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.

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

Procedure

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

Step 2 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:

Option	Description
disabled	Disables TPM
enabled	Enables TPM
Platform Default	Enables TPM

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

Option	Description
disabled	Disables TXT
enabled	Enables TXT
Platform Default	Disables TXT

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

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

Viewing TPM Properties

Procedure

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