This Technical Advisory describes an issue which may or may not affect the customer's product

Intel Technical Advisory

TA-1167-02

5200 NE Elam Young Parkway
Hillsboro, OR 97124

December 06, 2021

Intel® Server M50CYP Family have a hardware setting that prevents functionality of Intel® Trusted Execution Technology (Intel® TXT)

Products Affected

Product Code	MM#	TA#	PBA#
M50CYP2SB1U	99A3TR	K84407-350 K84407-351 K84407-352 K84407-353 M57662-352	K73719-350 K73719-351 K73719-352
M50CYP2SBSTD	99A5A0	K57870-350 K57870-351 K57870-352 K57870-353 M57661-352	K42381-350 K42381-351 K42381-352
M50CYP1UR204	99A3TX	M11364-001 M11364-002 M56641-001	K73719-350 K73719-351 K73719-352
M50CYP1UR212	99A3TW	M11351-001 M11351-002 M56640-001	K73719-350 K73719-351 K73719-352
M50CYP2UR208	99A3TT	M11349-001 M11349-002 M56269-001	K42381-350 K42381-351 K42381-352
M50CYP2UR312	99A3TV	M11350-001 M11350-002 M56272-001	K42381-350 K42381-351 K42381-352
LCY1*	Various	Various	K73719-350 K73719-351 K73719-352
LCY2*	Various	Various	K42381-350 K42381-351 K42381-352

Only systems that must use a technology that depends on Intel® Trusted Execution Technology (Intel® TXT), such as "Secured-core" in Microsoft* Windows 2022 or Microsoft* Azure* Stack HCI are affected, since no other functional areas are impacted by this setting. If the system is not utilizing Intel® TXT or related technologies, this is informational only for the system. The resolution below may be applied or not without affecting other operational characteristics of the system.

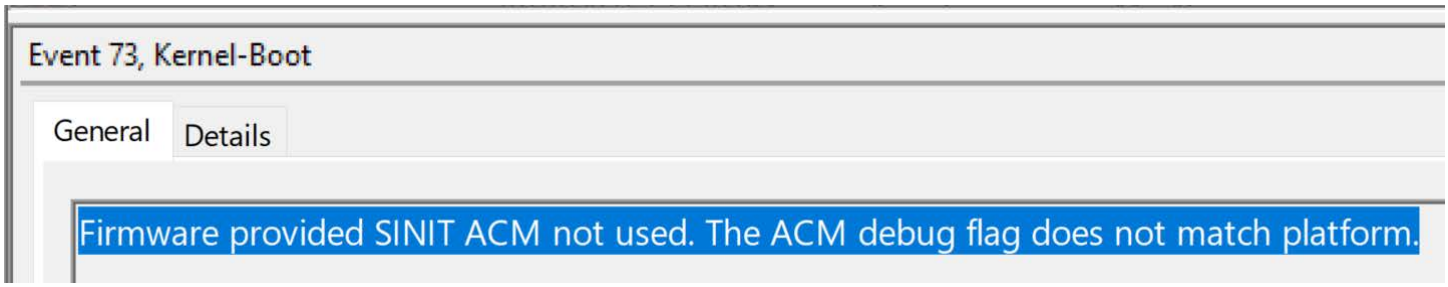
Description

The DIP Switch S5_2, which controls whether Intel® Trusted Execution Technology (Intel® TXT) may be enabled or not, is set incorrectly as shipped on the affected products. This switch is set to "ON" (which disables Intel® TXT) instead of "OFF" (which allows Intel® TXT to be enabled if the user desires). As a result, technologies, which depend upon Intel® TXT, such as the Microsoft Windows* Server 2022 and Azure* Stack HCI OSes Secured-Core capabilities, cannot be completely enabled prior to applying the below-documented resolution on the affected products.

To check in Windows* whether the DIP switch S5_2 is set incorrectly, launch the msinfo32 tool, scroll to the lines beginning with "Virtualization", and check the status of "Virtualization-based security Services Running". If "Virtualization-based security Services Running" does not show “Secure Launch”, this means that System Guard Secure Launch is not running and the DIP Switch S5_2 may be set incorrectly, as shown on the following screenshot.

Kernel DMA Protection	On
Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection,
Virtualization-based security Services Configured	Hypervisor enforced Code Integrity, Secure Launch
Virtualization-based security Services Running	Hypervisor enforced Code Integrity

Additionally, Windows* Event Log will report the following event under Applications and Services Log → Microsoft → Windows → Kernel-Boot → Operational

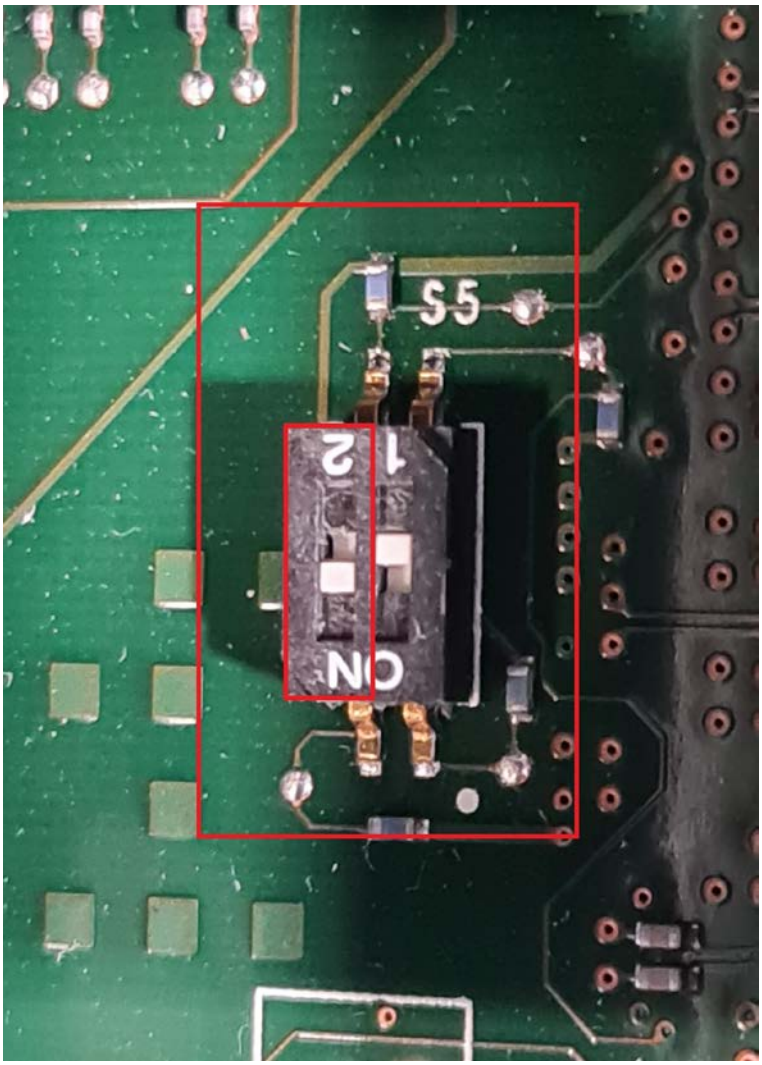


No functional failures have been observed with this issue but it does block the enabling of Intel® Trusted Execution Technology (Intel® TXT) which is a prerequisite for the “Secured-core” in Microsoft* Windows 2022 or Microsoft* Azure* Stack HCI solutions until the resolution below is implemented.

Any operating system that requires Intel® TXT may be affected by this issue and will require the solution mentioned below to fully enable and make use of Intel® TXT.

Root Cause

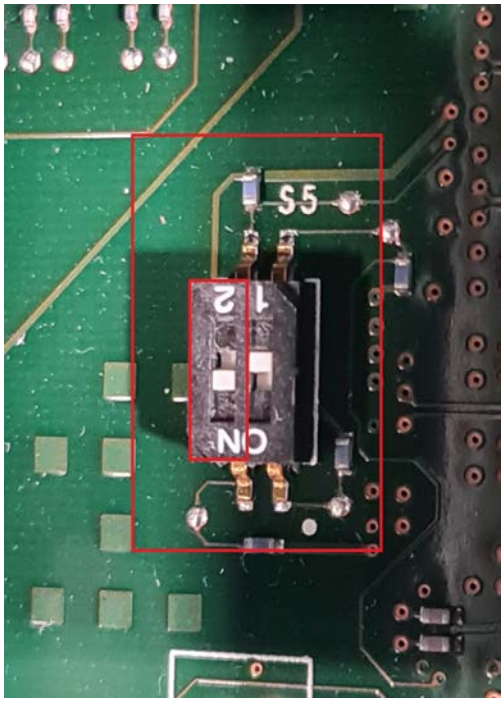
DIP Switch S5_2 switch position on the Intel® Server M50CYP family board is incorrectly set to “ON”, which prevents the system from enabling Intel® Trusted Execution Technology; the S5_2 incorrect switch pin setting can be observed in the following picture.



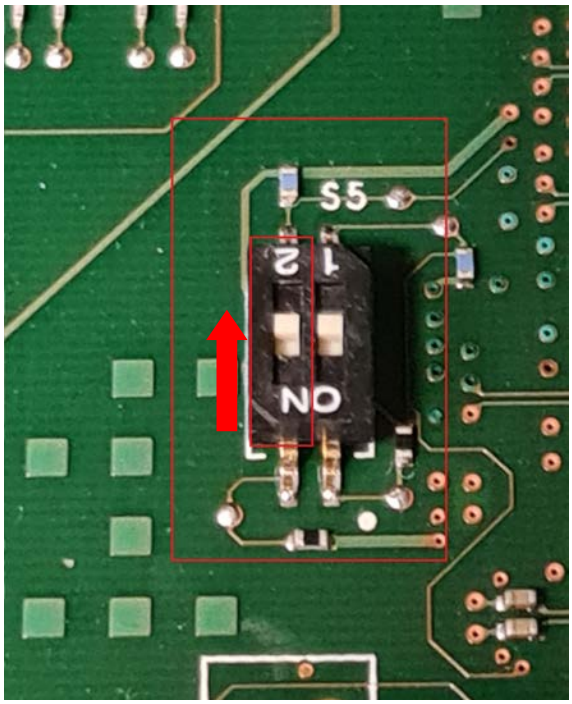
Corrective Action/Resolution

If you do not intend to use a technology that depends on Intel® Trusted Execution Technology (Intel® TXT), you do not need to perform this corrective action since no other functional areas are impacted by this setting.

To restore the ability to enable Intel® TXT, the Intel® M50CYP motherboard S5_2 switch pin must be manually moved from “ON” to “OFF” position, as shown in the pictures below. Unplug AC cord from server system before moving the pin number 2 on the S5 switch.

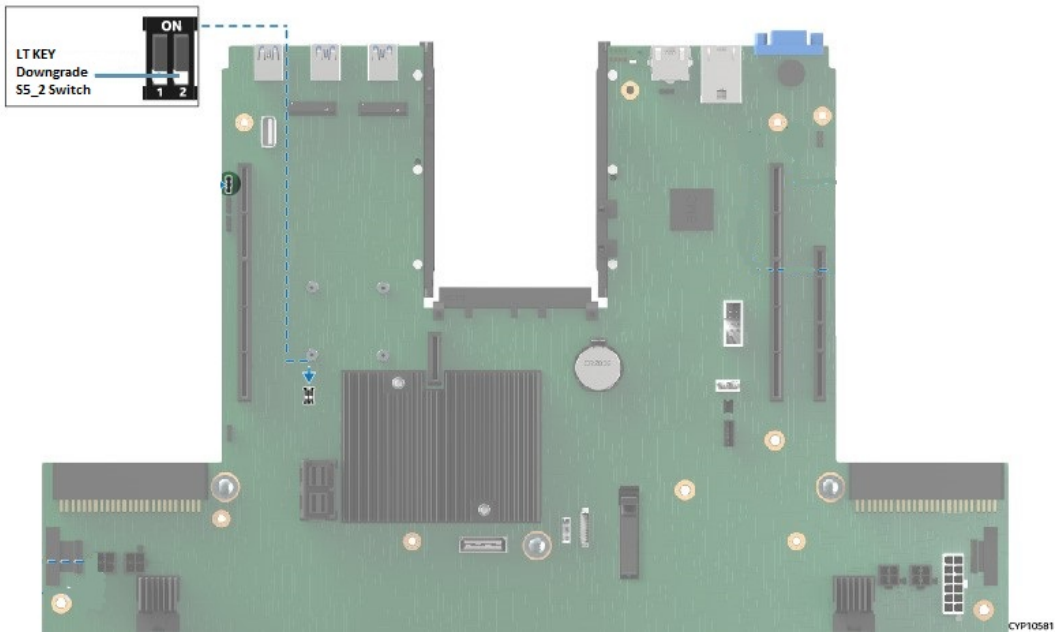


“Incorrect S5_2 “ON” position”



“Correct S5_2 “OFF” position”

The location of S5 switch can be observed in the picture below:



For instructions to open the server chassis top cover to access the Intel® M50CYP board, refer to the documents below that can be found at:
https://www.intel.com/content/www/us/en/products/details/servers/server-systems/server-system-m50cyp/docs.html?s=Newest

- Intel® Server System M50CYP1UR Family - System Integration and Service Guide (Production Version)
- Intel® Server System M50CYP2UR Family - System Integration and Service Guide (Production Version)

Contact your Intel Sales Representative if you require more specific information about this issue.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.