



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	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
Planer										
PCH Internal CMOS RAM	Non-Volatile	1	U_PCH1	256 Bytes	Battery-backed CMOS RAM	No	Real-time clock and BIOS configuration settings	BIOS	N/A – BIOS only control	Perform the following steps: 1) Set NVRAM_CLR jumper to clear BIOS configuration settings at boot and reboot system; 2) AC power off system, remove coin cell battery for 30 seconds, replace battery and power on; 3) Restore default configuration in F2 system setup menu.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
BIOS Password	Non-Volatile	1	U_PCH1	16 bytes	Battery-backed CMOS RAM	Yes	Password to change BIOS settings	Keyboard	N/A – BIOS only control	1) Place shunt on J_PSWD_NVRAM jumper pins 2 and 4. 2) AC power off is required after placing the shunt. 3) AC power on with the shunt in place and then can be removed
BIOS SPI Flash	Non-Volatile	1	U212 (PRIM_SPI_BIOS)	32 MB	SPI Flash	No	Boot code, system configuration information, UEFI environment, Flash descriptor, ME	SPI interface via PCH	Software write protected	You cannot remove the memory with any utilities or applications. Note: When memory is corrupted or removed, System becomes non-functional
BIOS Recovery SPI Flash	Non-Volatile	1	U216	16MB	SPI Flash	No	16MB Recovery SPI ROM exits as an aid to reprogram the primary ROM	SPI interface via PCH	Software write protected	User cannot clear the memory.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
iDRAC SPI Flash	Non-Volatile	1	U218 (UBOOT)	4 MB	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,	SPI interface via iDRAC	Embedded iDRAC subsystem firmware actively controls sub area based write protection as needed.	User cannot clear the memory completely. However, user data, lifecycle log and archive, SEL, firmware image repository can be cleared via Delete Configuration and Retire System, accessible in Lifecycle Controller interface
BMC EMMC	Non-Volatile	1	U_EMMC1	8 GB	eMMC NAND Flash	No	Operational iDRAC FW, Lifecycle Controller (LC) USC partition, LC service diags, LC OS drivers, USC firmware	NAND Flash interface via iDRAC	Embedded FW write protected	User cannot clear the memory completely. However, user data, lifecycle log and archive, SEL, firmware image repository can be cleared via Delete Configuration and Retire System, accessible in Lifecycle Controller interface
CPU Vcore Regulators	Non-Volatile	2	U40, U48	16 KB	ROM	No	Operational parameters	Programmed at factory via I2C	No write protect	User cannot clear the memory.
CPU Vmem Regulators	Non-Volatile	2	U61, U69	16 KB	ROM	No	Operational parameters	Programmed at factory via I2C	no write protect	User cannot clear the memory.
System CPLD RAM	Volatile	1	U_CPLD1	92Kb	RAM	No	Not utilized	Not utilized	Not accessible	Not accessible

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
System CPLD FLASH	Non-Volatile	1	U_CPLD1	256Kb	RAM	No	Power on System Firmware	Firmware update	BIOS Security Protocols	User cannot clear the memory.
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	DRAM	Yes	System OS RAM	System OS	OS Control	Reboot or power down the system.
System Memory: NVDIMM-N	Non-Volatile	Up to 6 per CPUs 1 and 2 (12 total in system)	CPU<2:1>_CH<5:0>_D1	16GB per NVDIMM-N	Flash - NVDIMM	No	Data integrity	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	Using BIOS menu option, select NVDIMM factory reset.
Internal USB Key	Non-Volatile	Up to 1	J55	Varies (not factory installed)	Flash	Yes	General purpose USB key drive	USB interface via PCH. Accessed via system OS	No write protect	Can be cleared in system OS
CPU	Volatile	1 or 2	CPU1 / CPU2	Various	Cache + registers	Yes	Processor cache + registers	Various	Various	Remove A/C

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
iDRAC DDR	Volatile	1	U_IDRAC9_DRAM1	256MByte	DRAM	No	iDRAC local memory	iDRAC Firmware	NA	Remove A/C
iDRAC	Volatile	1	U_IDRAC1	64 kbyte + registers	Cache + registers	No	Processor cache + registers	iDRAC Firmware	NA	Remove A/C
PIROM	Non-Volatile	1 or 2	CPU1 / CPU2	256 Bytes	EEPROM	no	Processor info + scratchpad	SMBus interface to iDRAC	128 bytes protected by Intel/128 bytes not protected	User cannot clear the memory.
LOM	Non-Volatile	1	U232	8MB	SPI Flash	no	LOM firmware	Pre-programmed before assembly	No write protect	User cannot clear the memory.
8x2.5" NVMe Backplane										
SEP internal flash	Non-Volatile	1	U_SEP1	64K Bytes	Flash	No	firmware	Pre-programmed before assembly	Not WP	User cannot clear the memory.
SEP internal EEPROM	Non-Volatile	1	U_SEP1	256 Bytes	EEPROM	No	FRU	Programmed at ICT during production.	Not WP	User cannot clear the memory.
18x3.5" EXP/Backplane										
NVSRAM memory	Non-Volatile	1	U3	1 Mb	MRAM	No	FW config data	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	User cannot clear the memory.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
Flash memory	Non-Volatile	1	U25	128 Mb	Flash	No	firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	User cannot clear the memory.
BP FRU image	Non-Volatile	1	U5	256 Bytes	EEPROM	No	FRU	Programmed at ICT during production.	Not WP	User cannot clear the memory.
Expander FRU image	Non-Volatile	1	U6	256 Bytes	EEPROM	No	FRU	Programmed at ICT during production.	Not WP	User cannot clear the memory.
16x2.5" EXP/Backplane										
NVSRAM memory	Non-Volatile	1	U_EXP_NV SRAM	1 Mb	MRAM	No	FW config data	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	User cannot clear the memory.
Flash memory	Non-Volatile	1	U_EXP_FLASH	128 Mb	Flash	No	firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	User cannot clear the memory.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
BP FRU image	Non-Volatile	1	U_BP_FRU	256 Bytes	EEPROM	No	FRU	Programmed at ICT during production.	Not WP	User cannot clear the memory.
Expander FRU image	Non-Volatile	1	U_EXP_FRU	256 Bytes	EEPROM	No	FRU	Programmed at ICT during production.	Not WP	User cannot clear the memory.
H730, H830 PERCs										
NVSRAM	Non-volatile	1	U1033	128KB	NVSRAM	No	Configuration data	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	User cannot clear the memory.
FRU	Non-volatile	1	U1019	256B	FRU	No	Card manufacturing information	Programmed at ICT during production.	Not WP	User cannot clear the memory.
1-Wire EEPROM	Non-volatile	1	U1004	128B	1-Wire EEPROM	No	Holds default controller properties/settings	ROC writes data to this memory	Not WP. Not visible to Host Processor	User cannot clear the memory.
SPD	Non-volatile	1	U22	256B	SPD	No	Memory configuration data	Pre-programmed before assembly	Not WP. Not visible to Host Processor	User cannot clear the memory.
SBR	Non-volatile	1	U1020	8KB	SBR	No	Bootloader	Pre-programmed before assembly	Not WP. Not visible to Host Processor	User cannot clear the memory.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
Flash	Non-volatile	1	U1031	16MB	Flash	No	Card firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	User cannot clear the memory.
ONFI Backup Flash	Non-volatile	1	U1059	4GB	ONFI Backup Flash	No	Holds cache data during power loss	FPGA backs up DDR data to this device in case of a power failure	Not WP. Not visible to Host Processor	Flash can be cleared by powering up the card and allowing the controller to flush the contents to VDs. If the VDs are no longer available, cache can be cleared by going into controller bios and selecting Discard Preserved Cache.
SDRAM	Volatile	5	U1043-U1047	512MB/1GB	SDRAM	No	Cache for HDD I/O	ROC writes to this memory - using it as cache for data IO to HDDs	Not WP. Not visible to Host Processor	Cache can be cleared by powering off the card
H330, H330M PERC										

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
NVSRAM	Non-volatile	1	U1033	128KB	NVSRAM	No	Configuration data	ROC writes configuration data to NVSRAM	Not WP. Not visible to Host Processor	User cannot clear the memory.
FRU	Non-volatile	1	U1019	256B	FRU	No	Card manufacturing information	Programmed at ICT during production	Not WP	User cannot clear the memory.
1-Wire EEPROM	Non-volatile	1	U1004	128B	1-Wire EEPROM	No	Holds default controller properties/settings	ROC writes data to this memory	Not WP. Not visible to Host Processor	User cannot clear the memory.
SBR	Non-volatile	1	U1020	8KB	SBR	No	Bootloader	Pre-programmed before assembly	Not WP. Not visible to Host Processor	User cannot clear the memory.
Flash	Non-volatile	1	U3	16MB	Flash	No	Card firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools	Not WP. Not visible to Host Processor	User cannot clear the memory.
HBA330 PERC										
NVSRAM	Non-volatile	1	U1033	128KB	NVSRAM	No	Configuration data	ROC writes configuration data to NVSRAM	no write protect. Not visible to Host Processor	User cannot clear the memory.

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
FRU	Non-volatile	1	U1019	256B	FRU	No	Card manufacturing information	Programmed at ICT during production	no write protect	User cannot clear the memory.
Serial Boot ROM	Non-volatile	1	U1020	8KB	Serial Boot ROM	No	Bootloader	Pre-programmed before assembly	no write protect. Not visible to Host Processor	User cannot clear the memory.
Flash	Non-volatile	1	U3	16MB	Flash	No	Card firmware	Pre-programmed before assembly. Can be updated using Dell/LSI tools	no write protect. Not visible to Host Processor	User cannot clear the memory.
PCIe SSD Extender Card										

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
Switch Configuration EEPROM	Non-Volatile	1	U2	256B	SPI Flash EEPROM	No (requires specialized SW)	Configuration for PLX PCIe switch, setting registers	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.	System becomes non-functional if memory is corrupted or removed.
Titan										
MCU	Non-Volatile	1	USAM7	32Mb	embedded Flash	No	For field maintenance. Have License, Service Tag and system information. Driving health and status LEDs	Pre-programmed before assembly	Hardware strapping	User cannot clear the memory.
Tiny										
MCU	Non-Volatile	1	U_TINY	8KB	embedded Flash	No	Driving Health and Status LED	Pre-programmed before assembly	Hardware strapping	User cannot clear the memory.
FIO										

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
SPI Flash	Non-Volatile	1	U_SPI_FLASH1	32Mb	SPI Flash	No	For field maintenance. Have License, Service Tag and system information.	SPI interface via iDRAC	Hardware strapping	User cannot clear the memory.
TPM										
Trusted Platform Module (TPM, TPM 2.0 only)	Non-Volatile	1	U_TPM	128 Bytes	EEPROM	Yes	Storage of encryption keys	Using TPM Enabled operating systems	SW write protected	F2 Setup option
ACE (IDSDM - vFlash)										
vFlash (uSD)	non-volatile	1	J3	16GB	NAND flash	yes	populate out-of-band or optionally connect to the host as mass storage and boot mechanism	User can provide data to iDRAC (entirely in the iDRAC domain) to be pushed into vFlash	no write protect	1. Card may be physically removed and destroyed or cleared via standard means, on a separate computer. OR 2. User has access to the card in the host domain and can clear it manually

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
iDSDM (uSD1, uSD2)	non-volatile	2	J1, J2	16GB, 32GB, 64GB	NAND Flash	Yes	Provides mass storage	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	1. Card may be physically removed and destroyed or cleared via standard means, on a separate computer. OR 2. User has access to the card in the host domain and can clear it manually
SPI Flash	Non-Volatile	1	U2	1MB	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 firmware update procedure.	Boot firmware storage, configuration and state data for iDSDM.	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.	iDRAC may issue a clear command to erase all contents of the SPI NOR. This action may leave the iDSDM non-functional.
BOSS										
SPI FLASH	Non-Volatile	1	U17	1024KB	FLASH EEPROM	No	Boot code, FW	By programming the image via firmware update process	N/A	Use Flash tool, type "go.nsh w y"

Item	Non-Volatile or Volatile	Quantity	Reference Designator	Size	Type (e.g. Flash PROM, EEPROM)	Can user programs or operating system write data to it during normal operation?	Purpose? (e.g. boot code)	How is data input to this memory?	How is this memory write protected?	How is memory cleared?
TFRU	Non-Volatile	1	U7	64KB	FLASH EEPROM	Yes	Thermal monitoring	During Manufacturing, by programming the image via firmware update process. During runtime, by I2C Proprietary Command Protocol	N/A	By writing to Flash
PSU										
Microcontroller	Non-Volatile	Up to 2	Microchip	Up to 64KB	Flash PROM and EEPROM	Yes	Report PSU information and control firmware	The data is flash via Dell Update Package(DUP)	Using signature and manufacture key to protect memory write	The memory is cleared before firmware update

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