

# BIOS Release Notes Form

*Supermicro disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. Supermicro and the Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries. Copyright © 2018 Super Micro Computer, Inc. All rights reserved.*

Product Name	X14DBT-FAP
Release Version	1.3
Release Date	04/01/2025
Previous Version	1.0
Update Category	Recommended
Dependencies	None
Important Notes	None
Enhancements	<ol style="list-style-type: none"><li>1. Updated code base to 5.35_0ACQZ_3544P36_GNRAP_GNRSP_SRFSP_073_BETA for BKCWW12 GNR MR1.</li><li>2. Updated Birch Stream Granite Rapids SP - MR1 OOB Candidate BKC.</li><li>3. Updated Secure Boot DBX to address the AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle)) security issue.</li><li>4. Implemented the TPM EK public certificate feature.</li><li>5. Removed the warning message, "Crystal Ridge is not support."</li><li>6. Fixed the CPU one core drop issue.</li><li>7. Exposed the "Enable SAF" item.</li><li>8. Enhanced SMC_STYLE_CPU_CORES_ENABLE function by Die Count.</li><li>9. Avoided how the mapped-out DIMM could not recover after an AC cycle.</li></ol>

	<p><b>10. When enabling block SID, set AUTO_ACCEPT_PPI to avoid having to wait for user acceptance to continue.</b></p> <p><b>11. Implemented SmcTpmlInfo module for the TPM Redfish MeasurementSet feature.</b></p> <p><b>12. Updated the built-in SuperDiag to ECO candidate 1.10.1 version, based on</b></p> <p><b>GIT_2bc33501019e721aa4722f4269f0e2bfbcf5c34c.</b></p>
<b>New features</b>	<b>None</b>
<b>Fixes</b>	<ol style="list-style-type: none"> <li><b>1. The attribute 'MaxTDPWatts' could not appear at URI '/redfish/v1/Systems/1/Processors/[number].'</b></li> <li><b>2. Fixed the system hang after executing PPR.</b></li> <li><b>3. Fixed the issue where some BIOS items' default value could not be changed.</b></li> </ol>