Technical Report

SANtricity drive security

Feature details using SANtricity OS

Eric Stanton, NetApp
November 2024 | TR-4474

Abstract

NetApp offers data-at-rest encryption for NetApp® E-Series through the full disk encryption feature. This technical report provides detailed information about the NetApp SANtricity® full disk encryption feature for E-Series systems, including support for FIPS 140-3 validated drives, and both internal and external key management support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Solution overview

A company's data is likely its most valuable asset. With data security attacks on the rise, protecting an organization's data against loss or theft is increasingly important. SANtricity full disk encryption technology provides comprehensive security for data at rest without sacrificing system performance or ease of use and supports both internal and external key management. The drive security capabilities described here are available on NetApp EF600, EF300, EF570, and EF280 all-flash arrays, as well as E2800, E4000, and E5700 hybrid arrays.

SANtricity full disk encryption use cases

SANtricity full disk encryption primarily protects your data if a physical security breach occurs. The goal is to prevent unauthorized access to the data by someone in possession of the physical drives who uses standalone tools to attempt to read the media or moves the drives to a different unauthorized storage array. SANtricity OS 11.40 and later addresses the threat for a storage array in transit by adding another level of protection to prevent unauthorized access to data by someone in possession of the entire storage array. This is achieved by adding support for a centralized key management implementation by using a third-party external key management solution. However, if the data center itself is compromised, the data is not protected from unauthorized access.

SANtricity full disk encryption addresses two main use cases:

- Prevents unauthorized access to data without the proper security credentials either by using the same storage array where the entire system is compromised, by using a different storage array where the secure drive is compromised, or through stand-alone tools.
- Enables you to upgrade controllers or legitimately move a set of drives from one array to another while maintaining data security.

With the information in this report, NetApp sales teams and partners can verify that the E-Series solution meets your security requirements. These requirements might vary according to the market, which includes the following sectors:

- U.S. public sector
- Financial
- Healthcare
- Retail

SANtricity 11.60 introduced the EF600 array, a full end-to-end NVMe storage array and unlike previous products which support only serial-attached SCSI (SAS) drives. SANtricity 11.70 introduces the EF300 array, also an end-to-end NVMe storage array. The EF600 and EF300 arrays support NVMe self-encrypting/FIPS drives. These drives use the TCG Opal standard instead of the TCG Enterprise standard that is used on the SAS self-encrypting/FIPS drives. Although the drives use a different standard, the SANtricity OS support is implemented so that the difference in standards is not visible when it comes to security features.

SANtricity drive security

The E-Series storage systems provide at-rest data encryption through self-encrypting drives. These drives encrypt data on write operations and decrypt data on read operations regardless of whether the full disk encryption feature is enabled. If the SANtricity feature is not enabled, the data is encrypted at rest on the media, but automatically decrypted on a read request.

When the drive security feature is enabled on the storage array, the drives protect the data at rest by locking the drive from read or write operations unless the storage array provides the correct security or authentication key. This process prevents another array from accessing the data without first importing

the appropriate security key file to unlock the drives. It also prevents any third-party tool from accessing the data by reading individual drives.

In addition to the internal key management just described, SANtricity 11.40 and later also provides further enhancements to the drive security feature. These additional enhancements enable you to manage the full disk encryption security key through a centralized external key management system, such as Thales CipherTrust Key Manager or Thales SafeNet KeySecure, that complies with the Key Management Interoperability Protocol (KMIP) standard. Another example that tested successfully is IBM Security Key Lifecycle Manager version 4.1 or higher. The primary requirement is compliance with KMIP 1.0.

The encryption and decryption operations performed by the hardware in the drive are invisible to the user and do not affect the performance or user workflow. Each drive has its own unique encryption key that cannot be transferred, copied, or read from the drive. The encryption key is a 256-bit key as specified in the National Institute of Standards and Technology (NIST) AES. The entire drive, not just a portion, is encrypted.

You can enable security at any time by selecting the Secure Drives option in the Volume Group or Disk Pool menus. You can make this selection at either volume group or pool creation or afterward. If you choose to secure the drives, it does not affect existing data on the drives.

Note: The option cannot be disabled without erasing all the data on the affected volume group or pool.

Figure 1 shows the technical components of the NetApp E-Series full disk encryption feature with an internally managed security key.

Figure 1) E-Series full disk encryption with an internally managed security key.

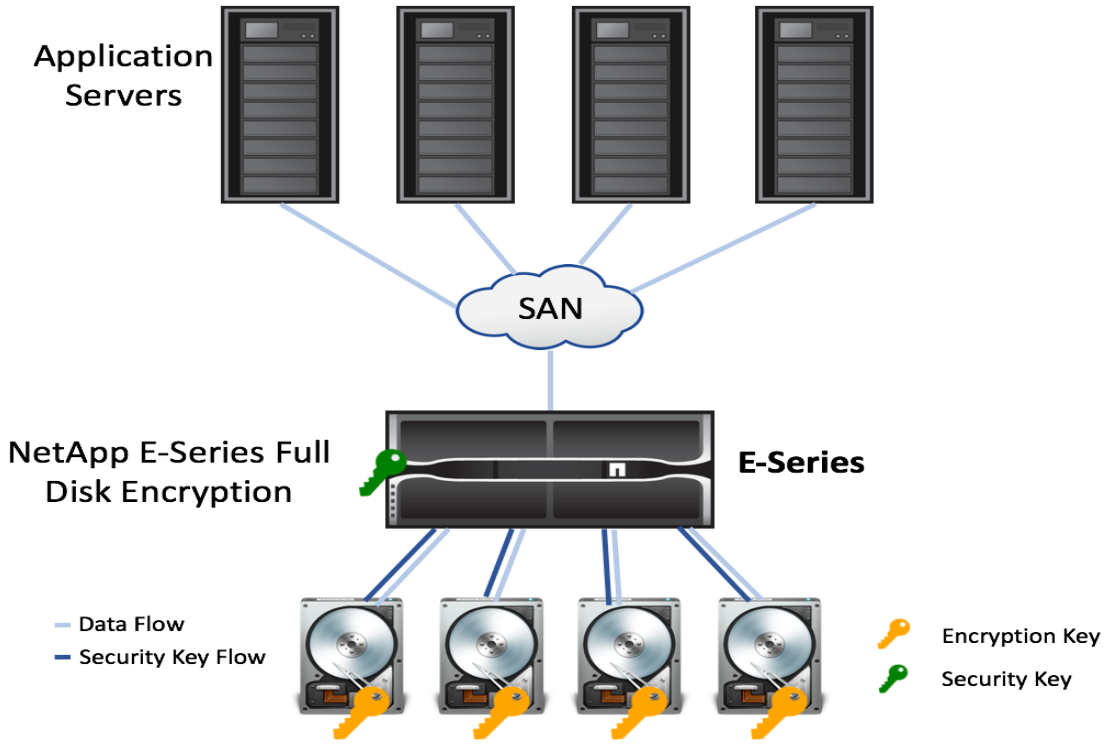
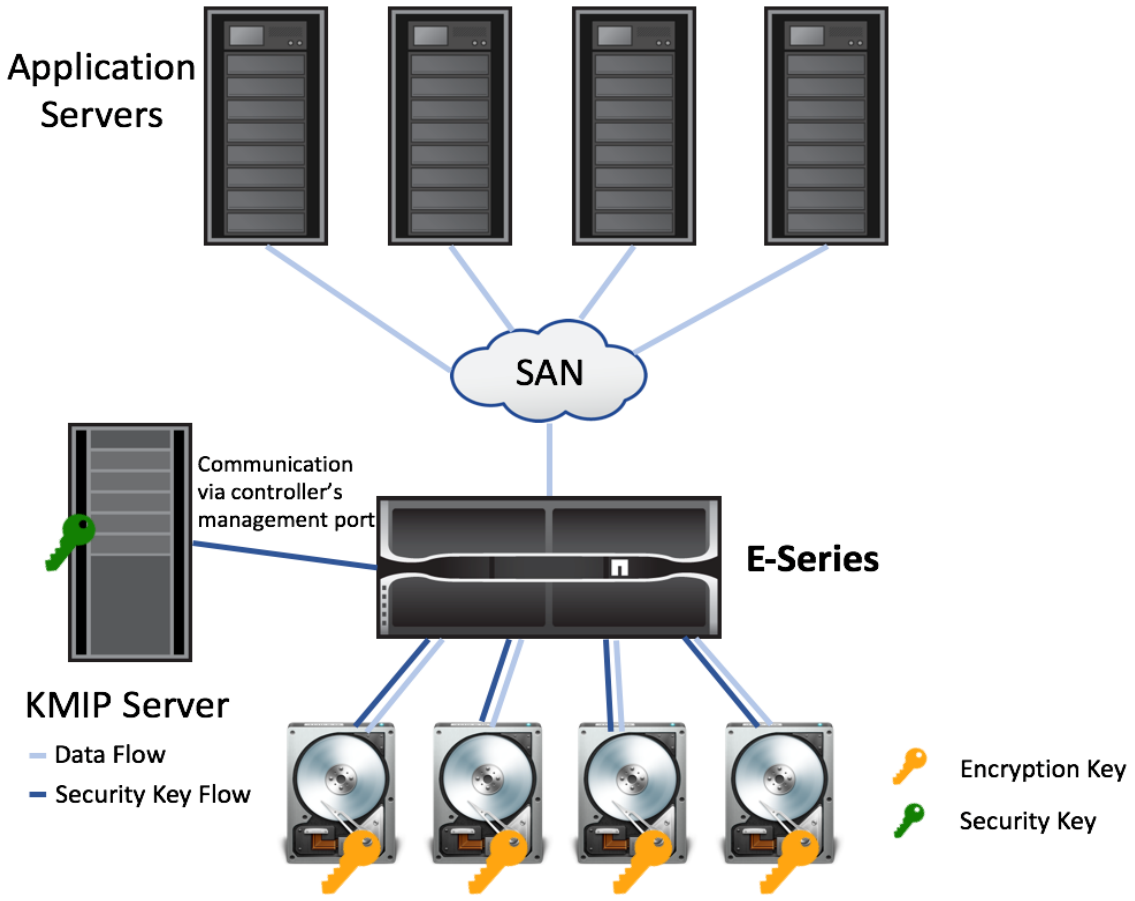


Figure 2 shows the technical components of the NetApp E-Series full disk encryption feature with an externally managed security key.

Figure 2) E-Series full disk encryption with an externally managed security key.



Security key authentication

When the NetApp E-Series full disk encryption feature is enabled, you must create a security key for the storage array. There is only one security key per storage array, and it is used to secure all volume groups or pools that are defined as secure-enabled. This security key is used to unlock the secure-enabled drives for read and write operations.

There is no partial use of full disk encryption security within a volume group or pool. To use the security feature, all drives in the volume group or pool must be secure-capable. All volumes configured from the secure-enabled volume group or pool are secured.

E-Series manages the security key using either internal or external key management. For the internal key management, the security key is maintained on the array. For the external key management, the security key is maintained on the external KMIP server. For either method, you must also back up the security key. The backup key is wrapped using a user-supplied passphrase and encrypted using AES-128. You can specify where the backup file is stored. The backup file contains two copies of the encrypted security key. You can validate the backup security key through the SANtricity Storage Manager software or CLI. This validation process verifies that the backup key can be unwrapped and matches the security key stored on the array or on the KMIP server. During the validation process, you must provide the same user-supplied passphrase used to create the backup security key file.

In addition to the security key, a security key identifier is created and changed any time the security key is changed. The purpose of the security key identifier is to identify the security key for a specific storage

array to the user without the user knowing the actual security key. The identifier is a string containing up to 255 bytes and is either set to a user-defined value (for internal key management) or automatically generated (for external key management) by the controller. Unlike the security key, the security key identifier is designed to be read by humans. The security key identifier is stored on the controller and on all drives associated with that security key and is backed up together with the security key.

When importing drives to another E-Series storage array, the new storage array does not allow read or write operations to the drives until the associated security key is imported. During the import of the security key, the new storage array compares the security key ID of the imported key with the security key ID on the imported drives. If both storage arrays use a centralized external key management system (such as the same KMIP server), there is no need for a manual import of the security key. The new storage array automatically obtains the key from the KMIP server to unlock the imported drives. After the imported drives are unlocked, they are rekeyed to the security key of the new storage array.

The array security key can be changed at any time without affecting the underlying user data. To protect against disruptions during the rekeying operation using internal key management, the old key is not deleted from the array until the new key is generated and applied to all secured drives. When using an external key management system, the keys (old and new) are always managed by the KMIP server and not stored persistently on the storage array.

External KMIP server authentication

SANtricity OS 11.40 and later enhances the existing full disk encryption (FDE) feature by introducing the ability for users to manage the FDE security key through a centralized key management platform like Gemalto SafeNet KeySecure Enterprise Encryption Key Management, which adheres to the Key Management Interface Protocol (KMIP) standard. This feature is in addition to the preexisting SANtricity internal security key management solution and is available with all storage systems running SANtricity OS 11.40 or later.

In the process of enabling the external key management feature, the administrator must install a set of certificates on the array. These certificates are used to establish both a secure connection and authentication between the storage system and the key management server. SANtricity System Manager provides an interface to walk the administrator through the process of generating a Certificate Signing Request (CSR) for the storage system controller and installing both the storage system's signed client certificate and the EKMS server's SSL certificate. This process can also be performed through SMcli.

Note: The following steps are appropriate for the Gemalto Key Management Server. Other sequences may be required for other Key Management Server products.

Steps to Enable External Key Management

There are several configuration steps that must be taken on the external key management server (EKMS) itself. This guide will not go in depth into those steps, but rather make references to artifacts that are obtained from the EKMS.

1. During the process of setting up your EKMS server you may choose what type of authentication to use for client requests. It is recommended to select *SSL session and username* as the most secure type. During this configuration step, you may choose what field in the *client's certificate* to use as the username. This allows a username to be passed in the client certificate to provide authentication.
2. Use SANtricity System Manager to generate a new CSR. In the CSR request dialog, you will want to designate a username in the same field you designated in step 1. See Alternative Workflow for External CSR Generation**Error! Reference source not found.**
3. Alternatively, a CSR can be generated externally using a different workflow. See section Alternative Workflow for External CSR Generation below for details.

4. Take the CSR information to the EKMS server and go through the certificate signing process. You will generate a new client certificate, which should be downloaded to your local system.
5. Use SANtricity System Manager to configure a connection to your EKMS server. This step requires you to provide the EKMS server's IP or host address, the port number and to import the storage array client certificate. The EKMS server certificate must also be imported so the storage array can trust the EKMS server. Note that the EKMS server's intermediate or root certificate may also be imported.
6. The next step is to optionally retrieve a backup key and finish the connection configuration. If the Create backup key checkbox is unchecked, then a backup key will **not** be downloaded.
7. Click the Finish button to complete the Create External Security Key workflow.

Figure 3 shows the open certificates tile in SANtricity System Manager, where the external key management server certificates are managed.

Figure 3) Option in SANtricity System Manager to complete a CSR, and to import the storage system's signed client certificate and EKMS server's SSL certificate.

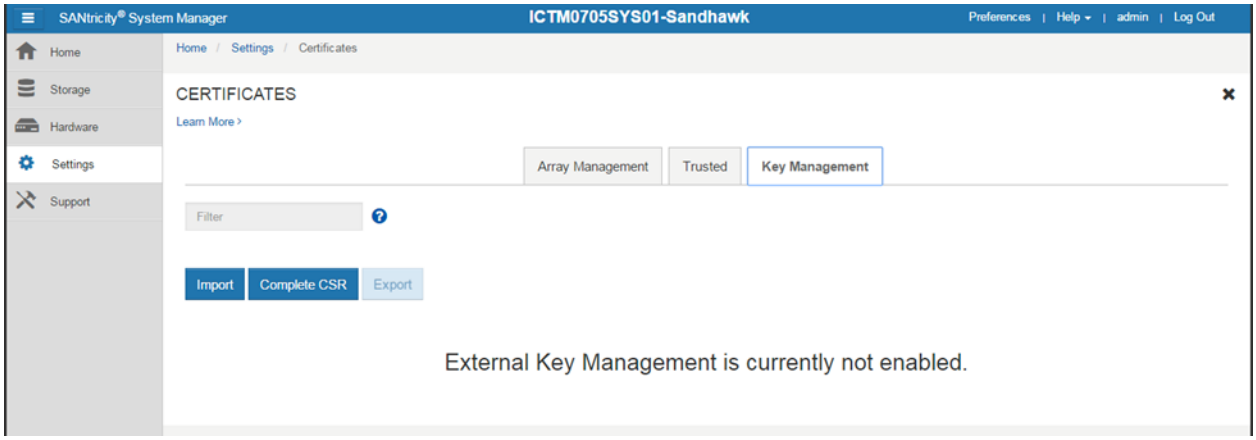


Figure 4 displays the certificate signing request dialog.

Figure 4) Certificate Signing Request Dialog

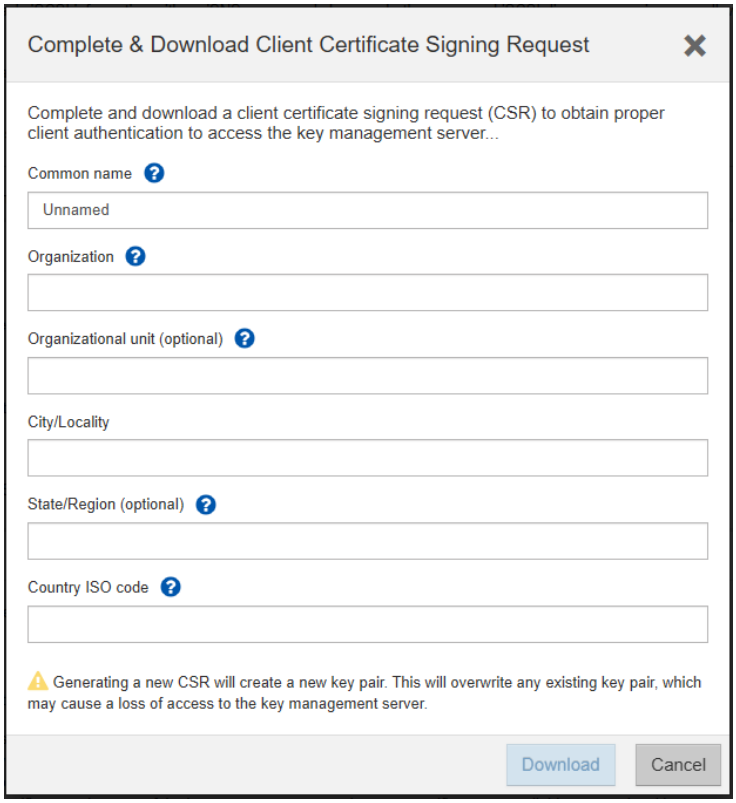


Figure 5 and Figure 6 show the two steps needed to create an external security key.

Figure 5) Connecting to a key management server

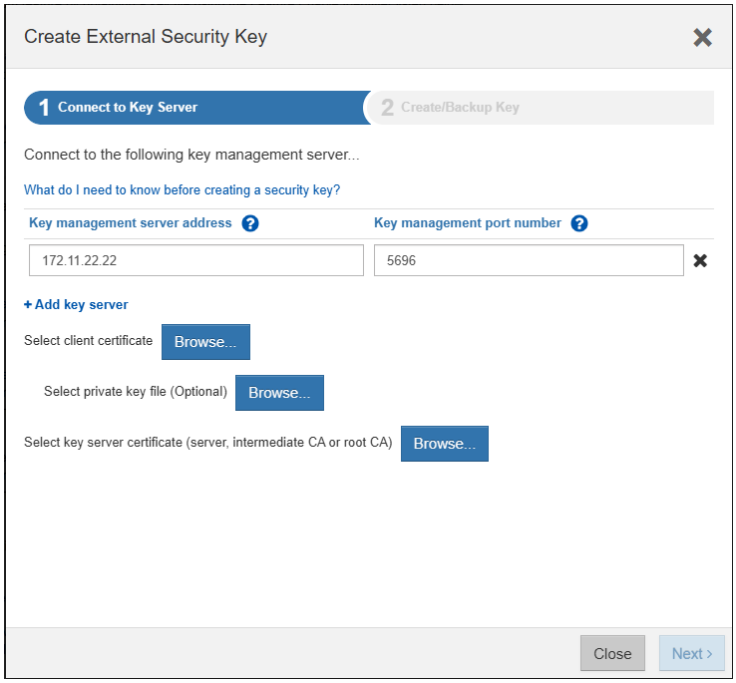
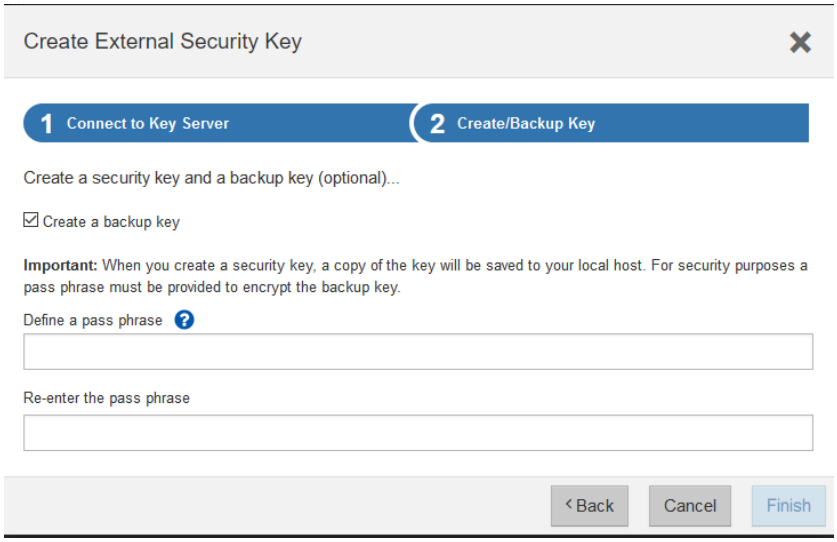


Figure 6) Creating an optional backup key



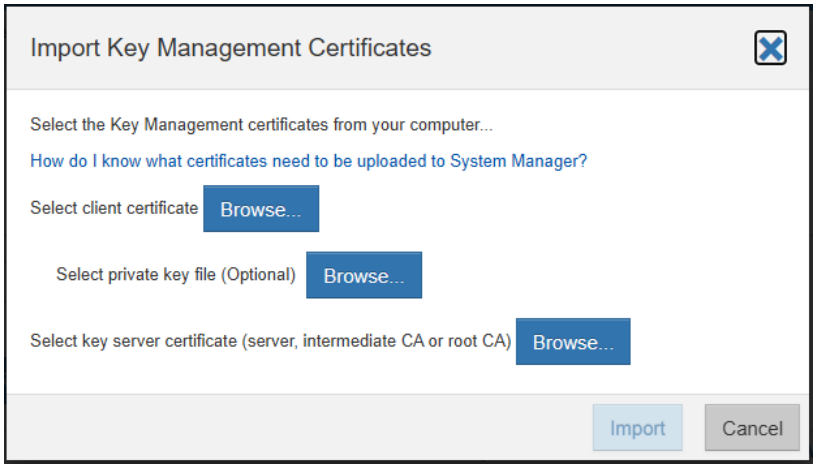
Alternative Workflow for External CSR Generation

For release 11.90 and forward, it is possible to import the signed certificate along with its associated private key, Figure 7. This provides a means to use OpenSSL or other certificate generation tool sets to generate a public / private key pair and CSR without needing to use the CSR generated from the storage array.

CSR generation on the storage array causes a new private key to be created. This can be problematic for situations where a key rotation strategy is desirable. If the private key is re-generated, then there can be a window where array connectivity to the KMS is compromised if a new signed certificate is not re-applied quickly.

Using an external CSR generation workflow, the public / private key pair and new CSR can be generated, then signed, and applied all in one atomic step, thus eliminating the window for connectivity issues.

Figure 7 Import Key Management Certificates with Private Key



FIPS 140-2 Level 2 compliance

With third-party certification becoming a fundamental business requirement for government and commercial customers, the full disk encryption feature offers a higher level of assurance with drives that have been validated against the FIPS 140-2 standard developed by the National Institute of Standards and Technology (NIST). FIPS 140-2 validated drives are level 2 compliant, which provides an added layer of security assurance by using tamper-resistant drives and other approved protocols. The process for creating and authenticating the security key does not change with FIPS 140-2 drives. Secure-capable drives in NetApp's Hardware Universe and other tools are now identified as either FIPS 140-2 Level 2, or full disk encryption (FDE). There is no difference in the cryptographic modules used, but the drives designated as FDE have not been validated by the NIST. To fully support FIPS 140-2 Level 2, an external key management server with FIPS 140-2 validated cryptographic modules is required. This enables E-Series storage arrays (such as the E2800/EF280, E5700/EF570, EF300, and EF600 array) running SANtricity OS 11.40 or later to provide secure external key management of FIPS 140-2 validated secure drives.

Operating in FIPS 140-2 Level 2 Compliant mode

With SANtricity 11.25 or later, when a FIPS 140-2 validated drive is installed on an E-Series system, an initialization process is performed in accordance with the specific drive model's FIPS 140-2 security policy. After the initialization process, the SANtricity UI identifies the FIPS drives as FIPS compliant. In releases earlier than SANtricity 11.25, which is no longer supported, FIPS drives function as full disk encryption and are not initialized in accordance with the FIPS 140-2 security policy. If the storage array is upgraded to the latest version for the hardware, and the volume group or pool is composed solely of FIPS 140-2 validated drives, the drives are initialized to place them into FIPS 140-2 compliant mode).

Secure drive operations

Standard volume groups (RAID) or pools are a grouped set of drives that must adhere to certain quality-of-service (QoS) rules, such as encryption capability. A nonsecure-capable volume group or disk pool can consist of a mix of secure-capable and nonsecure-capable drives, but a secure-capable volume group or disk pool must consist only of secure-capable drives. After enabling the security on a secure-capable volume group or pool, that group of drives are secure-enabled. Any volumes created on that secure-enabled volume group or disk pool are secured. An E-Series storage system can consist of a mix of secure-enabled, secure-capable, and nonsecure-capable volume groups or pools at the same time.

To move secure-enabled volume groups with the data intact between arrays, complete the following steps:

1. Export the volume group from the source array.
2. Import the volume group into the destination array.
3. For internal key management or if the security key does not reside on the KMIP server for the destination array, apply a copy of the backed-up security key to unlock the imported drives.

If both storage arrays use a centralized external key management system (such as the same KMIP server), there is no need for a manual import of the backup security key. The new storage array automatically obtains the security key from the KMIP server to unlock the imported drives.

Note: E-Series storage systems do not support movement of drives associated to a pool between storage arrays.

The storage array enforces configuration rules regarding the use of secure and FIPS drives, including how they can be used with the various features. For example, drives can be securely erased by reprovisioning them. This function triggers a rekeying of the individual drive's encryption keys, rendering

all previous data unreadable. See the following sections for additional information regarding the rules associated to each topic.

Volume group and disk pool configuration

A volume group or pool can consist of any mixture of nonsecure-capable and secure-capable drives on which both full disk encryption and FIPS 140-2 compliant drives are considered secure-capable. If you want to secure the volume group or disk pool, all the drives in that volume group or disk pool must be secure-capable (either full disk encryption or FIPS 140-2 compliant drives). If you require FIPS 140-2 compliant volume groups or pools, all the constituent drives must be FIPS 140-2 compliant. If global hot spares are used, they must be at least as secure as the volume group. Table 1 provides the configuration rules.

Table 1) Volume group and disk pool configuration rules.

Drive Type	FIPS Secure-Enabled or FIPS Secure-Capable Volume Group or Disk Pool	Full Disk Encryption Secure-Enabled Volume Group or Disk Pool	Full Disk Encryption Secure-Capable Volume Group or Disk Pool	Nonsecure-Capable Volume Group or Disk Pool
FIPS	Yes[1]	Yes[2]	Yes	Yes
Full disk encryption	No	Yes	Yes	Yes
Nonsecure capable	No	No	Yes[3]	Yes

[1] A volume group or disk pool can be FIPS enabled or FIPS capable only if all drives are FIPS-compliant.

[2] If an individual FIPS drive is used in a full disk encryption secure-enabled volume group or disk pool, it is placed into the FIPS-compliant mode, but the volume group or pool is not considered FIPS compliant.

[3] If a volume group or pool consists of a mix of secure-capable and nonsecure-capable drives, security cannot be enabled until the nonsecure-capable drives are replaced with secure-capable drives.

Global hot spare compatibility

Table 2 provides the requirements associated with using global hot spare drives with standard RAID configurations.

Note: If a volume group with all secure-capable drives is created, the spare or replacement drive must also be secure-capable, even when the volume group is not secure-enabled.

Pools do not use hot spare drives, but the rules provided in Table 2 still apply to a replacement for a failed drive.

Table 2) Global hot spare compatibility rules.

Drive type	FIPS secure-enabled or FIPS secure-capable volume group	Full disk encryption secure-enabled volume group	Full disk encryption secure-capable volume group	Nonsecure-capable volume group
FIPS	Yes	Yes[1]	Yes[1]	Yes[1]
Full disk encryption	No	Yes	Yes	Yes[2]
Nonsecure-capable	No	No	Yes[3]	Yes

[1] A FIPS 140-2 compliant drive is only used if there are no other options.

2. If both secure-capable and non-secure-capable drives are available, the non-secure-capable drives are chosen.

3. If both secure-capable and non-secure-capable drives are available, the secure-capable drives are chosen. If a nonsecure-capable drive is used, the volume group may not be secured until it is replaced with a secure-capable drive. This restores the volume group to a homogeneous secure-capable state.

Secure erase and disk sanitization

As mentioned, a secure erase (reprovisioning) of the drives can be performed on both secure and FIPS compliant drives. Starting with SANtricity OS 11.70.1, the sanitization options are also available on drives that are not secure-capable. In SANtricity System Manager, you can find all the erasure options by selecting Hardware and Drives. These options give you the capability to securely reuse, re-purpose, or dispose of drives.

To perform an erase operation, the drives must not be part of a configured volume group or pool. In SANtricity System Manager, you can find the volume groups and pools deletion option by selecting Storage and Pools & Volume Groups.

The erasure of a secure-capable drive triggers a rekeying of the individual drive's encryption key and renders all previous data unreadable. For SAS drives, both secure and FIPS drives are reprovisioned using the same process, with one exception: if the drive security key is not available for the FIPS drive, the physical secure ID (PSID) is required to execute a CLI command to perform the secure erase for the associated FIPS drives. The PSID is a human readable string on the label of the drive, and you must enter it manually through the SANtricity management software or the SANtricity CLI, Figure 8.

The EF600 and EF300 base controller enclosures use NVMe drives. For both secure and FIPS NVMe drives, any reprovisioning of the drive requires the PSID input if the drive security key is not available. You can complete this operation through either the CLI command or the SANtricity System Manager GUI.

After a drive has been erased, it must be initialized before you can use it again in the array. To accomplish this, in SANtricity System Manager, select Initialize from the drive's context menu, Figure 9.

Figure 8) Reset Locked Drive dialog box on the SANtricity System Manager GUI.

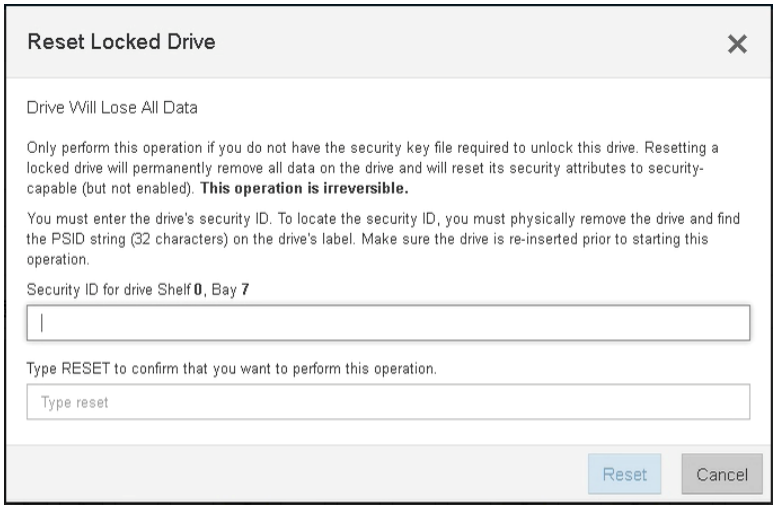
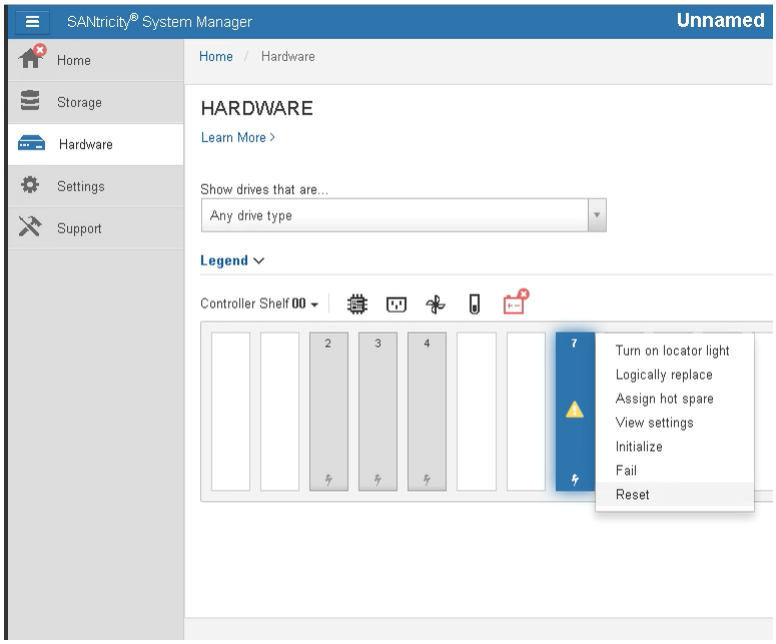


Figure 9) Drive reset/provisioning procedure on the SANtricity System Manager GUI.



Feature interaction

The following sections describe the rules associated with drive security as it relates to the listed features.

Volume copy

There are no restrictions on the volume copy feature. You can select any combination of security capabilities for the source and target of the copy operation. However, SANtricity Storage Manager generates a warning if you copy from a higher security volume to a lower security volume.

Snapshot images

The reserved NetApp Snapshot™ copy repository must be as secure as the volume from which the Snapshot copy is being created.

Synchronous mirroring

There are no restrictions on the synchronous mirroring feature. You can select any combination of security capabilities for the primary and secondary volumes. NetApp recommends that you select matching security capabilities as a best practice.

Note: Synchronous mirroring is not supported on the EF600 or EF300 array.

Asynchronous mirroring

The mirror repository must be as secure as the volume being mirrored. The QoS limitations on the primary and secondary volumes are outlined in Table 3.

Table 3) Asynchronous mirroring configuration rules.

Primary mirror security state	Secondary mirror security state
Nonsecure-capable	Non-secure-capable[1]

Primary mirror security state	Secondary mirror security state
Full disk encryption secure-capable[4]	Full disk encryption or FIPS secure-capable[2] or full disk encryption or FIPS secure-enabled
Full disk encryption secure-enabled	Full disk encryption or FIPS secure-enabled
FIPS secure-capable[4]	Full disk encryption or FIPS secure-capable or secure-enabled
FIPS secure-enabled	Full disk encryption or FIPS secure-enabled[3]

[1.] The secondary volume cannot be secure-capable because a role reversal results in an incompatible configuration that is not correctable (the new secondary volume cannot be made secure).

[2.] A role reversal results in an incompatible configuration. You can correct this by enabling security on the new secondary volume. The system generates an alert to this condition.

[3.] A role reversal results in a primary volume with a lower security level (full disk encryption secure-enabled) than the secondary volume (FIPS secure-enabled). This does not require any action by the user and the system does not generate an alert to the condition. The best practice is to create both the primary and secondary volumes from FIPS secure-capable drives.

[4.] Enabling security on the primary results in an incompatible configuration. You can correct this by enabling security on the secondary volume. The system generates an alert for the condition.

SSD read cache

SSD read cache can only be secure-enabled at the time of creation. The underlying HDD volume can be secure-enabled at any time, but only if the SSD read cache is already enabled. Table 4 provides the configuration rules.

Table 4) SSD read cache configuration rules.

SSD read cache	Nonsecure-capable HDD volume	Full disk encryption secure-capable HDD volume	Full disk encryption secure-enabled HDD volume	FIPS secure-capable HDD volume	FIPS secure-enabled HDD volume
Nonsecure-capable SSD cache	Yes	No	No	No	No
Full disk encryption secure-capable SSD cache	Yes	Yes	No	Yes[1]	No
Full disk encryption secure-enabled SSD cache	Yes	Yes	Yes	Yes	Yes[2]
FIPS secure-capable SSD cache	Yes	Yes	No	Yes	No
FIPS secure-enabled SSD cache	Yes	Yes	Yes	Yes	Yes

[1.] The system generates a message that the SSD read cache has a lower potential security than the HDD volume.

[2].The system generates a message that the SSD read cache has a lower enabled security than the HDD volume.

Frequently asked questions

Following are commonly asked questions regarding the rules and functionality of the SANtricity drive security feature.

Does the feature work with external key management products?

Answer: Yes. In addition to supporting internal key management, SANtricity 11.40 or later running on the E2800, EF280, E5700, EF570, EF600, EF300, or E4000 array also supports the use of a centralized key management system that adheres to the KMIP standard. An IMT is not maintained, but the product has been successfully tested with Thales CipherTrust Key Manager, Thales KeySecure, and IBM Secure Key Lifecycle Manager (version 4.1 or higher).

How does the storage array authenticate with the external key management server?

Answer: When enabling the external key management feature, the administrator must install a set of certificates on the array. These certificates are used to establish a secure connection between the array and the key management server. The SANtricity System Manager provides an interface to walk the administrator through the process of generating a Certificate Signing Request (CSR) and installing the signed client certificate and KMIP server Secure Sockets Layer (SSL) certificate. You may also perform this process through the CLI.

When is the backup security key file and passphrase needed?

Answer: The backup security key file is created and securely wrapped using a user-supplied passphrase. The backup security key file is created each time a new lock key is created. The backup security key file and passphrase are needed in the following scenarios to unlock the locked drives:

- The storage array power cycles and cannot access the KMIP server for the key.
- A volume group import where the drives are secured.
- A dual controller replacement where all drives in the storage array are secured.

Is IPv6 addressing supported for communication between the storage array and the KMIP server?

Answer: Yes, if it is supported by the external key management server.

Can I mix secured and unsecured drives in a single storage system?

Answer: Yes. A single storage system can consist of a mixture of secured and unsecured volume groups or pools. As mentioned previously, if a volume group or pool has a mix of secure-capable and nonsecure-capable drives, security cannot be enabled for the volume group or pool.

Can I have both secured and unsecured volumes in a single volume group or Dynamic Disk pool?

Answer: No. The entire volume group or pool must be either secured or unsecured.

Which types of drives support encryption?

Answer: Currently shipping HDDs and SSDs support encryption on selected capacities and models. In the NetApp Hardware Universe, these are described as FIPS or FDE.

Which types of drives are FIPS compliant?

Answer: Currently shipping HDDs and SSDs are FIPS compliant on selected capacities and models.

What level of encryption is used by this solution?

Answer: The drives use AES-256 encryption. The backed-up security key that is returned in a key file during key creation, rekeying, or a backup request, is wrapped using AES-128 encryption.

Can I enable or disable security on the drives at any time?

Answer: You can enable security at any time with data in place. The only exception is the SSD read cache feature. You can only enable security on the SSD read cache at the creation time of the cache. You can disable security on a drive through reprovisioning. Reprovisioning requires that the drive be no longer configured for user data. The drive reprovision process is a secure erase operation because the encryption key on the drive is changed and is irreversible.

Is the full disk encryption feature FIPS 140-2 validated?

Answer: Yes, when drives in use are described as FIPS 140-2. All drives with FIPS 140-2 Level 2 certification undergo rigorous testing and validation prescribed by the NIST standards. The cryptographic modules in the drive (hardware and software) are validated by the NIST in conjunction with the drive manufacturers. In E-series storage arrays, we follow the NIST guideline to properly authenticate and take ownership of an already certified FIPS drive. This process is different from authentication and ownership of a standard secure drive.

Are controller replacements allowed while full disk encryption is in use?

Answer: Yes. The security key and other configuration parameters are automatically synchronized after a single-controller replacement in a dual-controller system. In a simplex controller system or a dual controller replacement in a dual-controller system, you must provide the backed-up security key from the original controller. If a backup of the security key is not available, the data on the drives are not accessible.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- E-Series and SANtricity 11 Documentation Center
  http://docs.netapp.com/ess-11/index.jsp
- E-Series and SANtricity 11 Resources
  https://mysupport.netapp.com/info/web/ECMP1658252.html
- NetApp SANtricity System Manager Online Help v11.60
  https://mysupport.netapp.com/NOW/public/eseries/sam/index.html
- FIPS Publication
  Security Requirements for Cryptographic Modules (nist.gov)

Version history

Version	Date	Document version history
Version 1.0	October 2015	Initial version for SANtricity v11.20
Version 2.0	July 2016	Refresh for SANtricity v11.25
Version 3.0	July 2017	Refreshed for SANtricity v11.40. Added External Key Management Support.
Version 4.0	August 2019	Refreshed for SANtricity v11.60. Updated drive provisioning topic for NVMe drives.

Version	Date	Document version history
Version 4.1	April 2020	Updated section 3 on steps to configure the storage array and KMIP server to authenticate requests.
Version 5.0	May 2021	Updated for SANtricity v11.70.x. Introduced sanitization and erase availability for non-FDE drives; previously secure erase was available only on encryption-capable drives.
Version 6.0	July 2023	Updated for SANtricity v11.80. Includes support for FIPS 140-3.
Version 7.0	November 2024	Updated for new KMS setup workflow, v11.90 release.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

TR-4744-0723

NetApp