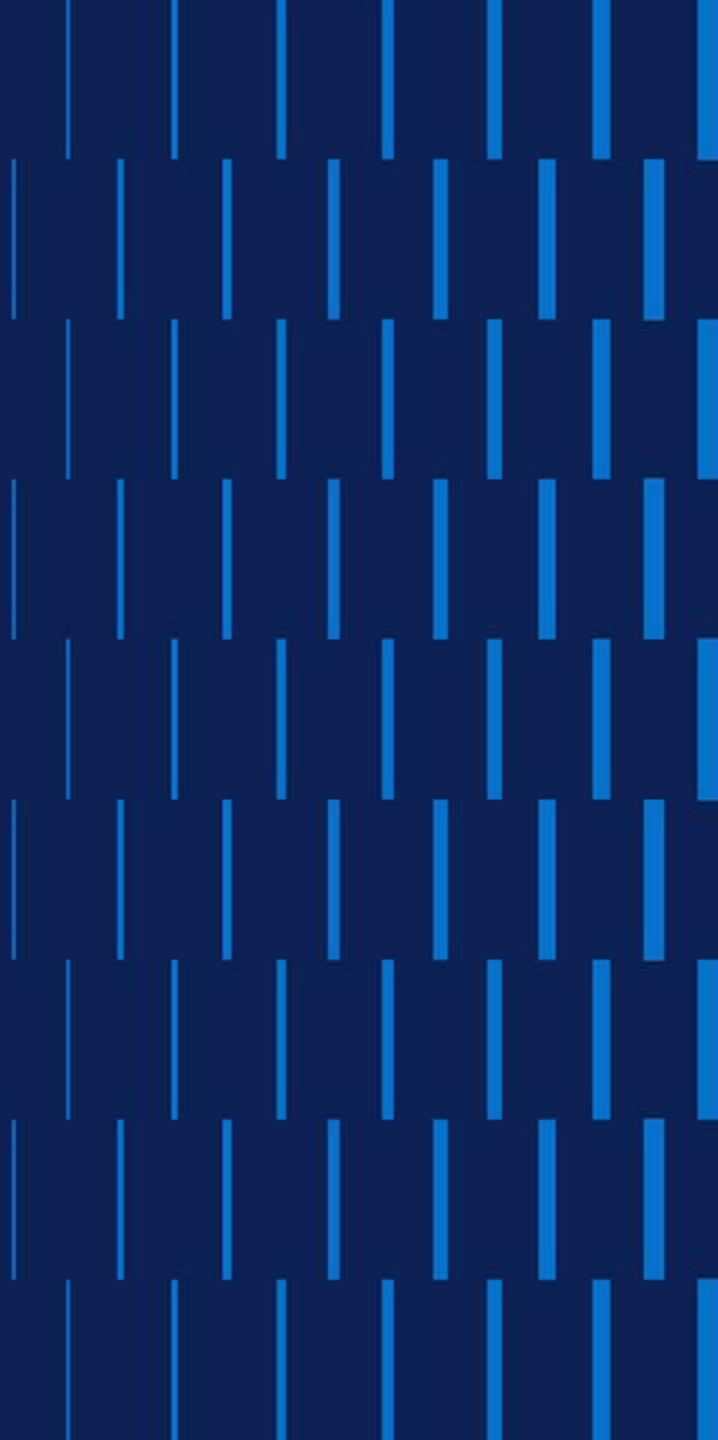


PowerVault ME5 Freya EKT



03/27/2025

Rina Binxhiu

Agenda

Introduction

ME5 to Freya Differences

Performance

New Features

- IDFU – Intelligent Drive Firmware Update

- KMIP

- Power Vault Manager Interface

Demo

Ali Elwakhi

ME5 MLK – Freya

- Freya is the ME5 Mid-Life kicker (MLK) targeted at the entry level SAN/DAS space where the ME5 Series currently resides. It comes with all-inclusive software, incredible performance, and the same management GUI as the ME5 has today. Aligned with PowerEdge servers, it supports the same connectivity as before (32Gb FC, 25Gb iSCSI SFP+/SFP28, 10 Gb iSCSI BaseT, 12Gb SAS). It offers Enterprise-Class Software Features such as Intelligent Drive FW Update and KMIP/MAS.

Current PowerVault ME5/Freya technical overview

Starting Configurations:					EBOD Expansion Enclosures ²						
					 ME5212 ¹ 2U-12 drives	 ME5224 ¹ 2U-24 drives	 ME5284 5U-84 drives	 ME512 2U-12 drives	 ME524 2U-24 drives	 ME584 5U-84 drives	
Max Raw Capacity	System	8PB	8PB	8PB ³	9 x 2U enclosures behind ME5012, ME5024 3 x 5U enclosures behind ME5012, ME5024, ME5084						
	22TB HDD / 7.68TB SSD	5.80PB	5.72PB	7.39PB ⁴							
Min/Max Drives		2/264	2/276	28/336 ³							
Controllers		Single & Dual	Single & Dual	Dual							
Controller Memory		16GB per controller									
Media Mix		ME5012: 3.5" HDD; ME5024: 2.5" SSD; ME5084: 2.5"/3.5" HDD/SSD - (FIPS,SED)									
Protocols		16/32Gb FC, 10Gb iSCSI BaseT, 10/25Gb iSCSI Optical, 12Gb SAS				12Gb SAS Backend					
Operational Modes		Virtual (all data services) & Linear (performance-based)									
Performance		640K IOPs @ 100% Sequential Reads, 16K block size, R5, Virtual =>750K IOPs									
Throughput		12GB/s Read & 10GB/s Write =>14GB/s Read, 12GB/s Write									
HW Availability		5-9's (Dual controller models only)									

1 Dual controller ME5212 and ME5224 models | 2 Expansion units that connect only to RAID Controller RBODs | 3 ME5 firmware is designed to support up to 8PB (4PB per controller) as higher drive capacities become available & ME4 Virtual = 2PB (so 4X) = 8PB & ME4 Linear = 4PB (so 2X) = 8PB | 4 Up to 8.0PB with 22TB HDDs or 336 drives, whichever occurs first

*No JBOD support for ME400 series

ME5 to Freya Differences

ME5 vs. Freya Controllers Hardware Features

Feature	ME5 Shipping Controllers	ME5 Freya Controllers
Performance	10GB/s Write Throughput , 640K Read IOPs	14GB/s Read – 12 GB/s Write Throughput, 750K IOPs (Processor speed change from 2.9 GHz to 3.2 GHz)
SC Memory	HEW-D with 8GByte Down on Board	HEW-D with 8GByte Down on Board (Design can support 16GByte)
Super Capacitors	25F Cells Down on Board	34F Cells Down on Board (36% more energy)
Host Interface	4-Port FC 32G (non-HPE customers) 4-Port iSCSI 25G and 10GbaseT 4-Port SAS 12G (SAS 3416)	Same FC and initial 25G iSCSI 4-Port SAS 12G (Aero SAS3816)
CPLD	MachX03, 6900 LUT, BGA400	MachX03D, 9400LUT, BGA484 (advanced security features, root of trust)
Daughterboard	None	Tick FPGA and/or open Titan (advanced security features, root of trust)
SAS Initiator	Broadcom Tomcat (SAS3406)	Broadcom Aero(SAS3816)
SAS Expander	MicroChip Belmont (PM8054) Same expander used on Pimico IOM	MicroChip Augusta (PM811) 42-port allows for local SAS wider port option

Freya Key New Requirements

- New Controllers – Continuity of Supply
- KMIP with MAS
- Intelligent drive firmware update
- Increase in performance –IOP's and BW
- ESE Updates – Latest Version of ESE

Freya Bezels

ME52xx DELL



ME5284 DELL



ME5 vs ME5 MLK Features Comparison

		PowerVault ME5	PowerVault ME5 MLK
CPU		Intel Xeon	No change
IOPS		640K (100% Sequential Read, 16K block) ⁽¹⁾	~750K
Read / Write Throughput		12GB/s / 10GB/s	14GB/s / 12GB/s
Enclosure / Expansion		2U12, 2U24, 5U84 (ME412/424/484); 12Gb SAS backend	No change
Async Replication between Arrays		ME5 to/from ME5, ME5 to/from ME4	ME5 MLK to/from ME5 MLK, ME5 MLK to/from ME5
Interface s: 4 ports per controller	Fibre Channel	16/32Gb	No change
	iSCSI (SFP)	10/25Gb	No change
	iSCSI (10GbaseT)	10Gb	No change
	SAS	12Gb	No change
Memory per Controller		16GB	No change
Max Virtual Pool Size (Total Usable Capacity)		4 PB per controller (8 PB total)	No change
Max Volume size		128TB	No change
Standard Density		2U12, 2U24	No change
High Density / Max Drives		5U84 / 336	No change
Capacity		8PB	No change
User Interface		Updated GUI – capacity and activity monitoring	No change
Embedded Support Assist		ESE with parity of Phone Home	No change
Key Management		At the (FIPS) drive level	KMIP
Power Supply		AC and DC	No change
New features			• Intelligent Firmware updates
			• Data-in-Place upgrades (ME5 to ME5 MLK)
Investigations			• Potential for Dell implementation of MAS (MC Auxiliary Services) plug-in framework • Any new Security requirements/enhancements • Additional Dell ecosystem support/integration

Seagate Freya Performance Run Results

IO Profile	Previous Indium Numbers	IOP's (IN310)	Avg Latency (ms) IN310	Max Latency(ms) IN310
4K Random Read	700293	813521 (16.6%)	0.31	13.39
4K 70/30 Random Read/Write	386256	458096(18.59%)	1.37	19.22
256K Sequential Read	14035	14231(1.39%)	0.66	198
256K Sequential Write	10839	11127(2.65%)	3.78	48.57

Chasis Configuration	Total Volumes	Number of Ports	Host Server	Disk Groups	Que Depth
2U24x1 960GB Seagate SSD's (Random reads and 70:30)	5 volumes per Disk group of each size 50GB	3 per Controller	Dell 840	2xR10 each of 12 Drives	32
5u81x1 18TB Seagate HDDs (Sequential Reads)	2 volumes per Disk group of each size of 50GB	3 per Controller	Dell 840	6xR5 each of 14 drives	3
5u84x1 18TB Seagate HDD's (Sequential Writes)	2 volumes per Disk group of each size of 50GB	3 per Controller	Dell 840	9xR5 each of 9 drives	9

Q&A

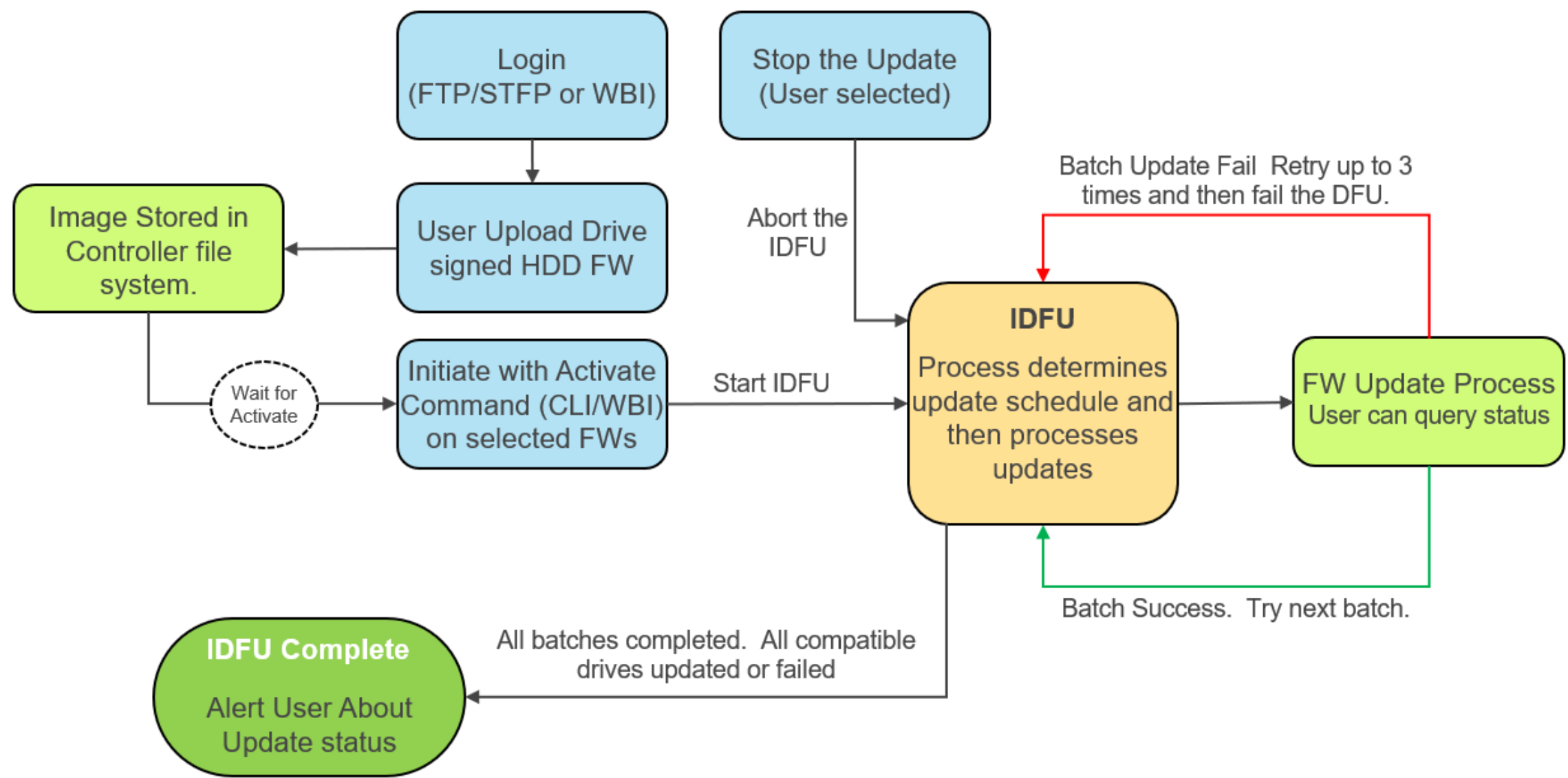
Douglas Yates

Intelligent Drive FW Update

IDFU – Intelligent Drive Firmware Update

- Enables the user to upload a signed encrypted drive FW bundle file (.sfw) to the enclosure controller for activation and update of compatible drives
 - During upload, the package is validated and matches drive models to a new correct FW binary if installed revision is different than the package revision.
 - The system displays supported drives and available updates based on listed drive model numbers and FW revisions built into in the package. Only supported drives and needed drive FW are displayed.
 - For any available updates listed, the user can select activation of the new FW image(s) on a per drive FW basis.
 - Up to 5 drive FW families can be selected at a time.
 - All drive models that are supported by a given FW, as defined by the package, will be included for update.
- The IDFU process will then schedule the drive FW updates based on the Enclosure usage conditions and number of drives requiring an operation
 - The engine will determine which drives and the number of drives to concurrently update to minimize disruption. Updates will automatically be handled in batches. Currently, 6 drives can be updated concurrently.
 - The process will display progress and alert the user when all updates are complete.
- IDFU process is available through the WBI and the CLI
 - GUI and CLI additions to support new IDFU features
- Legacy Drive FW update is still available for updating specific drives if needed.
 - IDFU or Legacy update is selectable in enclosure settings

Process Flow



WBI – New Drive FW Activation

Dashboard

Provisioning

Settings

Maintenance

Storage

Hardware

Firmware

About

Support

Applications

DELLTechnologies

PowerVault Manager | ME5224

Browse For File

Upload File

Cancel

Upload the firmware file to upgrade disk firmware intelligently.

Intelligent Disk Firmware Update is Enabled ?

[Click to toggle Intelligent Disk Firmware Update setting](#)

☐ Skip Intelligent Disk Firmware Upgrade ?

Disk Firmware Versions

Select Disk Firmware Action

Delete Firmware(s)

Activate Firmware(s)

		Revision	Compatible Model(s)	Status	
☒	DSG8.bin	DSG8	MZILG1T9HCJRAD3	AVAILABLE	Click to activate this firmware
☐	B02A.bin	B02A	KPM5XRUG960G	ACTIVE ✓	Click to activate this firmware

Disk Firmware

Location	Vendor	Model	Revision	Description	Health
0.2	TOSHIBA	KPM5XRUG960G	B02A	SSD SAS	✓
0.3	TOSHIBA	KPM5XRUG960G	B02A	SSD SAS	✓

Internal Use - Confidential

DELLTechnologies

WBI — Enable/Disable IDFU

PowerVault Manager | ME5224

Dashboard

Provisioning

Settings

Network

Users

System

Notifications

iSCSI

Peer Connections

Maintenance

Applications

Settings

System

IdentificationDate and TimePropertiesSecurity

Cache Properties

Disk Properties

Scrub Properties

Managed Logs Properties

Firmware Properties

☒ Partner Firmware Update ?

☒ Intelligent Disk Firmware Update ?

Enabling Disk Firmware Update allows the system to apply uploaded disk firmware to all compatible disks. It will update the disks in batches, intelligently choosing the disks based on usage and disk group protection.

Set Properties

CLI – New/Updated Commands for IDFU

- `show firmware-bundles disk`
 - Displays the active firmware files and available firmware files stored in the system's controller modules.
- `activate disk-firmware name [file]`
 - Initiates the IDFU batch update process. The update then determines which drives need to be updated with the selected image(s.)
- `show disks firmware`
 - Lists the drives including FW revisions
- `set advanced-settings disk-firmware-update [on/off]`
 - Enable or disable the IDFU process. Disabled allows legacy disk FW operation.
- `show advanced-settings`
 - Shows the settings for advanced system-configuration parameters, including IDFU enabled/disabled.
- `abort disk-firmware-update`
 - Aborts the disk firmware update process. Note: The disks in the current operating batch will continue updating, subsequent batches will be aborted.
- `delete disk-firmware [name]`
 - Deletes the uploaded disk firmware image file(s) from the controller. Note: Disable IDFU process prior to issuing.

Disk FW Related Alerts

- 280 - Disk firmware update initiated (Informational)
 - Disk firmware update process has initiated.
 - Recommended action:
 - Do not power cycle or restart the system.
- 281 - Batch disk firmware update successful (Informational)
 - Disk firmware update process has successfully updated disks in a batch.
 - Recommended action:
 - Check in the event log for events related to this component and follow the recommended actions for those events.
- 282 - Batch disk firmware update failed (Informational)
 - Disk firmware update process has failed to updated disks in a batch.
 - Recommended action:
 - Check in the event log for events related to this component and follow the recommended actions for those events.

Disk FW Related Alerts

- 283 - Disk firmware update successful (Informational)
 - Disk firmware update process has successfully updated all compatible disks.
 - Recommended action:
 - No action is required.

- 284 - Disk firmware update failed (Informational)
 - Disk firmware update process has failed to update all compatible disks.
 - Recommended action:
 - Check that the uploaded disk firmware file is compatible with the disks in system.
 - If this issue persists with compatible disk firmware, contact technical support.

ME5 Freya

Updated Drive Compatibility

List of Validated Drives Will be
Available in ME52xx Support Matrix

DEMO

Q&A

Rina Binxhiu

KMIP

Current ME5 Drive Secure vs KMIP

- Use a passphrase
- Manual
- Stored Local
- Singular to the enclosure

Data-at-rest Encryption via Self-Encrypting Drives (SEDs)

- **Auto-Lock** – Automatically secure user data when removed and powered off
- **Instant Secure Erase** – all drive data unreadable in less than 1 second

External Key Manager

- Industry standard OASIS Key Management Interoperability Protocol (KMIP)
- Keys are stored externally providing additional level of security
- Customer's key server manages all keys automatically
- Move drives to new data center, same key server, with auto-unlocking

Storage Array KMIP Client

- Storage array auto-locks/unlocks user data on SEDs using external key manager
- Storage array performs instant secure erase when commanded using external key manager
- KMIP Client microservice powers up independently providing fast auto-unlock timing
- KMIP Client microservice versioned and released independently

KMIP Client Architecture

Configuration

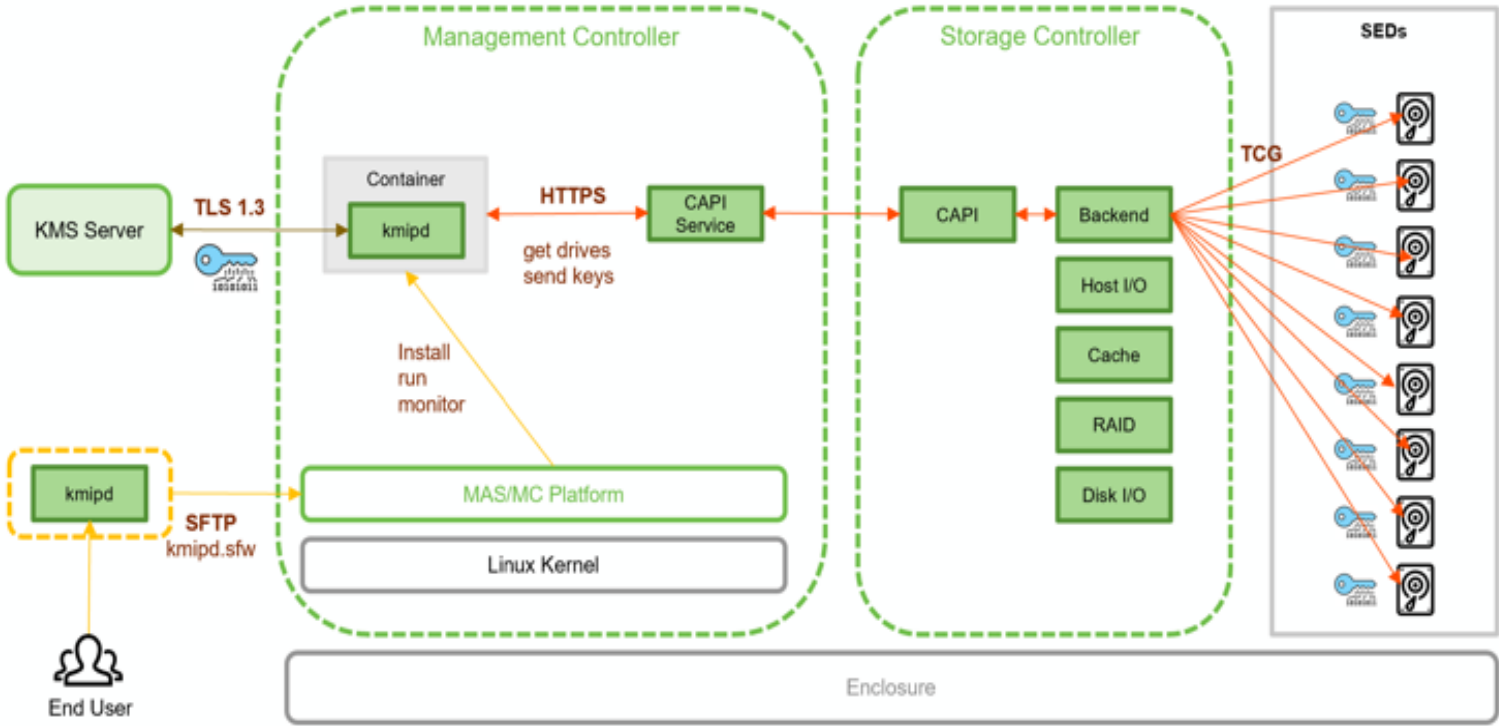
- Configure Key Management Server (KMS) Settings
 - IP / Port
- Store KMS Certificates
 - CA, Cert, Key
- Secure Drives

Automatic

- Discover SEDs
- Create/Get KMIP Keys
- Lock/Unlock SEDs

Updates

- FTP PUT kmip.sfw



KMIP Setup Requirements

- KMIP Server

Support KMIP versions 2.0 and 1.4

- Network Connectivity

- Certificates

- Certificate names need to include letters and certain characters only

- SED Drives

Create a User Role – Diagnostics

```
# create user base 2 interfaces wbi roles diagnostic rina_kmip test
Enter new password: *****
Re-enter new password: *****
Success: Command completed successfully. (rina_kmip test) - The new user was created. (2025-02-28
09:48:19)
```

Protocols & Ports

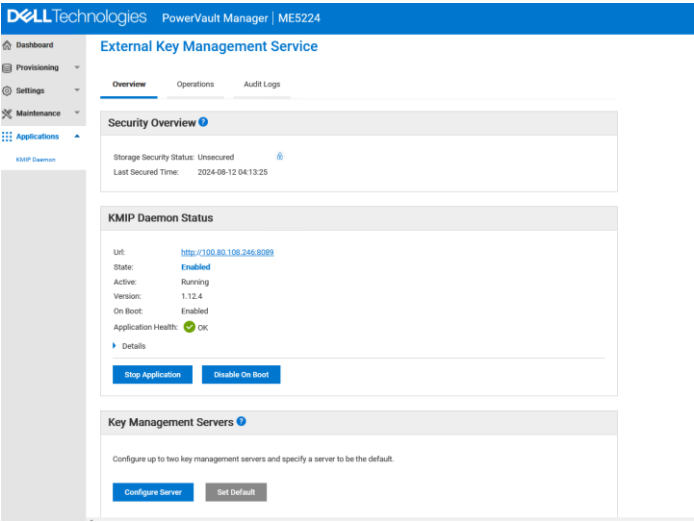
Protocol	Port	Description	Network	From	To
tls	5696	KMIP Protocol	Enterprise	kmipd	KMS
http	80	MC CLI (Console, JSON)	Local	user	MC
http	8082	kmipd web service (JSON)	Local	user	kmipd
http	8085	CAPI Web Service (JSON)	Internal	kmipd	capis

- Only secure protocols will be used in released product
- kmipd web service will NOT be accessible in released product
- capis web service will NOT be accessible in released product

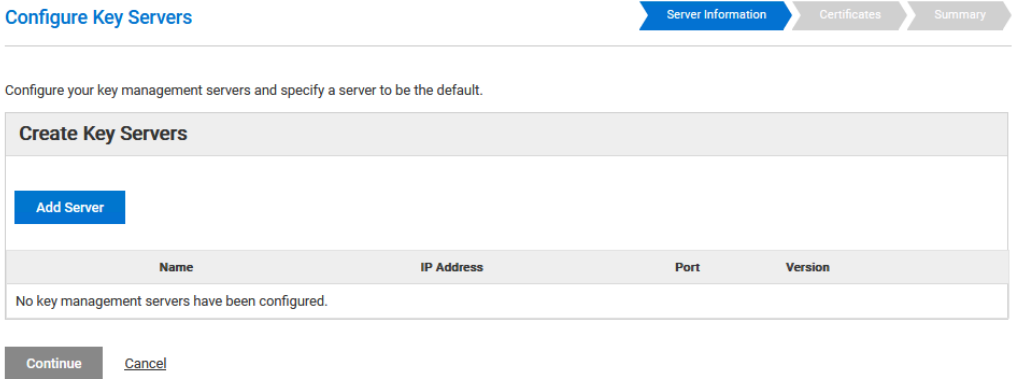
KMIP Setup - GUI

KMIP Setup Flow

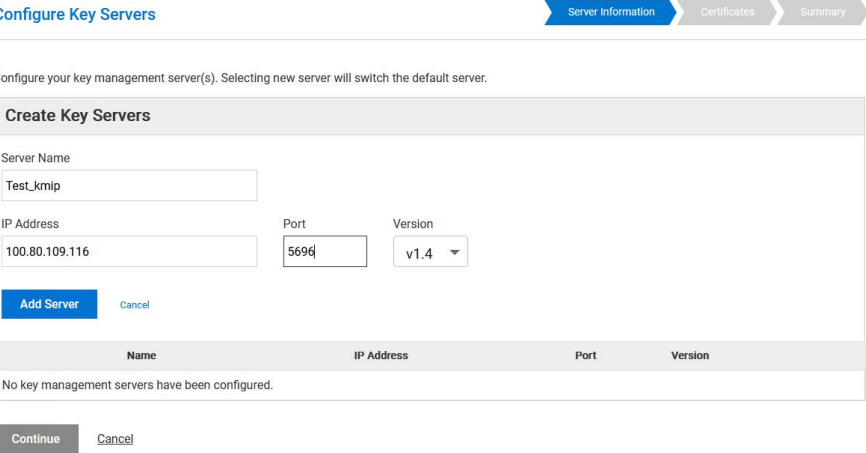
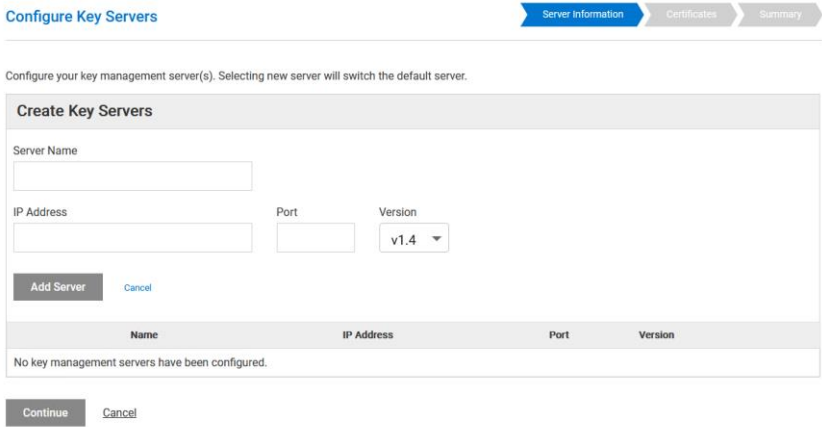
1. Log in to PowerVault Manager GUI with the Diagnostic User



2. Add Server – To connect to the KMIP server



3. Add the KMIP server



4. Select the server and Continue

Configure Key Servers

Server Information

Certificates

Summary

Configure your key management server(s). Selecting new server will switch the default server.

Create Key Servers

Only 2 key servers can be added.

Add Server

Name	IP Address	Port	Version
Test_kmip	100.80.109.116	5696	v1.4

The default key management server will be switched from justOneMoreKMS to Test_kmip.

Continue

Cancel

Private Key

Private Key:

Key246.pem

Private Key Checksum:

5ff211870b61321edc2d6f5db6e1d551fa49a0b55cc286a46c01b65ecd1c4da5

Certificate Authority (CA)

Certificate Authority (CA):

Certificate246.pem

Certificate Authority (CA) Checksum:

079a665be249e9144d580ffecfd32838a5fe050d368ff2c5b301e0da4d7e24d1

Certificate

Certificate:

Cert246.pem

Certificate Checksum:

fdf313c91334abe16d11c54d1935dc5b5b4cc7e0979641f84e2aedada04d5824

5. Upload the Private Key, CA and Certificate

Configure Key Servers

Server Information

Certificates

Summary

Each key management server needs three certificate files: private key, certificate authority, and certificate. Upload your PEM format file or enter the contents in the boxes below.

screenshottest

Private Key

Browse For File

Or

Certificate Authority (CA)

Browse For File

Or

Certificate

Browse For File

Or

Save

Cancel

Continue

Back

Cancel

Secure the drives using KMIP

PowerVault Manager | ME5224

Dashboard

Provisioning

Settings

Maintenance

Applications

KMIP Daemon

External Key Management Service

Overview

Operations

Audit Logs

Operations ?

Storage Security Status: KMIP

Last Secured Time: 2025-02-26 13:19:56

Generate new keys for your encrypted drives immediately or create a schedule to automatically generate r

Create Rekey Schedule

Rekey Now

Unsecure this system. This operation will unlock all the encrypted drives in the system. The keys used to s
operation and will need to be destroyed if desired.

Unsecure System

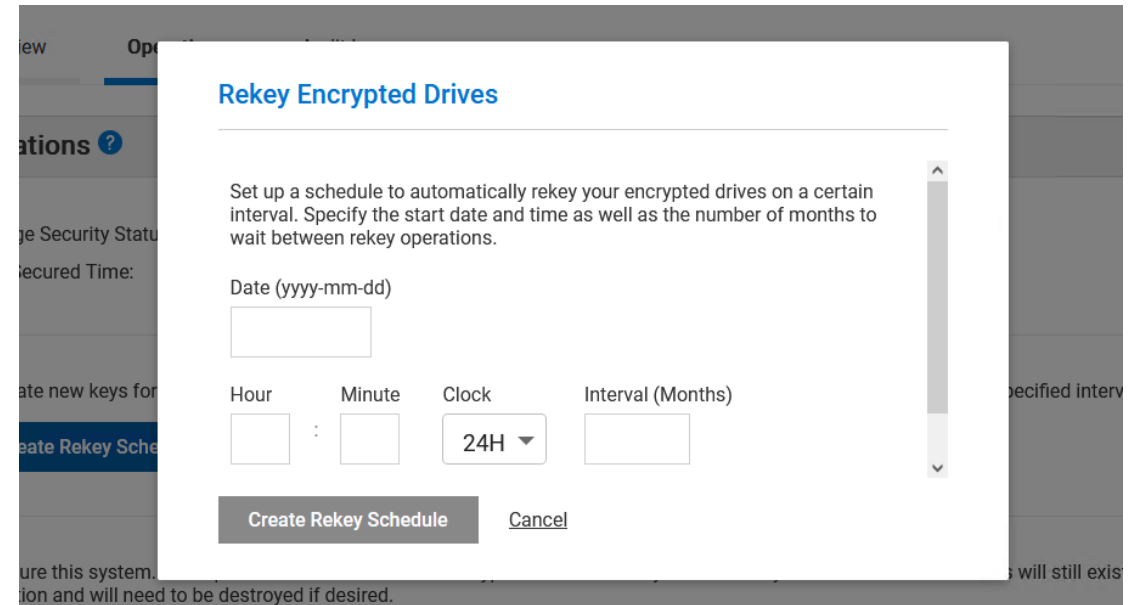
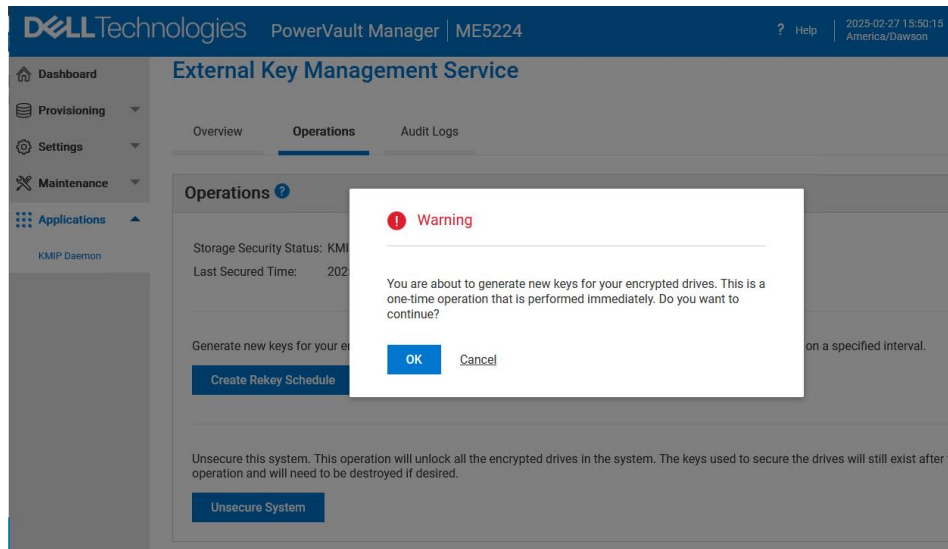
Internal Use - Confidential

34 Copyright © Dell Inc. All Rights Reserved.

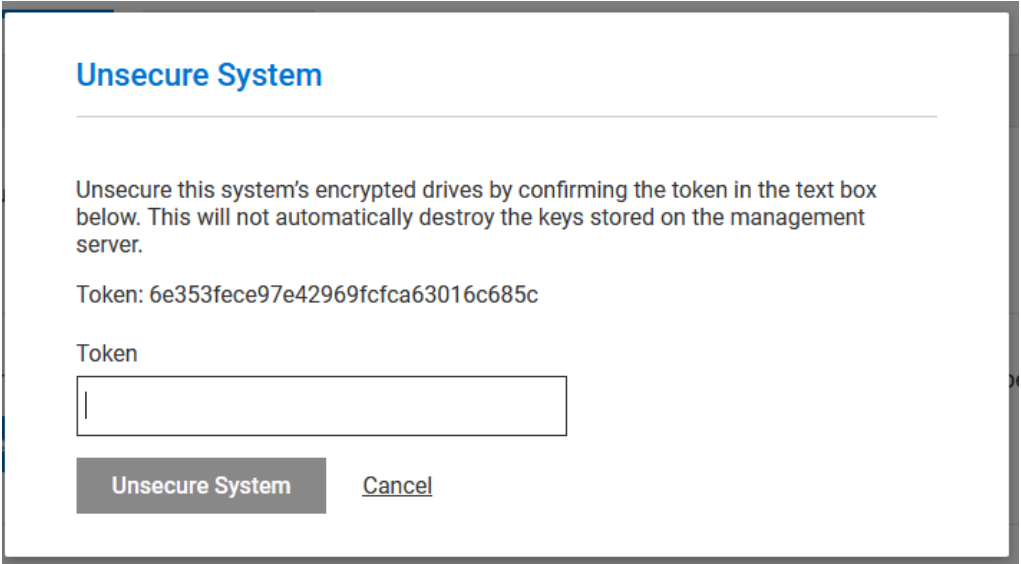
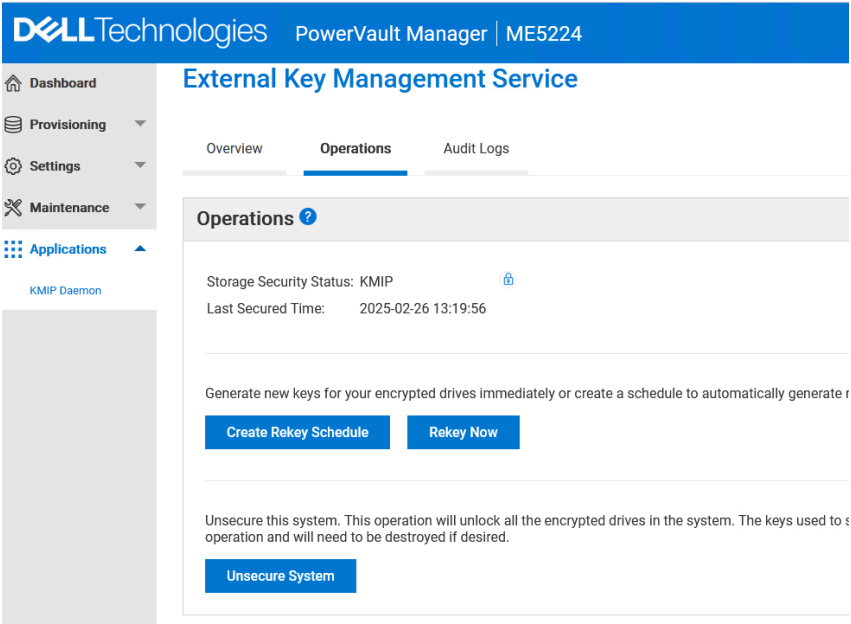


Rekey the drives using KMIP

1. Login to PV Manager
2. Applications -> KMIP Deamon
3. Select the Operations Tab
4. Select Rekey to generate a new key
5. Select Create Rekey Schedule to automate the rekey process



Unsecure the drives using KMIP



The Audit Log tab is used to display the audit log. If the audit log is larger than 4 KiB, it will be truncated, and the ftp option is required to retrieve the full kmipd.log and kmipd-auditreport.log files. The audit log report is used to verify past operations performed to configure and secure a system.

KMIP Setup - CLI

Initial Setup of KMIP - CLI

Step 0	Make sure kmipd is installed and running	show mas-services
Step 1	Specify the IP Address, Port and Name of the Key Server using the MC CLI or API.	send mas-service kmipd cmd-string "command=updatesettings,kms=<kms-label>,serverip=<ip>,serverport=<port>"
Step 2	Upload the Key Server CA PEM file.	curl -v -k --location --request POST "https://\$host/api/uploadMasService" \ --header "sessionKey: \$sessionid" \ --header "content-type: multipart/form-data" \ --header "datatype: json" \ --form "cert-data=@<filename>;type=text/plain" \ --form "service-name="kmipd";type=text/plain" \ --form "certificate-name="<filename>;type=text/plain" \ --form "certificate-type="ca";type=text/plain"seagate@ubuntu:~/seagit/mccli\$
Step 3	Upload the Key Server Private Key PEM file.	curl -v -k --location --request POST "https://\$host/api/uploadMasService" \ --header "sessionKey: \$sessionid" \ --header "content-type: multipart/form-data" \ --header "datatype: json" \ --form "cert-data=@<filename>;type=text/plain" \ --form "service-name="kmipd";type=text/plain" \ --form "certificate-name="<filename>;type=text/plain" \ --form "certificate-type="privatekey";type=text/plain"seagate@ubuntu:~/seagit/mccli\$
Step 4	Upload the Key Server Certificate PEM file.	curl -v -k --location --request POST "https://\$host/api/uploadMasService" \ --header "sessionKey: \$sessionid" \ --header "content-type: multipart/form-data" \ --header "datatype: json" \ --form "cert-data=@<filename>;type=text/plain" \ --form "service-name="kmipd";type=text/plain" \ --form "certificate-name="<filename>;type=text/plain" \ --form "certificate-type="certificate";type=text/plain"seagate@ubuntu:~/seagit/mccli\$

Step 5	Inform KMIP Client of the Key Server CA PEM file.	send mas-service kmipd cmd-string "command=addcertificate,kms=<kms-label>,name=<filename>,type=ca"
Step 6	Inform KMIP Client of the Key Server Private Key PEM file.	send mas-service kmipd cmd-string "command=addcertificate,kms=<kms-label>,name=<filename>,type=privatekey"
Step 7	Inform KMIP Client of the Key Server Certificate PEM file.	send mas-service kmipd cmd-string "command=addcertificate,kms=<kms-label>,name=<filename>,type=cert"
Step 8	Select the Key Server to use	send mas-service kmipd cmd-string "command=selectkms,kms=<kms-label>"
Step 2	Show Settings	send mas-service kmipd cmd-string "command=showsettings"

Secure the drives using KMIP - CLI

Step 1	Make sure kmipd is installed and running	show mas-services
Step 2	Secure all disk drives	send mas-service kmipd cmd-string "command=secure,kms=<server>"
Step 3	Show secure progress	show mas-services kmipd details
Step 4	Show system status	show system
Step 5	Show drive status	show disks secure
Step 6a	Show audit data. If the audit log is larger than 4 KiB, the ftp option below is required.	send mas-service kmipd cmd-string "command=audit"
Step 6b	Retrieve the kmipd audit log using ftp	ftp> get logs:mas:kmipd <file.zip>'

Unsecure the drives using KMIP - CLI

Step 1	Signal intend to unsecure	send mas-service kmipd cmd-string "command=unsecure"
Step 2	Unsecure disk drives	send mas-service kmipd cmd-string "command=unsecure,token=<uuid>"
Step 3	Remove keys from external key server	send mas-service kmipd cmd-string "command=destroy"

Manual Rekey System using KMIP - CLI

Step 1	Rekey	send mas-service kmipd cmd-string "command=rekey,kms=<kms>"
---------------	-------	---

Auto Rekey System using KMIP - CLI

Step 1	Create Rekey Schedule	send mas-service kmipd cmd-string "command=autorekey,kms=<kms>,op=start,year=yyyy,month=mm,day=dd,hour=hh,min=mn,interval=month"
Step 2	Show Rekey Schedule	send mas-service kmipd cmd-string "command=autorekey,kms=<kms>,op=show"
Step 3	Stop the Automatic Rekey Operation	send mas-service kmipd cmd-string "command=autorekey,kms=<kms>,op=stop"

Neha Chowdhary

Troubleshooting

Unable to connect to KMS

Alerts

▼ 17 minutes



kmipd_A

The KMIP agent is having network issues connecting with the key management server

Acknowledge

Detected Time:

2025-02-26 13:56:01

Resolved Time:

N/A

Description:

The KMIP agent is having network issues connecting with the key management server

- The service is experiencing network connection issues with the key management server. Review KMS settings, check network connectivity, and retrieve service log files.

Recommended Action:

View On System

Comments

Connection failed for kms server () ip (100.80.109.113:5696)

Events

Date/Time ▲	Severity ▼	Controller ▼	Event Code ▼	Message ▼
▼ 2025-02-26 14:41:33		A	683	KMIP MAS Service failed to communicate with key server. (IP address: 0.3.1740606081.0, port: 4294967295)
Additional Information:				
None.				
Recommended Action:				
- Verify KMIP key server configuration settings and network connectivity.				
▶ 2025-02-26 14:39:03		A	683	KMIP MAS Service failed to communicate with key server. (IP address: 0.3.1740605938.0, port: 4294967295)

Audit Logs ?

2025-02-26T 23:07:48.755Z: [KMIPD] - system (unlock) complete [elapsed=2m14.315752843s] err=unable to retrieve keys for drives (unlock): SessionError could not open a session with the KMIP Server, error: TLS Dial failure: dial tcp 100.80.109.113:5696: connect: connection timed out

2025-02-26T 23:07:48.749Z: [KMIPD] - Unable to retrieve keys for drives (unlock) status=SessionError, err=unable to retrieve keys for drives (unlock): SessionError could not open a session with the KMIP Server, error: TLS Dial failure: dial tcp 100.80.109.113:5696: connect: connection timed out

2025-02-26T 23:05:25.395Z: [KMIPD] - system (unlock) complete [elapsed=2m14.282076915s] err=unable to retrieve keys for drives (unlock): SessionError could not open a session with the KMIP Server, error: TLS Dial failure: dial tcp 100.80.109.113:5696: connect: connection timed out

2025-02-26T 23:05:25.389Z: [KMIPD] - Unable to retrieve keys for drives (unlock) status=SessionError, err=unable to retrieve keys for drives (unlock): SessionError could not open a session with the KMIP Server, error: TLS Dial failure: dial tcp 100.80.109.113:5696: connect: connection timed out

2025-02-26T 23:03:02.034Z: [KMIPD] - system (unlock) complete [elapsed=2m14.282150429s] err=unable to retrieve keys for drives (unlock): SessionError could not open a session with the KMIP Server, error: TLS Dial failure: dial tcp 100.80.109.113:5696: connect: connection timed out

2025-02-26T 23:03:02.029Z: [KMIPD] - Unable to retrieve keys for drives (unlock) status=SessionError, err=unable to retrieve keys for drives (unlock): SessionError could not open a session with the KMIP Server, error: TLS Dial failure: dial tcp 100.80.109.113:5696: connect: connection timed out

Insert FIPS drive to secured system

 Dell Technologies

PowerVault Manager | ME5212

 Dashboard

 Provisioning

 Settings

 Maintenance

 Applications

Applications

KMIP Daemon

Applications

External Key Management Service

Overview

Operations

Audit Logs

Audit Logs ?

2025-02-28T 22:48:09.068Z: [KMIPD] - system (secure) complete [elapsed=16.41554228s] err=, status=Success

2025-02-28T 22:48:09.065Z: [KMIPD] - SUCCESS securing the system

2025-02-28T 22:48:09.061Z: [CAPIS] - capis send keys [elapsed=10.673201s] success=true, total=1, slots=0.9

2025-02-28T 22:47:58.384Z: [CAPIS] - driveHandler batch add [elapsed=239.73784ms] status=Success

2025-02-28T 22:47:55.502Z: [CAPIS] - capi set kmip mode [elapsed=2.84785064s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully.

2025-02-28T 06:08:25.849Z: [KMIPD] - system (secure) complete [elapsed=15.08110692s] err=, status=Success

2025-02-28T 06:08:25.847Z: [KMIPD] - SUCCESS securing the system

2025-02-28T 06:08:25.844Z: [CAPIS] - capis send keys [elapsed=9.36959676s] success=true, total=2, slots=0.7:0.11

2025-02-28T 06:08:16.47Z: [CAPIS] - driveHandler batch add [elapsed=238.80748ms] status=Success

2025-02-28T 06:08:13.596Z: [CAPIS] - capi set kmip mode [elapsed=2.826866s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully.

2025-02-28T 06:08:06.06Z: [CAPIS] - driveHandler batch add [elapsed=54.06856ms] status=Success

2025-02-28T 06:07:27.629Z: [KMS] - kms session open tls=1.3, local=100.80.108.250:45438, remote=100.80.109.101:5696

2025-02-28T 06:06:03.486Z: [CAPIS] - kmipd capis=localhost, port=9143, batch=100

2025-02-28T 06:06:03.485Z: [KMIPD] - kmipd args=-d -ka

2025-02-28T 06:06:03.484Z: [KMIPD] - kmipd run version=1.12.21, build=2025-02-19T19:56:31

2025-02-28T 06:05:46.776Z: [KMIPD] - kmipd signaled exit signal=terminated, number=15

2025-02-28T 02:56:28.651Z: [CAPIS] - driveHandler batch add [elapsed=45.1864ms] status=Success

2025-02-28T 02:55:22.192Z: [KMIPD] - system (secure) complete [elapsed=8.32195388s] err=, status=RetrieveKeysFailure

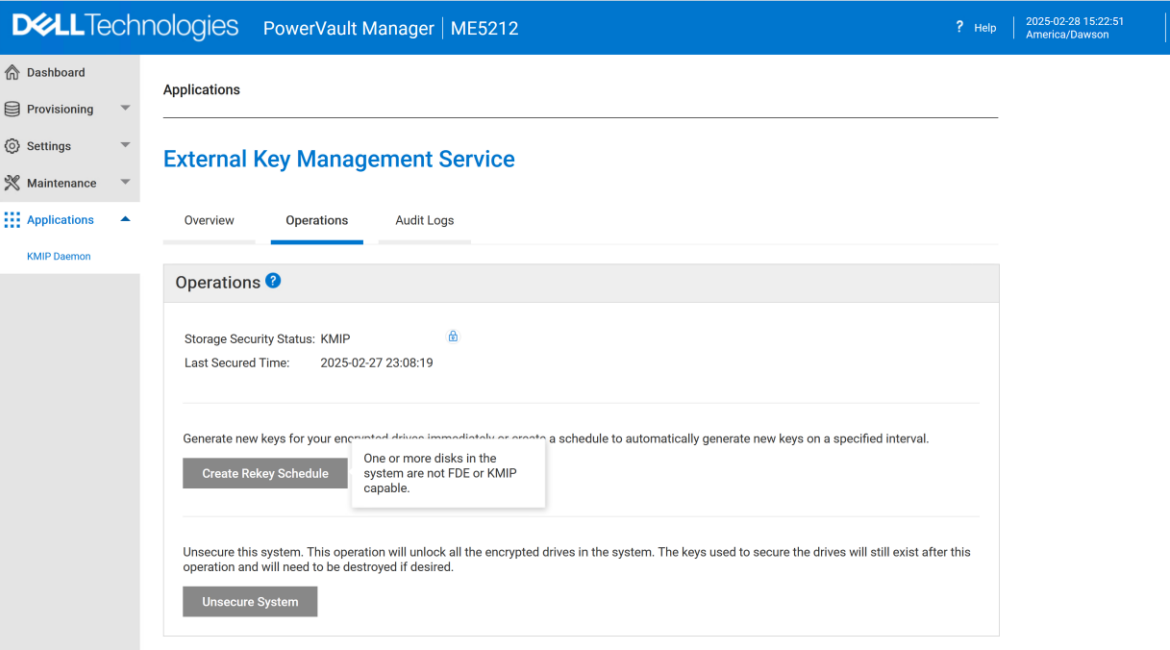
2025-02-28T 02:55:22.189Z: [CAPIS] - capi set kmip mode [elapsed=2.73859132s] mode=kmip-off, http=200, capis=SUCCESS, capi=Command completed successfully.

2025-02-28T 02:55:19.45Z: [KMIPD] - Unable to retrieve keys for drives (secure) status=BatchAddDriveError, err=unable to retrieve keys for drives (secure): BatchAddDriveError drive results drive sn (PMG0KUBU) error: batch add drive operation failed, error:

2025-02-28T 02:55:19.448Z: [CAPIS] - driveHandler batch add [elapsed=100.94648ms] status=BatchAddDriveError

- Drive is automatically secured after being inserted.
- Check your KMS for new keys

Insert Non-FIPS drive into secured system



*picture to be updated

KMIP Logs

- Can be downloaded separately from the controller logs

The screenshot shows the Dell Technologies PowerVault Manager ME5212 interface. On the left is a navigation menu with options: Dashboard, Provisioning, Settings, Maintenance, and Applications. The 'Applications' section is expanded, showing 'KMIP Daemon'. The main area is titled 'External Key Management Service' and has tabs for Overview, Operations, and Audit Logs. The 'Audit Logs' tab is active, displaying a list of log entries with timestamps and details. At the bottom, there are 'Refresh Log' and 'Clear Logs' buttons.

External Key Management Service

Audit Logs

2025-02-28T 22:48:09.068Z: [KMIPD] - system (secure) complete [elapsed=16.41554228s] err=, status=Success
2025-02-28T 22:48:09.065Z: [KMIPD] - SUCCESS securing the system
2025-02-28T 22:48:09.061Z: [CAPIS] - capis send keys [elapsed=10.673201s] success=true, total=1, slots=0-9
2025-02-28T 22:47:58.384Z: [CAPIS] - driveHandler batch add [elapsed=239.73784ms] status=Success
2025-02-28T 22:47:55.502Z: [CAPIS] - capi set kmip mode [elapsed=2.84785064s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully
2025-02-28T 06:08:25.849Z: [KMIPD] - system (secure) complete [elapsed=15.08110692s] err=, status=Success
2025-02-28T 06:08:25.847Z: [KMIPD] - SUCCESS securing the system
2025-02-28T 06:08:25.844Z: [CAPIS] - capis send keys [elapsed=9.36959676s] success=true, total=2, slots=0-7,0-11
2025-02-28T 06:08:16.47Z: [CAPIS] - driveHandler batch add [elapsed=238.80748ms] status=Success
2025-02-28T 06:08:13.596Z: [CAPIS] - capi set kmip mode [elapsed=2.826866s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully
2025-02-28T 06:08:06.06Z: [CAPIS] - driveHandler batch add [elapsed=54.06856ms] status=Success
2025-02-28T 06:07:27.629Z: [KMS] - kms session open [ls=1.3, local=100.80.108.250:45438, remote=100.80.109.101:5696]
2025-02-28T 06:06:03.486Z: [CAPIS] - kmipd capis=localhost, port=9143, batch=100
2025-02-28T 06:06:03.485Z: [KMIPD] - kmipd args=d -ka
2025-02-28T 06:06:03.484Z: [KMIPD] - kmipd run version=1.12.21, build=2025-02-19T19:56:31
2025-02-28T 06:05:46.776Z: [KMIPD] - kmipd signaled exit signal=terminated, number=15
2025-02-28T 02:56:28.651Z: [CAPIS] - driveHandler batch add [elapsed=45.1864ms] status=Success
2025-02-28T 02:55:22.192Z: [KMIPD] - system (secure) complete [elapsed=8.32195388s] err=, status=RetrieveKeysFailure
2025-02-28T 02:55:22.189Z: [CAPIS] - capi set kmip mode [elapsed=2.73859132s] mode=kmip-off, http=200, capis=SUCCESS, capi=Command completed successfully
2025-02-28T 02:55:19.45Z: [KMIPD] - Unable to retrieve keys for drives (secure) status=BatchAddDriveError, err=unable to retrieve keys for drives (secure); BatchAddDriveError drive results drive sn (PMGOKUBU) error: batch add drive operation failed, error:
2025-02-28T 02:55:19.448Z: [CAPIS] - driveHandler batch add [elapsed=100.94648ms] status=BatchAddDriveError

[Refresh Log](#) [Clear Logs](#)

```
DELL Technologies PowerVault ME5212
System Name: Uninitialized Name
System Location: Uninitialized Location
Version: IN310B001
mas send mas-service kmipd cmd-string "command=audit"
mas Service Output
-----
Agent Name: kmipd
Agent Display Name: KMIP Daemon
Agent URL: 169.254.255.101:2300
Agent Version: 1.12.21
Agent Status: Success
Agent Status Numeric: 1
Agent Health: OK
Agent Health Numeric: 0
Status: Success
Status Numeric: 0
Dri: /mas/v1/passthrough
Details: {"response-type":"Audit","response-type-numeric":2,"command":"command=audit","message":{"audit-log-report contains the last (21) entries","audit-log":{"total":25,"start-date":"2025-02-28T 02:47:53.181Z","next-date":"2025-02-28T 22:48:09.068Z","entries":[{"2025-02-28T 22:48:09.068Z: [KMIPD] - system (secure) complete [elapsed=16.41554228s] err=\u003cnill\u003e, status=Success","2025-02-28T 22:48:09.065Z: [KMIPD] - SUCCESS securing the system ","2025-02-28T 22:48:09.061Z: [CAPIS] - capis send keys [elapsed=10.673201s] success=true, total=1, slots=0-9","2025-02-28T 22:47:58.384Z: [CAPIS] - driveHandler batch add [elapsed=239.73784ms] status=Success","2025-02-28T 22:47:55.502Z: [CAPIS] - capi set kmip mode [elapsed=2.84785064s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully","2025-02-28T 06:08:25.849Z: [KMIPD] - system (secure) complete [elapsed=15.08110692s] err=\u003cnill\u003e, status=Success","2025-02-28T 06:08:25.847Z: [KMIPD] - SUCCESS securing the system ","2025-02-28T 06:08:25.844Z: [CAPIS] - capis send keys [elapsed=9.36959676s] success=true, total=2, slots=0-7,0-11","2025-02-28T 06:08:16.47Z: [CAPIS] - driveHandler batch add [elapsed=238.80748ms] status=Success","2025-02-28T 06:08:13.596Z: [CAPIS] - capi set kmip mode [elapsed=2.826866s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully","2025-02-28T 06:08:06.06Z: [CAPIS] - driveHandler batch add [elapsed=54.06856ms] status=Success","2025-02-28T 06:07:27.629Z: [KMS] - kms session open [ls=1.3, local=100.80.108.250:45438, remote=100.80.109.101:5696]","2025-02-28T 06:06:03.486Z: [CAPIS] - kmipd capis=localhost, port=9143, batch=100","2025-02-28T 06:06:03.485Z: [KMIPD] - kmipd args=d -ka","2025-02-28T 06:06:03.484Z: [KMIPD] - kmipd run version=1.12.21, build=2025-02-19T19:56:31","2025-02-28T 06:05:46.776Z: [KMIPD] - kmipd signaled exit signal=terminated, number=15","2025-02-28T 02:56:28.651Z: [CAPIS] - driveHandler batch add [elapsed=45.1864ms] status=Success","2025-02-28T 02:55:22.192Z: [KMIPD] - system (secure) complete [elapsed=8.32195388s] err=\u003cnill\u003e, status=RetrieveKeysFailure","2025-02-28T 02:55:22.189Z: [CAPIS] - capi set kmip mode [elapsed=2.73859132s] mode=kmip-off, http=200, capis=SUCCESS, capi=Command completed successfully","2025-02-28T 02:55:19.45Z: [KMIPD] - Unable to retrieve keys for drives (secure) status=BatchAddDriveError, err=unable to retrieve keys for drives (secure); BatchAddDriveError drive results drive sn (PMGOKUBU) error: batch add drive operation failed, error: \u003cnill\u003e","2025-02-28T 02:55:19.448Z: [CAPIS] - driveHandler batch add [elapsed=100.94648ms] status=BatchAddDriveError"}}}}
Success: Command completed successfully. (2025-02-28 16:28:26)
```

ftp> get logs:mas:kmipd <file.zip>

The KMIP Client iterates through all stored audit items and produces a Console, XML or JSON report.

The audit report contains a record of all interactions with the KMIP Server and will detail the drive serial number and KMIP unique identifier but will NOT contain any cryptographic key information. The end user will have to use drive serial number and KMIP unique identifier to debug any key issues.

When the FTP option is used, the zip file contains the kmipd.log and kmipd-auditreport.log files.

Mismatch cert/wrong cert

Use Case: CA & Client Certificate are switched.

Add Certificates

Certificate Type

Browse For File

Private Key

Private Key: ThursKey.pem

Private Key Checksum: 94873f576a464160e37336036a398ab80cab736f9000ce6b1d7bb7992c8b6289

Certificate Authority (CA)

Certificate Authority (CA): ThursClientCert.pem

Certificate Authority (CA) Checksum: 5d05326c19f458114e3053f0d379c592ed74f0d852409c19031d176282619aec

Certificate

Certificate: ThursCertificate.pem

Certificate Checksum: dc4f668daaa2e814880baccd84393a88bb9c5a36eb3b933f7c2963ae6bac11bc

DELLTechnologies

PowerVault Manager | ME5212

Dashboard

Provisioning

Settings

Maintenance

Applications

KMIP Daemon

Overview

Operations

Audit Logs

Audit Logs

2025-03-06T 15:47:32.091Z: [KMIPD] - system (secure) complete [elapsed=8.3831612s] err=, status=RetrieveKeysFailure

2025-03-06T 15:47:32.089Z: [CAPIS] - capi set kmip mode [elapsed=1.25731052s] mode=kmip-off, http=200, capis=SUCCESS, capi=Command completed successfully.

2025-03-06T 15:47:30.83Z: [KMIPD] - Unable to retrieve keys for drives (secure) status=SessionError, err=unable to retrieve keys for drives (secure): SessionError could not open a session with the KMIP Server, error: Failed to create x509 key pair

2025-03-06T 15:47:26.622Z: [CAPIS] - capi set kmip mode [elapsed=2.91297648s] mode=kmip-on, http=200, capis=SUCCESS, capi=Command completed successfully.

2025-03-05T 17:31:57.086Z: [CAPIS] - driveHandler batch add [elapsed=41.06184ms] status=Success

2025-03-04T 17:31:33.529Z: [CAPIS] - driveHandler batch add [elapsed=46.0958ms] status=Success

2025-03-04T 17:31:33.46Z: [KMS] - kms server kmip=1.4

2025-03-04T 17:31:33.343Z: [KMS] - kms session open tls=1.3, local=100.80.108.250:55580, remote=100.80.109.101:5696

2025-03-04T 16:15:53.308Z: [CAPIS] - kmipd capis=localhost, port=9143, batch=100

2025-03-04T 16:15:53.307Z: [KMIPD] - kmipd args=-d -ka

2025-03-04T 16:15:53.305Z: [KMIPD] - kmipd run version=1.13.1, build=2025-03-03T10:02:02

2025-03-04T 23:15:02.906Z: [KMIPD] - kmipd signaled exit signal=terminated, number=15

2025-03-04T 23:11:54.236Z: [CAPIS] - kmipd capis=localhost, port=9143, batch=100

2025-03-04T 23:11:54.234Z: [KMIPD] - kmipd args=-d -ka

2025-03-04T 23:11:54.233Z: [KMIPD] - kmipd run version=1.12.21, build=2025-02-19T19:56:31

2025-03-04T 23:10:37.186Z: [CAPIS] - get security information [elapsed=2.5978ms] err=ERROR: http get (https://localhost:9143/capi/v1/kms): Get "https://localhost:9143/capi/v1/kms": dial tcp 169.254.255.101:9143: connect: connection refused

2025-03-01T 01:17:34.801Z: [CAPIS] - driveHandler batch add [elapsed=96.83808ms] status=Success

2025-03-01T 01:16:02.653Z: [KMIPD] - system (unsecure) complete [elapsed=15.9298818s] err=, status=Success

2025-03-01T 01:16:02.651Z: [CAPIS] - capi set kmip mode [elapsed=2.8280216s] mode=kmip-off, http=200, capis=SUCCESS, capi=Command completed successfully.

2025-03-01T 01:15:59.82Z: [KMIPD] - SUCCESS deleting the system (unsecure)

2025-03-01T 01:15:59.816Z: [CAPIS] - capis send keys [elapsed=10.29784444s] success=true, total=3, slots=0:7,0:9,0:11

Refresh Log

Clear Logs

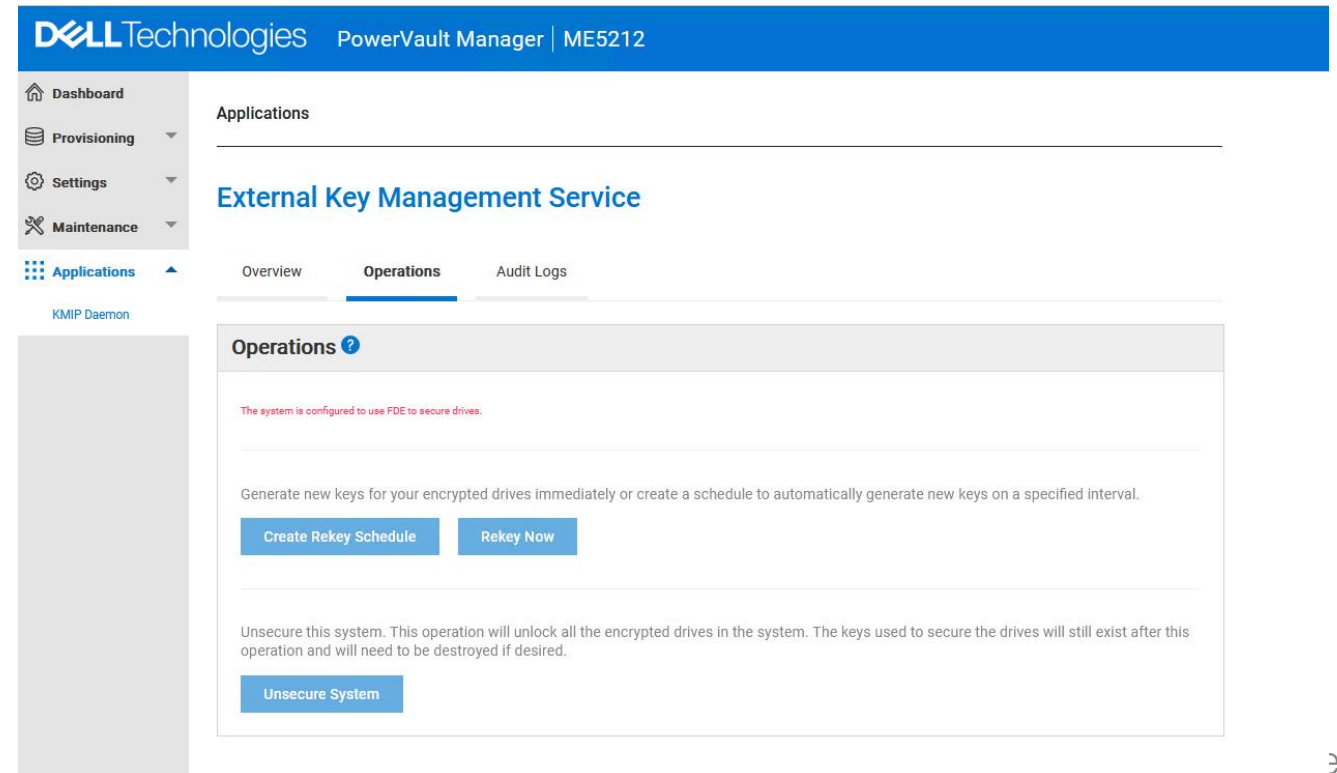
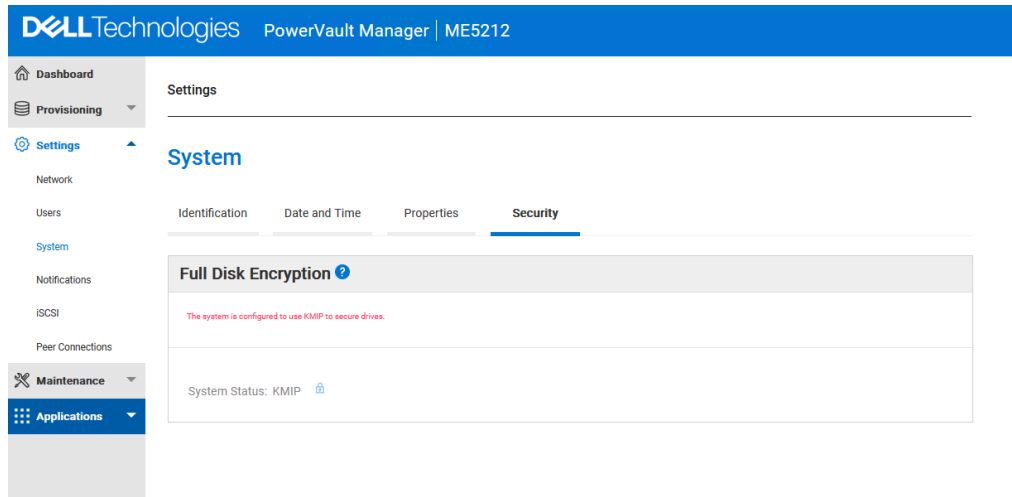
Internal Use - Confidential

45 Copyright © Dell Inc. All Rights Reserved.

DELLTechnologies

FDE to KMIP & vice-versa

- FDE and KMIP work are mutually exclusive.
- When system is KMIP secured, FDE commands are rejected.
- When system is FDE secured, KMIP commands are rejected.



Certificate Instructions

- Things to keep in mind:
 - PEM format file
 - Allowed characters

Dell Technologies PowerVault Manager | ME5212

Configure Key Servers [Server Information] [Certificates] [Summary]

Each key management server needs three certificate files: private key, certificate authority, and certificate. Upload your PEM format file or enter the contents in the boxes below.

▼ cipher

Private Key
Selected File:
Certificate file name can't contain any of the following characters: \$ & () , ; ' * | < > \ /
[Upload File] [Cancel]

Certificate Authority (CA)
[Browse For File] Or

Certificate
[Browse For File] Or

* For IBM Guardium Key Lifecycle Manager, Certificate Authority (CA) file needs to be renamed from .cer to .pem for successful upload.

Failover Scenarios

- **Controller Failover:**
 - The KMS certificates & private key must be uploaded to both the primary and secondary controller to ensure uninterrupted secure connection during failover.
- **KMS Failover**
 - The KMS agents need to be configured in a cluster node on the key management tool.
 - On the controller side, you would configure the two servers that are in a cluster but use the same certificates and private key from the primary server for redundancy.

Q&A





Back up slides

Firmware

Dell EMC PowerVault Manager | ME5012

Maintenance

Firmware

It is important to periodically check for new firmware updates that may be available for your system. Storage systems that are used by a replication set should run the same or compatible firmware versions. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

Current Firmware Bundle

Controller A (Currently using) Controller B

I200B011 I200B011

Partner Firmware Update is Enabled

Upload the firmware bundle to install the bundle on controller A. You will have the opportunity to compare versions and activate the installed bundle using the table below.

[Browse For File](#)

Firmware Versions		
Bundle Version	Build Date	Status
I200B011	2021-09-01T20:48:56Z	ACTIVE VERSION
I200B012	2021-09-08T19:49:59Z	INSTALLED / NOT ACTIVATED Activate this Version

Bundle Version: I200B012
 GEM Version: usm-rss_sbbas_indium_dell-v5.3_lite-2021.33.0_rc1_rel_736
 MC Firmware: IOM200B012-01
 MC Loader: 1.62.34850
 MC OS Version: IPM200B012-01
 CPLD Revision: 1.3
 ASIC Controller Version: 1.62.34850
 SC Firmware: INS200B12-01

- **System:**
 - Holds two controller images Active/Not Activated
 - Browse for File to upload new images.
 - Activate the Version to start Firmware Download.
 - ✓ Health Check. Will not proceed with Degraded health.
 - ✓ Transfer to Partner if PFU enabled
 - ✓ Partner update / Reboot
 - ✓ Local update / Reboot
 - ✓ Cleanup

Dell EMC PowerVault Manager | ME5012

System Disks

Upload the firmware file to install to the selected disks.

[Browse For File](#)

Disk Firmware						
	Location	Vendor	Model	Revision	Description	Health
☐	0.0	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.1	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.2	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.3	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.4	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.5	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.6	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.7	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.8	WDC	WUH721818ALS200	US05	SAS MDL	
☐	0.9	WDC	WUH721818ALS200	US05	SAS MDL	

- **Disks:**
 - Browse for File to upload new images
 - Select Disks to update
 - Upload File to begin update process to disk(s)

DEMO

Add CUP
 Add .bins
 Delete .bins
>5 .bin - reload
No match load.