



NetApp FAQ for Full Disk Encryption on DataONTAP

1. What is FDE?

Full Disk Encryption (FDE) refers to encryption of all blocks in a disk drive, whether by software or hardware. In our case, FDE refers to hardware-based data encryption embedded in disk drives. The disk drives receive cleartext data but write encrypted data to disk. Every block, usually even the Master Boot Record (MBR), is encrypted. The drive vendors are following Trusted Computing Group (TCG) standards released in January 2009.

The encrypting drives handle all the data encryption operations internally, including data encryption key management. To prevent unauthorized access to the data, the storage system must authenticate itself with the drive. This is done via a passphrase which is established the first time the drive is used. Only the storage system and the drive know the passphrase.

2. What type of access controls does FDE provide?

FDE does not provide additional ACL above those found in Data ONTAP – but it also doesn't interfere with ACLs.

3. Does FDE provide granular encryption? If so at what level?

FDE encrypts at the drive level (i.e. each drive has a unique key). However, since all drives in a RAID group have to be either encrypting or non-encrypting drives, FDE essentially provides encryption at the aggregate level.

The TCG standard does specify the ability to divide the disk drive into 1024 zones each with a unique encryption key. However, drive vendors do not consistently support this zoning capability, and it does not lend itself well to logical data units like Flex Volumes.

4. What assurance levels does FDE have? (FIPS/CC)

FDE relies on the drive manufacturer for assurance level certification. Currently, Seagate is in Implementation Under Test (IUT) phase with NIST for FIPS certification.

5. What is the performance impact?

The performance impact is considered negligible (< 1%) impact on drive access.

6. Compare FDE vis-a-vis DataFort?

Feature	DataFort	FDE
<i>Access Controls & Authentication</i>	Quorum based authentication 2-factor Authentication	Data ONTAP Access Controls and Auth
<i>Granularity of encryption</i>	Flexvols and Shares	Aggregates/Individual disks
<i>Performance</i>	Low performance	Very High (<1% Impact)

Channel Partners and Customers Only

Proprietary and Confidential. Restricted to NetApp channel partners and customers, each of whom is under NDA obligations. © Copyright 2009 NetApp. All rights reserved.



<i>Simplicity & Inter-op</i>	Very limited interop (e.g. breaks dedupe) & fairly complex to use/mange	Great inter-op; works with all Data ONTAP features. Easy to manage.
<i>Crypto Shred</i>	Yes	Yes
<i>Key Mgmt.</i>	Needs LKM or other key manager	No need for key manager
<i>Security</i>	-FIPS 140-2 level 3 -CC EAL4 Certification	-Vendors striving for FIPS 140-2 level 3 -Data ONTAP-CC EAL3 Certification
<i>Scaling Limits</i>	LUNs	None
<i>Bottom line</i>	Expensive appliance for high security needs (niche market)	Low cost solution integrated in storage array - meets most customer needs

7. How do I migrate my customers from DataFort to FDE?

First, make sure that FDE solves all the customer's needs. FDE may not be a suitable migration path for all DataFort customers since the DataFort has additional functionality like additional ACL management and more granular encryption. Second, migration involves deploying a new filer with FDE and copying the data over from the DataFort encrypted LUNs/volumes to the new filer. There is no in-place upgrade or migration since the DataFort and FDE use different encryption data formats.

8. How does introduction of encryption work with normal cluster or HA-Pair operations?

Introduction of FDE encryption will have no effect on HA-Pair operations because the encryption is occurring at a much lower level. However the administrator will have to ensure that the same passphrase is used on both HA-Pair nodes for failovers.

9. What is the operational impact of introducing FDE?

FDE requires a completely new installation of filers, shelves, and drives. See later questions for details on release and platform details.

10. Do my customers have to pay more to get this technology? If so how much?

FDE will be a licensed feature. There may also be a small incremental cost to get FDE disks. The exact details of pricing will be made available soon.

11. What release of Data ONTAP will this be supported on?

Although release content has not been finalized, FDE is currently targeted for Data ONTAP 8.0.1.

Channel Partners and Customers Only

Proprietary and Confidential. Restricted to NetApp channel partners and customers, each of whom is under NDA obligations. © Copyright 2009 NetApp. All rights reserved.



12. Are there any constraints on downgrade/revert?

As with support for any new hardware, you will not be able to downgrade or revert to any release before ONTAP 8.0.1. Earlier versions of Data ONTAP will not authenticate with the encrypting drives and therefore be unable to boot successfully.

13. What platforms/shelf combination will this be supported on?

We plan to limit FDE support to Shuar-XL and Sequoia shelves in ONTAP 8.0.1. We plan to support more platforms and shelves in future releases. If there are any specific platforms you would like to see supported in ONTAP 8.0.1 please contact the product manager, Narendar Shankar.

14. What kind of key management is needed to make FDE work?

Encrypting drives manage the data encryption keys internally, so there is no key management. Instead, management of passphrases used by the encrypting drives becomes necessary. Some proposed solutions include:

- Automatic passphrase generation and management within the filers
- Manual passphrase generation by administrator, specified through CLI
- An external storage device (USB drive, SmartCard, etc) to store the passphrase for emergency shredding use cases

15. My customer uses the red button on the DataFort. How can this be accomplished with FDE?

FDE wraps the data encryption key with the same passphrase used to authenticate the storage controller with the disk drives. Destruction of this passphrase eliminates access to the data encryption key and effectively shreds all the data. We plan to offer a means of storing the passphrase on external media (USB stick or SmartCard) so that the customer can physically destroy the media for effective CryptoShred capability.

16. How mature is this technology?

FDE has been around in one form or another for several years. Several major drive vendors such as Seagate and Hitachi have been investing heavily into implementing encrypting drives across their entire drive lines. All 6 major drive manufacturers have collaborated to create a Trusted Computing Group specification which standardizes encryption methods across all vendors' drives. Furthermore, the TCG standards utilize the well known AES-128 or AES-256 as the encryption algorithm.

17. Can I have a system which has a mixture of encrypting and non-encrypting disks?

Yes and no. In ONTAP 8.0.1 all drives attached to a FAS must be encrypting drives. In future releases, we are considering support for a mixture of encrypting and non-encrypting aggregates. Under no circumstances will you be able to mix encrypting and non-encrypting drives in a given aggregate.

Channel Partners and Customers Only

Proprietary and Confidential. Restricted to NetApp channel partners and customers, each of whom is under NDA obligations. © Copyright 2009 NetApp. All rights reserved.