Configuring Trusted Platform Module

- Trusted Platform Module, page 1
- Intel Trusted Execution Technology, page 1
- Configuring Trusted Platform, page 2

**Trusted Platform Module**

The Trusted Platform Module (TPM) is a component that can securely store artifacts that are used to authenticate the server. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. It is a requirement for the Intel Trusted Execution Technology (TXT) security feature, which must be enabled in the BIOS settings for a server equipped with a TPM. Only the modular servers in Cisco UCSME-2814 compute cartridges include support for TPM. TPM is enabled by default on these servers.

**Intel Trusted Execution Technology**

Intel Trusted Execution Technology (TXT) provides greater protection for information that is used and stored on the business server. A key aspect of that protection is the provision of an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data, invisible to the rest of the system. Intel TXT provides for a sealed portion of storage where sensitive data such as encryption keys can be kept, helping to shield them from being compromised during an attack by malicious code. Only the modular servers in Cisco UCSME-2814 compute cartridges include support for TXT. TXT is disabled by default on these servers.

TXT can be enabled only after TPM, Intel Virtualization technology (VT) and Intel Virtualization Technology for Directed I/O (VT-d) are enabled. When you only enable TXT, it also implicitly enables TPM, VT, and VT-d.
Configuring Trusted Platform

The modular servers in Cisco UCSME-2814 compute cartridges include support for TPM and TXT. UCS Manager Release 2.5(2) allows you to perform the following operations on TPM and TXT:

- Configuring Trusted Platform, on page 2
- Clearing TPM for a Modular Server, on page 3
- Viewing TPM Properties, on page 3

**Configuring Trusted Platform**

**Procedure**

**Step 1** In the Navigation pane, click the Servers tab.

**Step 2** On the Servers tab, expand Servers > Policies.

**Step 3** Expand the node for the organization where you want to configure TPM.

**Step 4** Expand BIOS Policies and select the BIOS policy for which you want to configure TPM.

**Step 5** In the Work pane, click the Advanced tab.

**Step 6** Click the Trusted Platform subtab.

**Step 7** To configure TPM, click one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disables TPM</td>
</tr>
<tr>
<td>enabled</td>
<td>Enables TPM</td>
</tr>
<tr>
<td>Platform Default</td>
<td>Enables TPM</td>
</tr>
</tbody>
</table>

**Step 8** To configure TXT, click one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disables TXT</td>
</tr>
<tr>
<td>enabled</td>
<td>Enables TXT</td>
</tr>
<tr>
<td>Platform Default</td>
<td>Disables TXT</td>
</tr>
</tbody>
</table>

**Step 9** Click Save Changes.
Clearing TPM for a Modular Server

You can clear TPM only on the modular servers that include support for TPM.

⚠️ Caution

Clearing TPM is a potentially hazardous operation. The OS may stop booting. You may also see loss of data.

Before You Begin

TPM must be enabled.

Procedure

1. In the Navigation pane, click the Equipment tab.
2. On the Equipment tab, expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
3. Choose the server for which you want to clear TPM.
4. In the Work pane, click the General tab.
5. In the Actions area, click Recover Server.
6. In the Recover Server dialog box, click Clear TPM, then click OK.

Viewing TPM Properties

Procedure

1. In the Navigation pane, click the Equipment tab.
2. On the Equipment tab, expand Equipment > Chassis > Chassis Number > Cartridges > Cartridge Number > Servers
3. Choose the server for which you want to view the TPM settings.
4. On the Work pane, click the Inventory tab.
5. Click the Motherboard subtab.