National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
NetApp Storage Encryption (NSE) Running ONTAP 9.16.1

Report Number: CCEVS-VR-VID11573-2026
Dated: February 26, 2026
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Lisa Mitchell
Lori Sarem
The MITRE Corporation

Russ Fink
Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Nil Folquer
Kevin Steiner
Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 provided by NetApp, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in February 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019.

The TOE is NetApp Storage Encryption (NSE) Running ONTAP 9.16.1. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Security Target*, Version 1.8, February 25, 2026, and analysis performed by the Validation team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile (PP) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	NetApp Storage Encryption (NSE) Running ONTAP 9.16.1
Sponsor and Developer	NetApp, Inc. 3060 Olsen Drive San Jose, CA 95128
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017.
CEM	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	*collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019
ST	*NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Security Target*, Version 1.8, February 25, 2026
Evaluation Technical Report	*NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Evaluation Technical Report*, Version 1.4, February 2026
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Nil Folquer and Kevin Steiner
CCEVS Validators	Jenn Dotson, Lisa Mitchell, Lori Sarem, and Russ Fink

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is NetApp Storage Encryption (NSE) running ONTAP 9.16.1, 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 FIPS validated third party SEDs that follow either the Trusted Computing Group's (TCG) Opal or Enterprise standards.

3.1. TOE Evaluated Configuration

The TOE is NetApp Storage Encryption (NSE) running ONTAP 9.16.1, an authorization acquisition product that obtains and manages authorization data used to access encrypted data stored on a FIPS validated full disk encryption product. The TOE provides authorization data to FIPS validated third party self-encrypting drives (SEDs).

3.2. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

a) External clients sending NFS (UNIX) and/or SMB/CIFS (Windows) data that interact with a protocol handler.
b) Physical drives

The non-TOE hardware required by and provisioned with the TOE are identified in the tables below:

Table 2: Non-TOE Hardware (Broadwell)

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
Intel Broadwell Xeon D Processor					
AFF A150	SSD	NAS/SAN	72 24 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 GHz
AFF A220	SSD	NAS/SAN	144 24 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 GHz

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
AFF A300	SSD	NAS/SAN	384	3U	Intel Xeon D-1587 (Broadwell) 2 x 64-bit 16-core 1.70 GHz
AFF C190	SSD	NAS/SAN	24 24 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 8-core 1.50 GHz
ASA A150	SSD	SAN	72 24 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 GHz
ASA AFF A220	SSD	SAN	144 24 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 GHz
FAS2720	HDD/SSD	NAS/SAN	144/136 12 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 GHz
FAS2750	HDD/SSD	NAS/SAN	144/144 24 internal drives	2U	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 GHz)
FAS8200	HDD/SSD	NAS/SAN	480/480	3U	Intel Xeon D-1587 (Broadwell) 2 x 64-bit 16-core 1.70 GHz

Table 3: Non-TOE Hardware (Skylake)

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
Intel Skylake Xeon Scalable Processors					
AFF A320	NVMe	NAS/SAN	96	2U	Intel Xeon Silver 4114 (Skylake-SP) 4 x 64-bit 10-core 2.20 GHz
AFF A800[1]	NVMe/SSD	NAS/SAN	240/240 48 internal drives	4U	Intel Xeon Platinum 8160 (Skylake-SP) 4 x 64-bit 24-core 2.10 GHz
ASA A800[2]	NVMe/SSD	SAN	240/240 48 internal drives	4U	Intel Xeon Platinum 8160 (Skylake-SP) 4 x 64-bit 24-core 2.10 GHz
Intel Skylake Xeon D Processor					
AFF A250	NVMe/SSD	NAS/SAN	48/24 24 internal drives	2U	Intel Xeon D-2164-IT (Skylake-D) 2 x 64-bit 12 core, 2.10 GHz
AFF C250	NVMe	NAS/SAN	48 24 internal drives	2U	Intel Xeon D-2164-IT (Skylake-D) 2 x 64-bit 12 core, 2.10 GHz

[1] AFF A800 models first shipped with the Intel Xeon Platinum 8160, later models shipped with the Intel Xeon Gold 5220R after the Platinum 8160 was discontinued.

[2] ASA A800 models first shipped with the Intel Xeon Platinum 8160, later models shipped with the Intel Xeon Gold 5220R after the Platinum 8160 was discontinued.

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
ASA A250	NVMe	SAN	48 24 internal drives	2U	Intel Xeon D-2164-IT (Skylake-D) 2 x 64-bit 12 core, 2.10 GHz
ASA C250	NVMe	SAN	48 24 internal drives	2U	Intel Xeon D-2164-IT (Skylake-D) 2 x 64-bit 12 core, 2.10 GHz
FAS500f	NVMe	NAS/SAN	48 24 internal drives	2U	Intel Xeon D-2164-IT (Skylake-D) 2 x 64-bit 12 core, 2.10 GHz

Table 4: Non-TOE Hardware (Cascade Lake)

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
Intel Cascade Lake 2nd Gen Xeon Scalable Processors					
AFF A400	NVMe/SSD	NAS/SAN	96/480	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core, 2.20 GHz

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
AFF A800[3]	NVMe/SSD	NAS/SAN	240/240 48 internal drives	4U	Intel Xeon Gold 5220R (Cascade Lake) 4 x 64-bit 24-core, 2.10 GHz
AFF C400	NVMe	NAS/SAN	96	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core, 2.20 GHz
AFF C800	NVMe	NAS/SAN	240 48 internal drives	4U	Intel Xeon Gold 5220R (Cascade Lake) 4 x 64-bit 24-core, 2.10 GHz
ASA A400	NVMe/SSD	SAN	96/480	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core, 2.20 GHz
ASA C400	NVMe	SAN	96	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core, 2.20 GHz

[3] AFF A800 models first shipped with the Intel Xeon Platinum 8160, later models shipped with the Intel Xeon Gold 5220R after the Platinum 8160 was discontinued.

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
ASA A800[4]	NVMe/SSD	SAN	240/240 48 internal drives	4U	Intel Xeon Gold 5220R (Cascade Lake) 4 x 64-bit 24-core, 2.10 GHz
ASA C800	NVMe	SAN	240 48 internal drives	4U	Intel Xeon Gold 5220R (Cascade Lake) 4 x 64-bit 24-core, 2.10 GHz
FAS8300	HDD/SSD	NAS/SAN	720/480	4U	Intel Xeon Silver 4210 (Cascade Lake) 4 x 64-bit 10-core, 2.20 GHz
FAS8700	HDD/SSD	NAS/SAN	1440/480	4U	Intel Xeon Gold 5218 (Cascade Lake) 4 x 64-bit 16-core, 2.30 GHz

Table 5: Non-TOE Hardware (Ice Lake)

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
Intel Ice Lake 3rd Gen Xeon Scalable Processors					

[4] ASA A800 models first shipped with the Intel Xeon Platinum 8160, later models shipped with the Intel Xeon Gold 5220R after the Platinum 8160 was discontinued.

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
AFF A900	NVMe/SSD	NAS/SAN	240/480	8U	Intel Xeon Platinum 8352Y (Ice Lake) 4 x 64-bit 32-core 2.20 GHz
ASA A900	NVMe/SSD	SAN	240/480	8U	Intel Xeon Platinum 8352Y (Ice Lake) 4 x 64-bit 32-core 2.20 GHz
FAS9500	HDD/SSD	NAS/SAN	1440/480	8U	Intel Xeon Platinum 8352Y (Ice Lake) 4 x 64-bit 32-core, 2.20 GHz
Intel Ice Lake Xeon D Processor					
FAS2820	HDD/SSD	NAS/SAN	144/138 12 internal drives	2U	Intel Xeon D-1735TR (Ice Lake-D) 2 x 64-bit 8-core 2.20 GHz

Table 6: Non-TOE Hardware (Sapphire Rapids)

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
Intel Sapphire Rapids 4th Gen Xeon Scalable Processors					
AFF A1K	NVMe/SSD	NAS/SAN	240/480	4U	Intel Xeon Platinum 8470N 2 x 64-bit 52-core 1.7 GHz

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
AFF A30	NVMe/SSD	NAS/SAN	72/120 24 internal drives	2U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
AFF C30	NVMe	NAS/SAN	72 24 internal drives	2U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
AFF A50	NVMe/SSD	NAS/SAN	120/120 24 internal drives	2U	Intel Xeon Gold 5411N 2 x 64-bit 24-core 1.9 GHz
AFF C60	NVMe	NAS/SAN	120 24 internal drives	2U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
AFF A70	NVMe/SSD	NAS/SAN	240/240 48 internal drives	4U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
AFF C80	NVMe	NAS/SAN	240 48 internal drives	4U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
AFF A90	NVMe/SSD	NAS/SAN	240/240 48 internal drives	4U	Intel Xeon Gold 6438N 2 x 64-bit 32-core 2.0 GHz

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
ASA A1K	NVMe	SAN	240	4U	Intel Xeon Platinum 8470N 2 x 64-bit 52-core 1.7 GHz
ASA A30	NVMe	SAN	72 24 internal drives	2U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
ASA C30	NVMe	SAN	72 24 internal drives	2U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
ASA A50	NVMe	SAN	120 24 internal drives	2U	Intel Xeon Gold 5411N 2 x 64-bit 24-core 1.9 GHz
ASA A70	NVMe	SAN	240 48 internal drives	4U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
ASA A90	NVMe	SAN	240 48 internal drives	4U	Intel Xeon Gold 6438N 2 x 64-bit 32-core 2.0 GHz
FAS50	HDD/SSD	NAS/SAN	480/120	2U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz

Values identified, including the CPU count, are for a single HA pair specification. All disk drives are third party devices.					
Storage Controller	**Disk Type**	**Storage Protocols**	**Max Drives**	**Controller Form Factor**	**Storage Controller Processor**
FAS70	HDD/SSD	NAS/SAN	1440/240	4U	Intel Xeon Gold 5416S 2 x 64-bit 16-core 2.0 GHz
FAS90	HDD/SSD	NAS/SAN	1440/480	4U	Intel Xeon Gold 6438N 2 x 64-bit 32-core 2.0 GHz
Intel Sapphire Rapids 5th Gen Xeon Scalable Processors					
AFF A20	NVMe/SSD	NAS/SAN	48/120 24 internal drives	2U	Intel Xeon Bronze 3508U 2 x 64-bit 8-core 2.0 GHz
ASA A20	NVMe	SAN	48 24 internal drives	2U	Intel Xeon Bronze 3508U 2 x 64-bit 8-core 2.0 GHz

3.3. 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 the ST. The features below are out of scope.

Feature	Description
Networking protocols	Security functional requirements associated with networking protocols (NFS, SMB, etc.) are not evaluated and/or validated in the evaluated configuration.

Feature	Description
High Availability	Security functional requirements associated with High Availability features provided by the TOE are not evaluated and/or validated in the evaluated configuration.
KMIP	KMIP client configurations provided by the TOE are not evaluated and/or validated in the evaluated configuration.
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). SnapLock was not included in the evaluation and was not tested in the evaluated configuration.
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.
System Manager GUI	The System Manager GUI is considered out of scope and all management is performed via the command line interface. Note: CLI management access excludes SSH access and is limited to serial console access only.
VMware Virtualization	VMware Virtualization was not included in the evaluation and was not tested in the evaluated configuration.
Cloud environments	ONTAP instances running within a cloud environment were not included in the evaluation and were not tested in the evaluated configuration.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. 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 initiating TOE software updates using a command line interface.

4.2. Protection of the TSF

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).

4.3. Cryptographic Support

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

5. Assumptions and Clarification of Scope

5.1. Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019

That information has not been reproduced here and CPP_FDE_AA_V2.0E should be consulted if there is interest in that material.

5.2. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_AA_V2.0E as described for this TOE in the ST. Other functionality provided by the devices was not assessed as part of this evaluation. All other functionality needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the assurance activities specified in the CPP_FDE_EE_V2.0E and performed by the Evaluation team.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_FDE_AA_V2.0E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, functionality defined in Section 3.3 is not covered by this evaluation.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *NetApp Storage Encryption: Common Criteria Configuration Guide*, Version 1.6, February 25, 2026
- *Set up, upgrade and revert ONTAP- ONTAP 9*, March 21, 2025
- *ONTAP 9.16.1 commands*, January 31, 2025

These documents are the only documentation that should be trusted to set-up, administer, or use the product in the evaluated configuration. Additional documentation was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

7. IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in the *NetApp Storage Encryption (NSE) running ONTAP 9.16.1 FDE Authorization Acquisition Test Plan*, Version 1.2, February 2026, which is not publicly available. The *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Assurance Activity Report*, Version 1.4, February 2026, provides an overview of testing and the prescribed evaluation activities.

7.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

7.2. Evaluation Team Independent Testing

Testing was performed by Nil Folquer from June 2025 through November 2025.

Testing of the models AFF A250 and FAS2820 was performed remotely in the Lightship Baltimore facility that has been accredited by NVLAP. Remote testing was approved by NIAP according to NIAP Policy #31. The remote equipment (TOEs and TOE setup) was in NetApp's isolated lab in a dedicated rack connected to an isolated subnet only accessible to the evaluator and 3 authorized NetApp personnel.

The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the Evaluation team verified that each test passed.

7.3. TOE Test Environment Configuration

The TOE testing environment components are identified in Figure 1 and Table 7 below.

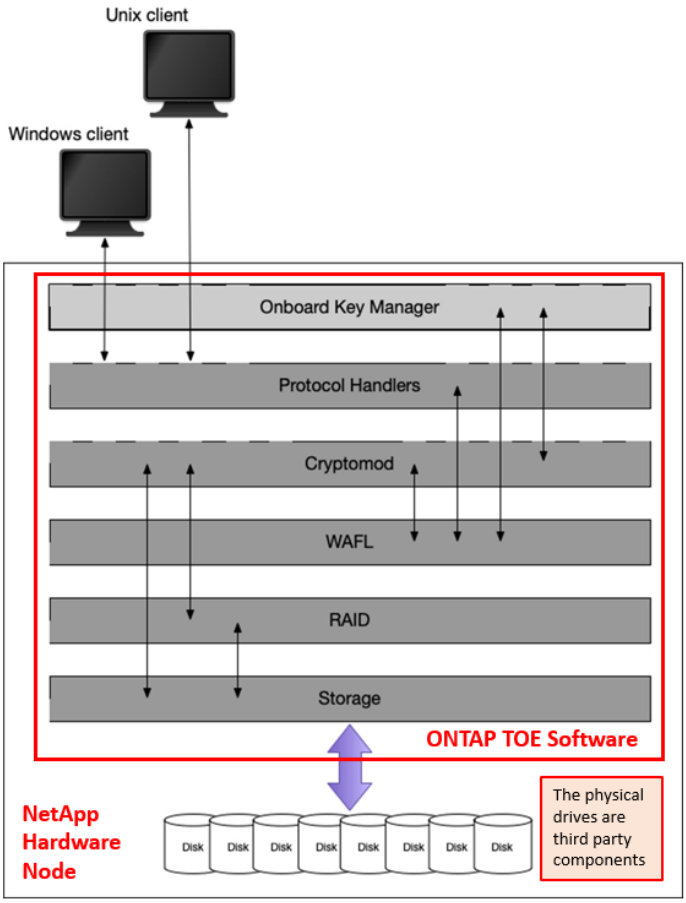

Figure 1: Testing Environment Overview

Table 7: Tools Used for Testing

Tool Name	Version	Description
NetApp ONTAP 9.16.1 (debug version)	9.16.1 <1d>	Instrumented TOE build to allow the evaluator to capture key values and dump the core of the TOE to verify key destruction. This tool was used for FCS_CKM.4(d) testing only.
bm-search	1.0	Proprietary tool used to search for patterns in memory dumps such as keys and random bytes.

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_FDE_AA_V2.0E and its supporting document.

8.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CPP_FDE_AA_V2.0E related to the examination of the information contained in the TOE Summary Specification (TSS).

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the CPP_FDE_AA_V2.0E and recorded the results in the DTR, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6. Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *NetApp NSE ONTAP v9.16 Vulnerability Assessment*, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities, last conducted on February 23, 2026, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database: https://web.nvd.nist.gov/view/vuln/search
- MITRE CVE List: https://cve.mitre.org/cve/search_cve_list.html
- CVE Details: https://www.cvedetails.com/vulnerability-search.php
- CISA - Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- NetApp Security Advisories: https://security.netapp.com/advisory

The Evaluation team performed a search using the following keywords:

NetApp ONTAP 9	NetApp Storage Encryption			
AFF A150	AFF A1K	AFF A20	AFF A50	AFF A30
AFF A70	AFF C250	AFF A90	AFF C60	AFF C400
AFF C800	AFF C30	AFF C80	ASA A20	ASA A90
ASA A400	ASA A70	ASA A900	ASA A800	ASA A30
ASA C30	ASA A250	ASA A50	ASA A150	ASA A1K
ASA C400	ASA C250	ASA AFF A220	ASA C800	FAS50
FAS70	FAS90	AFF A800	AFF A220	AFF C190
AFF A250	AFF A300	AFF A400	AFF A900	AFF A320
FAS2720	FAS2820	FAS9500	FAS2750	FAS8700
FAS8200	FAS500f	FAS8300		
Intel Xeon D-2164IT		Intel Xeon Bronze 3508U		Intel Xeon D-1557
Intel Xeon Silver 4114	Intel Xeon Platinum 8160		Intel Xeon Silver 4210	
Intel Xeon Gold 5218	Intel Xeon Gold 5220R		Intel Xeon D-1735TR	
Intel Xeon Gold 5416S	Intel Xeon Platinum 8352Y		Intel Xeon Gold 5411N	
Intel Xeon Gold 6438N	Intel Xeon Platinum 8470N		Intel Xeon D-1587	
NetApp CryptoMod	NetApp Cryptographic Security Module			
Intel Intelligent Storage Acceleration Library		OpenSSL 3.0.8		
Drive Encryption	Disk Encryption	Key destruction		
Key sanitization	Opal management software			
SED management software	Password caching	Key caching		

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7. Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Assurance Activities in CPP_FDE_AA_V2.0E and its supporting document and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the configuration instructions in the Guidance documents defined in Section 6. No other versions of the TOE software, either earlier or later, were evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST and only that functionality was evaluated. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The Validation team strongly recommends that all TOE hardware in the operational environment is kept up to date with patches as they are released. In addition, Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

10. Annexes

Not applicable.

11. Security Target

NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Security Target, Version 1.8, February 25, 2026

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance:** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature:** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition,* Version 2.0 + Errata 20190201, February 2019
6. *Supporting Document - Mandatory Technical Document Full Drive Encryption: Authorization Acquisition,* Version 2.0 + Errata 20190201, February 2019
7. *NetApp Storage Encryption: Common Criteria Configuration Guide,* Version 1.6, February 25, 2025
8. *Set up, upgrade and revert ONTAP- ONTAP 9,* March 21, 2025
9. *ONTAP 9.16.1 commands,* January 31, 2025
10. *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Security Target,* Version 1.8, February 25, 2026
11. *NetApp ONTAP 9.16.1 with NetApp Storage Encryption and Onboard Key Manager Common Criteria Full Drive Encryption – Authorization Acquisition Key Management Description*, Version 1.1, June 2, 2025
12. *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Assurance Activity Report*, Version 1.4, February 2026
13. *NetApp NSE ONTAP 9.16 Vulnerability Assessment,* Version 1.4, February 2026
14. *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 Evaluation Technical Report,* Version 1.4, February 2026
15. *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 cPP FDE AA 2.0E Test Plan,* Version 1.2, February 2026
16. *NetApp Storage Encryption (NSE) Running ONTAP 9.16.1 cPP FDE AA 2.0E Test Evidence,* Version 1.1, February 2026