

Contents

[Introduction](#)

[Problem](#)

[Potentially Impacted Systems:](#)

[Customer Visibility / Impact:](#)

[Solution](#)

[Work Around Options:](#)

[Work Around 1 - Reset the IMC to Factory Default Settings](#)

[Work Around 2 - Resetting to Factory Defaults via IMC CLI](#)

Introduction

The intent of this document is to address the issue seen regarding Trusted Platform Module (TPM) related System Event Logs (SEL) events on some C460 M4 servers. A small number of C460 M4 SPARE servers will see a critical SEL event related to TPM presence right out of the factory. The instructions below will assist you in resolving servers impacted by this issue.

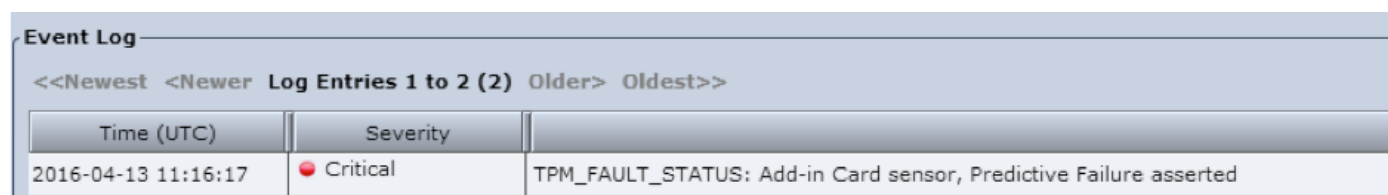
Problem

Potentially Impacted Systems:


About 614 SPARE C460 M4 Systems (Shipped between June 2nd 2014, and April 13th 2016.)

Customer Visibility / Impact:

Customers may see a critical SEL event similar to the one below on servers received from the factory.



The screenshot shows an 'Event Log' window with a navigation bar at the top containing '<<Newest <Newer Log Entries 1 to 2 (2) Older> Oldest>>'. Below the navigation bar is a table with three columns: 'Time (UTC)', 'Severity', and the event message. The first row of data shows the time '2016-04-13 11:16:17', a red circle icon followed by the word 'Critical', and the message 'TPM_FAULT_STATUS: Add-in Card sensor, Predictive Failure asserted'.

Time (UTC)	Severity	Message
2016-04-13 11:16:17	 Critical	TPM_FAULT_STATUS: Add-in Card sensor, Predictive Failure asserted

There is NO operational impact to the server, but the message may lead to unnecessary concern resulting in a call to TAC. This has to do with the way TPMs were handled in manufacturing. C460 M4 systems keep a "Cached" value for TPM presence, indicating if a TPM was ever installed in the server - every server has a TPM installed during testing. The C460 M4 also tracks the current presence of the TPM, and since all servers ordered as spares ship without a TPM, the system triggers an alarm thinking that the module that was once installed has been removed.

Solution

The work-around below will allow you to quickly address this SEL event should you wish to remove the messages. The work-around involves resetting the Integrated Management Controller

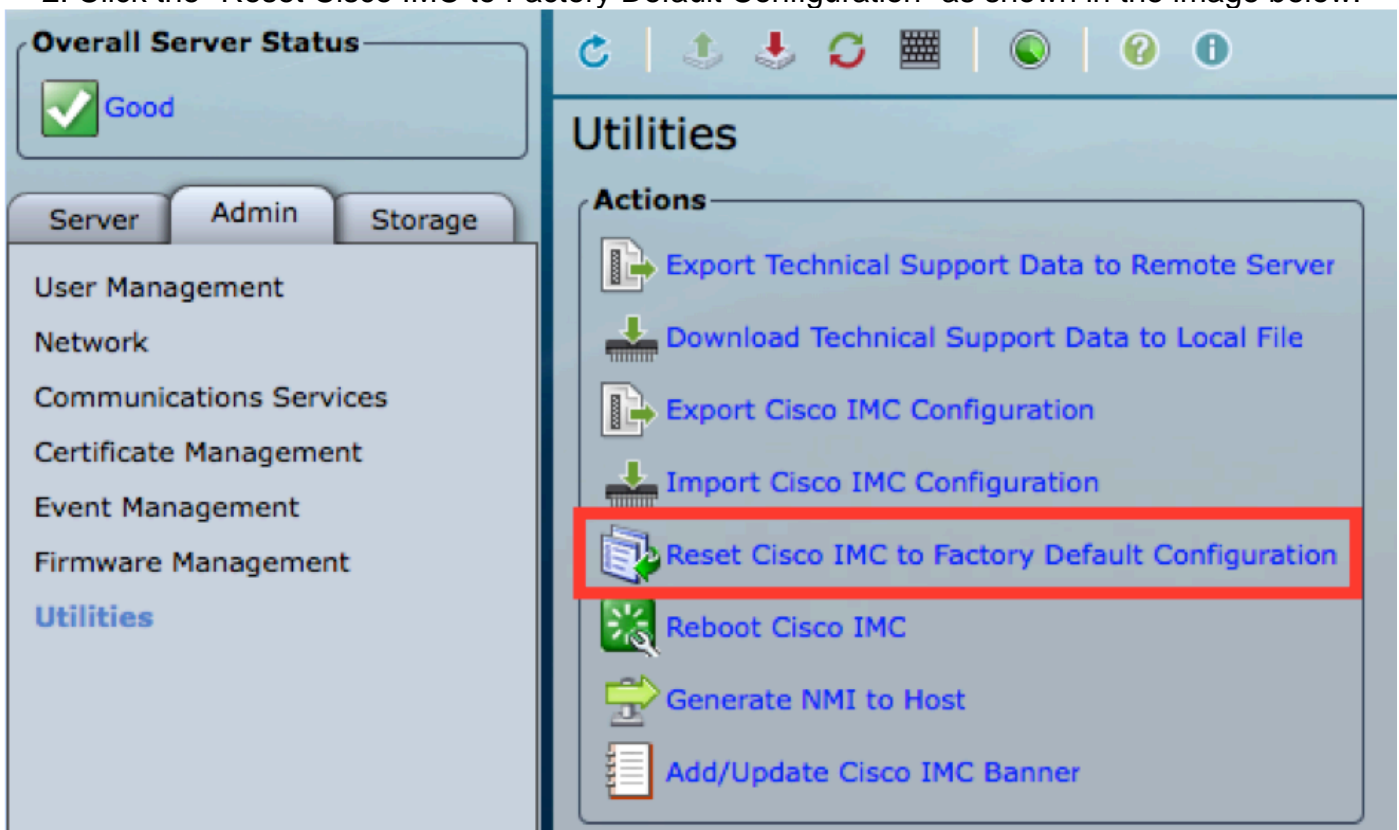
(IMC) to factory default settings, clearing any cached TPM Presence value.

Work Around Options:

Work Around 1 - Reset the IMC to Factory Default Settings

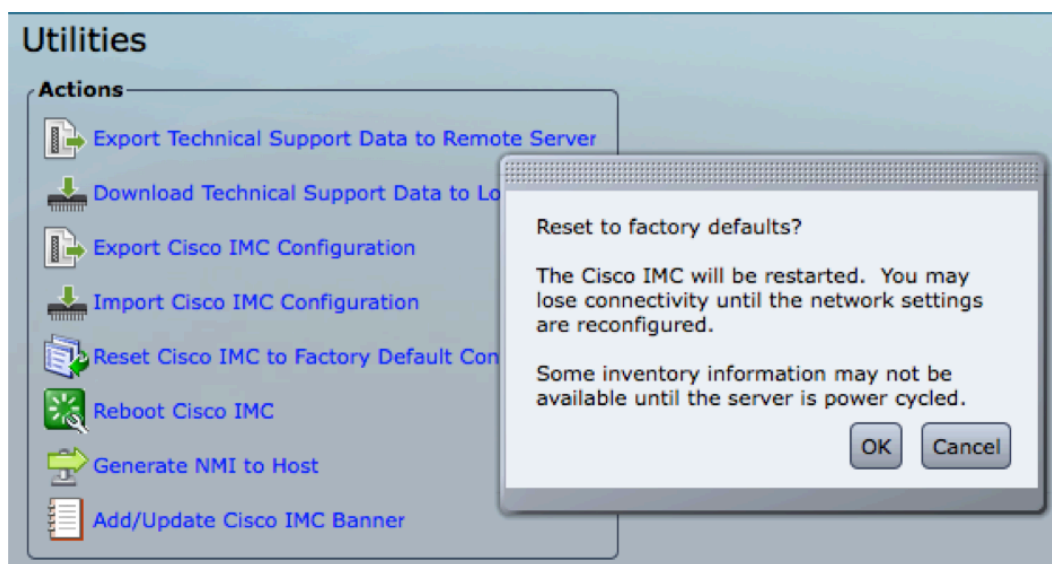
Resting to Factory Defaults via IMC WebUI

1. Point a browser to the IMC IP, login, and navigate to the Admin --> Utilities tab
2. Click the "Reset Cisco IMC to Factory Default Configuration" as shown in the image below.



3. You will be prompted with a pop up box. Click OK to proceed.

Note: *The IMC will reset completely and you will need to reconfigure all settings. Please record any information prior to the reset.*



Work Around 2 - Resetting to Factory Defaults via IMC CLI

1. SSH to the IMC IP using the user's credentials.
2. Type the following commands as shown below:
 - a. scope cimc
 - b. factory-default

```
[C240-FCH1825V2M3# scope cimc
[C240-FCH1825V2M3 /cimc # factory-default
This operation will reset the Cisco IMC configuration to factory default.
All your configuration will be lost. Some inventory information may
not be available until the server is powered on or power cycled.
Continue?[y|N]
```

3. Enter "y" to continue.

Note: *The IMC will reset completely and you will need to reconfigure all settings.*

Please record any information prior to the reset.