

# CN21007: Disabling SmartDebug Access to sNVM in Libero SoC Debug Policy Settings

March 14, 2021

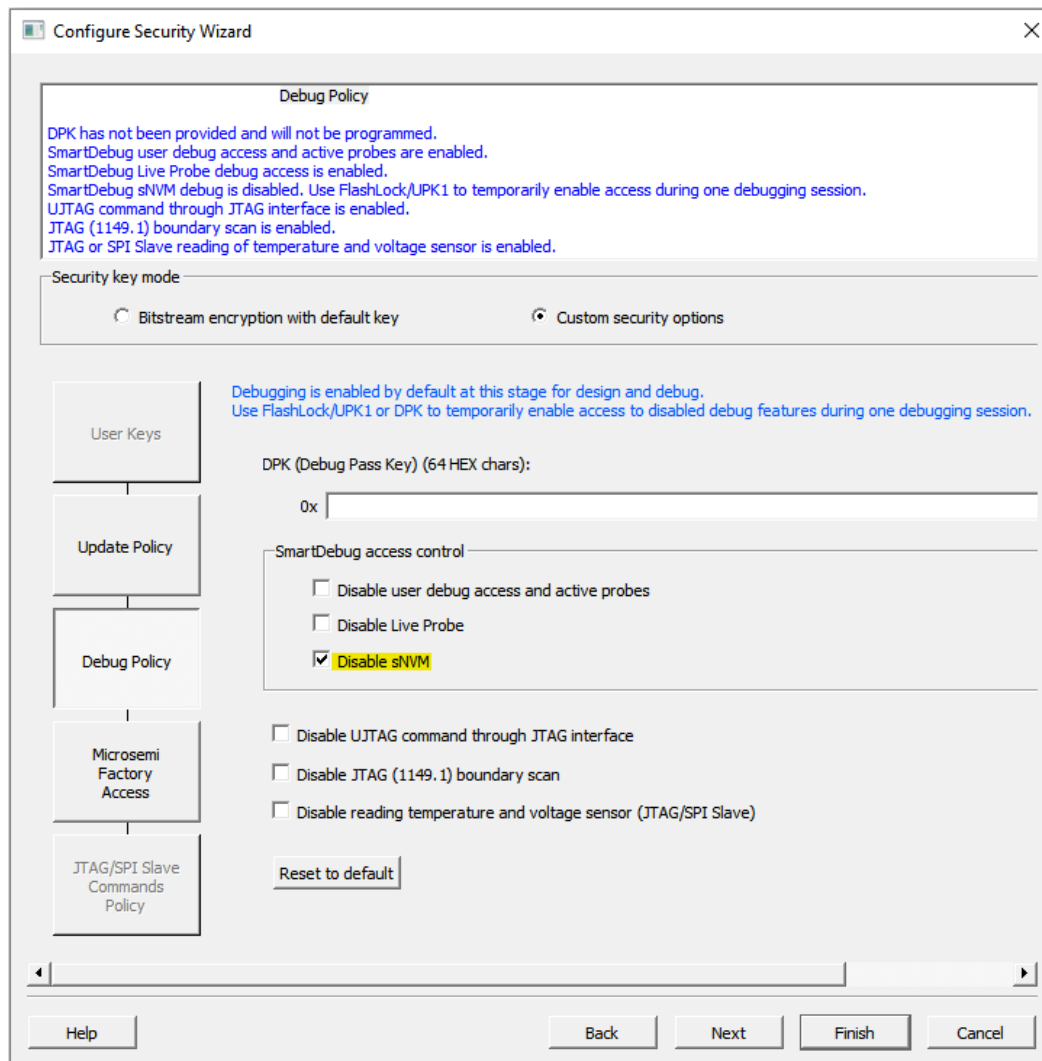
## Description

With Libero SoC v2021.1, the user setting to disable SmartDebug access to sNVM is now enforced in user/debug pass key protected devices.

## Reason for Change

Prior to Libero SoC v2021.1, disabling SmartDebug access to read the sNVM in Libero SoC's device Debug Policy settings did not affect the generated programming bitstream, and thus did not prevent SmartDebug access to the sNVM in user/debug pass key protected devices. This issue existed for PolarFire FPGAs starting with Libero SoC v12.0. The issue occurs if "Disable sNVM" is checked in the Libero SoC Debug Policy settings dialog of the "Configure Security" design flow step, or if the equivalent Tcl command is executed.

**Figure 1 • Debug Policy Settings Window**



Example Tcl command: `configure_tool -name {SPM} -params {disable_smartdebug_snvm:true}`

## Application Impact

Running "SmartDebug Design" from any Libero SoC project targeting the device on the board will allow SmartDebug to read the sNVM content from non-authenticated pages without requiring the user/debug pass key.

Similarly, running SmartDebug in standalone mode with any debug database file (.DDC) that targets the device on the board will allow reading of non-authenticated sNVM pages without requiring the user/debug pass key.

There is no impact for authenticated sNVM clients when the corresponding User Security Key (USK) is not programmed into the device sNVM (that is, the user has unchecked "Reprogram" option in USK\_CLIENT configuration) and the correct USK is not provided by the user during SmartDebug sNVM read. Reading these authenticated pages from SmartDebug without entering the correct USK will return all-zero data.

## Required Action

To disable SmartDebug access to the sNVM without the user/debug pass key, re-run the "Configure Security" design flow step using Libero SoC v2021.1 with the desired user/debug pass key and "Disable sNVM" checked, then regenerate the programming bitstream and reprogram the device with the updated security settings.

Pre-existing designs opened in v2021.1 that already have "Disable sNVM" SmartDebug access policy configured will receive a message in the Libero SoC log window that the Programming File Generation design flow steps have been invalidated. The user must then re-confirm the settings in the "Configure Security Wizard" and regenerate the bitstream before reprogramming the device security settings.

## Part Numbers Affected

MPF100T-1FCG484E	MPF200T-1FCG784E	MPF200TLS-FCG784I	MPF300T-FCG784E	MPF300TS-FCG784I
MPF100T-1FCG484I	MPF200T-1FCG784I	MPF200TLS-FCSG325I	MPF300T-FCG784I	MPF300TS-FCSG536M
MPPF100T-1FCSG325E	MPF200T-1FCSG325E	MPF200TLS-FCSG536I	MPF300T-FCSG536E	MPF300TS-FCSG536I
MPPF100T-1FCSG325I	MPF200T-1FCSG325I	MPF200TLS-FCVG484I	MPF300T-FCSG536I	MPF300TS-FCV484M
MPPF100T-1FCVG484E	MPF200T-1FCSG536E	MPF200TS- FCS325M	MPF300T-FCVG484E	MPF300TS-FCVG484I
MPPF100T-1FCVG484I	MPF200T-1FCSG536I	MPF200TS-1FCG484I	MPF300T-FCVG484I	MPF300XT-1FCG484I
MPPF100T-FCG484E	MPF200T-1FCVG484E	MPF200TS-1FCG784I	MPF300TL-FCG1152E	MPF500T-1FCG1152E
MPPF100T-FCG484I	MPF200T-1FCVG484I	MPF200TS-1FCSG325I	MPF300TL-FCG1152I	MPF500T-1FCG1152I
MPPF100T-FCSG325E	MPF200T-FCG484E	MPF200TS-1FCSG536I	MPF300TL-FCG484E	MPF500T-1FCG784E
MPPF100T-FCSG325I	MPF200T-FCG484I	MPF200TS-1FCVG484I	MPF300TL-FCG484I	MPF500T-1FCG784I
MPPF100T-FCVG484E	MPF200T-FCG784E	MPF200TS-FCG484I	MPF300TL-FCG784E	MPF500T-FCG1152E
MPPF100T-FCVG484I	MPF200T-FCG784I	MPF200TS-FCG784I	MPF300TL-FCG784I	MPF500T-FCG1152I
MPPF100TL-FCG484E	MPF200T-FCSG325E	MPF200TS-FCSG325I	MPF300TL-FCSG536E	MPF500T-FCG784E
MPPF100TL-FCG484I	MPF200T-FCSG325I	MPF200TS-FCSG536I	MPF300TL-FCSG536I	MPF500T-FCG784I
MPPF100TL-FCSG325E	MPF200T-FCSG536E	MPF200TS-FCVG484I	MPF300TL-FCVG484E	MPF500TL-FCG1152E
MPPF100TL-FCSG325I	MPF200T-FCSG536I	MPF300T-1FCG1152E	MPF300TL-FCVG484I	MPF500TL-FCG1152I
MPPF100TL-FCVG484E	MPF200T-FCVG484E	MPF300T-1FCG1152I	MPF300TLS-FCG1152I	MPF500TL-FCG784E
MPPF100TL-FCVG484I	MPF200T-FCVG484I	MPF300T-1FCG484E	MPF300TLS-FCG484I	MPF500TL-FCG784I
MPPF100TLS-FCG484I	MPF200TL-FCG484E	MPF300T-1FCG484I	MPF300TLS-FCG784I	MPF500TLS-FCG1152I
MPPF100TLS-FCSG325I	MPF200TL-FCG484I	MPF300T-1FCG784E	MPF300TLS-FCSG536I	MPF500TLS-FCG784I
MPPF100TLS-FCVG484I	MPF200TL-FCG784E	MPF300T-1FCG784I	MPF300TLS-FCVG484I	MPF500TS-1FCG1152I
MPPF100TS-1FCG484I	MPF200TL-FCG784I	MPF300T-1FCSG536E	MPF300TS-1FCG1152I	MPF500TS-1FCG784I
MPPF100TS-1FCSG325I	MPF200TL-FCSG325E	MPF300T-1FCSG536I	MPF300TS-1FCG484I	MPF500TS-FC1152M
MPPF100TS-1FCVG484I	MPF200TL-FCSG325I	MPF300T-1FCVG484E	MPF300TS-1FCG784I	MPF500TS-FC784M
MPPF100TS-FCG484I	MPF200TL-FCSG536E	MPF300T-1FCVG484I	MPF300TS-1FCSG536I	MPF500TS-FCG1152I
MPPF100TS-FCSG325I	MPF200TL-FCSG536I	MPF300T-FCG1152E	MPF300TS-1FCVG484I	MPF500TS-FCG784I
MPPF100TS-FCVG484I	MPF200TL-FCVG484E	MPF300T-FCG1152I	MPF300TS-FC484M	
MPPF200T-1FCG484E	MPF200TL-FCVG484I	MPF300T-FCG484E	MPF300TS-FCG1152I	
MPPF200T-1FCG484I	MPF200TLS-FCG484I	MPF300T-FCG484I	MPF300TS-FCG484I	

**Contact Information**

If you have any questions about this subject, contact Microsemi Technical Support department by using the support portal at <https://soc.microsemi.com/Portal/Default.aspx>

**Regards,**

Microsemi Corporation

Any projected dates in this notification are based on the most current product information at the time this notification is being issued, but they may change due to unforeseen circumstances. For the latest schedule and any other information, please contact your local Microsemi Sales Office, the factory contact shown above, or your local distributor.

This notification is confidential and proprietary information of Microsemi and is intended only for distribution by Microsemi to its customers, for customers' use only. It must not be copied or provided to any third party without Microsemi's prior written consent.

**Microsemi**

2355 W. Chandler Blvd.  
 Chandler, AZ 85224 USA

Within the USA: +1 (480) 792-7200  
 Fax: +1 (480) 792-7277

www.microsemi.com © 2021 Microsemi and its corporate affiliates. All rights reserved. Microsemi and the Microsemi logo are trademarks of Microsemi Corporation and its corporate affiliates. All other trademarks and service marks are the property of their respective owners.

Microsemi's product warranty is set forth in Microsemi's Sales Order Terms and Conditions. Information contained in this publication is provided for the sole purpose of designing with and using Microsemi products. Information regarding device applications and the like is provided only for your convenience and may be superseded by updates. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is your responsibility to ensure that your application meets with your specifications. THIS INFORMATION IS PROVIDED "AS IS." MICROSEMI MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MICROSEMI BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS, DAMAGE, COST OR EXPENSE WHATSOEVER RELATED TO THIS INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROSEMI HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROSEMI'S TOTAL LIABILITY ON ALL CLAIMS IN RELATED TO THIS INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, YOU PAID DIRECTLY TO MICROSEMI FOR THIS INFORMATION. Use of Microsemi devices in life support, mission-critical equipment or applications, and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend and indemnify Microsemi from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microsemi intellectual property rights unless otherwise stated.

Microsemi Corporation, a subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), and its corporate affiliates are leading providers of smart, connected and secure embedded control solutions. Their easy-to-use development tools and comprehensive product portfolio enable customers to create optimal designs which reduce risk while lowering total system cost and time to market. These solutions serve more than 120,000 customers across the industrial, automotive, consumer, aerospace and defense, communications and computing markets. Headquartered in Chandler, Arizona, the company offers outstanding technical support along with dependable delivery and quality. Learn more at [www.microsemi.com](http://www.microsemi.com).