Technical White Paper

Dell EMC PowerProtect DD Series Appliances: Encryption Software

Abstract

This document describes the Dell EMC™ PowerProtect DD series appliance encryption software and its capabilities with the Dell EMC Data Domain™ Operating System (DDOS).

October 2020

Revisions

Date	Description
June 2013	Initial release
October 2020	Updated for DDOS 7.3 release

Acknowledgments

Author: Vinod Kumar Kumaresan

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Table of contents

Executive summary

The Dell EMC™ Data Domain™ Operating System (DDOS) is the intelligence that powers Dell EMC PowerProtect DD series appliances. DD series encryption software enables organizations to enhance the security of the data that resides on DD series appliances using industry-standard encryption algorithms. DD series encryption software protects backup and archive data that is stored on DD series appliances with data encryption that is performed inline before the data is written to disk. The Encryption at Rest feature satisfies internal governance rules and compliance regulations. It also protects against the reading of customer data on individual disks or disk shelves that are removed from the system due to theft.

DD Replicator with encryption enables encrypted data to be replicated using collection, directory, MTree, or application-specific managed file replication with the various topologies.

This document details DD series data encryption features which provide the following benefits:

- Protect against unauthorized access if disks are stolen from the system
- Protect the system during transport from unauthorized access
- Meet IT governance and compliance

Audience

This technical white paper is intended for Dell Technologies customers, partners, and employees. It describes the DD series encryption features of DDOS, and details how they can be used to securely manage, protect, and recover data.

1 DD series encryption software overview

Data encryption protects user data if the protection system is stolen or if the physical storage media is lost during transit. It also eliminates accidental exposure of a failed drive if it is replaced. When data enters the protection system using any of the supported protocols (NFS, CIFS, DDVTL, DD Boost, and NDMP tape server), the stream is segmented, fingerprinted, and deduplicated (global compression). It is then grouped into multi-segment compression regions, locally compressed, and encrypted before being stored to disk. Once data encryption is enabled, the DD Encryption feature encrypts all data entering the appliance.

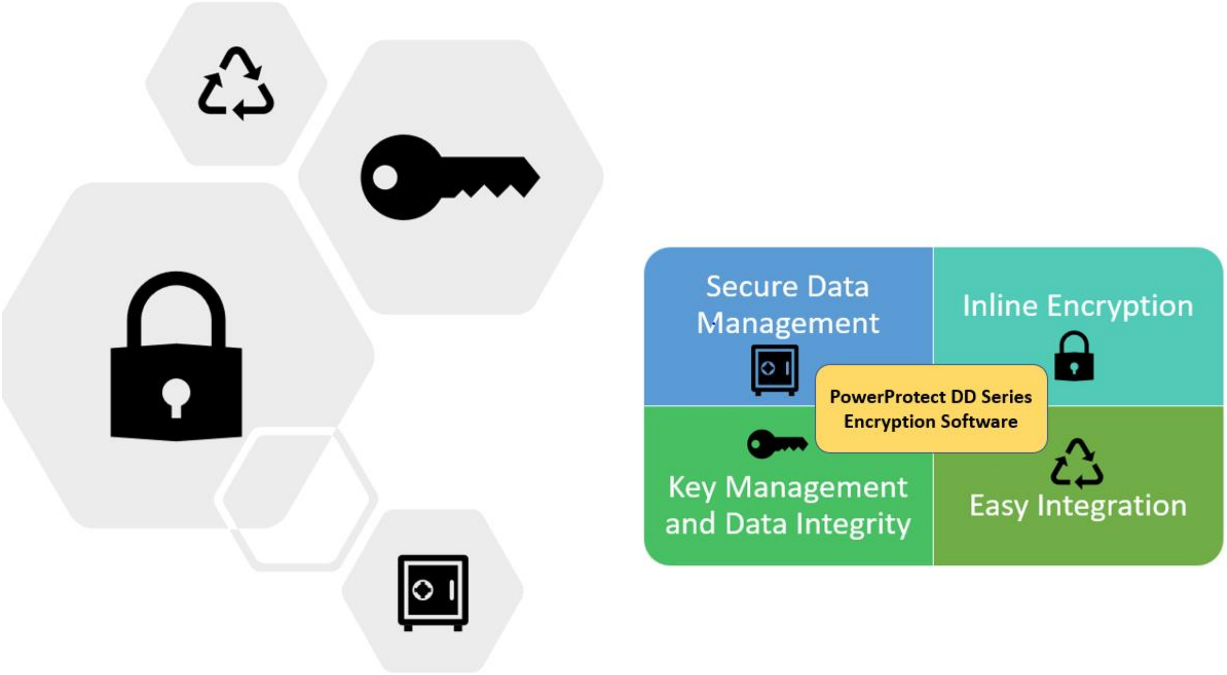

Secure Data Management
Inline Encryption
PowerProtect DD Series Encryption Software
Key Management and Data Integrity
Easy Integration

Figure 1 DD series encryption software overview

DD series encryption software provides the following benefits:

- Secure data management:
  - Encrypt all data stored on a DD series deduplication storage system
  - Protect data from theft or loss of the system, disk shelves, disks, or factory returned disks
  - Easily implement encryption to satisfy internal governance rules and compliance regulations
  - Meet compliance needs using industry-standard AES-128 or AES-256 encryption algorithms
  - Use RSA BSAFE FIPS 140-2 compliant cryptographic libraries
- Inline encryption:
  - Real-time, immediate data encryption with compression
  - Stream-Informed Segment Layout (SISL) architecture used for optimized encryption
  - Software-based approach requires no extra hardware
- Key management and data integrity:
  - Robust protection against accidental key loss
  - Passphrase protection of encryption keys
  - Data Invulnerability Architecture (DIA) with dual-disk parity RAID 6

- Easy integration:
  - Supports leading backup and archive applications
  - Supports leading enterprise applications for database and virtual environments
  - Allows simultaneous use of VTL, NAS, NDMP, and DD Boost

1.1 Encryption types offered by DD series encryption software

There are three types of encryption offered with DD series appliances:

- Inline encryption of data at rest using the DD Encryption feature
- Encryption of data in-flight using DD Replicator software, which is used for replicating data between sites over the WAN
- Encryption of data in-flight using DD Boost software, using Transport Layer Security (TLS)

1.1.1 Inline encryption of data at rest using DD Encryption

DD Encryption provides inline encryption. As data is ingested, the stream is deduplicated, compressed, and encrypted using an encryption key before it is written to the RAID group. DD Encryption uses RSA BSAFE libraries, which are validated according to the Federal Information Processing Standards (FIPS) 140-2.

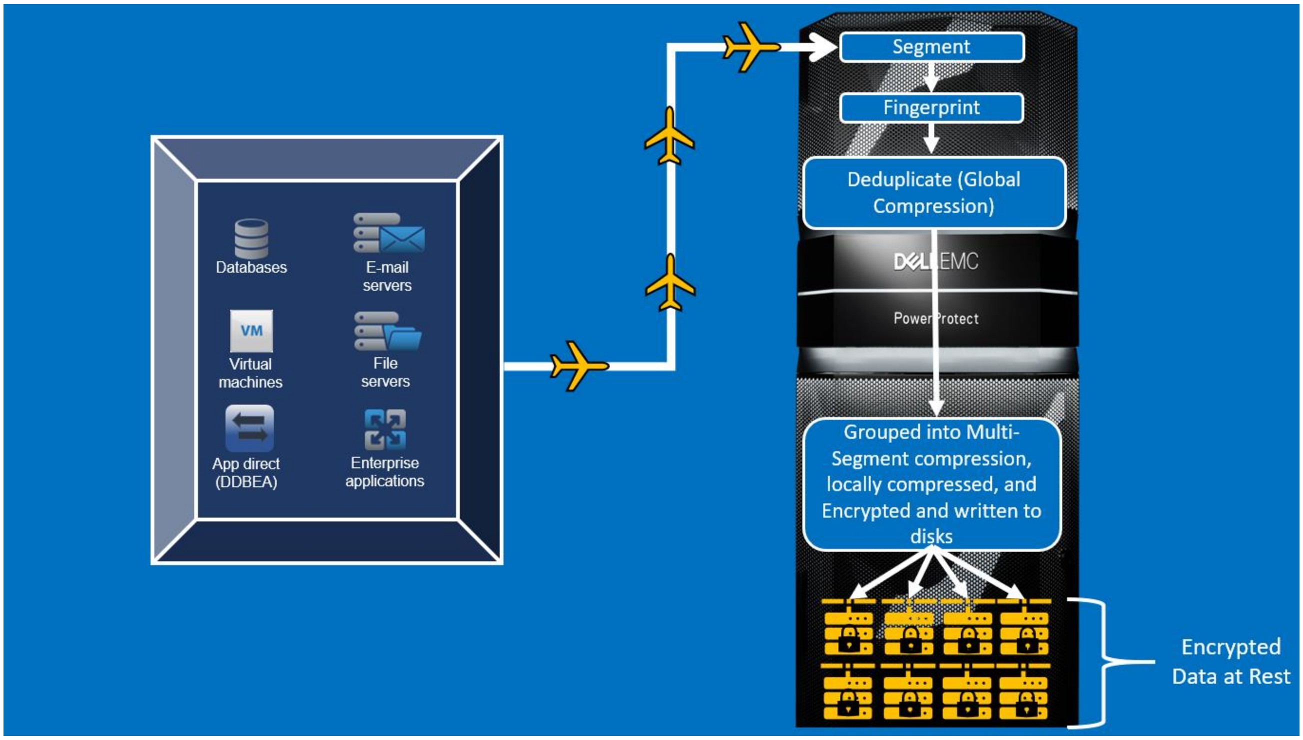


Figure 2 DD Encryption overview

Encryption is not enabled by default. When enabled, the Embedded Key Manager (EKM) is in effect. DD series appliances also support external key managers (SafeNet KeySecure and Vormetric Data Security Manager) that are compliant with the Key Management Interoperability Protocol (KMIP). External Certificate Authority (CA) and host certificates are required to set up SafeNet KeySecure Key Manager (KMIP). You can request these certificates from third-party certificate authorities or create them using the appropriate OpenSSL utility. If encryption is enabled on Cloud Tier, only EKM is supported.

You can select one of two cipher modes, Cipher Block Chaining (CBC) mode or Galois/Counter mode (GCM), to best fit your security and performance requirements. GCM is the most secure algorithm, but it is slower than the CBC mode. The system also uses a user-defined passphrase to encrypt that key before it is stored in multiple locations on disk. The system encryption key cannot be changed and is not accessible to a user. Without the passphrase, the file system cannot be unlocked, and data is not accessible. For more information, see the document Dell EMC DD OS Version 7.3 Administration Guide (may require login).

1.1.2 Encryption of data in-flight using DD Replicator

Encryption of data in flight encrypts data that is being transferred using DD Replicator between two DD series appliances. It uses AES 256-bit encryption to encapsulate the replicated data over the wire. The encryption-encapsulation layer is immediately removed when it transfers to the destination system. Data within the payload can also be encrypted using DD Encryption.

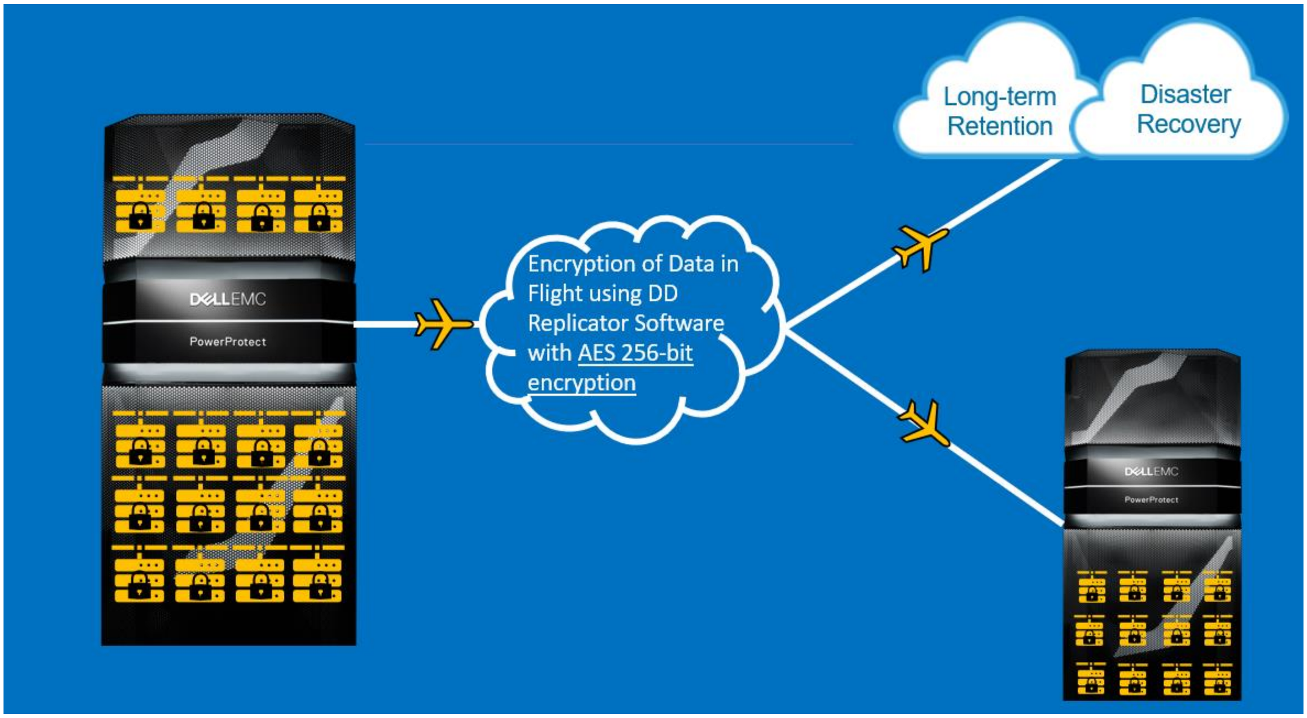

Long-term Retention
Disaster Recovery
DELL EMC
PowerProtect
Encryption of Data in Flight using DD Replicator Software with AES 256-bit encryption
DELL EMC
PowerProtect

Figure 3 DD Replicator overview

1.1.2.1 DD Replicator

DD Replicator provides automated, policy-based, network-efficient replication for disaster recovery, remote-office data protection, and multisite tape consolidation. DD Replicator software asynchronously replicates only the compressed, deduplicated data over the WAN or LAN during the backup process, making network-based replication fast, reliable, and cost-effective.

For environments that do not use a VPN for secure connections between sites, DD Replicator can securely encapsulate its replication payload over SSL with AES 256-bit encryption. This ability enables secure transmission over the wire, a process also known as encrypting data in flight.

1.1.2.2 Encryption of data in-flight over NFS

NFSv3 and NFSv4 support Kerberos v5 protocol with integrity checking using checksums (krb5i) and Kerberos v5 protocol with privacy service (krb5p) for integrity and privacy, respectively. However, there are performance penalties for encryption.

1.1.3 Encryption of data in-flight with DD Boost

The DD Boost protocol can be used with or without certificates for authentication and encryption of data. The use of certificates was introduced to offer a more secure data-transport capability.

In-flight encryption enables applications to encrypt in-flight backup or restore data over LAN from the system. When it is configured, the client can use TLS to encrypt the session between the client and the system. If TLS with certificates is used, the specific suites that are used are DHE-RSA-AES128-SHA and DHE-RSA-AES256-SHA for medium and high encryption, respectively. If anonymous TLS is used to encrypt the session, either of these options is used: ADH-AES256-SHA for the HIGH encryption option, or ADH-AES128-SHA for the MEDIUM encryption option.

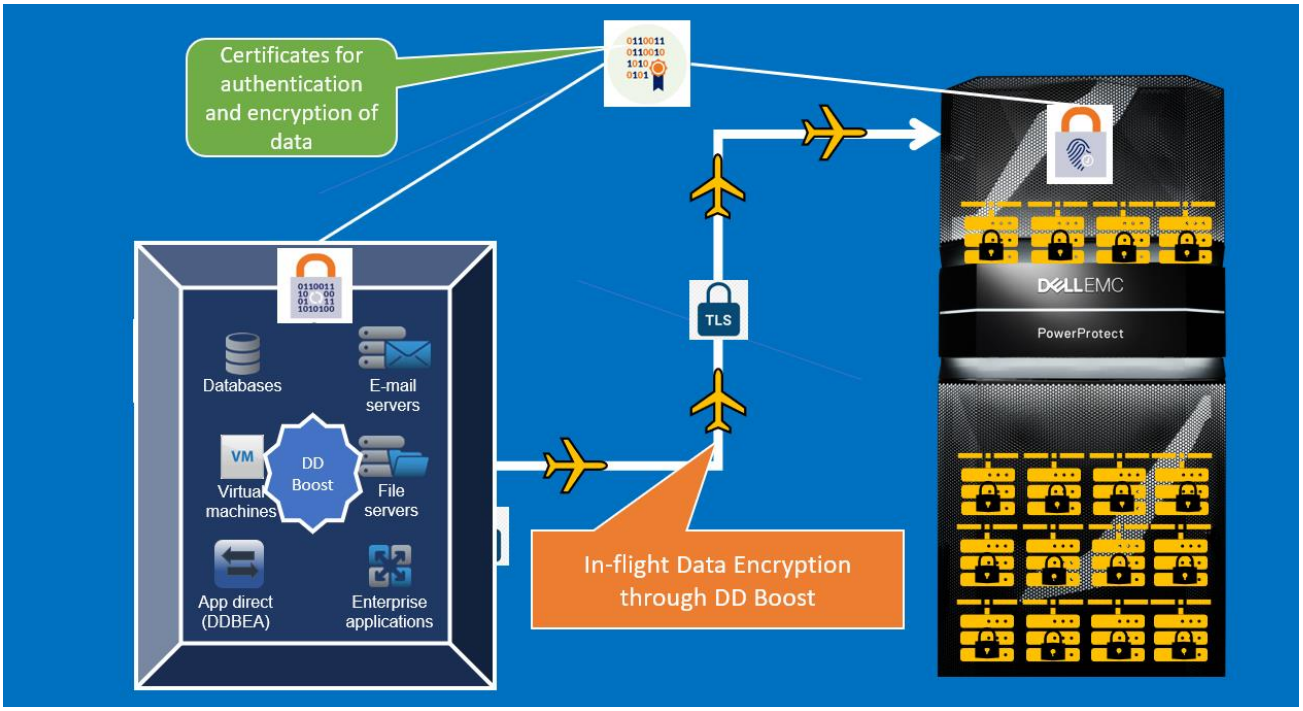
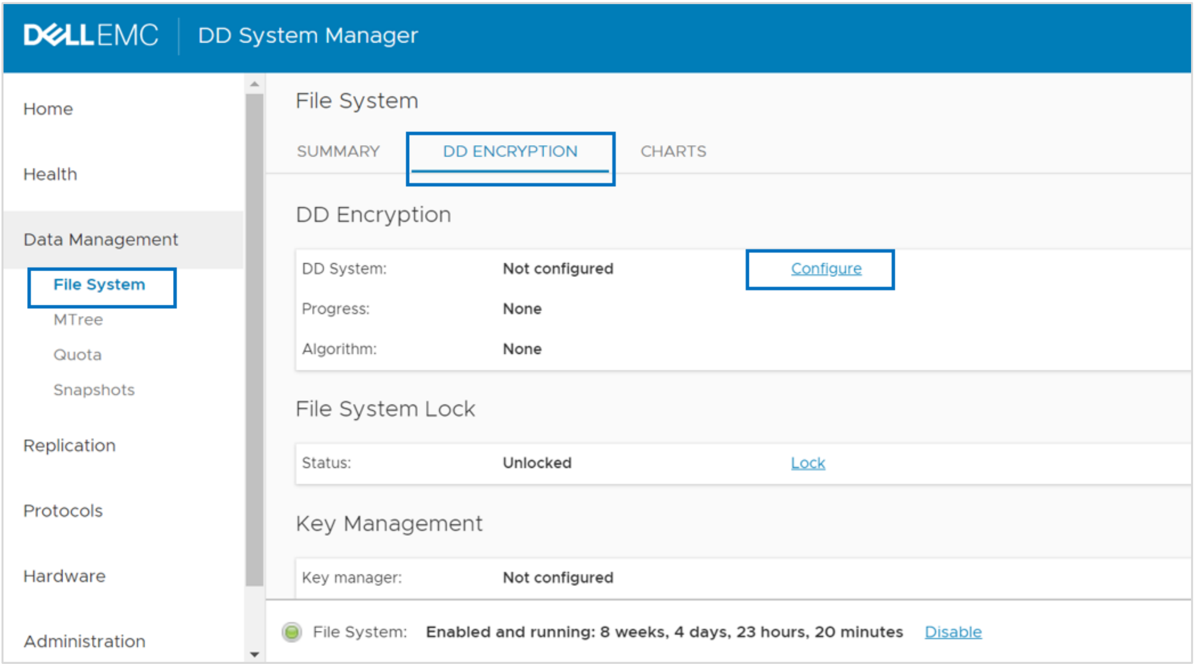


Figure 4 DD Boost overview

2 DD Encryption configuration

Use the following steps to configure DD Encryption.

1. To enable data encryption, in DD System Manager, click **Data Management** > **File System** > **DD ENCRYPTION** and click **Configure**.



DD Encryption

DD System: Not configured

Progress: None

Algorithm: None

File System Lock

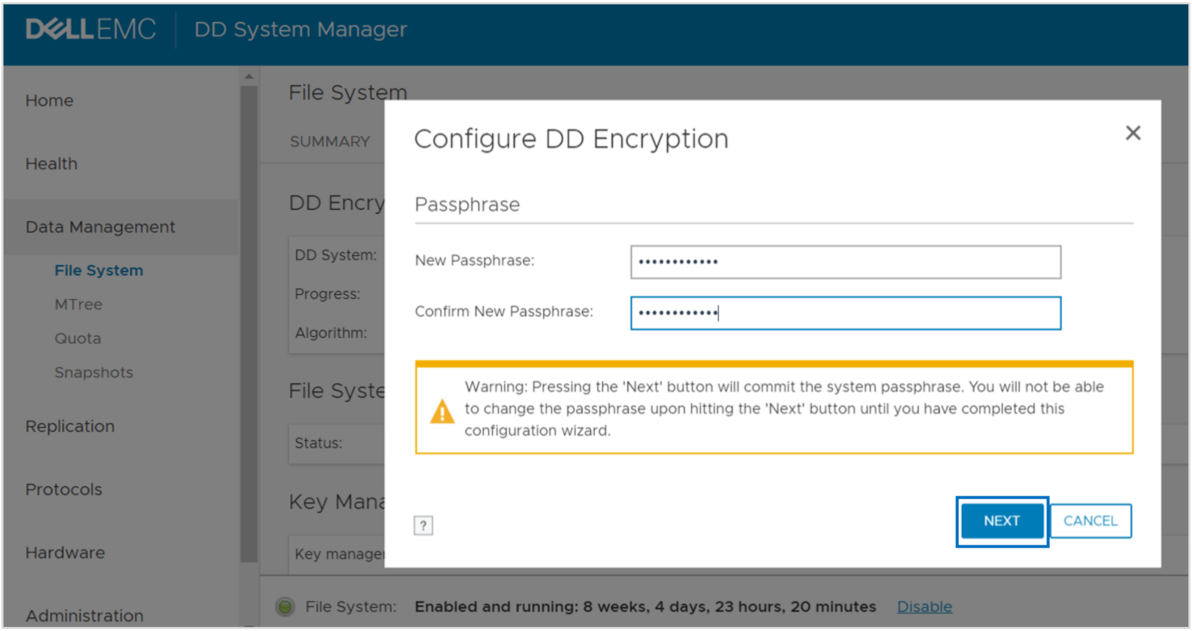
Status: Unlocked

Key Management

Key manager: Not configured

File System: Enabled and running: 8 weeks, 4 days, 23 hours, 20 minutes

2. Enter the system passphrase to enable encryption.



Configure DD Encryption

Passphrase

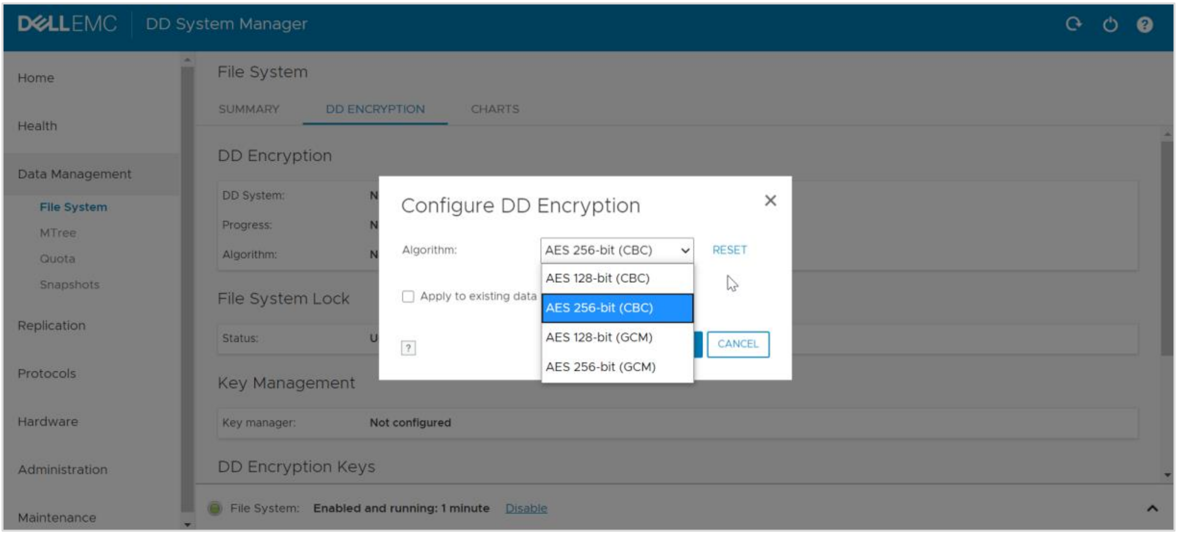
New Passphrase: ••••••••••••

Confirm New Passphrase: ••••••••••••

Warning: Pressing the 'Next' button will commit the system passphrase. You will not be able to change the passphrase upon hitting the 'Next' button until you have completed this configuration wizard.

File System: Enabled and running: 8 weeks, 4 days, 23 hours, 20 minutes

3. In the **Configure DD Encryption** window, use the **Algorithm** drop-down menu to select an encryption algorithm or accept the default **AES 256-bit (CBC).** The AES 256-bit GCM is the most secure algorithm, but it is slower than CBC mode.

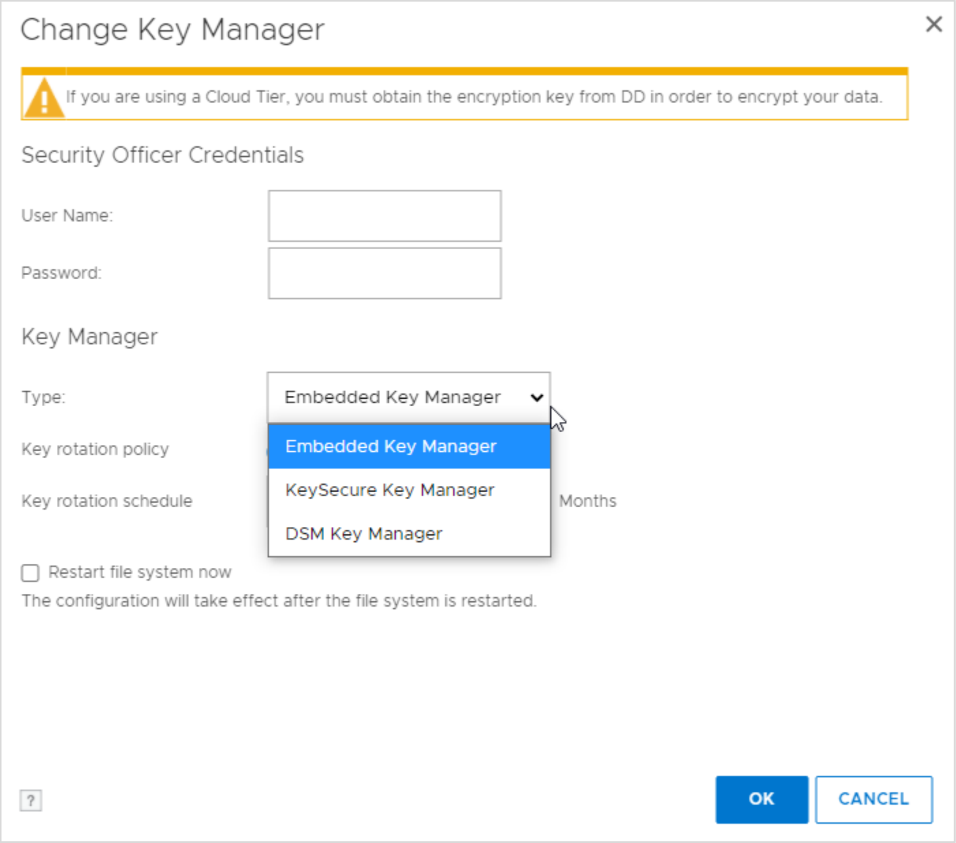


DD System: N
Progress: N
Algorithm: N
Status: U
Key manager: Not configured
Algorithm: AES 256-bit (CBC)
□ Apply to existing data
File System: Enabled and running: 1 minute

By checking the **Apply to existing data** option, the existing data will be encrypted during the first cleaning cycle after the file system is restarted. Encryption of existing data can take longer than a standard file-system-cleaning operation.

4. In the **Change Key Manager** window > **Key Manager** section, select one of the following options in the **Type** drop-down menu:

   - Embedded Key Manager
   - KeySecure Key Manager (SafeNet KeySecure Key Manager)
   - DSM Key Manager (Data Security Manager Key Manager)



Change Key Manager

⚠ If you are using a Cloud Tier, you must obtain the encryption key from DD in order to encrypt your data.

Security Officer Credentials

User Name:

Password:

Key Manager

Type: Embedded Key Manager

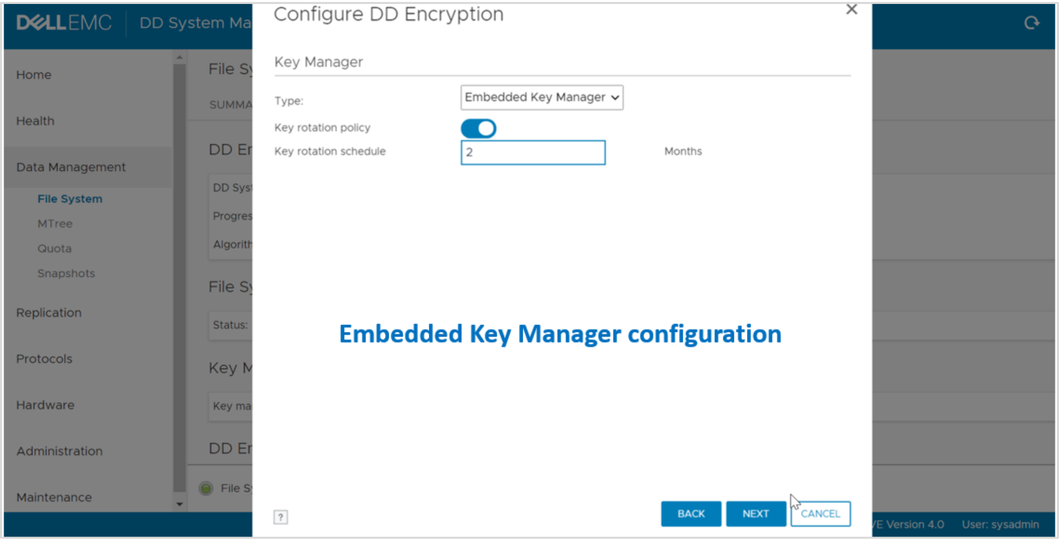
Key rotation policy

Key rotation schedule Months

□ Restart file system now

The configuration will take effect after the file system is restarted.

5. When the encryption is enabled, by default the Embedded Key Manager is in effect after the file system is restarted. You can enable or disable key rotation. If enabled, enter a rotation interval between 1 month and 12 months.



Configure DD Encryption

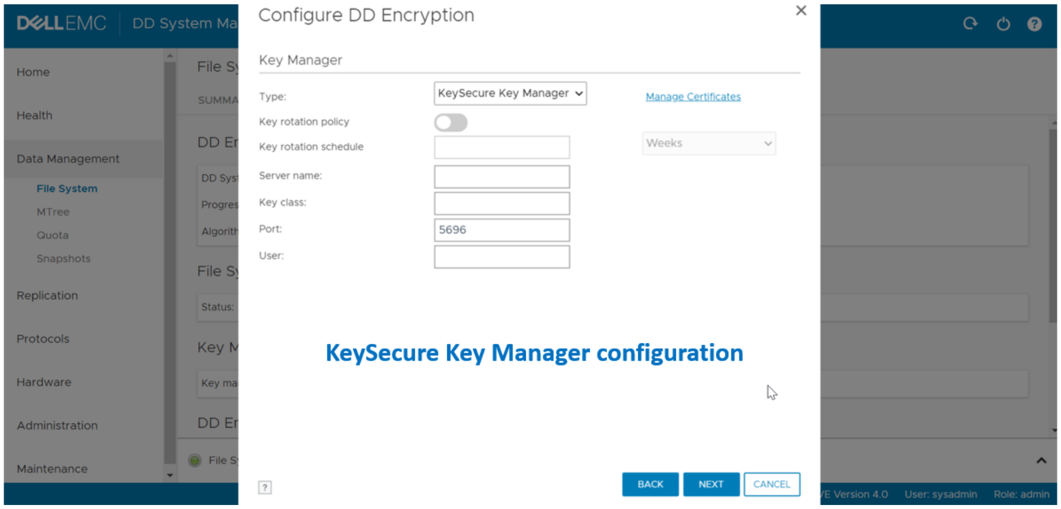
Key Manager

Type: Embedded Key Manager

Key rotation policy: ●

Key rotation schedule: 2 Months

Embedded Key Manager configuration



Configure DD Encryption

Key Manager

Type: KeySecure Key Manager

Key rotation policy: ○

Key rotation schedule: Weeks

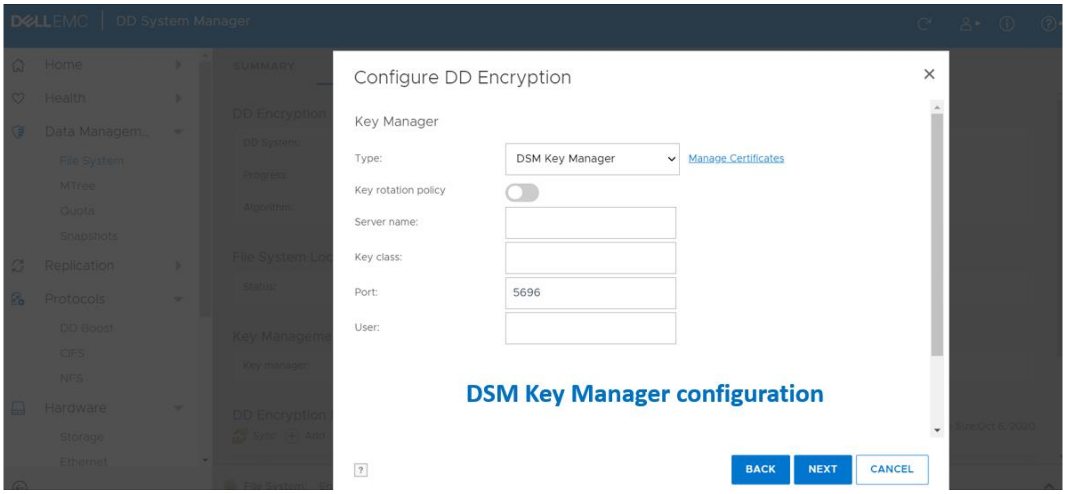
Server name:

Key class:

Port: 5696

User:

KeySecure Key Manager configuration



Configure DD Encryption

Key Manager

Type: DSM Key Manager

Key rotation policy: ○

Server name:

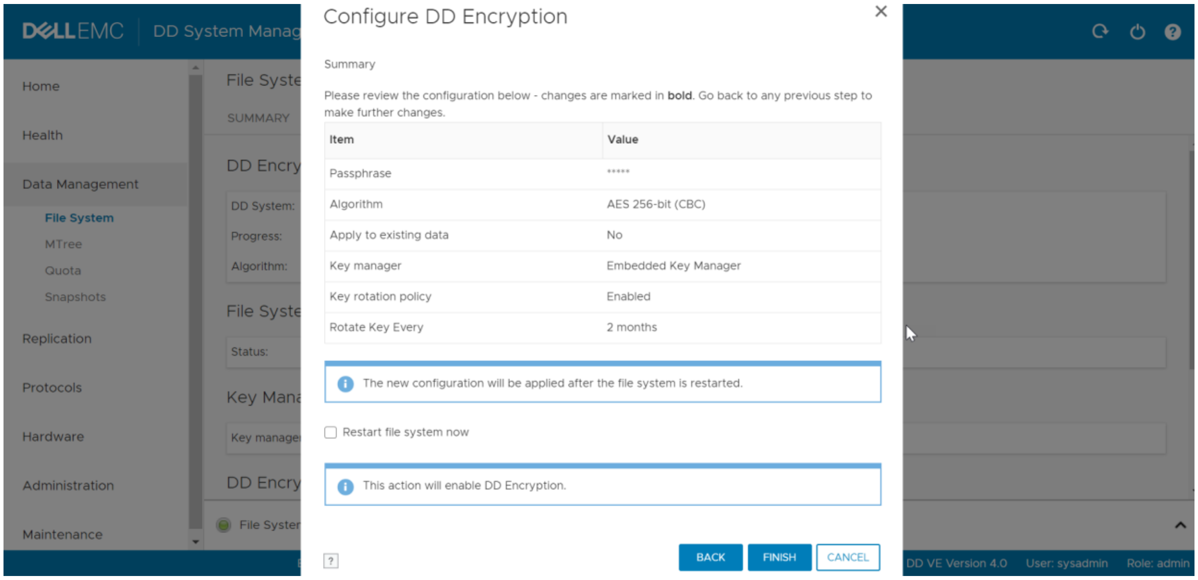
Key class:

Port: 5696

User:

DSM Key Manager configuration

6. Review the configuration confirmation page, and click **Finish**.



Configure DD Encryption

Summary

Please review the configuration below - changes are marked in **bold**. Go back to any previous step to make further changes.

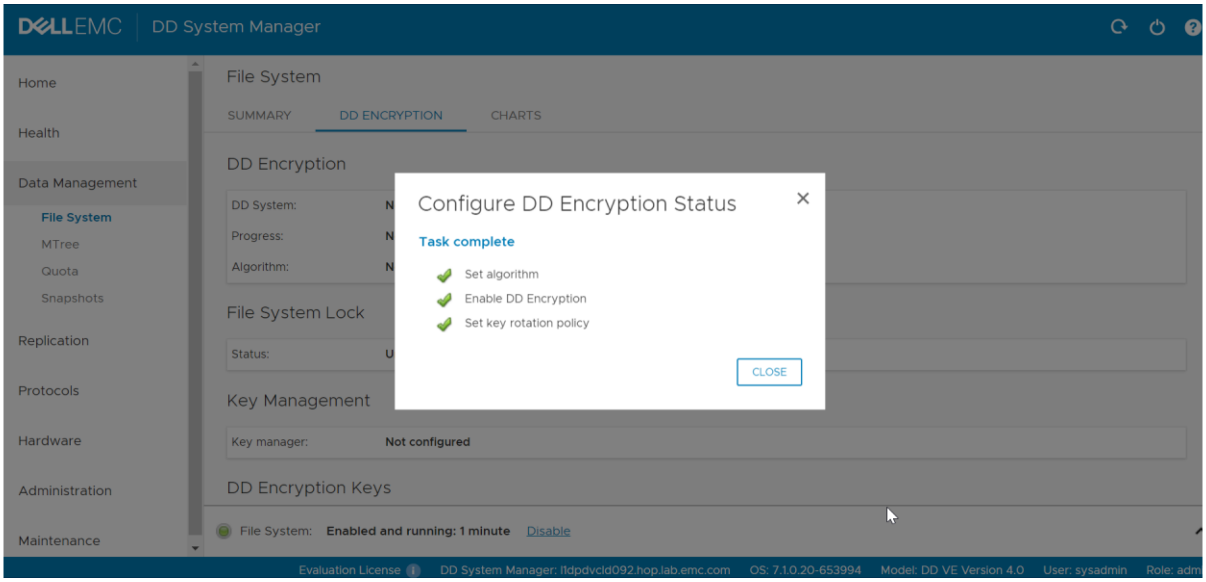
Item	Value
Passphrase	*****
Algorithm	AES 256-bit (CBC)
Apply to existing data	No
Key manager	Embedded Key Manager
Key rotation policy	Enabled
Rotate Key Every	2 months

The new configuration will be applied after the file system is restarted.

□ Restart file system now

This action will enable DD Encryption.

7. DD Encryption is now successfully configured with Embedded Key Manager.



Configure DD Encryption Status

Task complete

✓ Set algorithm
✓ Enable DD Encryption
✓ Set key rotation policy

Key manager: Not configured

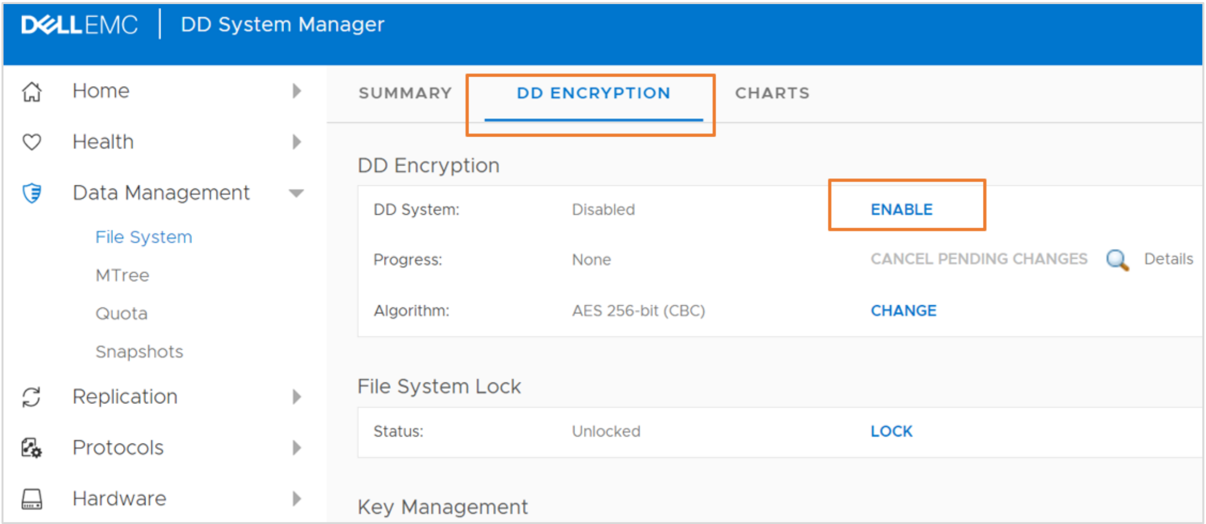
File System: Enabled and running: 1 minute Disable

2.1 Enabling and disabling DD Encryption

2.1.1 Enabling DD Encryption

Follow this procedure to enable the DD Encryption feature:

1. In DD System Manager, use the **Navigation** panel to select the protection system.
2. In the **DD Encryption** view, click **ENABLE**.



DD Encryption

DD System: Disabled

Progress: None

Algorithm: AES 256-bit (CBC)

File System Lock

Status: Unlocked

Key Management

3. Select one of the following options and click **OK**.

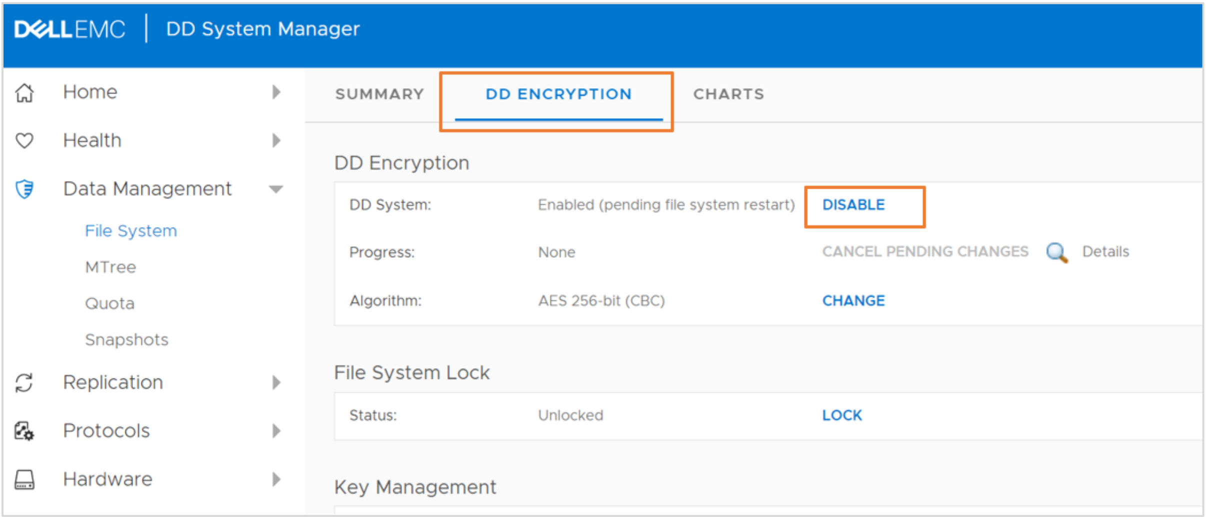
   - Apply to existing data: Encryption of existing data occurs during the first cleaning cycle after the file system is restarted.
   - **Restart the file system now:** DD Encryption is only enabled after the file system is restarted.

Note: Applications may experience an interruption while the file system is restarted.

2.1.2 Disabling DD Encryption

Follow this procedure to disable the DD Encryption feature:

1. In DD System Manager, use the **Navigation** panel to select the protection system.
2. In the **DD Encryption** view, click **DISABLE**.



DD System: Enabled (pending file system restart)

Progress: None

Algorithm: AES 256-bit (CBC)

Status: Unlocked

The **Disable Encryption** window displays.

3. In the **Security Officer Credentials** area, enter the username and password of a security officer.
4. Select one of the following and click **OK**.

   - **Apply to existing data:** Decryption of existing data occurs during the first cleaning cycle after the file system is restarted.
   - **Restart the file system now:** DD Encryption is only disabled after the file system is restarted.

3 Key management

Encryption keys determine the output of the cryptographic algorithm. They are protected by a passphrase, which encrypts the encryption key before it is stored in multiple locations on disk. The user generates the passphrase which requires both an administrator and a security officer to change it.

A key manager controls the generation, distribution, and life-cycle management of multiple encryption keys. A protection system can use either the embedded key manager or KMIP-complaint key manager such as SafeNet KeySecure or NextGen or Vormetric Data Security Manager. Only one key manager can be in effect at a time. When encryption is enabled on a protection system, the Embedded Key Manager is in effect by default. If the SafeNet KeySecure Key Manager is configured, it replaces the embedded key manager and remains in effect until it is disabled manually.

3.1 Embedded key manager

The embedded key manager provides and generates multiple keys internally, although the system uses only one key at a time to encrypt data coming into the system.

The embedded key manager rotates keys, supports a maximum of 254 keys, and allows you to specify how long a key will be in effect before it is replaced. The key rotation of the embedded key manager is managed on the protection system.

3.2 KMIP-compliant external key managers: KeySecure and Data Security Manager

DD series appliances support a KMIP-compliant key manager: KeySecure v8.5, v8.9, v8.10 and v8.12.1; NextGen v1.9.1 and v.10 from SafeNet or Gemalto; or Data Security Manager (DSM) 6.3 from Thales/Vormetric. To use a KMIP key manager, users must configure both the key manager and the protection system or DDVE to trust each other. A protection system retrieves these keys and their states from the key manager after establishing a secure TLS connection.

You can encrypt file-system data (active tier only) by configuring KeySecure, NextGen, or DSM as the key manager. You may manage keys from DD series appliances and configure a key-rotation policy for weekly or monthly automatic key rotation. You cannot enable external key managers (which include KeySecure, NextGen, and DSM) on systems that have encryption enabled on one or more cloud units, similar to Key Secure.

See the document KMIP Integration Guide for DD OS for more information about how to create keys and use them on a protection system.

3.3 Key manager support

All key managers support all DDOS file-system protocols.

3.3.1 Replication

When configuring protection systems for directory or MTree replication, configure each system separately. The two systems can use either the same or a different key class, and the same or different key managers. For collection-replication configuration, you must configure the protection system on the source. All replicated data is encrypted with the key set on the source. New data that is written to the destination after a replication break uses either the last active key set on the source or a new key if the key manager is configured.

3.3.2 Embedded key manager setup

When the embedded key manager is selected, the protection system creates its own keys. After the key-rotation policy is configured, a new key is automatically created at the next rotation. To disable the key-rotation policy, click the **Disable** button that is associated with the key-rotation status of the embedded key manager.

Create an encryption key:

1. Click Data Management > File System > DD Encryption.
2. In the **Encryption Keys** section, click **Create.**
3. Enter the security officer username and password.

   A new protection system key is created and activated immediately.

4. Click **Create**.

Destroy an encryption key:

1. Click Data Management > File System > Encryption.
2. In the **Encryption Keys** section, click the key in the list to be destroyed.
3. Click **Destroy**.

   The system displays the **Destroy** window that includes the tier and state for the key.

4. Enter the security officer username and password.
5. To confirm destroying the key, click **Destroy.**

You can delete key manager keys that are in the Destroyed or Compromised-Destroyed states. However, you can delete a key only when the number of keys has reached the maximum limit of 254 limit. This procedure requires security officer credentials.

Delete an encryption key:

1. Click Data Management > File System > Encryption.
2. In the **Encryption Keys** section, click the key or keys in the list to be deleted.
3. Click **Delete**.

   The system displays the key to be deleted, and the tier and state for the key.

4. Enter the security officer username and password.
5. To confirm deleting the key or keys, click **Delete.**

3.3.3 Setting up a KMIP-complaint external key manager (KeySecure and DSM)

DD series appliances support external key managers by using KMIP, and centrally manage encryption keys in a single, centralized platform. Note the following:

- When applicable, you can precreate keys on the Key Manager.
- You cannot enable a KMIP key manager on systems that have encryption enabled on one or more cloud units.

3.3.3.1 Using DD System Manager to set up and manage a KMIP-complaint key manager

Follow this procedure to create a key for the KMIP-complaint key manager:

1. In DD System Manager, scroll down to the **Key Manager Encryption Keys** table.
2. Click **Add** to create a new key manager encryption key.
   a. Enter the security officer username and password.
   b. Click **Create**.

A new KMIP key is created and activated immediately.

3.3.3.2 Configuring the KMIP-complaint key manager

Follow this procedure to configure a KMIP-complaint key manager:

1. Click **Data Management** > **File System** > **DD Encryption**.
2. In the **Key Management** section, click **Configure**. The **Change Key Manager** dialog box opens.
3. Enter the security officer username and password.
4. In the **Key Manager Type** drop-down menu, click **KeySecure** or **DSM**. The **Change Key Manager** information appears.
5. Set the key rotation policy:
   a. To enable the key-rotation policy, click the **Enable Key rotation policy** button.
   b. Enter the appropriate dates in the **Key rotation schedule** field.
   c. In the **Weeks** or **Months** drop-down menu, select the duration for the policy and click **OK**.

3.4 Key manager setup

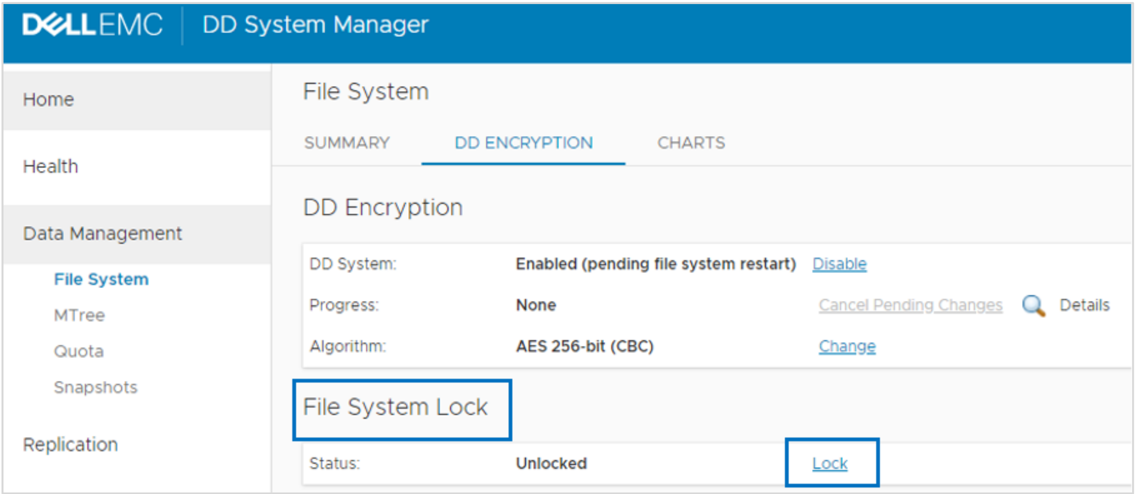
For more information about setting up SafeNet KeySecure or the Thales/Vormetric DSM Key Manager, see the section “Setting up KMIP key manager” in the document Dell EMC DD OS Version 7.3 Administration Guide.

4 File system lock

You can enable the file system lock when the DD-Encryption-enabled protection system and its external storage devices are being transported, or to lock a disk that is being replaced. This procedure requires two roles: security officer and system administration.

Follow this procedure to lock the file system:

1. Click **Data Management > File System** > **DD Encryption**.
2. In the **File System Lock** area, click **Lock**.



DD System: Enabled (pending file system restart)

Progress: None

Algorithm: AES 256-bit (CBC)

Status: Unlocked

3. In the **Lock File System** window, enter the following and click **OK**.

   - The username and password of a security officer account (an authorized user in the Security User group on that protection system)
   - The current and a new passphrase

   This procedure re-encrypts the encryption keys with the new passphrase. This process destroys the cached copy of the current passphrase (both in memory and on disk).

4. Shut down the system.
5. Transport the system or remove the disk being replaced.
6. Power on the system and use the following procedure to unlock the file system.

Follow this procedure to unlock the file system:

1. Select **Data Management > File System** > **Encryption** and click **Unlock**.
2. In the text fields, type the passphrase that was used to lock the file system.
3. Click **OK**, and click **Close** to exit.

Note: If the passphrase is incorrect, the file system does not start, and the system reports the error. Enter the correct passphrase as directed in the previous step.

5 Changing the encryption algorithm

If necessary, you can reset the encryption algorithm. Also, you can select options to encrypt new and existing data, or encrypt only new data.

Follow this procedure to change the encryption algorithm:

1. Click **Data Management** > **File System** > **Encryption**.
2. To change the Encryption Algorithm used to encrypt the protection system, click **Change Algorithm**.

   The **Change Algorithm** window displays the supported encryption algorithms:

   - AES-128 CBC
   - AES-256 CBC
   - AES-128 GCM
   - AES-256 GCM

3. Select an encryption algorithm from the drop-down box, or accept the default option of **AES 256-bit (CBC).**

   The AES 256-bit GCM is the most secure algorithm, but it is slower than CBC mode.

Note: To reset the algorithm to the default AES 256-bit (CBC), click **Reset to default**.

4. Determine what data will be encrypted:

   - To encrypt existing and new data on the system:

     i. Click **Apply to Existing data**,
     ii. Restart the file system.
     iii. Click **OK.**
     iv. Existing data will be encrypted during the first cleaning cycle after the file system is restarted.

Note: Encryption of existing data can take longer than a standard file-system-clean operation.

   - To encrypt only new data, click **Restart file system now** and click **OK.**

5. The status is displayed. Click **Close** when the process is complete.

Note: Applications may experience an interruption while the file system is restarted.

6 DD Encryption with DD Replicator

DD Replicator can be used with the optional DD Encryption feature, enabling encrypted data to be replicated using collection, directory, or MTree replication.

Replication contexts are always authenticated with a shared secret. That shared secret is used to establish a session key using a Diffie-Hellman key exchange protocol. That session key is also used to encrypt and decrypt the protection system encryption key when appropriate.

6.1 Collection replication

In collection replication, the source and destination must have the same encryption configuration because the destination data is expected to be an exact replica of the source data. In particular, the encryption feature must be turned on or off at both the source and destination. If the feature is turned on, the encryption algorithm and the system passphrases must also match. The parameters are checked during the replication-association phase.

During collection replication, the source transmits the data in encrypted form, and transmits the encryption keys to the destination. The data can be recovered at the destination because the destination has the same passphrase and the same system encryption key.

Note: Collection replication is not supported for cloud-tier-enabled systems.

6.2 MTree or directory replication

In MTree or directory replication, encryption configuration does not have to be the same at both the source and destination. Instead, the source and destination securely exchange the destination’s encryption key during the replication-association phase. The data is re-encrypted at the source using the destination’s encryption key before transmission to the destination.

If the destination has a different encryption configuration, the data transmitted is prepared appropriately. For example, if the feature is turned off at the destination, the source decrypts the data, and it is sent to the destination as unencrypted.

6.3 Cascaded replication

In a cascaded-replication topology, a replica is chained among three systems. The last system in the chain can be configured as a collection, MTree, or directory. If the last system is a collection-replication destination, it uses the same encryption keys and encrypted data as its source. If the last system is an MTree or directory-replication destination, it uses its own key, and the data is encrypted at its source. The encryption key for the destination at each link is used for encryption. Encryption for systems in the chain works the same as in a replication pair.

7 DD Encryption and Cloud Tier

DD Encryption can be enabled at three levels: system, active tier, and cloud unit. Encryption of the active tier is only applicable if encryption is enabled for the system. Cloud units have separate controls for enabling encryption. Follow these steps to enable DD encryption for cloud units:

1. Click **Data Management** > **File System** > **DD Encryption**.

Note: If no encryption license is present on the system, the **Add Licenses** page is displayed.

2. In the **DD Encryption** panel, perform one of the following actions:

    - To enable encryption for **Cloud Unit *X***, click **Enable.**
    - To disable encryption for **Cloud Unit *X***, click **Disable.**

Note: You are prompted to enter security officer credentials to enable encryption.

3. Enter the security officer **Username** and **Password**.
4. Optionally, check **Restart file system now**.
5. Click **Enable** or **Disable**, as appropriate.
6. In the **File System Lock** panel, lock or unlock the file system.
7. In the **Key Management** panel, click **Configure**.
8. In the **Change Key Manager** window, configure the security officer credentials and the key manager.

Note: Cloud encryption is allowed only through the Embedded Key Manager. External key managers are not supported.

9. Click **OK**.
10. Use the **DD Encryption Keys** panel to configure the encryption keys.

If encryption is enabled for the cloud tier, any data written to the cloud or buckets is encrypted using the Embedded Key Manager (eKM) keys. The data is encrypted on the DD series appliance before it is written to the cloud. There is no end-to-end encryption, but data is always encrypted throughout the data movement.

If the encryption is disabled on the cloud tier, data is decrypted on the DD series appliance before it is sent over a TLS connection to the cloud. If the encryption is enabled on the cloud-provider side (for example, using ECS native encryption), the data is encrypted when it reaches that end point. Similarly, the data is decrypted at the endpoint and is transmitted over TLS when it is recalled or read from the DD series appliance.

Note: When using an embedded key manager, only the newly ingested data is encrypted. For example, encryption occurs for data that is ingested after embedded encryption is enabled, unless you run the **Apply changes** command. This command converts or encrypts all the existing unencrypted data.

8 Conclusion

DD series encryption software provides a robust, secure, data-management solution that can encrypt all user data stored on a DD series deduplication storage appliance. It protects user data from theft or loss of system, disk shelves, or disks, or for disks returned to factory. The DD series encryption software can help satisfy internal governance rules and helps with meeting compliance regulations.

DD Encryption helps meet compliance regulations by using industry standard AES- 128 or AES-256 encryption algorithms and the RSA BSAFE FIPS 140-2 validated cryptographic libraries. It also supports standard CBC and the stronger cipher mode GCM for additional security.

DD Encryption is transparent to all ingest protocols and backup or archiving applications, works with all DD series replication types.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage and data protection technical white papers and videos provide expertise that helps to ensure customer success with Dell EMC storage and data protection products.

A.1 Related resources

- Dell EMC PowerProtect DDOS Admin Guide
- Dell EMC DD OS Version 7.3 Administration Guide
- KMIP Integration Guide for DDOS
- DD_OS_7.3_KMIP_Integration_Guide