DELL EMC UNITY: DATA AT REST ENCRYPTION

A Detailed Review

ABSTRACT

This white paper explains the Data at Rest Encryption feature, which provides controller-based encryption of data stored on Dell EMC™ Unity storage systems to protect against unauthorized access to lost or stolen drives or system. The encryption technology as well as its implementation on Dell EMC Unity storage systems are discussed.

July, 2017

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.

Dell EMC believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

With data security concerns at an all-time high, it is no surprise companies continue to place a premium on ensuring sensitive data is protected from unauthorized access. Whether it is due to internal policies or external compliance, securing data continues to be a high priority for organizations of all sizes. Dell EMC Unity storage systems address these concerns through controller-based Data at Rest Encryption (D@RE), which encrypts stored data as it is written to disk. Whether drives are lost, stolen, or failed, unauthorized access is prevented by rendering the drive unreadable without the encryption key within the storage system. In addition to peace of mind, D@RE offers additional benefits including regulatory compliance, secure decommissioning, and the possibility to eliminate the need for physical drive shredding.

D@RE is enabled by license file on Dell EMC Unity storage systems, and, is designed to be largely invisible to administrative end users, requiring almost no effort to enable or manage. Enabling the feature or backing up the encryption keys externally takes just seconds, and redundant keystore backups stored on array ensures that user data is always as available as it is secure. Whether seeking to secure data as part of an internal security initiative, or to comply with government regulations, Dell EMC Unity D@RE ensure all user data is kept safe and secure against unauthorized disk access.

As of Dell EMC Unity OE version 4.2, the system supports external key management through use of the Key Management Interoperability Protocol (KMIP). This allows the system to offload an ignition key to an external key management application ensuring additional protection in case an entire system is lost or stolen whereby unauthorized access is prevented without the ignition key.

AUDIENCE

This white paper is intended for Dell EMC customers, partners, and employees who are interested in learning about the Data at Rest Encryption functionality for securing user data on Dell EMC Unity storage systems. It assumes the reader has general IT experience, including knowledge as a system or network administrator.

TERMINOLOGY

Background Zeroing – A background process that zeroes new drives when they are inserted into the system.

Controller-Based Encryption (CBE) – Encryption of data occurring within the SAS controller before being sent to disk.

Data at Rest Encryption (D@RE) – The process of encrypting data and protecting it against unauthorized access unless valid keys are provided. This prevents data from being accessed and provides a mechanism to quickly crypto-erase data.

Data Encryption Key (DEK) – A randomly generated key that is used to encrypt data on a disk. For Dell EMC Unity, there is a unique key for every bound drive.

Key Encryption Key (KEK) – A randomly generated key that encrypts (wraps) Data Encryption Keys to protect them as they travel from the Key Manager to the SAS controller. It is passed to the SAS controller at system start up and is protected by the KEK Wrapping Key. When external key management is enabled, the KEK acts as the ignition key and is migrated off the system to the remote key management server.

Key Management Interoperability Protocol (KMIP) – Developed and standardized by OASIS, a global nonprofit consortium for standards on security, KMIP is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server.

KEK Wrapping Key (KWK) – A randomly generated key that is generated and persisted to the SAS encryption module upon installation of a D@RE enabled license. It's used to wrap the KEK as it travels from the Key Manager to the SAS controller.

Keystore – An embedded and independently encrypted container which holds all D@RE encryption keys on the array.

Sanitization – The process of removing data from media to prevent it from being recovered.

SAS (Serial Attached SCSI) Controller – The device that manages the SAS bus that is connected to the drives. On Dell EMC Unity systems, this is embedded on the storage processor and on 12Gb/s SAS I/O Modules.

Solid State Drive (SSD) – A device that uses flash memory chips, instead of rotating platters, to store data. Also known as a Flash drive.

Scrubbing – The process of writing random data to unused space on drives or zeroing unbound drives to erase residual data from previous use.

Self-Encrypting Drive (SED) – A drive that has built-in electronics to encrypt all data before it is written to the storage medium, and decrypts the same data before it is read.

Storage Pool – A single repository of homogeneous or heterogeneous physical drives from which LUNs may be created.

Storage Processor (SP) – A hardware component that manages the system I/O between hosts and the drives.

Unisphere – The management interface for creating, managing, and monitoring Dell EMC Unity storage systems.

OVERVIEW

Dell EMC Unity Data at Rest Encryption (D@RE) protects against unauthorized access to lost, stolen, or failed drives by ensuring all sensitive user data on the system is encrypted as it is written to disk. It does this through hardware-based encryption modules located in the SAS controllers and 12Gb/s SAS IO modules which encrypt data as it is written to the backend drives, and decrypt data as it is retrieved from these drives. Because of the controller-based approach, Dell EMC Unity D@RE supports all drive types currently supported in Dell EMC Unity storage systems, and those that will be offered in the future. This offers an advantage over the self-encrypting drives offered by some other storage systems, which only exist in certain capacities, can be more expensive than regular drives, and must be qualified individually by storage vendors. Additionally, controller-based D@RE has minimal performance impact for typical mixed workloads, and no impact to other Dell EMC Unity data services due to the level at which the encryption is performed, which is after all data services have been applied.

For key generation and management, Dell EMC Unity D@RE by default uses an internal, fully-automated key manager. This key manager has several responsibilities including generating keys using RSA BSAFE®, storing keys in a secure keystore, monitoring drive status changes that result in key creating/deletion, and encryption of all data encryption keys prior to moving them within the array. For all encryption operations, Dell EMC Unity D@RE utilizes symmetric encryption and does not use public-key encryption (also known as asymmetric key encryption).Dell EMC Unity D@RE data security is achieved through the combined use of several encryption keys, which together ensure that neither the drives themselves, nor the keys which encrypt these drives, can be read by unauthorized parties finding themselves in possession of drives that have been removed from the storage system. The three types of encryption keys used are referred to as the Data Encryption Keys (DEK), Key Encryption Key (KEK), and Key Encryption Key Wrapping Key (KWK). Information about how data is encrypted and secured on the system using these keys is described below.

As of Dell EMC Unity OE version 4.2, the D@RE feature functionality has been extended to offer external key management as an additional security option. Utilizing external key management gives the additional benefit of preventing unauthorized access in the event where an entire Dell EMC Unity system including drives is lost or stolen.

DATA ENCRYPTION KEYS

A Data Encryption Key (DEK) is a 512-bit randomly generated key that is used to encrypt data on a particular drive. There is a unique DEK for each bound drive, which is created when that drive is bound, and deleted when that drive is unbound. New DEKs will be created through any method of binding drives to a private RAID group, such as creating or expanding a storage pool or FAST Cache. They will also be permanently deleted as a result of unbinding drives, such as when a storage pool or FAST Cache is deleted or FAST Cache is shrunk. Each time a drive is bound, an entirely new, unique key will be created. As an example, deleting and recreating a storage pool would generate a new DEK for each drive, distinct from the keys that existed prior to the pool being deleted, even if the same drives were used. Because DEKs are permanently deleted whenever drives are unbound, simply deleting storage pools and FAST Cache can be an effective method of rendering residual data unreadable, as the drives will never again be able to be decrypted without their corresponding DEKs. Similarly, if a thief succeeds in stealing an encrypted drive from a functioning system, they will be unable to read the drive’s contents because they do not possess the DEK stored securely on the Dell EMC Unity system.

Dell EMC Unity D@RE utilizes RSA BSAFE to randomly generate each unique DEK. Within the SAS controller, the DEK is used to encrypt/decrypt user data using 256-bit Advanced Encryption Standard (AES) algorithm with the XOR Encrypt XOR Tweakable Block Cipher with Ciphertext Stealing (XTS) mode of operation. XTS-AES is standardized by the Institute of Electrical and Electronics Engineers (IEEE) and the United States National Institute of Standards and Technology (NIST). Refer to IEEE P1619 and NIST SP 8000-38E for more information on XTS-AES. All DEKs are stored in a redundant encrypted keystore, which must be available in order to access encrypted data on the system.

KEY ENCRYPTION KEY

The Key Encryption Key (KEK) is a 256-bit randomly generated key created by RSA BSAFE and is used to wrap the DEKs at the time of DEK generation so that the DEKs are protected and secured as they move through the storage system, such as to the SAS controller. The wrapped KEK is transferred to the SAS controller, where it is unwrapped with the KWK, and is subsequently used to unwrap DEKs. The algorithm used to wrap and unwrap the DEKs using the KEK is 256-bit AES Key Wrap, as specified in RFC 3394.

KEY ENCRYPTION KEY WRAPPING KEY

The Key Encryption Key Wrapping Key (KWK) is a 256-bit randomly generated key created by RSA BSAFE and is used to wrap the KEK at the time of generation so that the KEK is protected as it travels throughout the array and to the SAS controller. The KWK is persisted in the SAS controller and is used to decrypt the KEK when it arrives at the SAS controller. The algorithm used to wrap and unwrap the KEK using the KWK is 256-bit AES Key Wrap, as specified in RFC 3394.

M.2 SATA ENCRYPTION

An M.2 SSD device is located inside each storage processor and serves as a backup device in the event of an SP failure. In the event of a power failure, the memory contents of the SP's cache is written to the M.2 SSD device so it can be recovered once the SP is restored. The M.2 SSD device also holds a copy of the boot image that is used to boot the operating environment, as well as other private system space. Because sensitive user data may exist on this device, it must be encrypted as with the backend hard drives. However because this device resides within the storage processor and is not attached to the SAS controller, is requires a different encryption method to be used. To meet the requirement of encrypting all sensitive user data, including that which is vaulted to the M.2, this device utilizes Linux's native XTS-AES capable dm-crypt functionality for data at rest encryption. Because the M.2 device is encrypted differently, it is encrypted by default on all arrays, even those where a Data at Rest Encryption capable license has not been installed. For countries with cryptographic import restrictions, it is possible to order Dell EMC Unity systems with the M.2 encryption factory-disabled, in which case the Data at Rest Encryption feature will not be available to be enabled.

FIPS 140-2 VALIDATION

D@RE leverages RSA BSAFE, a FIPS 140-2 compliant cryptographic library, for D@RE operations including key generation, hashing, and random number generation. Dell EMC Unity's controller-based D@RE has been FIPS-140-2 validated by the NIST Cryptographic Module Validation Program (CMVP). Certificate number is #2912.

EXTERNAL KEY MANAGEMENT

In Dell EMC Unity OE version 4.2 and later, the system offers the ability to enable external key management via KMIP and through supported key management vendors' applications. Using an external key management solution allows the system to migrate an ignition key to an off-array application. The offloaded ignition key will then act as the boot key which is required upon system initial boot or reboot.

Once the key management server information like username, password, and port is configured including certificates, and once KMIP is enabled, a cryptographic ignition key is sent to the key management server from the system. Upon system initial boot, the system will look for the configured key management server and request the ignition key to boot successfully. If the KMIP server is available and the correct key is validated, the system will boot normally and continue operations as usual. If the KMIP server is not available or an incorrect key is provided, the system will boot into Service Mode which means no access to user data and requires user interaction to troubleshoot any incorrect configurations. In this mode, the system cannot return to Normal Mode until the issue is resolved. During troubleshooting, users can utilize the "svc_kmip" service commands to upload updated server information and certificates in cases where a new server needs to be configured for successful retrieval of the ignition key. Note that if the ignition key is lost, there will be no way to recover the system. Therefore, it is highly recommended to both back up the keystore file when any changes are made to drive configuration as well as create a separate secured copy of the ignition key using the KMIP server solution.

Having an external key management server ensures the overall system is protected in the case where it is stolen or lost. For example, if a system is powered off and being transported from one datacenter to another datacenter, user data will not be accessible even if powered on unless there is system access to the configured KMIP server with the correct ignition key. Therefore this extends the protection of user data from a drives perspective with D@RE to the entire system perspective when utilizing external key management.

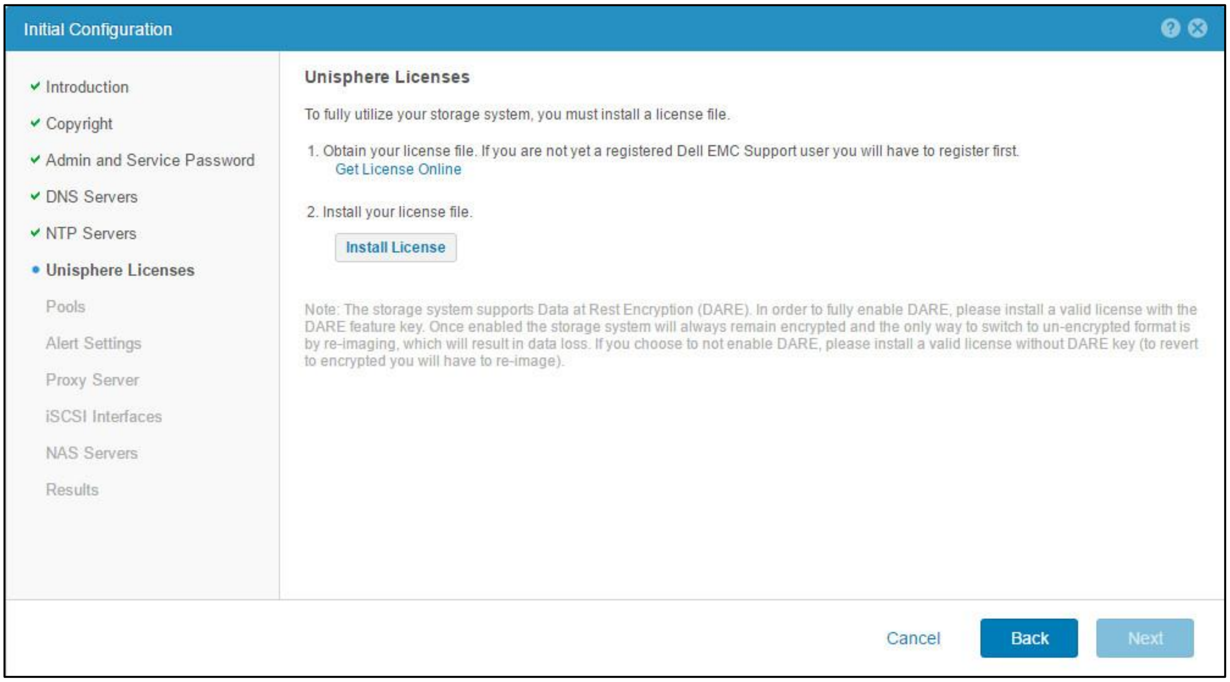
For a list of supported key management vendors, please see the Dell EMC Unity Simple Support Matrix on Dell EMC Online Support.

ENCRYPTION PROCEDURES

Dell EMC Unity D@RE is designed to be largely automated and requires very little management by administrators. While D@RE administration is extremely light, several D@RE-related tasks can be performed, including enabling D@RE, external keystore backup, and keystore restoration.

ENABLING D@RE

D@RE is included by default on Dell EMC Unity arrays and included in the license file unless otherwise requested during ordering. Therefore, all that is needed to activate D@RE is to install the D@RE enabled license file. The license installation process is not specific to D@RE, and is required to be performed before using the array. When logging into Unisphere for the first time, license installation appears as a step of the Unisphere Initial Configuration Wizard, prompting the administrator to install the license file obtained from Dell EMC. If this license file includes D@RE functionality, D@RE will be enabled once the license file is installed successfully. Encryption is either completely enabled or completely disabled at a system level; there is no ability to partially encrypt the system, such as specific drives, pools, or LUNs. Once the encryption enabled license is installed, the entire system will be encrypted.



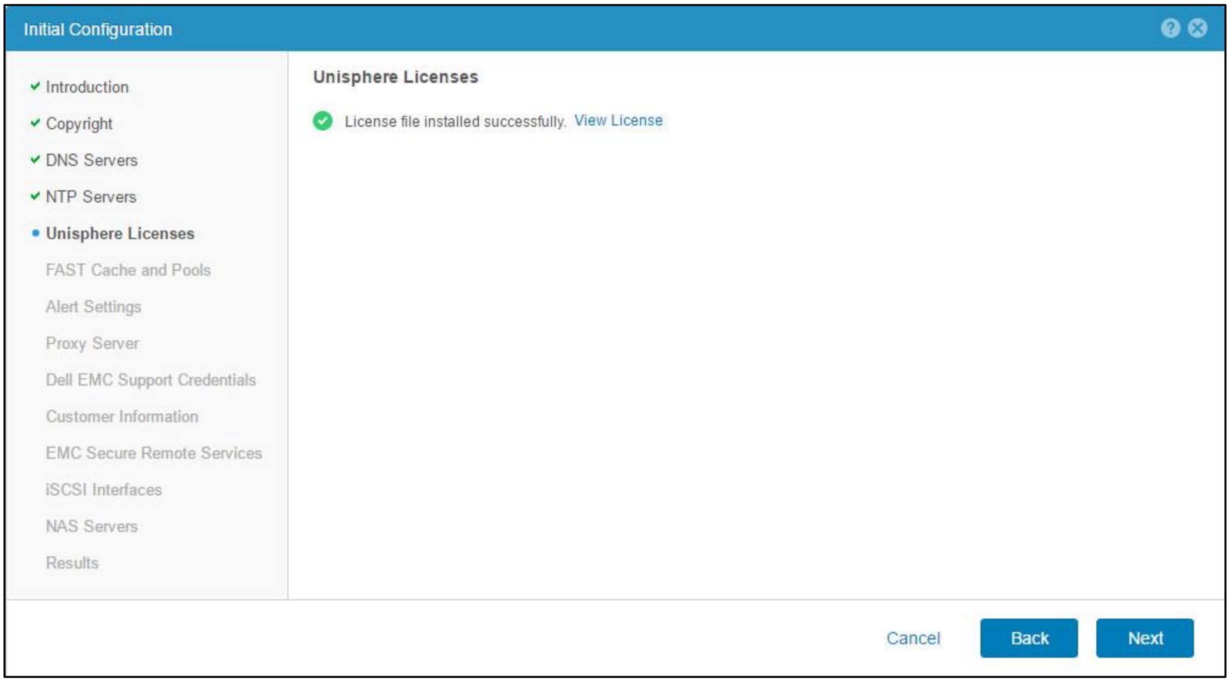
Unisphere Licenses

To fully utilize your storage system, you must install a license file.

1. Obtain your license file. If you are not yet a registered Dell EMC Support user you will have to register first.
   Get License Online
2. Install your license file.
   Install License

Note: The storage system supports Data at Rest Encryption (DARE). In order to fully enable DARE, please install a valid license with the DARE feature key. Once enabled the storage system will always remain encrypted and the only way to switch to un-encrypted format is by re-imaging, which will result in data loss. If you choose to not enable DARE, please install a valid license without DARE key (to revert to encrypted you will have to re-image).

Figure 1 - Installing License

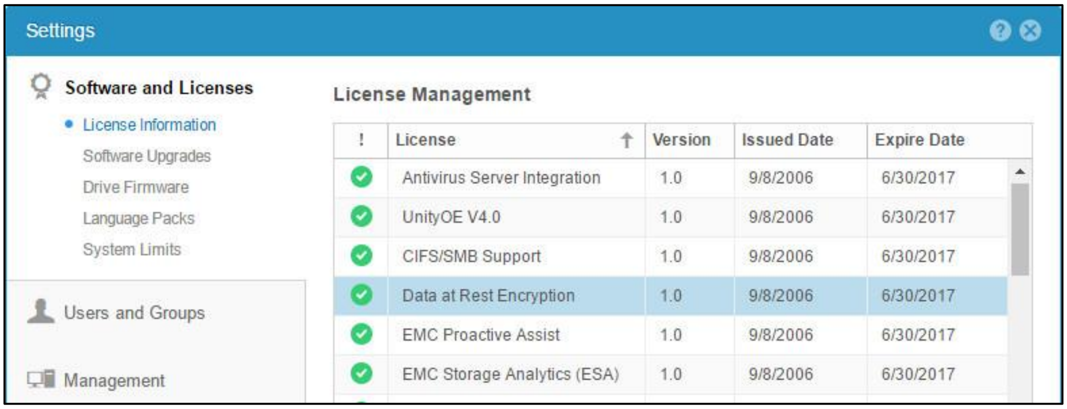


Unisphere Licenses

✓ License file installed successfully. View License

Figure 2 - Installed License

It is important to note that installing the license on the array is the point of no return with regard to D@RE activation. If the license file includes D@RE, D@RE will be permanently enabled on the system and cannot be disabled in the future. Similarly, if the license file does not include D@RE, D@RE will be permanently disabled on the system and cannot be enabled in the future. Dell EMC Unity D@RE can only be enabled at the time of initial installation, and does not support enabling encryption on non-D@RE enabled systems at a later time. Once the license has been installed successfully, the D@RE feature will appear as licensed, which can be verified from within the Unisphere Initial Configuration Wizard or from the Licenses page. If a license file without D@RE functionality was installed, D@RE will be permanently disabled and will not appear on the Licenses page.

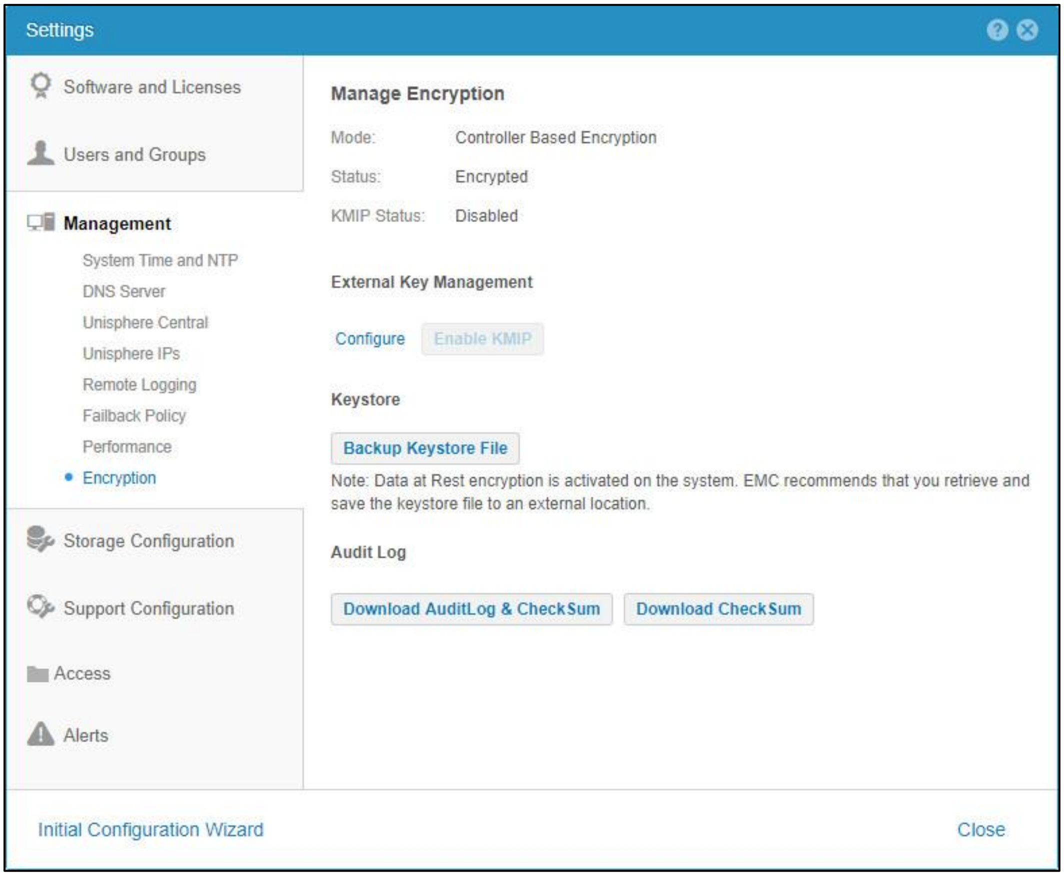


License Management

!	License	Version	Issued Date	Expire Date
✓	Antivirus Server Integration	1.0	9/8/2006	6/30/2017
✓	UnityOE V4.0	1.0	9/8/2006	6/30/2017
✓	CIFS/SMB Support	1.0	9/8/2006	6/30/2017
✓	Data at Rest Encryption	1.0	9/8/2006	6/30/2017
✓	EMC Proactive Assist	1.0	9/8/2006	6/30/2017
✓	EMC Storage Analytics (ESA)	1.0	9/8/2006	6/30/2017

Figure 3 - Data at Rest Encryption License

Once D@RE is activated, the Scrubbing process will initiate, which will begin to overwrite all addressable space on the drives. All drives will be overwritten with zeroes in order to sanitize any potential residual data on the drives, for example, if the drives have previously been used in another array. This is essentially a background zeroing process which will complete when all drives have been zeroed, which may take a long time depending on the capacity and speed of the drives in the array. When the scrubbing process is complete, the encryption status on the Encryption page in Unisphere will change to “Encrypted”. Note that for SAS Flash 2 drives, unmap is used to scrub the drives rather than zeroing.



Manage Encryption

Mode: Controller Based Encryption

Status: Encrypted

KMIP Status: Disabled

External Key Management

Keystore

Note: Data at Rest encryption is activated on the system. EMC recommends that you retrieve and save the keystore file to an external location.

Audit Log

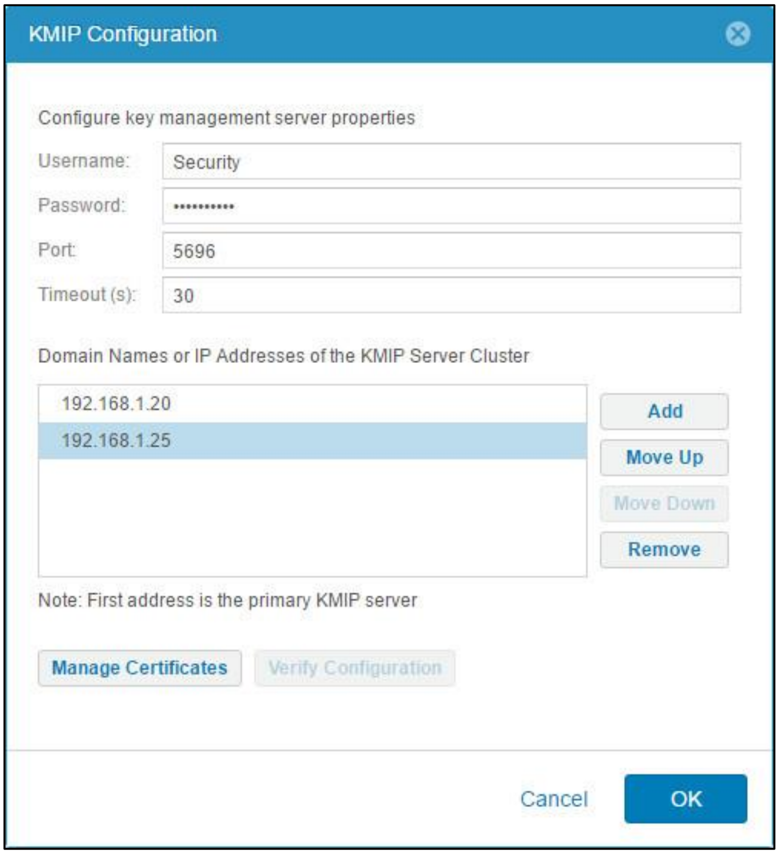
Figure 4 - Data at Rest Encryption Page

Note that the scrubbing process is only concerned with sanitizing preexisting unencrypted addressable space on the drives, and any user data written to the storage array will still be encrypted inline while this process in ongoing. The array is protected and available to create pools and store data securely as soon as the D@RE feature is enabled. Also note that the scrubbing process does not sanitize non-addressable drive space which may contain hidden residual data if the drives were used previously. This data is not readily retrievable through standard interfaces, but may be accessible through advanced laboratory techniques. If potential access to data remnants from previous use of a drive violates your company's security policy, the drive must be independently sanitized prior to being used in an encrypted Dell EMC Unity storage system. Scrubbing also does not perform multiple overwrites of residual data. If this is a requirement, drives must be independently sanitized prior to being used in an encrypted Dell EMC Unity storage system.

ENABLING EXTERNAL KEY MANAGEMENT

Once D@RE is enabled, external key management can be configured and enabled (see Figure 5). In Unisphere, this status will be shown as "KMIP Status" (see Figure 7). To utilize external key management, a supported key management server vendor application must be deployed which will manage the ignition encryption key once configured and enabled properly. External key management does not need to be enabled at initial configuration of the system to be able to be used and can be enabled at a later time as needed. It can also be disabled if it had been already enabled to return key management back to the local system instead of the remote KMIP server. Note that enabling/disabling KMIP must be done when the system is in Normal mode and cannot be done in Service mode. To configure external key management, the following information will be needed:

- KMIP Server Username and Password
- KMIP Server IP(s) and Port
- KMIP Server Client Certificate and Certificate Authority (CA) Certificate (Figure 6)



KMIP Configuration

Configure key management server properties

Username: Security

Password: ••••••••••

Port: 5696

Timeout (s): 30

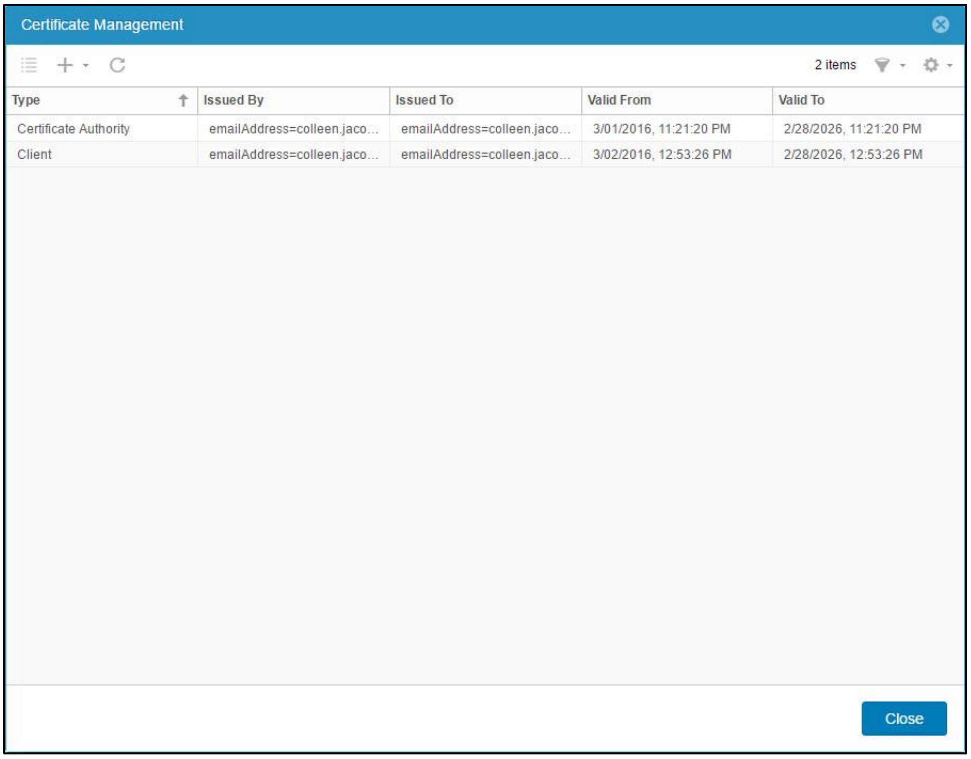
Domain Names or IP Addresses of the KMIP Server Cluster

192.168.1.20

192.168.1.25

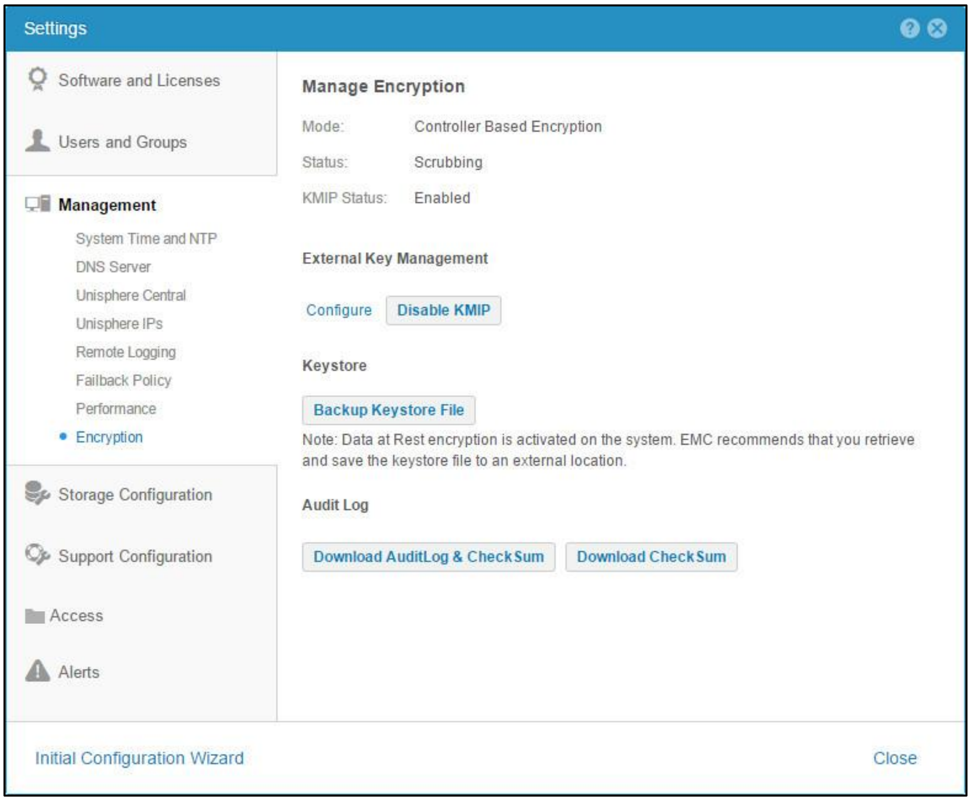
Note: First address is the primary KMIP server

Figure 5 - KMIP Configuration



Type	Issued By	Issued To	Valid From	Valid To
Certificate Authority	emailAddress=colleen.jaco...	emailAddress=colleen.jaco...	3/01/2016, 11:21:20 PM	2/28/2026, 11:21:20 PM
Client	emailAddress=colleen.jaco...	emailAddress=colleen.jaco...	3/02/2016, 12:53:26 PM	2/28/2026, 12:53:26 PM

Figure 6 - Certificate Management



Manage Encryption

Mode: Controller Based Encryption

Status: Scrubbing

KMIP Status: Enabled

External Key Management

Keystore

Note: Data at Rest encryption is activated on the system. EMC recommends that you retrieve and save the keystore file to an external location.

Audit Log

Figure 7 - Enabled KMIP (External Key Management)

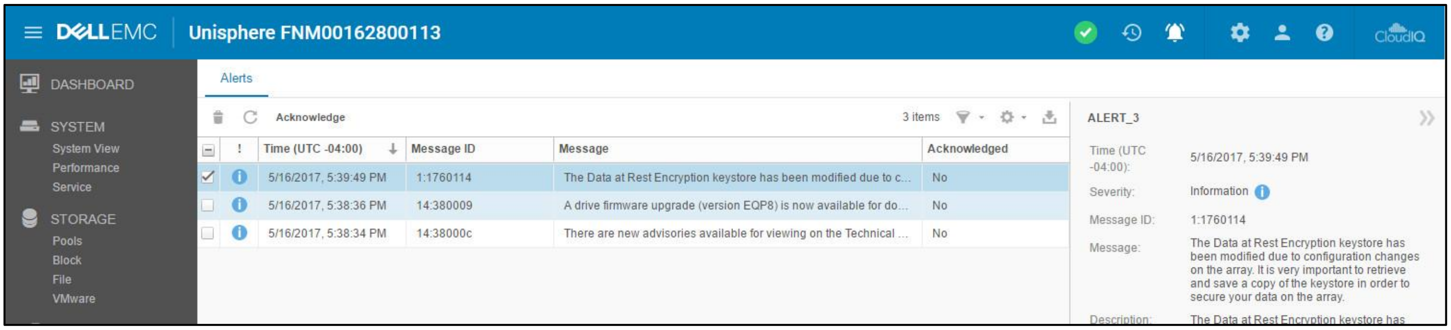
Note: In case of IBM’s SKLM key management solution, the username and password may not be mandatory for configuration. Instead, the system serial number needs to be used in the username field with a null value for the password field.

KEYSTORE BACKUP

All DEKs are stored in an encrypted keystore which is stored redundantly on the system drives as well as the M.2 flash device within each storage processor. Because the keystore contains the DEKs required to decrypt the drives, data will be unavailable in the unlikely event the keystore becomes inaccessible. As Dell EMC does not retain copies of customers' keystores, it is recommended to back up the keystore externally. Administrators can back up the keystore externally from Unisphere, CLI, or RESTful API, allowing it to be recovered in the unlikely event that all keystore copies on the system become corrupted or otherwise unavailable. As the keystore contains all DEKs for the system, and DEKs are created and deleted as drives are bound and unbound, the keystore will change whenever any operation occurs which causes a drive to be bound or unbound. As a result, Dell EMC recommends backing up the keystore externally when such a change is made to the system, including:

- Creating or deleting a storage pool
- Expanding a storage pool
- Creating or deleting FAST Cache
- Expanding or shrinking FAST Cache
- Hot Sparing

When the keystore is altered as a result of a drive configuration change, an informational alert is generated in Unisphere informing the administrator that the keystore has been changed and should be backed up externally. Backing up the keystore can be performed through the Unisphere GUI, CLI, or RESTful API. In Unisphere, the keystore can be backed up externally from the Encryption page by clicking the Backup Keystore File button. This will download the encrypted keystore .lbb file to the client computer accessing Unisphere, from which the file may then be transferred to the desired secure external location.



☐	!	Time (UTC -04:00)	Message ID	Message	Acknowledged
☑	ⓘ	5/16/2017, 5:39:49 PM	1:1760114	The Data at Rest Encryption keystore has been modified due to c...	No
☐	ⓘ	5/16/2017, 5:38:36 PM	14:380009	A drive firmware upgrade (version EQP8) is now available for do...	No
☐	ⓘ	5/16/2017, 5:38:34 PM	14:38000c	There are new advisories available for viewing on the Technical ...	No

ALERT_3

Time (UTC -04:00): 5/16/2017, 5:39:49 PM

Severity: Information ⓘ

Message ID: 1:1760114

Message: The Data at Rest Encryption keystore has been modified due to configuration changes on the array. It is very important to retrieve and save a copy of the keystore in order to secure your data on the array.

Description: The Data at Rest Encryption keystore has

Figure 8 - Keystore Backup Alert

KEYSTORE RESTORATION

In the unlikely event all redundant keystore copies stored securely on array become corrupted or otherwise unavailable, the external keystore backup file can be used to restore access to the data. In this case the storage system will boot into a protective service mode, after which the keystore can be restored by running a CLI service script via SSH or Serial over LAN. To do this, copy the manually backed up file to the storage processor, then run the `svc_restore_keys –p <keystore backup filename>` command to restore the keystore to the system. Afterward reboot the storage system out of service mode.

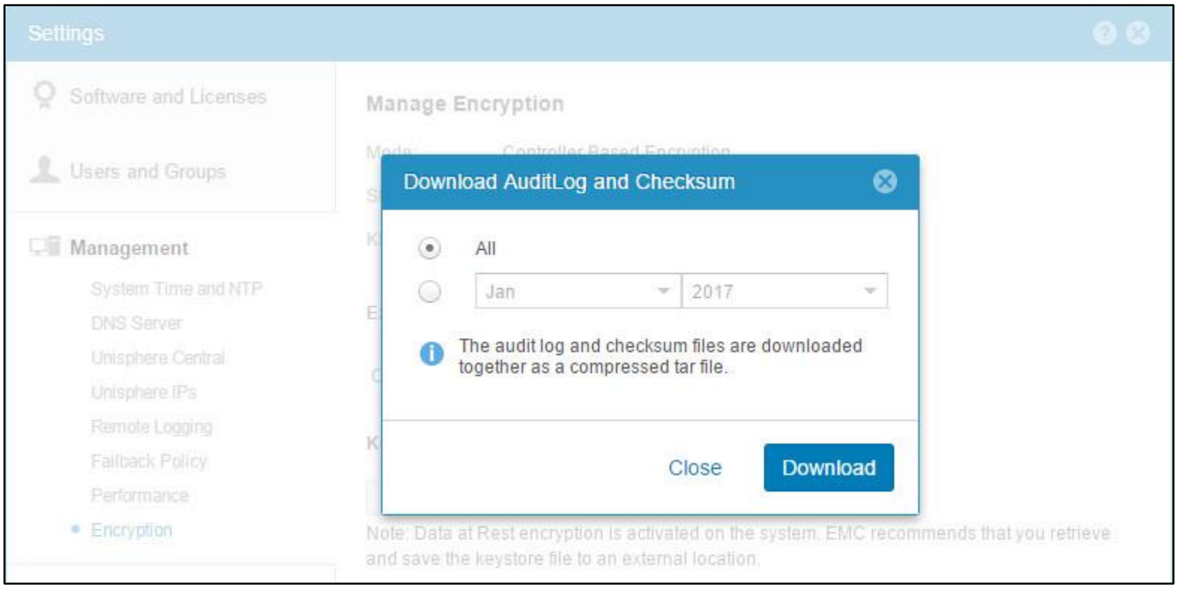
AUDIT LOG AND CHECKSUM RETRIEVAL

Dell EMC Unity also maintains an audit log as part of the D@RE feature, which supports logging of the following keystore operations:

- Feature activation
- Key creation
- Key deletion

- Keystore backup
- Disk encryption completion
- I/O module addition

The audit log can be downloaded along with its corresponding checksum information from the Encryption page in Unisphere. When downloading the audit log, the administrator has the ability to download the entire log, or a partial log for a specific month and year. The checksum can also be downloaded from the system independently from the audit log file by specifying the name of the audit log file for which to download the corresponding checksum file. In this case, the filename specified must match exactly to the filename of the audit log retrieved previously.



● All

○ Jan 2017

The audit log and checksum files are downloaded together as a compressed tar file.

Note: Data at Rest encryption is activated on the system. EMC recommends that you retrieve and save the keystore file to an external location.

Figure 9 - Download Audit Log and Checksum

CONSIDERATIONS

While D@RE protects the storage system data from unauthorized access in many cases, including drive theft or loss, it does not protect against all types of security breaches. Due to the nature of D@RE, there are some scenarios, outside of the protection of data at rest, which must be secured through other means. Also, because of the feature’s relationship with the storage software and hardware, there are additional considerations that users wishing to implement D@RE should be aware of. These considerations are discussed in this section.

HARDWARE REPLACEMENTS

The keystore discussed previously is tied to the storage processors, so care must be taken when performing service operations in order to preserve the encryption keys. In the event that the chassis and both storage processors need to be replaced, both storage processors should not be replaced at the same time. Instead, the chassis replacement should be followed while retaining one SP until the array is back online before replacing the second SP. In the case that storage processors have already been replaced at the same time and the keystore was lost, the keystore may be restored from an external backup.

DATA IN FLIGHT

As discussed previously, the Data at Rest Encryption feature encrypts and decrypts data as it passes the SAS controller level. Data is only protected when it is at REST, stored on the backend drives or the internal M.2 SATA device. Therefore, data in flight to external hosts is not protected by the Data at Rest Encryption feature as it travels throughout the network. In order to protect data at this level, an external form of data in flight encryption must be used such as SMB protocol encryption or host-based encryption software. It should also be understood that, while D@RE protects against unauthorized access to drives removed from the system. With the Dell EMC Unity OE version 4.2 or later, the D@RE feature functionality has been extended to offer external key management as an additional security option. Utilizing external key management gives the additional benefit of preventing unauthorized access in the event where an entire Dell EMC Unity system including drives is lost or stolen.

PERFORMANCE & CAPACITY

Under normal operating conditions, the encryption feature has little to no impact on I/O. By simply using encryption keys to encrypt and decrypt data as it passes the SAS controller, Dell EMC Unity Data at Rest Encryption provides a scalable solution that is not likely to negatively impact host I/O traffic. This is especially true for the typical mixed workloads for which D@RE was designed. These workloads are characterized as those containing a reasonable read/write I/O mix with smaller block sizes. For workloads such as these, D@RE usage exhibits little to no I/O impact, which equates to less than 5%. However, some additional performance impact may be seen on large block or high bandwidth workloads (256KB+) when approaching the limits of the array. Dell EMC recommends sizing storage systems for less than 100% CPU utilization. For more information, refer to the Dell EMC Unity: Best Practices Guide on Dell EMC Online Support.

There is no impact to capacity utilization when encryption is enabled. Data written in encrypted form consumes the same amount of space compared to unencrypted data. Data efficiency services, such as compression, are also applied prior to the data being encrypted. This enables capacity savings to be applied on the actual dataset, instead of the encrypted dataset, so there is no impact to space savings.

ENCRYPTION CONVERSIONS

As mentioned earlier, Dell EMC Unity does not currently support the ability to modify an existing system from an unencrypted to encrypted state. The encryption state of the system is set permanently when the license is first applied, and cannot be changed in either direction afterward.

CONCLUSION

With ever increasing concerns over data security, storage systems need to offer the ability to secure data for peace of mind, compliance, and general security use cases faced by companies of all types. Whether drives or full systems are lost, stolen, or failed, unauthorized parties must not be able to compromise an organization’s security by gaining access to the sensitive data under any circumstances.

Dell EMC Unity Data at Rest Encryption ensures that all sensitive user data stored on array is encrypted when being written to disk, so that private data does not fall into the wrong hands. And in using external key management, data is further protected even if the system along with the drives are taken by unauthorized parties. With simple activation, management, and auditing functionality, D@RE is a powerful tool to protect user data, regardless of the organization’s size, industry, or use case. As a result, organizations can rest assured that their data is always safe and secure when stored on a Dell EMC Unity storage system.

REFERENCES

For additional information regarding any of the topics covered in this white paper, refer to the following resources available on Dell EMC Online Support:

- **Dell EMC Unity: FAST Technology Overview White Paper**
- **Dell EMC Unity: Introduction to the Platform White Paper**
- **Dell EMC Unity: Unisphere Overview White Paper**

For additional information on encryption and compliance, refer to the following documents available online:

- **IEEE P1619 – Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices**
- **NIST SP 800-88 – Guidelines for Media Sanitization**
- **NIST SP 800-38E – Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices**
- **RFC 3394 – Advanced Encryption Standard (AES) Key Wrap Algorithm**