


PowerEdge T550 Information Update - Tech Sheet

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Chapter 1: Overview	4
Revision history.....	4
Chapter 2: Minimum configuration to POST	5
Chapter 3: System Security	6
Chapter 4: PSU specifications	10

Overview

The information in this document supersedes the information in the pertinent sections of the Installation and Service Manual, BIOS and UEFI Reference Guide, and Technical Specifications.

For a complete list of information, see the documents available at <https://www.dell.com/poweredgemanuals>.

Topics:

- [Revision history](#)

Revision history

This section provides a description of document changes.

Table 1. Document Revision history

Document Revision	Date	Description of changes
1	November, 2022	<ol style="list-style-type: none">1. Updated BIOS, System Security, Intel(R) SGX2. Updated PSU's3. Updated minimum config to POST

Minimum configuration to POST

- One processor in socket processor 1
- One memory module (DIMM) in socket A1
- Power Interposer Board (PIB) and cables
- One power supply unit
- System board

System Security

To view the **System Security** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > System Security**.

Table 2. System Security details

Option	Description
CPU AES-NI	Improves the speed of applications by performing encryption and decryption by using the Advanced Encryption Standard Instruction Set (AES-NI). This option is set to Enabled by default.
System Password	Sets the system password. This option is set to Enabled by default and is read-only if the password jumper is not installed in the system.
Setup Password	Sets the setup password. This option is read-only if the password jumper is not installed in the system.
Password Status	Locks the system password. This option is set to Unlocked by default.
TPM Information	Indicates the type of Trusted Platform Module, if present.

Table 3. TPM 1.2 security information


Option	Description
TPM Information	
TPM Security	<p> NOTE: The TPM menu is available only when the TPM module is installed.</p> <p>Enables you to control the reporting mode of the TPM. The TPM Security option is set to Off by default. You can only modify the TPM Status, and TPM Activation if the TPM Status field is set to either On with Pre-boot Measurements or On without Pre-boot Measurements.</p> <p>When TPM 1.2 is installed, the TPM Security option is set to Off, On with Pre-boot Measurements, or On without Pre-boot Measurements.</p>
TPM Information	Displays the operational state of the TPM.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Status	Specifies the TPM status.
TPM Command	Controls the Trusted Platform Module (TPM). When set to None , no command is sent to the TPM. When set to Activate , the TPM is enabled and activated. When set to Deactivate , the TPM is disabled and deactivated. When set to Clear , all the contents of the TPM are cleared. This option is set to None by default.
TPM Advance Settings	TPM PPI Bypass Provision When set to Enabled , allows the Operating System to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power interface (ACPI) provisioning operations.
	TPM PPI Bypass Clear When set to Enabled allows the Operating System to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) clear operations.

Table 4. TPM 2.0 security information

Option	Description
TPM Information	

Table 4. TPM 2.0 security information (continued)


Option	Description
TPM Security	<p> NOTE: The TPM menu is available only when the TPM module is installed.</p> <p>Enables you to control the reporting mode of the TPM. The TPM Security option is set to Off by default.</p> <p>When TPM 2.0 is installed, the TPM Security option is set to On or Off. This option is set to Off by default.</p>
TPM Information	Displays the operational state of the TPM.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Hierarchy	<p>Enables, disables, or clears the storage and endorsement hierarchies. When set to Enabled, the storage and endorsement hierarchies can be used.</p> <p>When set to Disabled, the storage and endorsement hierarchies cannot be used.</p> <p>When set to Clear, the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled.</p>
TPM Advanced Settings	<p>TPM PPI Bypass Provision</p> <p>When set to Enabled, allows the Operating System to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power interface (ACPI) provisioning operations.</p>
	<p>TPM PPI Bypass Clear</p> <p>When set to Enabled allows the Operating System to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) clear operations.</p>
	<p>TPM2 Algorithm Selection</p> <p>Allows the user to change the cryptographic algorithms used in the Trusted Platform Module (TPM). The available options are dependent on the TPM firmware.</p> <p>To enable TPM2 Algorithm Selection, Intel(R) TXT technology must be disabled.</p> <p>The TPM2 Algorithm Selection option supports SHA1, SHA128, SHA256, SHA512 and SM3 by detecting the TPM module. This option is set to SHA1 by default.</p>

Table 5. System Security details

Option	Description
Intel(R) TXT	Enables you to set the Intel Trusted Execution Technology (TXT) option. To enable the Intel TXT option, virtualization technology and TPM Security must be enabled with Pre-boot measurements for TPM 1.2 or set to On with SHA256 algorithm for TPM 2.0. This option is set to Off by default. It is set On for Secure Launch (Firmware Protection) support on Windows 2022.
Memory Encryption	Enables or disables the Intel Total Memory Encryption (TME) and Multi-Tenant (Intel® TME-MT). When option is set to Disabled , BIOS disables both TME and MK-TME technology. When option is set to Single Key BIOS enables the TME technology. When option is set to Multiple Keys , BIOS enables the TME-MT technology, the CPU Physical Address Limit option must be disabled for selecting Multiple Keys option. This option is set to Disabled by default.
Intel(R) SGX	Enables you to set the Intel Software Guard Extension (SGX) option. To enable the Intel SGX option, processor must be SGX capable, memory population must be compatible (minimum x8 identical DIMM1 to DIMM8 per CPU socket, not support on persistent memory configuration), memory operating mode must be set at optimizer mode, memory encryption must be enabled and node interleaving must be disabled. This option is set to Off by default. When this option is to Off , BIOS disables the SGX technology. When this option is to On , BIOS enables the SGX technology.
SGX Package Info In-Band Access	Enables you to access the Intel Software Guard Extension (SGX) package info in-band option. This option is set to Off by default.
PPMRR Size	Sets the PPMRR size.
SGX QoS	Enables or disables the SGX quality of service.

Table 5. System Security details (continued)



Option	Description
Select Owner EPOCH input type	Enables you to select Change to New random Owner EPOCHs or Manual User Defined Owner EPOCHs . Each EPOCH is 64-bit. After generating new EPOCH by selecting Change to New random Owner EPOCHs , the selection reverts back to Manual User Defined Owner EPOCHs .
	Software Guard Extensions Epoch n: Sets the Software Guard Extensions Epoch values.
Enable writes to SGXLEPUBKEYHASH[3:0] from OS/SW	Enables or disables the Enable writes to SGXLEPUBKEYHASH[3:0] from OS/SW.
	SGX LE Public Key Hash0: Sets the bytes from 0-7 for SGX Launch Enclave Public Key Hash.
	SGX LE Public Key Hash1: Sets the bytes from 8-15 for SGX Launch Enclave Public Key Hash.
	SGX LE Public Key Hash2: Sets the bytes from 16-23 for SGX Launch Enclave Public Key Hash.
SGX LE Public Key Hash3: Sets the bytes from 24-31 for SGX Launch Enclave Public Key Hash.	
Enable/Disable SGX Auto MP Registration Agent	Enables or disables the SGX Auto MP Registration. The MP registration agent is responsible to register the platform.
SGX Factory Reset	Enables you to reset the SGX option to factory settings. This option is set to Off by default.
Power Button	Enables or disables the power button on the front of the system. This option is set to Enabled by default.
AC Power Recovery	Sets how the system behaves after AC power is restored to the system. This option is set to Last by default.  NOTE: The host system will not power on up until iDRAC Root of Trust (RoT) is completed, host power on will be delayed by minimum 90 seconds after the AC applied.
AC Power Recovery Delay	Sets the time delay for the system to power up after AC power is restored to the system. This option is set to Immediate by default. When this option is set to Immediate , there is no delay for power up. When this option is set to Random , the system creates a random delay for power up. When this option is set to User Defined , the system delay time is manually to power up.
User Defined Delay (60 s to 600 s)	Sets the User Defined Delay option when the User Defined option for AC Power Recovery Delay is selected. The actual AC recovery time needs to add iDRAC root of trust time (around 50 seconds).
UEFI Variable Access	Provides varying degrees of securing UEFI variables. When set to Standard (the default), UEFI variables are accessible in the operating system per the UEFI specification. When set to Controlled , selected UEFI variables are protected in the environment and new UEFI boot entries are forced to be at the end of the current boot order.
In-Band Manageability Interface	When set to Disabled , this setting hides the Management Engine's (ME), HECI devices, and the system's IPMI devices from the operating system. This prevents the operating system from changing the ME power capping settings, and blocks access to all in-band management tools. All management should be managed through out-of-band. This option is set to Enabled by default.  NOTE: BIOS update requires HECI devices to be operational and DUP updates require IPMI interface to be operational. This setting needs to be set to Enabled to avoid updating errors.
SMM Security Migration	Enables or disables the UEFI SMM security migration protections. It is enabled for Windows 2022 support.

Table 5. System Security details (continued)

Option	Description								
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to Disabled by default.								
Secure Boot Policy	When Secure Boot policy is set to Standard , the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot policy is set to Custom , the BIOS uses the user-defined key and certificates. Secure Boot policy is set to Standard by default.								
Secure Boot Mode	<p>Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx).</p> <p>If the current mode is set to Deployed Mode, the available options are User Mode and Deployed Mode. If the current mode is set to User Mode, the available options are User Mode, Audit Mode, and Deployed Mode.</p> <p>Table 6. Secure Boot Mode</p> <table border="1" data-bbox="517 674 1481 1285"> <thead> <tr> <th data-bbox="521 680 675 719">Options</th> <th data-bbox="678 680 1476 719">Descriptions</th> </tr> </thead> <tbody> <tr> <td data-bbox="521 723 675 880">User Mode</td> <td data-bbox="678 723 1476 880">In User Mode, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes.</td> </tr> <tr> <td data-bbox="521 884 675 1126">Audit mode</td> <td data-bbox="678 884 1476 1126">In Audit Mode, PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table, but executes the images whether they pass or fail verification. Audit Mode is useful for programmatic determination of a working set of policy objects.</td> </tr> <tr> <td data-bbox="521 1131 675 1281">Deployed Mode</td> <td data-bbox="678 1131 1476 1281">Deployed Mode is the most secure mode. In Deployed Mode, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.</td> </tr> </tbody> </table>	Options	Descriptions	User Mode	In User Mode , PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes.	Audit mode	In Audit Mode , PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table, but executes the images whether they pass or fail verification. Audit Mode is useful for programmatic determination of a working set of policy objects.	Deployed Mode	Deployed Mode is the most secure mode. In Deployed Mode , PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.
Options	Descriptions								
User Mode	In User Mode , PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes.								
Audit mode	In Audit Mode , PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table, but executes the images whether they pass or fail verification. Audit Mode is useful for programmatic determination of a working set of policy objects.								
Deployed Mode	Deployed Mode is the most secure mode. In Deployed Mode , PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.								
Secure Boot Policy Summary	Specifies the list of certificates and hashes that secure boot uses to authenticate images.								
Secure Boot Custom Policy Settings	<p>Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to Custom option. The list below provides the descriptions of different Secure Boot Custom Policy Settings available:</p> <ul style="list-style-type: none"> ● Platform Key (PK) - Import, export, delete, or restore the Platform Key (PK) ● Key Exchange Key Database (KEK) - Import, export, delete, or restore entries in the key exchange key (KEK) database ● Authorized Signature Database (db) - Import, export, delete, or restore entries in the authorized signature database (db) ● Forbidden Signature Database (dbx) - Import, export, delete, or restore entries in the forbidden signature database (dbx) ● Delete All Policy Entries (PK, KEK, db, and dbx) - Restore the system manufacturer's default entries for the PK, KEK, db, and dbx database. All imported entries will be removed. ● Export Firmware Hash Values - Export values for third-party firmware images such as network controller firmware and storage controller firmware <ul style="list-style-type: none"> ○ Select Firmware Image - This is a list of third-party firmware images that the system attempted to load on this boot. Choose an image and then select "Export" to write the SHA-256 hash value of the image to a file ○ Export Selected Entry - Write the selected database entry to a file 								

PSU specifications

The PowerEdge T550 system supports up to two AC power supply units (PSUs).

Table 7. PSU specifications

PSU	Class	Heat dissipation (maximum)	Frequency	Voltage	AC		DC	Current
					High line 200–240 V	Low line 100–120 V		
600 W Mixed Mode	Platinum	2250 BTU/hr	50/60 Hz	100 - 240 V, autoranging	600 W	600 W	N/A	7.1 A - 3.6 A
	N/A	2250 BTU/hr	N/A	240 V DC	N/A	N/A	600 W	2.9 A
800 W Mixed Mode	Platinum	3000 BTU/hr	50/60 Hz	100 - 240 V, autoranging	800 W	800 W	N/A	9.2 A - 4.7 A
	N/A	3000 BTU/hr	N/A	240 V DC	N/A	N/A	800 W	3.8 A
1100 W DC	N/A	4265 BTU/hr	N/A	-48 VDC – -60 VDC	N/A	N/A	1100 W	27 A
1100 W Mixed Mode	Titanium	4,125 BTU/hr	50/60 Hz	100 - 240 V	1100 W	1050 W	N/A	12 A - 6.3 A
	N/A	4,125 BTU/hr	N/A	240 V DC	N/A	N/A	1100 W	5.2 A
1400 W Mixed Mode	Platinum	5250 BTU/hr	50/60 Hz	100 - 240 V	1400 W	1050 W	N/A	12 A - 8 A
	N/A	5250 BTU/hr	N/A	240 V DC	N/A	N/A	1400 W	6.6 A
2400 W Mixed Mode	Platinum	9000 BTU/hr	50/60 Hz	100 - 240 V	2400 W	1400 W	N/A	16 A - 13.5 A
	N/A	9000 BTU/hr	N/A	240 V DC	N/A	N/A	2400 W	11.2 A
700 W Mixed Mode	Titanium	2,625 BTU/hr	50/60 Hz	200–240 V AC	700 W	NA	NA	4.1 A
	NA	2,625 BTU/hr	NA	240 V DC	NA	NA	700 W	3.4 A

Table 7. PSU specifications (continued)

PSU	Class	Heat dissipation (maximum)	Frequency	Voltage	AC		DC	Current
					High line 200–240 V	Low line 100–120 V		
1800 W Mixed Mode	Titanium	6,000 BTU/hr	50/60 Hz	200–240 V AC	1800 W	NA	NA	10 A
	NA	6000 BTU/hr	NA	240 V DC	NA	NA	1800 W	8.2 A

NOTE: This system is also designed to connect to the IT power systems with a phase-to-phase voltage not exceeding 240 V.

NOTE: Heat dissipation is calculated using the PSU wattage rating.

NOTE: When selecting or upgrading the system configuration, to ensure optimum power utilization, verify the system power consumption with the Enterprise Infrastructure Planning Tool available at Dell.com/calc.