

# PowerEdge T640 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.

- Chapter 1: Overview..... 4**
  - Revision history..... 4
- Chapter 2: Information Update..... 5**
  - Backplane connectors..... 5
  - System Security..... 7
    - Viewing System Security..... 7
    - System Security Settings details..... 7

# 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	June, 2022	<ol style="list-style-type: none"><li>1. Updated backplane connectors</li><li>2. Updated system security settings</li><li>3. Updated storage</li></ol>

# Information Update

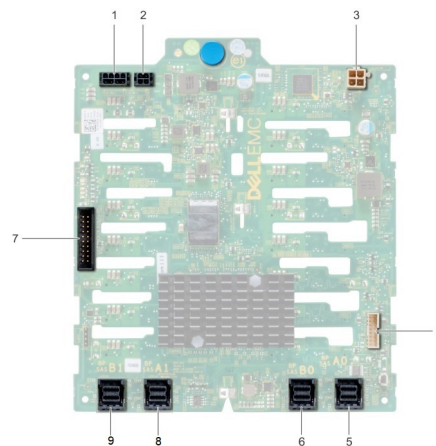
## Topics:

- [Backplane connectors](#)
- [System Security](#)

## Backplane connectors

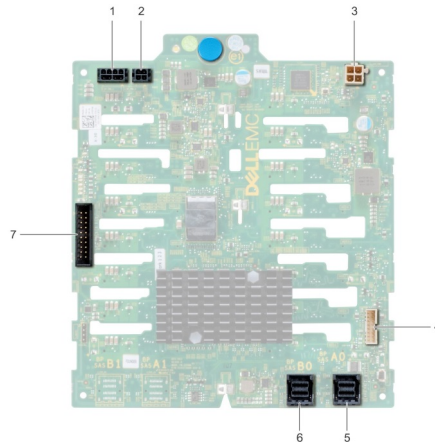
Depending on the configuration, your system supports one of the following:

- 8 x 3.5 inch SAS/SATA backplane
- 18 x 3.5 inch SAS/SATA backplane
- 8 x 2.5 inch Dell PowerEdge Express Flash (NVMe) backplane
- 16 x 2.5 inch SAS/SATA backplane with the optional additional backplanes below:
  - 8 x 2.5 inch NVMe backplane
  - 16 x 2.5 inch SAS/SATA backplane (FlexBay)
- 32 x 2.5 inch SAS/SATA backplane



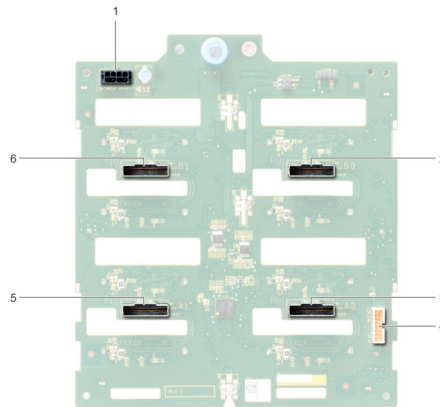
**Figure 1. 16 x 2.5 inch SAS/SATA backplane for FlexBay (upper)**

- |  |   |
|--|---|
| 1. backplane power connector A [J_BP_PWR_A]  | 2. backplane power connector B [J_BP_PWR_B] |
| 3. optical drive power connector [J_ODD_PWR] | 4. backplane signal connector [J_BP_SIG]    |
| 5. SAS A0 connector [J_SAS_A0]               | 6. SAS B0 connector [J_SAS_B0]              |
| 7. I2C connector                             | 8. SAS A1 connector [J_EXP_A1]              |
| 9. SAS B1 connector [J_EXP_B1]               |   |



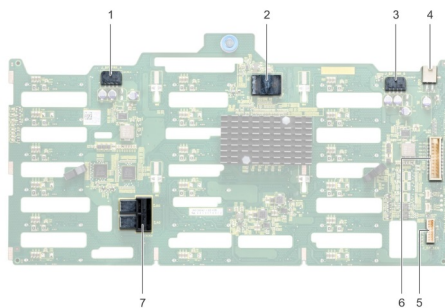
**Figure 2. 16 x 2.5 inch SAS/SATA backplane (lower)**

- |  |   |
|--|---|
| 1. backplane power connector A [J_BP_PWR_A]  | 2. backplane power connector B [J_BP_PWR_B] |
| 3. optical drive power connector [J_ODD_PWR] | 4. backplane signal connector [J_BP_SIG]    |
| 5. SAS A0 connector [J_SAS_A0]               | 6. SAS B0 connector [J_SAS_B0]              |
| 7. I2C connector                             |   |



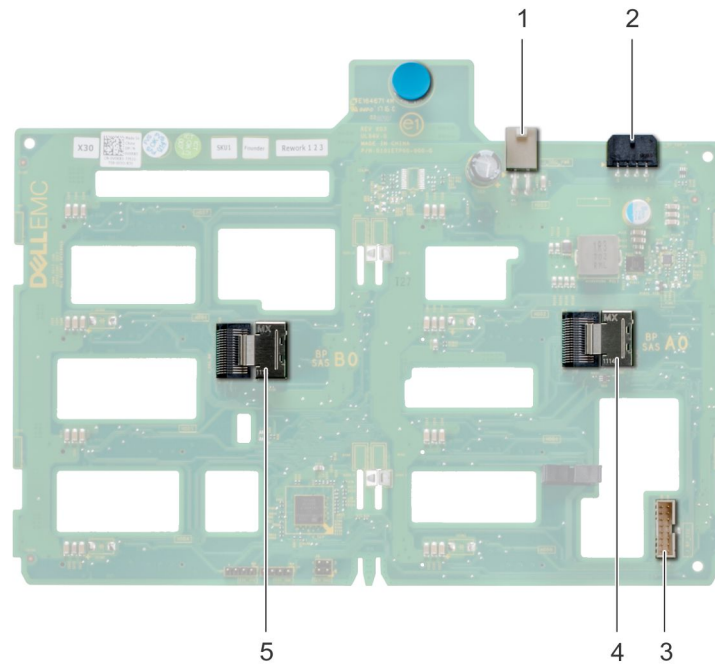
**Figure 3. 8 x 2.5 inch NVMe backplane**

- |  |   |
|--|---|
| 1. backplane power connector [J_BP_PWR1] | 2. PCIe B0 connector [J_PCIE_B0]          |
| 3. PCIe A0 connector [J_PCIE_A0]         | 4. backplane signal connector [J_BP_SIG1] |
| 5. PCIe A1 connector [J_PCIE_A1]         | 6. PCIe B1 connector [J_PCIE_B1]          |



**Figure 4. 18 x 3.5 inch SAS/SATA backplane**

- |  |   |
|--|---|
| 1. backplane power connector A [J_BP_PWR_A1] | 2. controller                             |
| 3. backplane power connector B [J_BP_PWR_B1] | 4. optical drive power connector [J_ODD1] |
| 5. I2C connector                             | 6. backplane signal connector [J_BP_SIG1] |
| 7. SAS A0_B0 connector [J_SAS_A0_B0]         |   |



**Figure 5. 8 x 3.5 inch SAS/SATA backplane**

- |   |   |
|---|---|
| 1. optical drive power connector [J_ODD1] | 2. backplane power connector [J_BP_PWR_A] |
| 3. SAS A0 connector [J_BP_SIG]            | 4. backplane signal connector [J_SAS_A0]  |
| 5. SAS B0 connector [J_SAS_B0]            |   |

## System Security

You can use the **System Security** screen to perform specific functions such as setting the system password, setup password and disabling the power button.

### Viewing System Security

To view the **System Security** screen, perform the following steps:

#### Steps

1. Power on, or restart your system.
2. Press F2 immediately after you see the following message:

F2 = System Setup




**NOTE:** If your operating system begins to load before you press F2, wait for the system to finish booting, and then restart your system and try again.

3. On the **System Setup Main Menu** screen, click **System BIOS**.
4. On the **System BIOS** screen, click **System Security**.

### System Security Settings details

#### About this task

The **System Security Settings** screen details are explained as follows:

Option	Description
<b>CPU AES-NI</b>	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 <b>Enabled</b> by default.
<b>System Password</b>	Enables you to set the system password. This option is set to <b>Enabled</b> by default and is read-only if the password jumper is not installed in the system.
<b>Setup Password</b>	Enables you to set the system setup password. This option is read-only if the password jumper is not installed in the system.
<b>Password Status</b>	Enables you to lock the system password. This option is set to <b>Unlocked</b> by default.
<b>TPM Security</b>	<p> <b>NOTE:</b> 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 <b>TPM Security</b> option is set to <b>Off</b> by default. You can only modify the TPM Status TPM Activation, and the Intel TXT fields if the <b>TPM Status</b> field is set to either <b>On with Pre-boot Measurements</b> or <b>On without Pre-boot Measurements</b>.</p>
<b>TPM Information</b>	Enables you to change the operational state of the TPM. This option is set to <b>Type: 2.0-NTZ</b> by default.
<b>TPM Status</b>	Specifies the TPM status.
<b>TPM Command</b>	<p>Controls the Trusted Platform Module (TPM). When set to <b>None</b>, no command is sent to the TPM. When set to <b>Activate</b>, the TPM is enabled and activated. When set to <b>Deactivate</b>, the TPM is disabled and deactivated. When set to <b>Clear</b>, all the contents of the TPM are cleared. This option is set to <b>None</b> by default.</p> <p> <b>CAUTION:</b> Clearing the TPM results in the loss of all keys in the TPM. The loss of TPM keys may affect booting to the operating system.</p> <p>This field is read-only when <b>TPM Security</b> is set to <b>Off</b>. The action requires an additional reboot before it can take effect.</p>
<b>TPM Heirarchy</b>	<p>Allow enabling, disabling, or clearing the storage and endorsement hierarchies.</p> <p>When set to <b>Enabled</b>, the storage and endorsement hierarchies can be used.</p> <p>When set to <b>Disabled</b>, the storage and endorsement hierarchies cannot be used.</p> <p>When set to <b>Clear</b>, the storage and endorsement hierarchies are cleared of any values, and then reset to <b>Enabled</b>.</p>
<b>TPM Advanced Settings</b>	This setting is enabled only when TPM Security is set to ON.
<b>Intel(R) TXT</b>	Enables you to set the Intel Trusted Execution Technology (TXT) option. To enable the <b>Intel TXT</b> option, virtualization technology and TPM Security must be enabled with Pre-boot measurements. This option is set to <b>Off</b> by default.
<b>Power Button</b>	Enables you to set the power button on the front of the system. This option is set to <b>Enabled</b> by default.
<b>AC Power Recovery</b>	Sets how the system behaves after AC power is restored to the system. This option is set to <b>Last</b> by default.
<b>AC Power Recovery Delay</b>	Enables you to set the time that the system should take to turn on after AC power is restored to the system. This option is set to <b>Immediate</b> by default.
<b>User Defined Delay (60 s to 600 s)</b>	Enables you to set the <b>User Defined Delay</b> option when the <b>User Defined</b> option for <b>AC Power Recovery Delay</b> is selected.
<b>UEFI Variable Access</b>	Provides varying degrees of securing UEFI variables. When set to <b>Standard</b> (the default), UEFI variables are accessible in the operating system per the UEFI specification. When set to <b>Controlled</b> , 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.
<b>In-Band Manageability Interface</b>	<p>When set to <b>Disabled</b>, 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 <b>Enabled</b> by default.</p> <p> <b>NOTE:</b> BIOS update requires HECI devices to be operational and DUP updates require IPMI interface to be operational. This setting needs to be set to <b>Enabled</b> to avoid updating errors.</p>



Option	Description								
<b>Secure Boot</b>	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 <b>Disabled</b> by default.								
<b>Secure Boot Policy</b>	When Secure Boot policy is set to <b>Standard</b> , the BIOS uses the system manufacturer key and certificates to authenticate pre-boot images. When Secure Boot policy is set to <b>Custom</b> , the BIOS uses the user-defined key and certificates. Secure Boot policy is set to <b>Standard</b> by default.								
<b>Secure Boot Mode</b>	<p>Enables you to configure how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx).</p> <p>If the current mode is set to <b>Deployed Mode</b>, the available options are <b>User Mode</b> and <b>Deployed Mode</b>. If the current mode is set to <b>User Mode</b>, the available options are <b>User Mode</b>, <b>Audit Mode</b>, and <b>Deployed Mode</b>.</p> <table> <tr> <th>Options</th><th>Description</th></tr> <tr> <td><b>User Mode</b></td><td> <p>In <b>User Mode</b>, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p>BIOS allows unauthenticated programmatic transitions between modes.</p> </td></tr> <tr> <td><b>Audit Mode</b></td><td> <p>In <b>Audit mode</b>, PK is not present. BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p><b>Audit Mode</b> is useful for programmatically determining a working set of policy objects.</p> <p>BIOS performs signature verification on pre-boot images. BIOS also logs the results in the image Execution Information Table, but approves the images whether they pass or fail verification.</p> </td></tr> <tr> <td><b>Deployed Mode</b></td><td> <p><b>Deployed Mode</b> is the most secure mode. In <b>Deployed Mode</b>, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p><b>Deployed Mode</b> restricts the programmatic mode transitions.</p> </td></tr> </table>	Options	Description	<b>User Mode</b>	<p>In <b>User Mode</b>, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p>BIOS allows unauthenticated programmatic transitions between modes.</p>	<b>Audit Mode</b>	<p>In <b>Audit mode</b>, PK is not present. BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p><b>Audit Mode</b> is useful for programmatically determining a working set of policy objects.</p> <p>BIOS performs signature verification on pre-boot images. BIOS also logs the results in the image Execution Information Table, but approves the images whether they pass or fail verification.</p>	<b>Deployed Mode</b>	<p><b>Deployed Mode</b> is the most secure mode. In <b>Deployed Mode</b>, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p><b>Deployed Mode</b> restricts the programmatic mode transitions.</p>
Options	Description								
<b>User Mode</b>	<p>In <b>User Mode</b>, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p>BIOS allows unauthenticated programmatic transitions between modes.</p>								
<b>Audit Mode</b>	<p>In <b>Audit mode</b>, PK is not present. BIOS does not authenticate programmatic updates to the policy objects, and transitions between modes.</p> <p><b>Audit Mode</b> is useful for programmatically determining a working set of policy objects.</p> <p>BIOS performs signature verification on pre-boot images. BIOS also logs the results in the image Execution Information Table, but approves the images whether they pass or fail verification.</p>								
<b>Deployed Mode</b>	<p><b>Deployed Mode</b> is the most secure mode. In <b>Deployed Mode</b>, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.</p> <p><b>Deployed Mode</b> restricts the programmatic mode transitions.</p>								
<b>Secure Boot Policy Summary</b>	Specifies the list of certificates and hashes that secure boot uses to authenticate images.								
<b>Secure Boot Custom Policy Settings</b>	Configures the Secure Boot Custom Policy. To enable this option, set the <b>Secure Boot Policy</b> to <b>Custom</b> .								