



Statement of Volatility – Dell EMC PowerEdge T640

Dell EMC PowerEdge T640 contains both volatile and non-volatile (NV) components. Volatile components lose their data immediately upon removal of power from the component. Non-volatile components continue to retain their data even after the power has been removed from the component. Components chosen as user-definable configuration options (those not soldered to the motherboard) are not included in the Statement of Volatility. Configuration option information (pertinent to options such as microprocessors, remote access controllers, and storage controllers) is available by component separately. The following NV components are present in the PowerEdge T640 server.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
Planer				
PCH Internal CMOS RAM	Non-Volatile	1	U_PCH1	256 Bytes
BIOS Password	Non-Volatile	1	U_PCH1	16 bytes
BIOS SPI Flash	Non-Volatile	1	U212 (PRIM_SPI_BIOS)	32 MB
BIOS Recovery SPI Flash	Non-Volatile	1	U216	16MB
iDRAC SPI Flash	Non-Volatile	1	U218 (UBOOT)	4 MB
BMC EMMC	Non-Volatile	1	U_EMMC1	8 GB
CPU Vcore Regulators	Non-Volatile	2	U40, U48	16 KB
CPU Vmem Regulators	Non-Volatile	2	U61, U69	16 KB
System CPLD RAM	Volatile	1	U_CPLD1	92Kb
System CPLD FLASH	Non-Volatile	1	U_CPLD1	256Kb
System Memory: RDIMM and LRDIMM	Volatile	Up to 12 per CPU	CPU<2:1>_CH<5:0>_D<1:0> >	Up to 32GB per DIMM
System Memory: NVDIMM-N	Non-Volatile	Up to 6 per CPUs 1 and 2 (12 total)	CPU<2:1>_CH<5:0>_D1	16GB per NVDIMM-N

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
		in system)		
Internal USB Key	Non-Volatile	Up to 1	J55	Varies (not factory installed)
CPU	Volatile	1 or 2	CPU1 / CPU2	Various
iDRAC DDR	Volatile	1	U_IDRAC9_DRAM1	256MByte
iDRAC	Volatile	1	U_IDRAC1	64 kbyte + registers
PIROM	Non-Volatile	1 or 2	CPU1 / CPU2	256 Bytes
LOM	Non-Volatile	1	U232	8MB
8x2.5" NVMe Backplane				
SEP internal flash	Non-Volatile	1	U_SEP1	64K Bytes
SEP internal EEPROM	Non-Volatile	1	U_SEP1	256 Bytes
18x3.5" EXP/Backplane				
NVSRAM memory	Non-Volatile	1	U3	1 Mb
Flash memory	Non-Volatile	1	U25	128 Mb
BP FRU image	Non-Volatile	1	U5	256 Bytes
Expander FRU image	Non-Volatile	1	U6	256 Bytes
16x2.5" EXP/Backplane				
NVSRAM memory	Non-Volatile	1	U_EXP_NVSRAM	1 Mb
Flash memory	Non-Volatile	1	U_EXP_FLASH	128 Mb
BP FRU image	Non-Volatile	1	U_BP_FRU	256 Bytes
Expander FRU image	Non-Volatile	1	U_EXP_FRU	256 Bytes
H730, H830 PERCs				
NVSRAM	Non-volatile	1	U1033	128KB

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
FRU	Non-volatile	1	U1019	256B
1-Wire EEPROM	Non-volatile	1	U1004	128B
SPD	Non-volatile	1	U22	256B
SBR	Non-volatile	1	U1020	8KB
Flash	Non-volatile	1	U1031	16MB
ONFI Backup Flash	Non-volatile	1	U1059	4GB
SDRAM	Volatile	5	U1043-U1047	512MB/1GB
H330, H330M PERC				
NVSRAM	Non-volatile	1	U1033	128KB
FRU	Non-volatile	1	U1019	256B
1-Wire EEPROM	Non-volatile	1	U1004	128B
SBR	Non-volatile	1	U1020	8KB
Flash	Non-volatile	1	U3	16MB
HBA330 PERC				
NVSRAM	Non-volatile	1	U1033	128KB
FRU	Non-volatile	1	U1019	256B
Serial Boot ROM	Non-volatile	1	U1020	8KB
Flash	Non-volatile	1	U3	16MB
PCIe SSD Extender Card				
Switch Configuration EEPROM	Non-Volatile	1	U2	256B
Titan				
MCU	Non-Volatile	1	USAM7	32Mb
Tiny				
MCU	Non-Volatile	1	U_TINY	8KB

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size
FIO				
SPI Flash	Non-Volatile	1	U_SPI_FLASH1	32Mb
TPM				
Trusted Platform Module (TPM, TPM 2.0 only)	Non-Volatile	1	U_TPM	128 Bytes
ACE (iDSDM - vFlash)				
vFlash (uSD)	non-volatile	1	J3	16GB
iDSDM (uSD1, uSD2)	non-volatile	2	J1, J2	16GB, 32GB, 64GB
SPI Flash	Non-Volatile	1	U2	1MB
BOSS				
SPI FLASH	Non-Volatile	1	U17	1024KB
TFRU	Non-Volatile	1	U7	64KB
PSU				
Microcontroller	Non-Volatile	Up to 2	Microchip	Up to 64KB

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
Planer			
PCH Internal CMOS RAM	Battery-backed CMOS RAM	No	Real-time clock and BIOS configuration settings
BIOS Password	Battery-backed CMOS RAM	Yes	Password to change BIOS settings
BIOS SPI Flash	SPI Flash	No	Boot code, system configuration information, UEFI environment, Flash descriptor, ME

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
BIOS Recovery SPI Flash	SPI Flash	No	16MB Recovery SPI ROM exits as an aid to reprogram the primary ROM
iDRAC SPI Flash	SPI Flash	No	iDRAC Uboot (bootloader), server management persistent store (i.e. iDRAC MAC Address, iDRAC boot variables), lifecycle log cache, virtual planar FRU and EPPID, rac log, system event log, JobStore, iDRAC Secure boot code,
BMC EMMC	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware
CPU Vcore Regulators	ROM	No	Operational parameters
CPU Vmem Regulators	ROM	No	Operational parameters
System CPLD RAM	RAM	No	Not utilized
System CPLD FLASH	RAM	No	Power on System Firmware
System Memory: RDIMM and LRDIMM	DRAM	Yes	System OS RAM
System Memory: NVDIMM-N	Flash - NVDIMM	No	Data integrity
Internal USB Key	Flash	Yes	General purpose USB key drive
CPU	Cache + registers	Yes	Processor cache + registers
iDRAC DDR	DRAM	No	iDRAC local memory

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
iDRAC	Cache + registers	No	Processor cache + registers
PIROM	EEPROM	no	Processor info + scratchpad
LOM	SPI Flash	no	LOM firmware
8x2.5" NVMe Backplane			
SEP internal flash	Flash	No	firmware
SEP internal EEPROM	EEPROM	No	FRU
18x3.5" EXP/Backplane			
NVSRAM memory	MRAM	No	FW config data
Flash memory	Flash	No	firmware
BP FRU image	EEPROM	No	FRU
Expander FRU image	EEPROM	No	FRU
16x2.5" EXP/Backplane			
NVSRAM memory	MRAM	No	FW config data
Flash memory	Flash	No	firmware
BP FRU image	EEPROM	No	FRU
Expander FRU image	EEPROM	No	FRU
H730, H830 PERCs			
NVSRAM	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
1-Wire EEPROM	1-Wire EEPROM	No	Holds default controller properties/settings
SPD	SPD	No	Memory configuration data
SBR	SBR	No	Bootloader
Flash	Flash	No	Card firmware
ONFI Backup Flash	ONFI Backup Flash	No	Holds cache data during power loss
SDRAM	SDRAM	No	Cache for HDD I/O
H330, H330M PERC			
NVSRAM	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information
1-Wire EEPROM	1-Wire EEPROM	No	Holds default controller properties/settings
SBR	SBR	No	Bootloader
Flash	Flash	No	Card firmware
HBA330 PERC			
NVSRAM	NVSRAM	No	Configuration data
FRU	FRU	No	Card manufacturing information
Serial Boot ROM	Serial Boot ROM	No	Bootloader
Flash	Flash	No	Card firmware
PCIe SSD Extender Card			
Switch Configuration EEPROM	SPI Flash EEPROM	No (requires specialized SW)	Configuration for PLX PCIe switch, setting registers

Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
Titan			
MCU	embedded Flash	No	For field maintenance. Have License, Service Tag and system information. Driving health and status LEDs
Tiny			
MCU	embedded Flash	No	Driving Health and Status LED
FIO			
SPI Flash	SPI Flash	No	For field maintenance. Have License, Service Tag and system information.
TPM			
Trusted Platform Module (TPM, TPM 2.0 only)	EEPROM	Yes	Storage of encryption keys
ACE (iDSDM - vFlash)			
vFlash (uSD)	NAND flash	yes	populate out-of-band or optionally connect to the host as mass storage and boot mechanism
iDSDM (uSD1, uSD2)	NAND Flash	Yes	Provides mass storage
SPI Flash	SPI Flash	SPI flash is only indirectly connected to iDRAC. iDRAC can read any address in the SPI flash, but may only write the primary firmware storage area as a part of a	Boot firmware storage, configuration and state data for iDSDM.


Item	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)
		firmware update procedure.	
BOSS			
SPI FLASH	FLASH EEPROM	No	Boot code, FW
TFRU	FLASH EEPROM	Yes	Thermal monitoring
PSU			
Microcontroller	Flash PROM and EEPROM	Yes	Report PSU information and control firmware

Item	How is data input to this memory?	How is this memory write protected?
Planer		
PCH Internal CMOS RAM	BIOS	N/A – BIOS only control
BIOS Password	Keyboard	N/A – BIOS only control
BIOS SPI Flash	SPI interface via PCH	Software write protected
BIOS Recovery SPI Flash	SPI interface via PCH	Software write protected
iDRAC SPI Flash	SPI interface via iDRAC	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.
BMC EMMC	NAND Flash interface via iDRAC	Embedded FW write protected
CPU Vcore Regulators	Programmed at factory via I2C	No write protect
CPU Vmem Regulators	Programmed at factory via I2C	No write protect
System CPLD RAM	Not utilized	Not accessible
System CPLD FLASH	Firmware update	BIOS Security Protocols
System Memory: RDIMM and LRDIMM	System OS	OS Control
System Memory: NVDIMM-N	When system initiates a Save (AC loss, shutdown, etc.), NVDIMM-N controller will transfer data from DRAM to Flash	Neither system nor OS can access the flash, only a system initiated Save will trigger the NVDIMM-N controller to transfer data from DRAM to flash

Item	How is data input to this memory?	How is this memory write protected?
Internal USB Key	USB interface via PCH. Accessed via system OS	No write protect
CPU	Various	Various
iDRAC DDR	iDRAC Firmware	NA
iDRAC	iDRAC Firmware	NA
PIROM	SMBus interface to iDRAC	128 bytes protected by Intel/128 bytes not protected
LOM	Pre-programmed before assembly	No write protect
8x2.5" NVMe Backplane		
SEP internal flash	Pre-programmed before assembly	Not WP
SEP internal EEPROM	Programmed at ICT during production.	Not WP
18x3.5" EXP/Backplane		
NVSRAM memory	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor
Flash memory	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor
BP FRU image	Programmed at ICT during production.	Not WP
Expander FRU image	Programmed at ICT during production.	Not WP
16x2.5" EXP/Backplane		
NVSRAM memory	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor
Flash memory	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor
BP FRU image	Programmed at ICT during production.	Not WP
Expander FRU image	Programmed at ICT during production.	Not WP
H730, H830 PERCs		
NVSRAM	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor
FRU	Programmed at ICT during production.	Not WP
1-Wire EEPROM	ROC writes data to this memory	Not WP. Not visible to Host Processor
SPD	Pre-programmed before assembly	Not WP. Not visible to Host Processor
SBR	Pre-programmed before assembly	Not WP. Not visible to Host Processor
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor

Item	How is data input to this memory?	How is this memory write protected?
ONFI Backup Flash	FPGA backs up DDR data to this device in case of a power failure	Not WP. Not visible to Host Processor
SDRAM	ROC writes to this memory - using it as cache for data IO to HDDs	Not WP. Not visible to Host Processor
H330, H330M PERC		
NVSRAM	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor
FRU	Programmed at ICT during production	Not WP
1-Wire EEPROM	ROC writes data to this memory	Not WP. Not visible to Host Processor
SBR	Pre-programmed before assembly	Not WP. Not visible to Host Processor
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor
HBA330 PERC		
NVSRAM	ROC writes configuration data to NVSRAM	No write protect. Not visible to Host Processor
FRU	Programmed at ICT during production	No write protect
Serial Boot ROM	Pre-programmed before assembly	No write protect. Not visible to Host Processor
Flash	Pre-programmed before assembly. Can be updated using Dell/LSI tools	No write protect. Not visible to Host Processor
PCIe SSD Extender Card		
Switch Configuration EEPROM	The EEPROM image is pre-loaded at factory before assembly. Once assembled on the card, data can be entered via PLX Device Editor or PLX EEP DOS based tool.	Device can be write protected via hardware pin. Alternatively, device contents can be write protected via WPEN bit in status register.
Titan		
MCU	Pre-programmed before assembly	Hardware strapping
Tiny		
MCU	Pre-programmed before assembly	Hardware strapping
FIO		
SPI Flash	SPI interface via iDRAC	Hardware strapping
TPM		
Trusted Platform Module (TPM, TPM 2.0 only)	Using TPM Enabled operating systems	SW write protected
ACE (IDSDM - vFlash)		

Item	How is data input to this memory?	How is this memory write protected?
vFlash (uSD)	User can provide data to iDRAC (entirely in the iDRAC domain) to be pushed into vFlash	no write protect
iDSDM (uSD1, uSD2)	device resides in host domain; they are exposed to the user via an internally connected, non-removable USB mass storage device	physical write protect switch on ACE card
SPI Flash	User can initiate a firmware update of the iDSDM device.	There is no mechanism provided to iDRAC to write any SPI NOR area outside of the primary iDSDM firmware region.
BOSS		
SPI FLASH	By programming the image via firmware update process	N/A
TFRU	During Manufacturing, by programming the image via firmware update process.	N/A
	During runtime, by I2C Proprietary Command Protocol	
PSU		
Microcontroller	The data is flash via Dell Update Package(DUP)	Using signature and manufacture key to protect memory write

 **NOTE:** For any information that you may need, direct your questions to your Dell Marketing contact.

© 2017 Dell Inc.

Trademarks used in this text: Dell™, the DELL logo, and PowerEdge™ are trademarks of Dell Inc.