DELL Technologies

Technical White Paper

# Dell EMC PowerMax: End-to-End Efficient Encryption


## Abstract

This document describes how Dell EMC™ PowerMax end-to-end encryption protects data confidentiality by encrypting data from the application host.



September 2020

# Revisions

| Date | Description |
|---|---|
| September 2020 | Initial release: PowerMaxOS Q3 2020 |

# Acknowledgments

Author: Richard Pace

# Table of contents

# Executive summary

Securing sensitive data is one of the greatest challenges faced by organizations today. Increasing regulatory and legislative demands and the constantly changing threat landscape have brought data security to the forefront of IT issues.

Dell EMC™ PowerMax end-to-end efficient encryption addresses these challenges with two powerful capabilities:

- Increasing data security on the application host, combined with Data at Rest Encryption (D@RE) on the PowerMax array
- Providing maximum data reduction on the PowerMax array

End-to-end efficient encryption integrates PowerMax storage with Thales software to provide host-LUN encryption along with data reduction on the PowerMax system.

# 1 End-to-end efficient encryption

End-to-end efficient encryption increases data security by combining Thales host encryption with PowerMax back-end Data at Rest Encryption (D@RE). This combination protects information from any unauthorized access, whether in flight or at rest on hard drives. End-to-end efficient encryption uses industry-standard AES encryption technology.

End-to-end efficient encryption protects data while taking advantage of PowerMax space-saving data reduction technology. Thales software encrypts and decrypts data that are written from the application host to the PowerMax array. PowerMax decrypts the data to process through the data reduction engine, and D@RE re-encrypts the data.

## 1.1 End-to-end encryption architecture

PowerMaxOS and Thales software work together to encrypt data from the application host without sacrificing the space-saving efficiency of data reduction.

Here is a summary of the encryption process:

1. Thales VTE software encrypts data when written from the host application.
2. Encrypted data arrives at the PowerMax in system cache.
3. Data is decrypted using an additional I/O module that is installed.
4. The PowerMax array applies the data reduction process to the data.
5. The data is re-encrypted using back-end D@RE encryption before it is written to storage.

Figure 1 shows the architecture for end-to-end encryption with a PowerMax system.

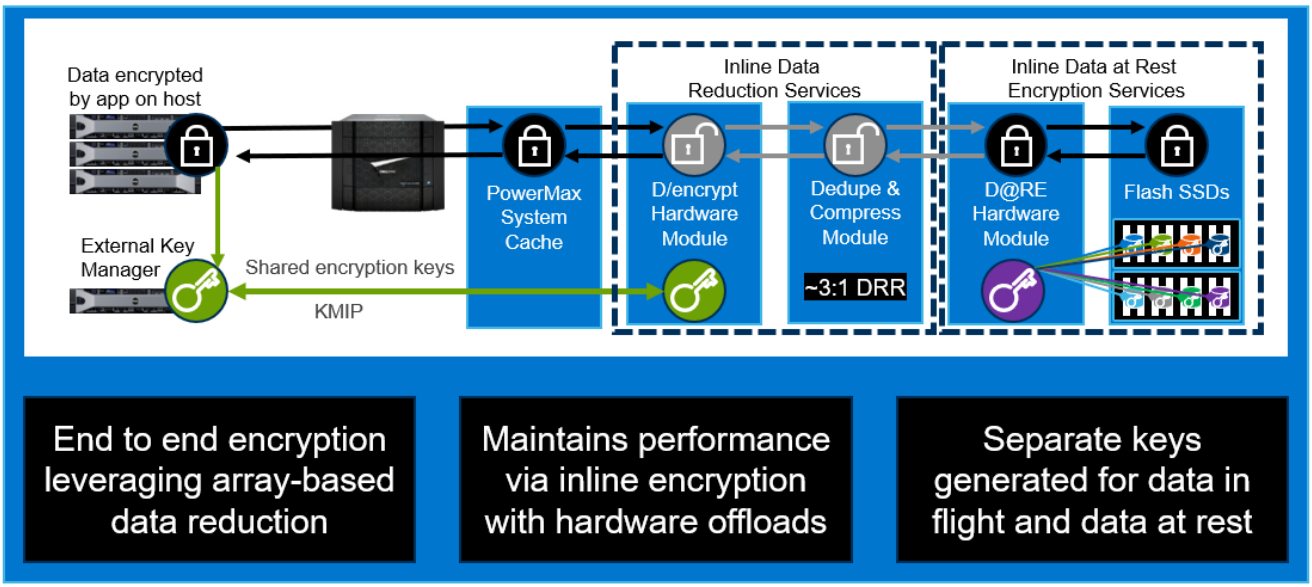



Figure 1 Efficient data-encryption architecture

## 1.2 Terminology

**PowerMaxOS**: The PowerMax operating environment that runs on PowerMax and VMAX™ All Flash arrays.

**Management module control station (MMCS)**: Monitors the array environment, provides remote notification and remote support capabilities, and allows authorized Dell Technologies personnel to access the array locally or remotely.

**Key Management Interoperability Protocol (KMIP):** OASIS protocol used between encryption-capable applications (for example, PowerMax and VMAX D@RE) and key-manager servers to obtain and manage the keys that the encryption processes use.

**Public Key Infrastructure (PKI):** A set of roles, policies, and procedures to manage digital certificates and public key encryption.

**Certificate Authority (CA):** Entity that issues digital certificates.

**AES Algorithm:** Advanced Encryption Standard (AES) algorithm.

**Hash-based Message Authentication Code (HMAC):** Used to sign I/O module firmware to check integrity of cryptographic operations.

**Key Trust Platform (KTP):** This component resides on the MMCS and communicates using the OASIS KMIP with the key manager to manage encryption keys. The component is also called the KMIP client.

**Vormetric Data Security Manager (DSM):** Thales™ key manager that is available in hardware and virtual versions.

**Cluster**: Multiple DSM VMs or appliances sharing configuration settings and encryption keys. Configuration and key life-cycle changes made to one cluster node are replicated to all members within the same cluster.

**Vormetric Transparent Encryption (VTE):** Thales agent or driver which runs on the application host.

**Guarded device:** Host device that is encrypted by Thales VTE.

# 2 Efficient encryption with PowerMax

PowerMax and Thales integrate to provide an end-to-end encryption solution. PowerMax uses its existing D@RE solution to provide back-end encryption, and Thales provides two external components for encryption at the application host:

- Data Security Manager (DSM)
  - Provides centralized management of policies and keys
  - Communicates with KMIP communication protocol that resides on the PowerMax MMCS
  - Is deployed either as a virtual or hardware-based appliance
- Vormetric Transparent Encryption (VTE)
  - Host-based agent which encrypts user data before sending it to the array
  - Coordinates with DSM for management of encryption keys

In addition to the Thales external components, the requirements for PowerMax are as follows:

- D@RE must be enabled on the PowerMax array at initialization
- An additional encryption-capable I/O module must be installed in each director of the PowerMax array

## 2.1 Prerequisites for deployment

The following prerequisites are required before deploying end-to-end efficient encryption with PowerMax.

- IPv4 network connectivity between PowerMax and all DSM appliances
- Static IP assignments for all DSM-appliance network interfaces that connect to the PowerMax array
- PKI infrastructure and internal or external Certificate Authority
  - Self-signed certificates are not recommended for production
- Both DSM and VTE running an approved version of software releases

## 2.2 Configuring DSM and VTE

Before integration with PowerMax, you must deploy both Thales DSM key manager and VTE host-based software.

For installation and configuration information, see the Dell EMC PowerMax End-to-End Encryption Deployment Guide.

## 2.3 Data at Rest Encryption

End-to-end efficient encryption uses Data at Rest Encryption (D@RE) for the on-array back-end at rest encryption. You must add D@RE at the initial array installation and configure it to use embedded key management. The embedded key manager with D@RE provides encryption for all data written to the system and requires little to no management after installation.

For more information about D@RE, see the document Dell EMC PowerMax and VMAX All Flash: Data at Rest Encryption.

## 2.4 Enabling the PowerMax array

You must enable the PowerMax array before using end-to-end efficient encryption. Enabling the PowerMax is done when both the additional I/O module is installed in each director and the MMCS is registered with the DSM.

### 2.4.1 Encryption I/O module

To use end-to-end efficient encryption, you must add the encryption I/O modules to the PowerMax system. The encryption I/O modules are necessary to encrypt and decrypt data in cache when the application host reads from or writes to the system. This addition allows the system to take advantage of the space-saving data-reduction features.

When you order a PowerMax system with end-to-end efficient encryption, it is delivered with the additional I/O modules installed and configured. You can add end-to-end efficient encryption to an existing D@RE-enabled PowerMax system as an upgrade. The upgrade requirements are as follows:

- Add one encryption I/O module per director, inserted in any available front-end slot (2, 3, 8, or 9)
- Change the system BIN file
  - Change the **Hbe_capable_system** flag to **YES**
  - The BIN file must reflect the addition of the new I/O modules
- No ports must be configured

Figure 2 Encryption I/O module slots

**Note**: If you are adding an engine to an existing PowerMax system and also adding end-to-end efficient encryption, you must add the engine first. Once you add the engine, you must perform an online configuration change to satisfy the requirements listed previously.

### 2.4.2 Registering the MMCS and DSM

Registering the MMCS and DSM together establishes communication. Communication between both components uses the KMIP communication protocol that resides on the MMCS to communicate with the DSM. The DSM acts as an external key manager for the encryption at the host applications. When an encryption policy is set for a volume, keys are generated and shared with the MMCS for decryption when the data is in cache.

After the MMCS and DSM are registered, the PowerMax system is in the Encryption Enabled state. See Figure 3 and Figure 4.

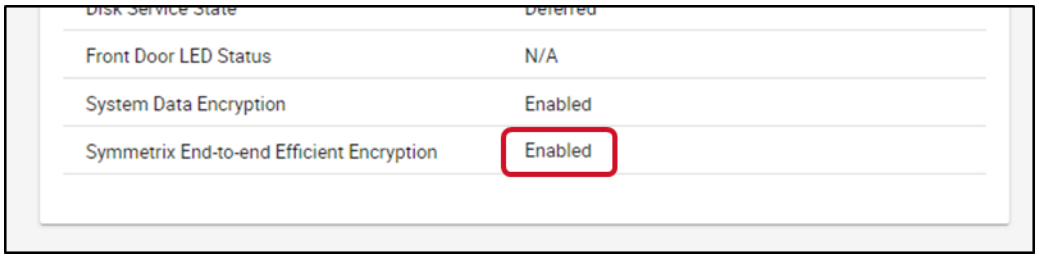



Figure 3 System set as Enabled in Unisphere System Properties

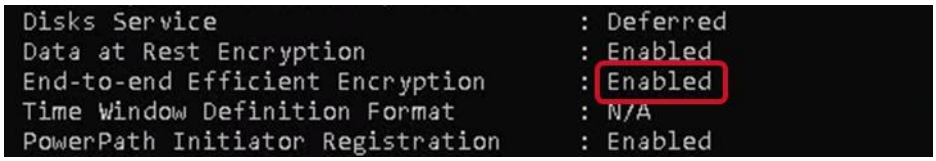



Figure 4 System set as Enabled in Solutions Enabler (symcfg list -v)

**Note**: Registering the MMCS and DSM is a field-support activity that must be performed by Dell Technologies personnel.

## 2.5 Encrypting a volume

Efficient encryption from the host using Thales is set per volume. You can set encryption on a subset of volumes, and not all volumes are required to participate in end-to-end efficient encryption. Encryption on the back-end with D@RE encrypts all data, regardless if it set for efficient encryption or not.

You can encrypt a volume in two steps, which are described in the following subsections:

- Create an encryption-capable volume
- Guard a volume

### 2.5.1 Creating an encryption-capable volume

The encryption capable attribute identifies volumes that participate in encryption from the host and benefit from the PowerMax data reduction capabilities. You cannot add the attribute to an existing volume or remove it after a volume is created. A volume that is created with the encryption-capable attribute does not automatically encrypt the host data, and it must go through the encryption process. If a capable volume is to be encrypted, it must be guarded.

You can set a volume as encryption capable when creating a volume using one of the following methods:

- Solutions Enabler: Add the option **-eff_encrypt_capable** (Figure 5).
- Unisphere: Apply the setting under the **Advanced** tab (Figure 6).

```
symdev -sid 626 create -tdev -emulation fba -cap 10000 -captype mb -n 1 -eff_encrypt_capable -v

Execute a create devices operation (y/[n]) ? y
STARTING a TDEV Create Device operation on Symm 000197600626.
Wait for device create.............................Started.
Wait for device create.............................Done.
     The TDEV Create Device operation SUCCESSFULLY COMPLETED: 1 devices created.
1 TDEVs create requested in request 1 and devices created are 1[ 00050 ]

Create devices operation succeeded.
```

Figure 5 Creating a volume through Solutions Enabler with the **-eff_encrypt_capable** option

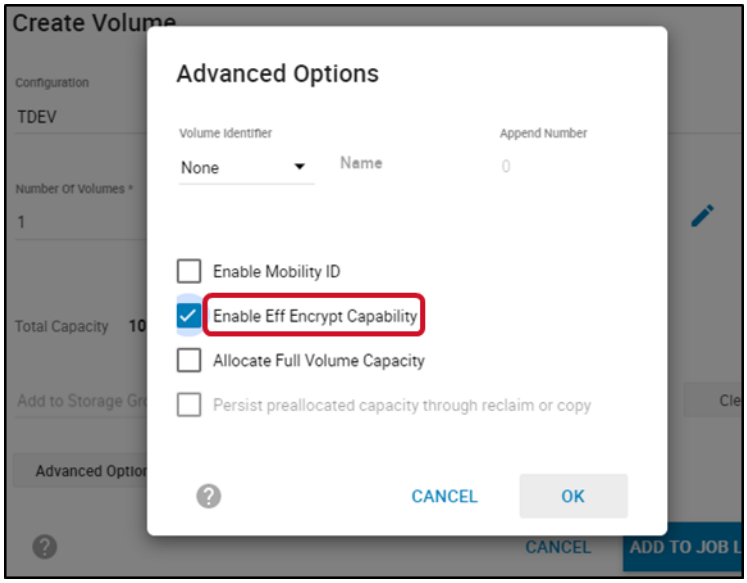



Figure 6 Creating an encryption-capable volume through Unisphere

After you create a volume, the volume properties reflect it as encryption capable (see Figure 7 and Figure 8).

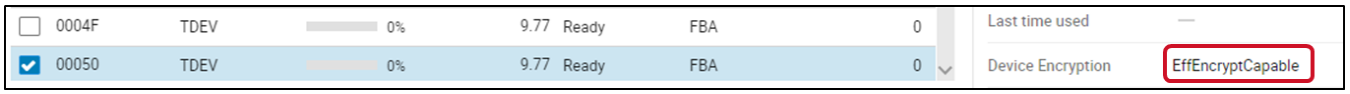



Figure 7 Viewing volume properties using Unisphere

```
Vendor ID                  : EMC
Product ID                 : SYMMETRIX
Product Revision           : 5978
Device WWN                 : 60000970000197600626533030303530
Device ID Type             : Compatibility
Device Emulation Type      : FBA
Device Encryption          : EffEncryptCapable
```

Figure 8 Viewing volume properties using Solutions Enabler > **symdev show** command

### 2.5.2 Guarding a volume

Guarding an encryption-capable volume activates encryption for all I/O to that volume from the host application. Guarding a capable volume encrypts all new data and does not encrypt any data that had previously been written to that volume.

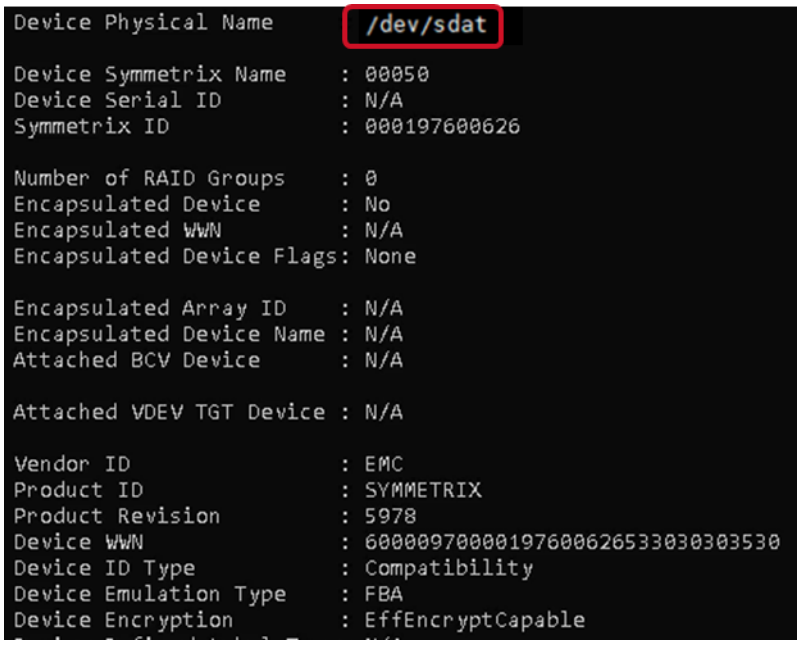
Guarding a volume requires the following configuration:

- VTE enabled host
- Access to set policy on the DSM

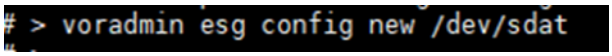
For more information about guarding a volume, see the *Thales Data Security Manager, DSM Administration Guide for DSM release* and *Thales VTE Agent Installation and configuration Guide for VTE release*.

The following is an example of the process for guarding a volume.

1. Use the **symdev show** command to show the volume physical name (Figure 9).




2. From the VTE enabled host, enter the VTE-specific command **voradmin esg config new <volume_physical_name>** to prepare the volume to be encrypted.

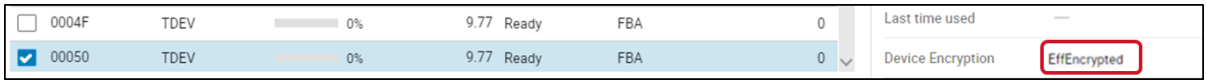



3. DSM sets the encryption policy, and the volume path is identified using the volume physical name. Check the **Efficient Storage Device** option in DSM.


4. Guard the volume with the VTE command **secfsd -guard <volume_physical_name>.**

```
# > secfsd -guard /dev/sdat
secfsd: Path is guarded
```

5. Once the policy is set and the volume is guarded, DSM and PowerMax generate and share encryption keys (see 0).
6. The volume properties from Unisphere and Solutions Enabler reflect the new encryption status.




```
Vendor ID                  : EMC
Product ID                 : SYMMETRIX
Product Revision           : 5978
Device WWN                 : 60000970000197600626533030303530
Device ID Type             : Compatibility
Device Emulation Type      : FBA
Device Encryption          : EffEncrypted
```

# 3 Requirements, limitations, and restrictions

The following list includes the requirements, limitations, and restrictions for PowerMax end-to-end efficient encryption.

- End-to-end efficient encryption is available only through a request for product qualification (RPQ).
- D@RE using only an internal key server is required.
- Installing one back-end I/O module in a front-end slot (2, 3, 8, 9) for each director is required.
- You must set the encryption capable setting upon device creation. This configuration cannot be set or removed from existing devices.
- Devices to be guarded must be in a storage group with compression enabled.
- Encryption-capable devices cannot be used with local or remote replication (SnapVX or SRDF).
- VMware® vSphere® Virtual Volumes™ (vVols) are not supported.
- VPLEX devices are not supported.
- Mixed CKD and FBA arrays are not supported.
- Thales rekey is not supported.

# 4 Conclusion

End-to-end efficient encryption prevents unauthorized access to sensitive data that is in flight from a host application, or data at rest within the PowerMax safe. This solution brings together encryption from Thales (using Vormetric transparent encryption with data security external key management) and PowerMax Data at Rest Encryption with easy-to-manage internal key management. Incorporating both encryption technologies allows you to take advantage of the space-saving data reduction while ensuring that all sensitive data is secure.

# 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 ensure customer success with Dell EMC storage and data protection products.

## A.1 Related documentation

See the following Dell Technologies and Thales publications for additional information.

- Dell EMC PowerMax End-to-End Efficient Encryption Deployment Guide
- Dell EMC PowerMax and VMAX All Flash: Data at Rest Encryption
- Dell EMC PowerMax: Data Reduction
- Dell EMC Solutions Enabler Array Controls and Management CLI user Guide
- Dell EMC Unisphere for PowerMax Product Guide
- Thales Data Security Manager, DSM Administration Guide for DSM release
- Thales VTE Agent Installation and Configuration Guide for VTE release