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:

- Enabling or Disabling TPM, on page 2
- Enabling or Disabling TXT, on page 3
- Clearing TPM for a Modular Server, on page 4
- Viewing TPM Properties, on page 5

Enabling or Disabling TPM

SUMMARY STEPS

1. UCS-A# scope org org-name
2. UCS-A /org # create bios-policy policy-name
3. UCS-A /org/bios-policy* # set trusted-platform-module-config tpm-state {enabled | disabled | platform-default}
4. UCS-A /org/bios-policy* # commit-buffer
5. UCS-A /org # create service-profile sp-name}
6. UCS-A /org/service-profile* # set bios-policy policy-name
7. UCS-A /org/service-profile* # commit-buffer
8. UCS-A /org/service-profile # associate server chassis-id / cartridge-id / slot-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>UCS-A# scope org org-name</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the org-name.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>UCS-A /org # create bios-policy policy-name</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>UCS-A /org/bios-policy* # set trusted-platform-module-config tpm-state {enabled</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Specifies whether TPM is enabled or disabled. platform-default is TPM enabled.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>UCS-A /org/bios-policy* # commit-buffer</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>
| **Step 5** | UCS-A /org # create service-profile sp-name}
| **Purpose** | Creates the service profile specified and enters service profile configuration mode. |
| **Step 6** | UCS-A /org/service-profile* # set bios-policy policy-name |
| **Purpose** | Associates the specified BIOS policy with the service profile. |
### Enabling or Disabling TXT

#### SUMMARY STEPS

1. UCS-A# scope org org-name
2. UCS-A /org # create bios-policy policy-name
3. UCS-A /org/bios-policy* # set intel-trusted-execution-technology-config txt-support {enabled | disabled | platform-default}
4. UCS-A /org/bios-policy* # commit-buffer
5. UCS-A /org # create service-profile sp-name
6. UCS-A /org/service-profile* # set bios-policy policy-name
7. UCS-A /org/service-profile* # commit-buffer
8. UCS-A /org/service-profile # associate server chassis-id / cartridge-id / slot-id

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# scope org org-name</td>
<td>Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the org-name.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A /org # create bios-policy policy-name</td>
<td>Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A /org/bios-policy* # set intel-trusted-execution-technology-config txt-support {enabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

The following example shows how to enable TPM:

```
UCS-A # scope org
UCS-A /org # create bios-policy bp1
UCS-A /org/bios-policy* # set trusted-platform-module-config tpm-state enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org/service-profile* # associate server
```

---

### Configuring Trusted Platform Module

#### Purpose

- Enters the organization mode for the specified organization.
- Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.
- Specifies whether TXT is enabled or disabled. platform-default is TXT disabled.
## 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.

### SUMMARY STEPS

1. UCS-A# `scope server chassis-id/cartridge-id/server-id`
2. UCS-A# `/chassis/cartridge/server # scope tpm tpm-ID`
3. UCS-A# `/chassis/cartridge/server/tpm # set adminaction clear-config`
4. UCS-A# `/chassis/cartridge/server/tpm # commit-buffer`

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>UCS-A /org/bios-policy* # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>UCS-A /org # create service-profile sp-name</td>
<td>Creates the service profile specified and enters service profile</td>
</tr>
<tr>
<td></td>
<td>configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>UCS-A /org/service-profile* # set bios-policy policy-name</td>
<td>Associates the specified BIOS policy with the service profile.</td>
</tr>
<tr>
<td>Step 7</td>
<td>UCS-A /org/service-profile* # commit-buffer</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td>Step 8</td>
<td>UCS-A /org/service-profile # associate server</td>
<td>Associates the service profile with a single server.</td>
</tr>
</tbody>
</table>

The following example shows how to enable TXT:

```
UCS-A # scope org
UCS-A /org # create bios-policy bp1
UCS-A /org/bios-policy* # set intel-trusted-execution-technology-config txt-support enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org # create service-profile sp1
UCS-A /org/service-profile* # set bios-policy bp1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # associate server chassis-id / cartridge-id / slot-id
```
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# <code>scope server chassis-id/cartridge-id/server-id</code></td>
<td>Enters server mode for the specified server.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A# <code>/chassis/cartridge/server # scope tpm tpm-ID</code></td>
<td>Enters org TPM mode for the specified TPM.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A# <code>/chassis/cartridge/server/tpm # set adminaction clear-config</code></td>
<td>Specifies that the TPM is to be cleared.</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A# <code>/chassis/cartridge/server/tpm # commit-buffer</code></td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

The following example shows how to clear TPM for a modular server:

```
UCS-A# scope server 1/3/1
UCS-A# /chassis/cartridge/server # scope tpm 1
UCS-A# /chassis/cartridge/server/tpm # set adminaction clear-config
UCS-A#/chassis/cartridge/server/tpm* # commit-buffer
```

### Viewing TPM Properties

#### SUMMARY STEPS

1. UCS-A# `scope server chassis-id/cartridge-id/server-id`
2. UCS-A `/chassis/cartridge/server # scope tpm tpm-id`
3. UCS-A `/chassis/cartridge/server/tpm # show`
4. UCS-A `/chassis/cartridge/server/tpm # show detail`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> UCS-A# <code>scope server chassis-id/cartridge-id/server-id</code></td>
<td>Enters server mode for the specified server.</td>
</tr>
<tr>
<td><strong>Step 2</strong> UCS-A <code>/chassis/cartridge/server # scope tpm tpm-id</code></td>
<td>Enters TPM mode for the specified TPM ID.</td>
</tr>
<tr>
<td><strong>Step 3</strong> UCS-A <code>/chassis/cartridge/server/tpm # show</code></td>
<td>Displays the TPM properties.</td>
</tr>
<tr>
<td><strong>Step 4</strong> UCS-A <code>/chassis/cartridge/server/tpm # show detail</code></td>
<td>Displays detailed TPM properties.</td>
</tr>
</tbody>
</table>

The following example shows how to display the TPM properties a modular server:

```
UCS-A# scope server 1/3/1
UCS-A /chassis/cartridge/server # scope tpm 1
```
UCS-A /chassis/cartridge/server/tpm # show

Trusted Platform Module:
  Presence: Equipped
  Enabled Status: Enabled
  Active Status: Activated
  Ownership: Unowned

UCS-A /chassis/cartridge/server/tpm # show detail

Trusted Platform Module:
  Enabled Status: Enabled
  Active Status: Activated
  Ownership: Unowned
  Tpm Revision: 2
  Model: UCSX-TPM2-001
  Vendor: Cisco Systems Inc
  Serial: FCH19257E58
  Admin Action: Unspecified
  Config State: Not Applied

UCS-A /chassis/cartridge/server/tpm #