Install TPM Module after RMA of SNS3700 Chassis

Contents

Introduction

Considerations

Problem

Solution

- Install the TPM Hardware and Enable it in the BIOS
- Enable the Module in CIMC
- Power Cycle the Server and Reset CIMC
- Validate that CIMC Detects the Module as Equipped and Activated
- Re-install ISE Application

Verification

Introduction

This document describes the process to install the TPM module on SNS3700 servers that got a replacement of the chassis.

Considerations

The Trusted Platform Module (TPM) is a hardware component that improves the security of the server by storing encryption keys.

Nevertheless, the server can run the Identity Services Engine (ISE) without its presence.

⚠ **Caution**: If you have ISE application installed and it runs on a server without a TPM, you need to execute the process documented here to install the module and make it usable by the system.

- This server supports TPMversion 2.0 (UCSX-TPM-002C) as defined by the Trusted Computing Group (TCG). TheTPMis also SPI-based.
- TPM cannot be replaced. Meaning, if the module is already installed, it cannot be removed and replaced since it is installed with a tamper proof screw.
- If the TPM is missing in the motherboard, then a module can be installed.
- If a server with aTPMis returned, the replacement server must be ordered with a newTPM.
- If TPM2.0 becomes unresponsive, reboot the server.

Problem

SNS 3700 series or higher, shipped from Cisco Manufacturing, have a TPM included.

However, SNS 3700 series chassis replacements, shipped from Cisco Service Depots, do not have such device included.

The next process must be executed to install the TPM and enable both hardware and software to leverage the benefits of the module.

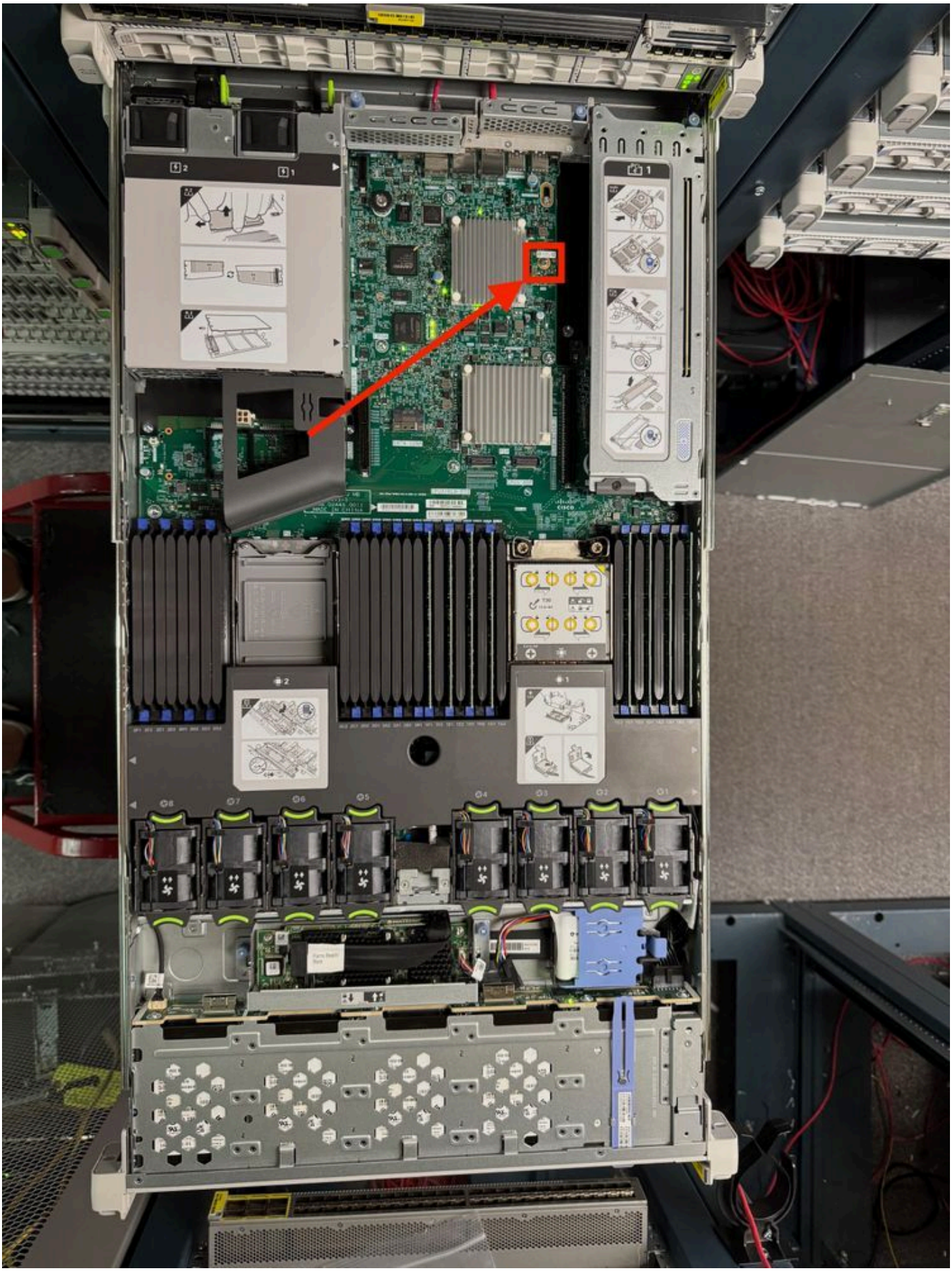


Image 1. Location of the TPM Module in the SNS 3700 Series Appliance

Solution

Execute the next steps in the given order to install the module, initialize it, and leverage the security features provided by it.

Install the TPM Hardware and Enable it in the BIOS

Use this article to complete Steps 1: [Cisco UCS C220 M6 Server Installation and Service Guide - Maintaining the Server]

The process is finished once you have completed the steps in the Enabling the TPM in the BIOS chapter.

Enable the Module in CIMC

Log in to CIMC.

Click the **menu icon > Compute > Configure BIOS > Security > Change the Trusted Platform Module State** to Enabled.

Click **Save**.

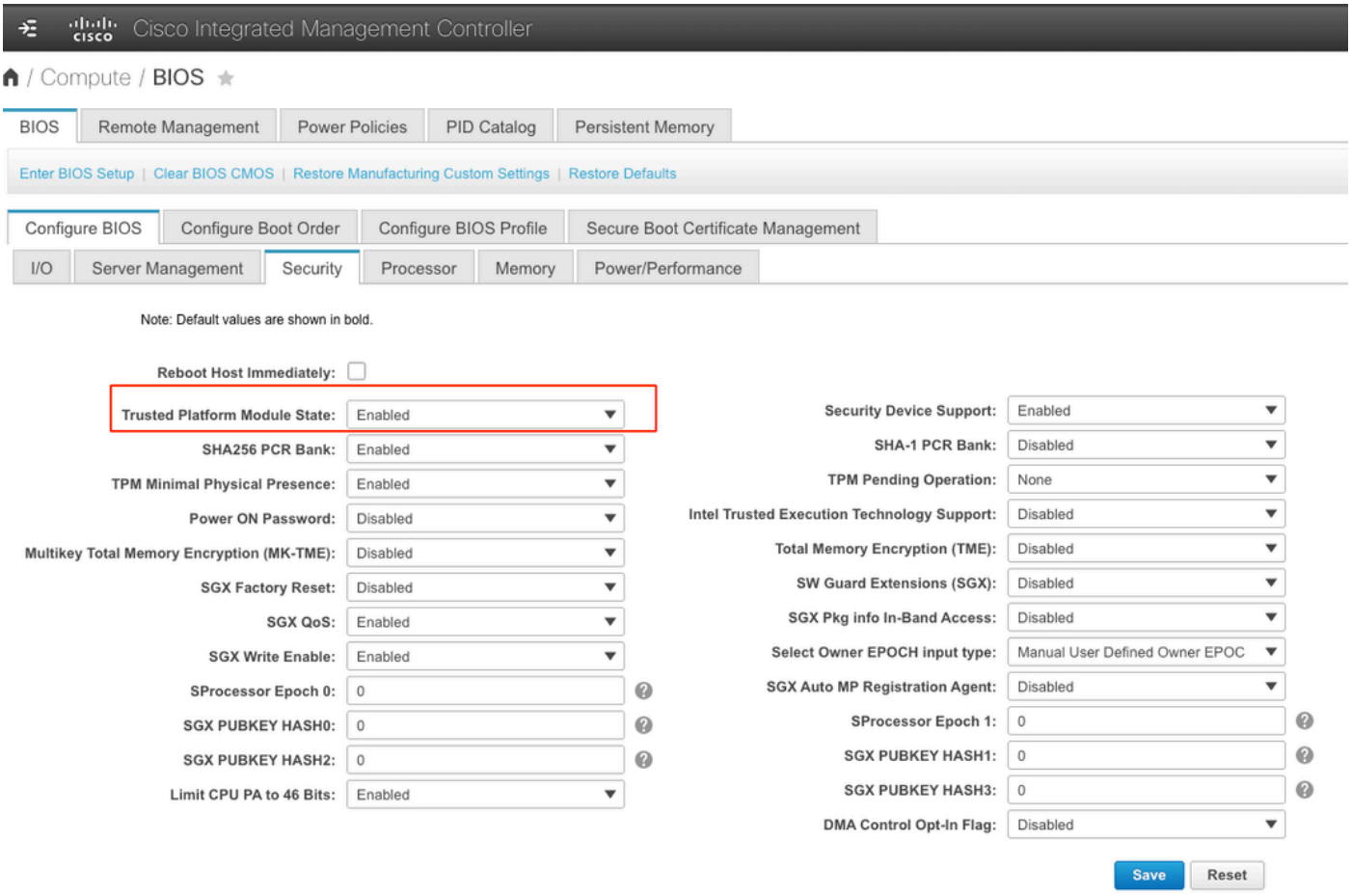


Image 2. Enabling TPM in CIMC

Power Cycle the Server and Reset CIMC

At the top of CIMC interface, click **Host Power**.

Select **Power Cycle**.

Wait 5 minutes.

At the top of the CIMC interface, click **CIMC Reboot**.

Wait for the CIMC to come back.

Validate that CIMC Detects the Module as Equipped and Activated

Once the CIMC is back, click the **menu** icon and navigate to: **Chassis > Inventory > TPM**.

The TPM must be detected and the next information must be displayed.

Presence: Equipped

Enabled Status: Enabled

Active Status: Activated



Image 3. TPM dectected, enabled and activated from CIMC perspective

Re-install ISE Application

To complete Step 5, navigate to the **next link** and access the **installation guide** for the ISE version you need to install on the server:

[Install and Upgrade Guides - Install Cisco ISE]

Once in the installation guide, navigate to the **Install Cisco ISE** section.

Verification

Once this step is completed, you must have ISE installed and running.

Get into the CLI of the node and use the next command to generate a show tech file.

ISE/user#**show tech-support file <filename>**

You can then copy the file to a repo using the **copy** command or you can download the file by accessing the

GUI and going to:

Administration > System > Maintenance > Local Disk Management

Once you have the file, open it with a **text editor** and validate that the next output shows the TPM as present.

```
**********************************************
Displaying ISE Profile ...
**********************************************
Profile : sns3755
TPM: Module Present
```