NetApp Volume Encryption: Common Criteria Configuration Guide

Version 1.6

November 7, 2024

NetApp, Inc.

3060 Olsen Drive

San Jose, CA 95128

Contents

List of Tables

1 About the Guide

1.1 Overview

This guide provides supplemental instructions and relation information to configure ONTAP 9.14.1 in the Common Criteria evaluated configuration when using NetApp Volume Encryption (NVE).

1.2 Audience

This guide is intended for ONTAP storage administrators, and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers of this guide will use this guide in conjunction with the related documents listed in Table 4.

1.3 About the Common Criteria Evaluation

The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15048) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org.

1.3.1 Protection Profile Conformance

The Common Criteria evaluation was performed against the requirements of:

- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, V2.0 + Errata 20190201*, or, as referred to in other places in this document, *cPP FDE-AA*,
- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine, V2.0 + Errata 20190201*, or, as referred to in other places in this document, *cPP FDE-EE*,
- NIAP Technical Decisions per Table 2 in [NVE-ST].

The collaborative Protection Profile documents listed above are available at https://www.niap-ccevs.org/Profile/PP.cfm.

1.3.2 Evaluated Software

The Target of Evaluation (TOE) is NetApp Volume Encryption (NVE) Appliances running ONTAP 9.14.1. Supported controllers are listed in Table 1Table 5.

Users may verify that they have the correct version of the TOE, after login, by running the `system version` CLI command.

1.3.3 TOE Components

The NetApp controllers included in the evaluated configuration are as follows:

Table 1: NetApp Controllers Covered by the Evaluation

NetApp Controllers	Disk Type	Controller Form Factor
AFF A150	SSD	2U/24 internal drives
AFF A220	SSD	2U/24 internal drives
AFF A250	NVMe/SSD	2U/24 internal drives
AFF A300	SSD	3U
AFF A320	NVMe	2U
AFF A400	NVMe/SSD	4U
AFF A800	NVMe/SSD	4U/48 internal drives
AFF A900	NVMe/SSD	8U
AFF C190	SSD	2U/24 internal drives
AFF C250	NVMe	2U/24 internal drives
AFF C400	NVME	4U
AFF C800	NVMe	4U
ASA A150	SSD	2U/24 internal drives
ASA A250	NVMe	2U/24 internal drives
ASA A400	NVMe/SSD	4U
ASA A800	NVMe/SSD	4U/48 internal drives
ASA A900	NVMe/SSD	8U
ASA C250	NVMe	2U/24 internal drives
ASA C400	NVMe	4U
ASA C800	NVMe	4U
ASA AFF A220	SSD	2U/24 internal drives
FAS2720	HDD/SSD	2U/12 internal drives
FAS2750	HDD/SSD	2U/24 internal drives
FAS2820	HDD/SSD	2U/12 internal drives
FAS500f	NVMe	2U/24 internal drives
FAS8200	HDD/SSD	3U
FAS8300	HDD/SSD	4U
FAS8700	HDD/SSD	4U
FAS9500	HDD/SSD	8U

1.3.4 Evaluated Functions

The following functions have been evaluated under Common Criteria:

a) **Data Protection.** The TOE performs volume encryption to protect user data from unauthorized disclosure.

b) **Secure Key Material.** The TOE ensures key material used for volume encryption is properly generated and protected from disclosure. The TOE implements cryptographic key and key material destructions during transitioning to a complaint power saving state, or when all keys and key material are no longer needed.

c) **Secure Management.** The TOE enables management of its security functions.

d) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through digital signatures using RSA-3072 with SHA2-384.

e) **Cryptographic Operations.** The cryptographic algorithms used in the above functions have been validated for correct implementation and are described in section 7.1 of [NVE-ST].

Note: No claims are made regarding any other security functionality.

1.3.5 Evaluation Assumptions

The following assumptions are defined by the *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, V2.0 + Errata 20190201*. The guidance shown in Table 2 should be followed to uphold these assumptions in the operational environment.

Table 2: Evaluation Assumptions for cPP FDE-AA

Assumption	Guidance
A. INTIAL_DRIVE_STATE: The Operational Environment (OE) provides a newly provision or initialize storage device free of protected data in areas not targeted for encryption.	No action is required, ONTAP automatically initializes spare drives prior to use.
A. SECURE_STATE: Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.	Provisioning of the TOE should be completed per all guidance documents and instructions to ensure nominal operation.
A. TRUSTED_CHANNEL: Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure.	The TOE is both the Authorization Acquisition (AA) component and the Encryption Engine (EE) component. No action is required.
A. TRAINED_USER: Authorized users follow all provided user guidance, including keeping passwords/passphrases and external tokens securely stored separately from the storage device and/or platform.	ONTAP cluster storage administrators should be aware of any organizational password policies.
A. 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.	While ONTAP 9.14.1 does provide anti-ransomware protection, storage administrators should use anti-malware software, when possible, to protect their NAS/SAN contents.
A. SINGLE_USE_ET: External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.	Not applicable, the TOE does not use an external token.

Assumption	Guidance
A. POWER_DOWN: The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a "hibernation mode".	No action required.
A. PASSWORD_STRENGTH: Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.	Storage administrators should follow their organizational password policies.
A. PLATFORM_I&A: The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface.	No action required. Normal ONTAP 9.14.1 authentication requirements/methods are not impacted.
A. STRONG_CRYPTO: All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.	No action required. ONTAP 9.14.1 automatically uses FIPS validated cryptography when meeting the requirements listed in the cPPs.
A. PHYSICAL: The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.	The NetApp storage controller and any attached shelves should be physically protected (during operation) in accordance with organizational policies.

The following assumptions are defined by the *collaborative Protection Profile for Full Drive Encryption – Encryption Engine, V2.0 + Errata 20190201*. The guidance shown in Table 3 should be followed to uphold these assumptions in the operational environment.

Table 3: Evaluation Assumptions for cPP FDE-EE

Assumption	Guidance
A. INTIAL_DRIVE_STATE: The Operational Environment (OE) provides a newly provision or initialize storage device free of protected data in areas not targeted for encryption.	No action is required, ONTAP automatically initializes spare drives prior to use.

Assumption	Guidance
A. TRUSTED_CHANNEL: Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure.	The TOE is both the Authorization Acquisition (AA) component and the Encryption Engine (EE) component. No action is required.
A. TRAINED_USER: Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained how to power off the system.	ONTAP cluster storage administrators should be aware of any organizational password policies and be trained in how to use NetApp Volume Encryption.
A. 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.	While ONTAP 9.14.1 does provide anti-ransomware protection, storage administrators should use anti-malware software, when possible, to protect their NAS/SAN contents.
A. POWER_DOWN: The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.	No action required.
A. STRONG_CRYPTO: All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.	No action required. ONTAP 9.14.1 automatically uses FIPS validated cryptography when meeting the requirements listed in the cPPs.
A. PHYSICAL: The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform’s correct operation.	The NetApp storage controller and any attached shelves should be physically protected (during operation) in accordance with organizational policies.

1.4 Related Documents

This guide supplements the following documents (described below).

Table 4: Related Documents

Reference	Documents
[NVE-ST]	NetApp Volume Encryption (NVE) Appliances running ONTAP 9.14.1 Security Target, Version 1.6.
[ONTAP CR]	NetApp ONTAP 9.14.1 commands, June 26, 2024
[SUUR]	NetApp Set up, upgrade and revert ONTAP – ONTAP 9, July 02, 2024

1.5 Terminology

Table 5 defines terms and acronyms used within this document that may not be commonly known.

Table 5: Acronyms

Acronym	Definition
AA	Authorization Acquisition
AFF	All Flash FAS
AK	Authentication Key
ASA	All SAN Array
BEV	Border Encryption Value
CC	Common Criteria
CLI	Command Line Interface
cPP	Collaborative Protection Profile
DEK	Data Encryption Key
EE	Encryption Engine
FAS	Fabric Attached Storage
HDD	Hard Disk Drive
NAS	Network Attached Storage
NSE	NetApp Storage Encryption
NVMe	Non-Volatile Memory Express
OKM	Onboard Key Manager
RBG	Random Bit Generator
SAN	Storage Attached Network
SSD	Solid State Drive
TOE	Target of Evaluation

2 Guidance

2.1 Configuration

Note: while in Common Criteria (CC) mode, all administration needs to be performed via the CLI accessed using a console directly connected to the appliance's RS-232 port.

To configure ONTAP 9.14.1 for use with NetApp Volume Encryption (NVE), the Onboard Key Manager (OKM) must be enabled for the admin Vserver in Common Criteria (CC) mode. The following command will enable OKM in CC mode:

```
security key-manager onboard enable -cc-mode-enabled yes
```

When CC mode is enabled, the cluster administrator will be required to provide a cluster passphrase that is between 64 and 256 ASCII characters long. This passphrase must be entered at the console each time that a node in the cluster boots.

Notes:

1. The security key-manager onboard enable command is available to cluster administrators at the admin privilege level
2. Volume encryption is enabled by default for all evaluated/tested configurations while in Common Criteria mode.
3. If unencrypted metadata volumes are required for non-evaluated/non-tested configurations (examples include metadata volumes for SnapMirror and Vserver migrate operations), then set the optional `-are-unencrypted-metadata-volumes-allowed-in-cc-mode {yes|no}` parameter to `yes` when enabling OKM.

2.2 Authorization Factors

ONTAP 9.14.1 with NetApp Volume Encryption (NVE) requires that a cluster admin setup OKM in CC mode (see above) with a cluster passphrase consisting of between 64 and 256 ASCII characters. Each time a node in the cluster boots, the boot process will stop until the passphrase is entered at the node's console. If the wrong passphrase is entered at boot, then user volumes will not be mounted and the TOE must be rebooted.

2.3 Cryptographic Key Destruction

ONTAP 9.14.1 handles the destruction of cryptographic keys and key material when they are no longer required.

Key destruction also occurs when the TOE transitions to a Compliant power saving state (see the next section).

2.4 Compliant Power Saving States

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

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

When the TOE is fully rebooted from either Compliant power saving state, non-persistent/unencrypted BEV and DEK key material contained within volatile memory is cleared within 30 seconds of the system halting.

An administrator can reboot the TOE via the `system reboot` CLI command. See the CLI command `system reboot` in [ONTAP CR].

2.5 Management Functions

ONTAP 9.14.1 provides the following management functions as relevant to both *cPP FDE-AA* and *cPP FDE-EE*:

a) **Request change of a volume's DEK:** See Section 2.5.1.
b) **Request cryptographic erasure of the volume's DEK:** See Section 2.5.2
c) **Request change of authorization factors:** See Section 2.5.3.
d) **Initiate TOE firmware/software updates:** See Section 2.5.4.

2.5.1 Request Change of a Volume's DEK

While in CC mode, ONTAP volumes are automatically encrypted using AES-XTS-256 DEKs. Volumes can be either be rekeyed "in-place" or "migrated" to use a new AES-XTS-256 DEK.

In-place rekeying is performed with the `volume encryption rekey` set of commands. See the CLI command `volume encryption rekey` in [ONTAP CR].

Volume migration is performed with the `volume move` set of commands. See the CLI command `volume move` in [ONTAP CR].

2.5.2 Request Cryptographic Erase of a Volume's DEK

The `volume delete` command is used in ONTAP to delete a volume. When an encrypted volume is deleted, the DEK associated with the volume is deleted after the volume is deleted. Normally, an ONTAP volume isn't deleted immediately but is deleted after a system-wide configurable "recovery time" (default: 24 hours) elapses. The `volume delete` command will take an optional parameter `-force` to force immediate deletion. When the `volume delete` command is used with the `-force true` parameter, then the volume is not moved to ONTAP's recovery-queue; therefore, the DEK keys associated with the volume are deleted immediately. If the `-force true` command is not used, then the keys associated with the volume are deleted only when the volume is automatically deleted from the recovery-

query or when the volume is purged from the recovery-queue. ONTAP's default behavior is to delete volumes from the recovery-queue after they have been in the queue for 24-hours.

2.5.3 Request Change of Authorization Factors

The cluster passphrase associated with the Onboard Key Manager (OKM) may be modified by the cluster admin. The command to modify the cluster passphrase is `security key-manager onboard update-passphrase`. For additional details see the CLI command (`security key-manager onboard update-passphrase`) in [ONTAP CR].

2.5.4 Initiate ONTAP Software Updates

ONTAP cluster admins are allowed to update the TOE via the `cluster image update` CLI command. ONTAP CC updates are cryptographically signed using a 3072-bit RSA digital signature on SHA-384 hashes. If the signature validation fails, then the update is stopped and, an error message is displayed ("Failed to verify the signatures of the image. The image might have been corrupted. Replace the image, and then try the command again.").

For specific instructions on how to update the TOE, refer to [SUUR].

2.6 Cryptography

ONTAP 9.14.1 with NetApp Volume Encryption (NVE) supports 256-bit volume DEKs (AES-XTS-256) and 256-bit BEVs (AES-KWP).

Hash size functionality is fixed for each of the individual hash sizes and uses described in section 7.1.11 of [NVE-ST]. As such, no configuration guidance is necessary.

Volume encryption is enabled by default, no other configuration of cryptographic parameters is possible/required.

2.6.1 Validation

ONTAP 9.14.1 requires a successful validation of the BEV during the boot process or when recovering from a failure in the boot media. If the cluster passphrase is entered incorrectly during either of these processes, then the system will not be able to mount any of its data volumes. Consequently, ONTAP will not be able to service any user data. This condition can only be cleared by rebooting the node and entering the correct cluster passphrase.

When modifying the cluster passphrase, an administrator 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.

Limits for the number of validation attempts are not user configurable.