 will be destroyed by the removal of power to the memory when entering the G3 and G2(S5) Compliant power saving states.

The following table summarizes the CSPs and keys used by the TOE. The keys are identified as which are stored in volatile memory and non-volatile memory.

Table 11 Critical Security Parameters

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
CP	Authorization factor	64 to 256-byte ASCII passphrase	Supplied by cluster administrator when "security key-manager onboard enable" is executed, when	Temporarily "stored" as a variable or a CPU register value in functions involved in the	Not stored in non-volatile memory.	1

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
			"security key-manager onboard update-passphrase" is executed and when ONTAP is rebooted.	calculation of the CP-KEK. Not stored in the cryptomod key table.		
CP-Salt	Salt used with CP when creating CP Hash	64-byte random salt	Cryptomod DRBG	Temporarily "stored" as a variable or CPU register value in functions involved in the calculation of the CP-KEK or functions that need to store the CP-Salt in non-volatile memory. Not stored in the cryptomod key table.	Persistently stored in non-volatile memory in an RDB table and the OKM database.	2
CP-Hash	Used to validate the CP	SHA-256(CP-Salt || CP)	Cryptomod SHA-256 performed on the CP	Temporarily "stored" as a variable or CPU register value in functions that need to validate the cluster passphrase, or functions that need to store the CP-Hash in non-volatile memory. Not stored in the cryptomod key table.	Persistently stored in non-volatile memory within an RDB table.	2

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
Cluster-Salt	Salt used in creation of CP-KEK	64-byte random salt	Cryptomod DRBG	Temporarily "stored" as a variable or CPU register value in functions that need to calculate the CP-KEK, or functions that need to store the Cluster-Salt in non-volatile memory. Not stored in the cryptomod key table.	Persistently stored in non-volatile memory within an RDB table and the OKM DB.	2,3
CP-KEK	Used to protect the CKEK.	AES-256 key derived using PBKDF2 function with HMAC-SHA-512 used as the PRF (1024 iterations).	Cryptomod PBKDF2	Temporarily "stored" as a variable or CPU register value in functions that need to wrap/unwrap the CKEK. Stored in cryptomod's key table.	Not stored in non-volatile memory.	4
CKEK	Used to protect each of the SVM-KEKs.	AES-256 key	Cryptomod DRBG	Temporarily "stored" as a variable or CPU register value in functions that need to wrap/unwrap keys wrapped by the CKEK. Stored in cryptomod's key table.	Not stored in non-volatile memory.	4

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
wCKEK	Encrypted form of CKEK	Wrapped (encrypted) form of CKEK using [NIST 800-38F] KWP-AE with CP-KEK used as the encrypting key	Cryptomod KWP	Temporarily "stored" as a variable or CPU register value in functions that need to calculate the wCKEK, functions that need to unwrap the wCKEK, or functions that need to store the wCKEK in non-volatile memory. Not stored in the cryptomod key table.	Persistently stored in non-volatile memory within an RDB table and the OKM DB.	2,3
AK	Authentication Key	32-byte random value	Cryptomod DRBG	Temporarily "stored" as a variable or CPU register value in functions that need to calculate the wAK and functions that need to use the AK to authenticate to a SED. Stored in the cryptomod key table.	Not stored in non-volatile memory	5
wAK	Encrypted form of AK	Wrapped (encrypted) form of AK using [NIST 800-38F] KWP-AE with CKEK used	Cryptomod KWP	Temporarily "stored" as a variable or CPU register value in functions that need to	Persistently stored in non-volatile memory within an RDB	2,3,6

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
		as the encrypting key		calculate the wAK, functions that need to unwrap the wAK, and functions that need to store the wAK to non-volatile memory. Not stored in the cryptomod key table.	table and the OKM DB.	

Notes:

1. The cluster passphrase (CP) is required when setting up OKM, when updating the passphrase, when ONTAP reboots, and when performing a recovery operation.
2. RDB is the replicated, cluster-wide database used by ONTAP.
3. The OKM DB file, located at */cfcard/kmip/km_onboard.wkeydb*, contains the cluster salt, the node salt (not used in Common Criteria mode), encrypted key material (wCKEK, wAK1, and wAK2), and key IDs.
4. The cryptomod key table memory utilizes memory that is auto zeroed during core dumps.
5. There are two AKs generated: AK1 and AK2. AK is used to generically refer to both instances.
6. There are two wAKs generated: wAK1 and wAK2. wAK is used to generically refer to both instances.

The TOE temporarily stores key material such as the unwrapped AK and the PBKDFv2 based upon the Cluster Passphrase and salt. The TOE clears the keys from memory by removal of power. The TOE also clears the keys when they are no longer needed.

The following keys are destroyed when the Cluster Passphrase is changed or the OKM is deleted:

- CP-KEK
- CKEK
- wCKEK
- AK (AK1 and AK2)
- wAK (wAK1 and wAK2).

The OKM is deleted on the following conditions:

- No further need for a key manager
- Migration to an external configuration.

The OKM cannot be deleted if any NSE drive within the ONTAP cluster is locked with either AK1 or AK2.

7.1.6 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)

The TOE shall delete all keys and key material when no longer needed. The keys are destroyed when the OKM is deleted. The OKM DB is deleted when the Onboard Key Manager is deleted.

Neither the AK1 nor AK2 is persistently stored. The wrapped versions of the AKs (wAK1 and wAK2) are persistently stored in the OKM DB. The internal Onboard Key Manager (OKM) is used to manage the authentication key (AK) used by the array's SED capable drives.

7.1.7 FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management)

The CP, CP-KEK, CKEK, AK1, and AK2 will be destroyed by the removal of power to the memory when entering the G3 and G2(S5) Compliant power saving states.

An authorized user can execute the `system node halt` command for the G2(S5) Compliant power saving state. The TOE must be fully rebooted from each Compliant power saving state.

7.1.8 FCS_COP.1(a): Cryptographic Operation (Signature Verification)

The TOE implements the RSA Digital Signature Algorithm with a key size (modulus) of 3072-bits with SHA-384 signatures to verify authenticity of the trusted updates. Upon receiving an update and the signature file, the TOE uses the embedded public key stored in the firmware on the NetApp Appliance. The TOE will verify the signature before installing it and reject any update with an invalid signature.

7.1.9 FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)

The TOE performs SHA-256, SHA-384 and SHA-512 cryptographic hashing services that meet the following: ISO/IEC 10118-3:2004. The TOE uses the SHA-384 hash functions as part of the RSA signature verification function for the trusted updates. The TOE uses the SHA-512 hash function as part of the PBKDFv2 to produce the cluster passphrase. A SHA-256 digest is used to validate the cluster passphrase (CP).

7.1.10 FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm)

The TOE performs HMAC-SHA-512 message authentication using cryptographic key sizes 512-2048 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". HMAC-SHA-512 is used for PBKDF2. In PBKDF2, the OKM passphrase is used as the HMAC-SHA-512 key.

Table 12: HMAC Details

HMAC Function	Key Length	Block Size	Output MAC Length	Hash Function Used
HMAC-SHA-512	L2 = 512, L1 = 2048	1024	512	SHA-512

7.1.11 FCS_COP.1(d): Cryptographic Operation (Key Wrapping)

The TOE uses the NIST 800-38F KWP-AE(P) routine to encrypt (or "wrap") a key and the corresponding NIST 800-38F KWP-AD(C) routine to decrypt ("unwrap") an encrypted, or wrapped, key.

7.1.12 FCS_KDF_EXT.1: Cryptographic Key Derivation

The TOE implements PBKDFv2 with HMAC-SHA-512, 1024 iterations, and a salt value of 512 bits to transform the Cluster Passphrase into a derived key as specified in SP800-132; the CP-KEK is used to unwrap the wrapped CKEK, which in turn is used to unwrap the wrapped AKs, which in turn are passed to the EE as BEVs . The output is at least of equivalent security strength (in number of bits) to the BEV.

7.1.13 FCS_KYC_EXT.1: Key Chaining (initiator)

The TOE uses the PBKDFv2 key derivation function to transform the Cluster Passphrase into the CP-KEK, which is used to unwrap the wCKEK, which is then used to unwrap the wAK, which then constitutes the BEV. The Cluster Passphrase is validated by hashing it along with the CP Salt and comparing the result to the persistently stored CP Hash. If the two values are equal, the Cluster Passphrase is correct and so it can be used to derive the CP-KEK.

7.1.14 FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning

The TOE accepts passwords up to 256 characters. The character set can consist of all upper-case characters, lower-case characters, numbers, and all printable ASCII characters. The password is conditioned using PBDKFv2 that meets SP800-132. The cryptographic algorithm implements HMAC-SHA-512, a salt value of 512 bits from the DRBG, and 1024 iterations to produce a cryptographic key size of 256-bits.

7.1.15 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Random bits are produced by a DRBG implemented within the NetApp CryptoMod module. The DRBG uses the CTR_DRBG algorithm from NIST SP 800-90A. The implementation of CTR_DRBG uses AES-256 (maximum of 256 bits of security strength) as the block cipher along with the appropriate derivation function. Entropy will be provided from the OS /dev/random device, which can provide as much entropy as is requested by the calling function.

The CTR_DRBG (AES) is seeded with at least 384-bits from:

- software-based noise sources
    - Software interrupts

  - Internal event interrupts
- hardware-based noise sources
  - Ethernet interrupts
  - Intel RDRAND instruction set.

7.1.16 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

The TOE generates salts using its CTR_DRBG (AES) to generate the cluster salt, a 64-byte random number. The cluster salt is used along with the cluster passphrase to derive the cluster passphrase key encryption key (CP-KEK) using a NIST SP 800-132 approved PBKDFv2 algorithm.

The TOE does not implement any of these modes of AES: (CBC, CCM, XTS, or GCM), so this requirement is vacuously satisfied.

7.1.17 FCS_VAL_EXT.1 Validation

The Cluster Passphrase is a 64–256-byte customer generated ASCII string that is used as an authorization factor. The Cluster Passphrase is used in conjunction with a salt value to derive a cluster passphrase key encryption key (CP-KEK) via a NIST SP 800-132 ([NIST 800-132]) approved PBKDFv2 algorithm. The CP-Hash is used by OKM when there is a need to validate that the Cluster Passphrase has been entered correctly by a storage administrator. As indicated in Table 10, the CP-Hash is defined as SHA-256(CP-Salt || Cluster Passphrase) where '||' denotes concatenation.

During booting ONTAP or recovering from a failure in the boot media, if an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives. As a consequence, ONTAP will not see any drives and will panic, resulting in a system reboot. The only way to recover is to manually reboot and enter the correct passphrase.

When modifying the cluster passphrase, a customer is allowed 5 consecutive failed attempts to authenticate with the current cluster passphrase. After 5 consecutive failed attempts, the cluster passphrase may be modified only by (a) rebooting one or more nodes within the cluster, or (b) waiting for 24 hours to elapse before re-attempting to modify the cluster passphrase.

There are three operations that require a user to enter the existing cluster passphrase:

1. Changing the cluster passphrase (security key-manager onboard update-passphrase);
2. Booting ONTAP (CC mode only);
3. Recovering from a failure in the boot media.

The ONTAP limit on the number of failed authentication attempts for each of the scenarios listed above, as well as a description of how ONTAP behaves when the limit is reached, is provided in the following table.

Table 13 Maximum Failed Attempts

Scenario	Maximum Failed Authentication Attempt Limit	ONTAP Behavior When Limit Reached
Changing Cluster Passphrase	5	When the maximum is exceeded, either one (or more) nodes within the cluster must be successfully rebooted or a 24-hour time period needs to elapse before the administrator is allowed to change the cluster passphrase.
Booting ONTAP	1	If an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives. As a consequence, ONTAP will not see any drives and will panic, resulting in a system reboot.
Recovering from a failure in the boot media	1	If an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives. As a consequence, ONTAP will not see any drives and will panic, resulting in a system reboot.

7.2 Security Management

7.2.1 FMT_MOF.1 Management of Functions Behavior

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

The TOE enters the G3 (mechanical off) state when the administrator removes the device power via a mechanical switch. Only an authorized user can execute the `system node halt` command for the G2(S5) Compliant power saving state.

7.2.2 FMT_SMF.1: Specification of Management Functions

The TOE is capable of performing the following management functions:

- Forwarding requests to change the DEK to the EE

  The TOE can send a request to the drive to change the DEK via the `storage encryption disk sanitize` CLI command.

- Forwarding requests to cryptographically erase the DEK to the EE

  The TOE can send a request to cryptographically erase the disk, followed by changing the AK to random value that is not retained by ONTAP using the `storage encryption disk destroy` CLI command.

- Allowing authorized users to change authorization factors or set of authorization factors used

  Authorized users can change authorization factors or set of authorization factors used by the `security key-manager onboard update-passphrase` command.

- Initiate TOE firmware/software updates

  The authorized user can initiate TOE software updates via the `cluster image update` CLI command.

7.2.3 FMT_SMR.1: Security Roles

The TOE maintains the role of authorized user.

7.3 Protection of the TSF

7.3.1 FPT_KYP_EXT.1: Protection of Key and Key Material

The TOE stores the following encrypted keys in the Onboard Key Manager (OKM):

- wAK – (Encrypted form of AK) - wrapped (encrypted) form of AK using [NIST 800-38F] KWP-AE with CKEK used as the encrypting key,
- wCKEK –(Encrypted form of CKEK) - Wrapped (encrypted) form of CKEK using [NIST 800-38F] KWP-AE with CP-KEK used as the encrypting key.

7.3.2 FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States

The TOE enters the G3 (mechanical off) state when the administrator removes the device power via a mechanical switch. An authorized user can execute the `system node halt` command for the G2(S5) Compliant power saving state. The TOE must be fully rebooted from each Compliant power saving state.

7.3.3 FPT_TST_EXT.1: TSF Testing

The TOE includes power-on self-tests to ensure that the TOE is operating correctly. The power-on self-tests include a Known Answer Test (KAT) to verify the correctness of the cryptographic algorithms and the software integrity test to ensure that the module is not corrupted.

The KATs for cryptographic functions consist of executing each function on data for which the correct answer is already known. The output produced by the tested function is compared with the known answer. If they are not identical, the KAT fails.

The TOE includes the following power-on self-tests to ensure that the cryptographic functionality is performing correctly:

The Known Answer Tests (KATs) include the following:

- AES-128 CBC, AES-256 CBC – encryption/decryption test
- 256-AES-KWP – encryption/decryption test
- DRBG – Tested per SP800-90A, including the Health Testing identified in Section 11.3.
- HMAC SHA-512 - keyed-hash message authentication code test
- PBKDF2 - Password-Based Key Derivation Function 2 test

- SHA-256, SHA-384, SHA-512 - hashing test
- RSA Signature Generation/Verification – 2048 bits and 3072-bits

The TOE performs the following software integrity test to ensure that the module is not corrupted.

- Software integrity test - During power-on self-testing, the module performs a self-integrity check and compares the results against the build time generated hash digests. During power on, the bootloader validates the whitelist database of secure boot keys with the signature associated with each module that is loaded. After each module is validated and loaded, the boot process continues with the ONTAP initialization. If signature validation fails for any module, the system reboots.

7.3.4 FPT_TUD_EXT.1: Trusted Update

The TSF provides authorized users the ability to query the current version of the TOE. The administrator executes the `cluster image show` or the `version` command to display the current version of the TOE.

NetApp code signing ensures that ONTAP images installed through non-disruptive image updates or automated non-disruptive image updates are authentically produced by NetApp and have not been tampered with. The NetApp updates are cryptographically signed using an RSA Digital Signature algorithm with a key size of 3072-bits with a SHA-384 signature. The private keys, used for code signing, are stored in a limited access HSM at NetApp. If the TOE's public keys are tampered with then an update will fail.

The TOE will verify the signature before installing the update and reject any update with an invalid signature.

This is a no-touch security feature for upgrading ONTAP versions. The user is not expected to do anything differently except for optionally verifying the top-level image.tgz signature.

8 Protection Profile Claims

The ST conforms to:

- collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata, February 1, 2019 [CPP_FDE_AA_V2.0E] with the following optional and selection-based SFRs: FCS_CKM.1(b), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_KDF_EXT.1, FCS_PCC_EXT.1, FCS_RBG_EXT.1, FCS_VAL_EXT.1, FPT_TST_EXT.1.

As explained in Section 3, the Security Problem Definition of the [cPP_FDE_AA_V2.0E] has been included by reference into this ST.

As explained in Section 5, Security Objectives, the Security Objectives of the [cPP_FDE_AA_V2.0E] has been included by reference into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is reproduced from the [cPP_FDE_AA_V2.0E] and operations completed as appropriate.

Table 14: Security Functional Requirements

Requirement Class	Requirement Component	Source
FCS: Cryptographic Support	FCS_AFA_EXT.1 Authorization Factor Acquisition	[cPP_FDE_AA_V2.0E]
	FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition	[cPP_FDE_AA_V2.0E]
	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)	[cPP_FDE_AA_V2.0E]
	FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)	[cPP_FDE_AA_V2.0E]
	FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)	[cPP_FDE_AA_V2.0E]
	FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)	[cPP_FDE_AA_V2.0E]
	FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)	[cPP_FDE_AA_V2.0E]
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)	[cPP_FDE_AA_V2.0E]
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)	[cPP_FDE_AA_V2.0E]
	FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm)	[cPP_FDE_AA_V2.0E]
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)	[cPP_FDE_AA_V2.0E]
	FCS_KDF_EXT.1: Cryptographic Key Derivation	[cPP_FDE_AA_V2.0E]
	FCS_KYC_EXT.1: Key Chaining (Initiator)	[cPP_FDE_AA_V2.0E]

Requirement Class	Requirement Component	Source
	FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning	[cPP_FDE_AA_V2.0E]
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	[cPP_FDE_AA_V2.0E]
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	[cPP_FDE_AA_V2.0E]
	FCS_VAL_EXT.1: Validation	[cPP_FDE_AA_V2.0E]
FMT: Security Management	FMT_MOF.1: Management of Functions Behavior	[cPP_FDE_AA_V2.0E]
	FMT_SMF.1: Specification of Management Functions	[cPP_FDE_AA_V2.0E]
	FMT_SMR.1: Security Roles	[cPP_FDE_AA_V2.0E]
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Key and Key Material	[cPP_FDE_AA_V2.0E]
	FPT_PWR_EXT.1: Power Saving States	[cPP_FDE_AA_V2.0E]
	FPT_PWR_EXT.2: Timing of Power Saving States	[cPP_FDE_AA_V2.0E]
	FPT_TST_EXT.1: TSF Testing	[cPP_FDE_AA_V2.0E]
	FPT_TUD_EXT.1: Trusted Update	[cPP_FDE_AA_V2.0E]

9 Rationale

This security target includes by reference the [cPP_FDE_AA_V2.0E] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [cPP_FDE_AA_V2.0E] assumptions. [cPP_FDE_AA_V2.0E] and security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [cPP_FDE_AA_V2.0E] application notes and assurance activities. Consequently, [cPP_FDE_AA_V2.0E] rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

9.1 TOE Summary Specification Rationale

Each subsection in Section 7, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The security functions work together to satisfy all of the security functional requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 7, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 13

"Security Functions vs. Requirements Mapping" demonstrates the relationship between security requirements and security functions.

Table 15: Security Functions vs. Requirements Mapping

Specification	Cryptographic support	Security management	Protection of the TSF
FCS_AFA_EXT.1	X		
FCS_AFA_EXT.2	X		
FCS_CKM.1(b)	X		
FCS_CKM.4 (a)	X		
FCS_CKM.4 (d)	X		
FCS_CKM_EXT.4 (a)	X		
FCS_CKM_EXT.4 (b)	X		
FCS_COP.1(a)	X		
FCS_COP.1(b)	X		
FCS_COP.1(c)	X		
FCS_COP.1(d)	X		
FCS_KDF_EXT.1	X		
FCS_KYC_EXT.1	X		
FCS_KYC_EXT.2	X		
FCS_PCC_EXT.1	X		
FCS_RBG_EXT.1	X		
FCS_SNI_EXT.1	X		
FCS_VAL_EXT.1	X		
FMT_MOF.1		X	
FMT_SMF.1		X	
FMT_SMR.1		X	
FPT_KYP_EXT.1			X
FPT_PWR_EXT.1			X
FPT_PWR_EXT.2			X
FPT_TUD_EXT.1			X
FPT_TST_EXT.1			X