Configuring Trusted Platform Module

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.

Only very basic enable/activate hardware component status is provided for TPM 2.0 and later. Nearly all status indications are software status. BIOS uses “Enable/Disable “ to abstract status **Enable/Disable Platform Hierarchy**, **Enable/Disable Storage Hierarchy**, and **Enable/Disable Endorsement Hierarchy**. That is, Enable and Activate TPM will enable all three Hierarchies, and Disable and De-activate TPM will Disable these three Hierarchies. For more information on TPM flag definitions and enabling, activation, and taking ownership of these hierarchies, specific to your implementation, refer to the TCG Trusted Platform Module Specification.

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.

Trusted Platform

The modular servers in Cisco UCSME-2814 compute cartridges include support for TPM and TXT. Cisco UCS M4 blade and rack-mount servers include support for TPM and TXT. UCS Manager Release 2.5(2)UCS Manager Release 2.2(4) allows you to perform the following operations on TPM and TXT:

- Enabling or Disabling TPM
- Clearing TPM for a Blade Server

  or

- Clearing TPM for a Rack-Mount Server

Note For Cisco UCS M3 blade servers, press **F2** to enter the BIOS setup menu and change the settings.

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

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

	Command or Action	Purpose
Step 6	UCS-A /org/service-profile* # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile.
Step 7	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.
Step 8	UCS-A /org/service-profile # **associate server** *chassis-id / cartridge-id / slot-id*	Associates the service profile with a single server.

Example

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 # 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 1/3/1
```

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

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter **/** as the *org-name*.
Step 2	UCS-A /org # **create bios-policy** *policy-name*	Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode.

	Command or Action	Purpose
Step 3	UCS-A /org/bios-policy* # **set intel-trusted-execution-technology-config txt-support** {**enabled** | **disabled** | **platform-default**}	Specifies whether TXT is **enabled** or **disabled**. **platform-default** is TXT disabled.
Step 4	UCS-A /org/bios-policy* # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCS-A /org # **create service-profile** *sp-name*}	Creates the service profile specified and enters service profile configuration mode.
Step 6	UCS-A /org/service-profile* # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile.
Step 7	UCS-A /org/service-profile* # **commit-buffer**	Commits the transaction to the system configuration.
Step 8	UCS-A /org/service-profile # **associate server** *chassis-id / cartridge-id / slot-id*	Associates the service profile with a single server.

Example

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 1/3/1
```

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**

DETAILED STEPS

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

Example

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

	Command or Action	Purpose
Step 1	UCS-A# **scope server** *chassis-id*/*cartridge-id*/*server-id*	Enters server mode for the specified server.
Step 2	UCS-A /chassis/cartridge/server # **scope tpm** *tpm-id*	Enters TPM mode for the specified TPM ID.
Step 3	UCS-A /chassis/cartridge/server/tpm # **show**	Displays the TPM properties.
Step 4	UCS-A /chassis/cartridge/server/tpm # **show detail**	Displays detailed TPM properties.

Example

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 #
```