Instructions on How to Enable Intel® SGX Support on Supermicro X12DP Series/X12SP Series Motherboards

USER'S GUIDE

Revision 1.0

The information in this user's guide has been carefully reviewed and is believed to be accurate. The manufacturer assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this user's guide, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this user's guide, please see our website at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this user's guide at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL SUPER MICRO COMPUTER, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING, OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in an industrial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.

User's Guide Revision 1.0

Release Date: December 10, 2021

Preface

Target Audience and Writing Purpose

This user's guide is written for system integrators, IT technicians, and knowledgeable end users. It provides information on how to enable Intel® SGX support on Supermicro X12DP Series/X12SP Series motherboards.

About This User's Guide

This user's guide provides detailed instructions for the user to enable Intel® Software Guard Extensions (SGX) support on Supermicro X12DP Series/X12SP Series motherboards that are based on the 3rd Gen Intel® Xeon® Scalable Processors (in Socket P+ (LGA-4189)). Intel SGX is a set of instruction codes built into certain high-level processors to allow the user and the operating system (OS) to define particular regions of memory as private regions and encrypt the contents which reside in these regions to protect the data and instruction codes therein from any exposure to outside threats. SGX, essentially, creates a private, protected, and safe environment for the processor to operate by denying access to a perceived outsider, effectively eliminating the threats caused by any outside intrusions and encroachments. It is an effective measure to achieve data protection and security. However, for SGX to function properly, please ensure that the processor(s) installed on the motherboard and the BIOS utility used in the system are capable of supporting Intel SGX and then follow the instructions provided in this user's guide to enable SGX support for your system.

Please also note that all Supermicro's products are intended to be installed, configured, and serviced by professional technicians only. For processor/memory updates, please refer to our website at http://www.supermicro.com/products/.

Conventions Used in the Manual

Special attention should be given to the symbol below for proper BIOS configuration and for prevention of accidental damage to your system components:

Note: Important Information given for proper system setup or for proper firmware configuration.

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Website:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Website:	www.supermicro.com.tw

Table of Contents

Chapter 1

Steps to Enable Intel® SGX in the UEFI BIOS Setup Utility

This section provides detailed instructions on how to enable Intel® Software Guide Extensions support on the UEFI BIOS. Please follow the instructions carefully to configure your BIOS settings for Intel SGX to work properly.

1.1 Pre-Requirements

To ensure that Intel SGX is supported by your system, please be sure to meet the following requirements first before enabling Intel SGX in the BIOS utility:

1. Be sure to use the correct type of processors that support Intel SGX.
2. Please be sure to use BIOS Rev. 1.1a or a newer version.
3. Install DIMM modules based on the memory configuration supported by Intel SGX as listed in the tables below.

Memory Configuration Tables for SGX Support

a.Memory Configuration Table for X12DP Series Motherboards

X12 DP SGX-Supported Memory Configuration																
DDR4	**F1**	**F2**	**E1**	**E2**	**H1**	**H2**	**G1**	**G2**	**C2**	**C1**	**D2**	**D1**	**A2**	**A1**	**B2**	**B1**
8 DIMMs	DDR4		DDR4		DDR4		DDR4			DDR4		DDR4		DDR4		DDR4
12 DIMMs	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	
	DDR4	DDR4	DDR4		DDR4		DDR4	DDR4	DDR4	DDR4	DDR4		DDR4		DDR4	DDR4
	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4
	DDR4		DDR4	DDR4	DDR4	DDR4	DDR4		DDR4		DDR4	DDR4	DDR4	DDR4	DDR4	
16 DIMMs	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4

b Memory Configuration Table for X12SP Series Motherboards

X12 UP SGX-Supported Memory Configuration								
DDR4	**F1**	**E1**	**H1**	**G1**	**C1**	**D1**	**A1**	**B1**
8 DIMMs	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4

Processor Requirements

- 3rd Gen Intel® Xeon® Scalable Processors (in Socket P+ (LGA-4189))

OS Requirements

- Windows Server 2019
- Linux: Ubuntu 20.04, Ubuntu 18.04, Red Hat Enterprise Linux Server 8.2
- For more information on OS requirements for Intel's SGX support, please refer to Intel's website.

Software Requirements

Intel® SGX Platform Software

- For Intel® SGX application to work properly in a system, Intel® SGX PSW is required to be pre-installed before shipping.
- A standalone Intel® SGX PSW for Windows OS is also available. (Please refer to Intel's website.)

Note: Depending on Windows version, PSW and drivers may already be automatically installed.

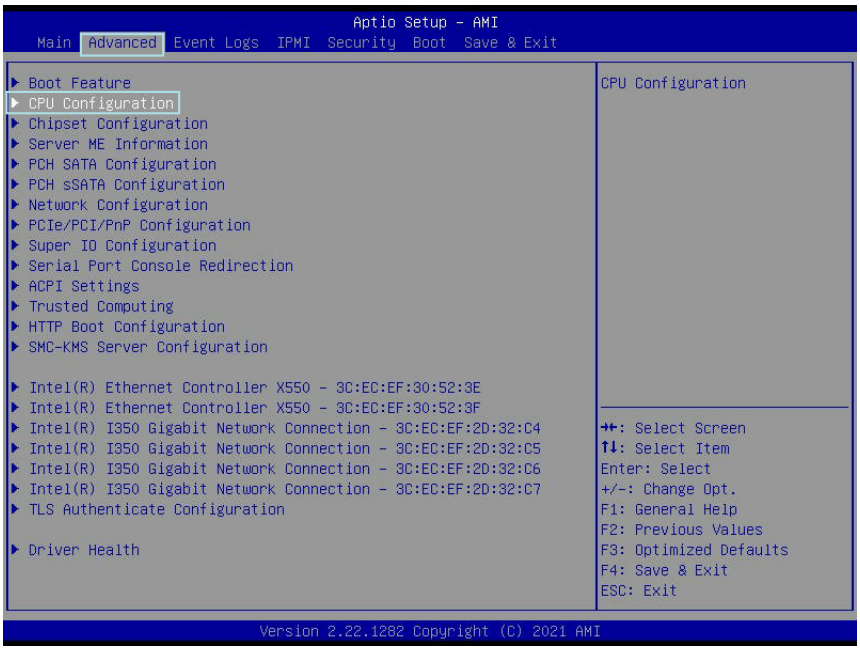
Supermicro Platform Support

- X12DP Series motherboards
- X12SP Series motherboards
- Supermicro servers/systems based on X12DP Series/X12SP Series motherboards

1.2 Step 1: Entering the UEFI BIOS Utility to Enable Intel SGX Support

To enable Intel SGX support on the BIOS setting, you will need to enter the BIOS Setup utility by following the instructions below:

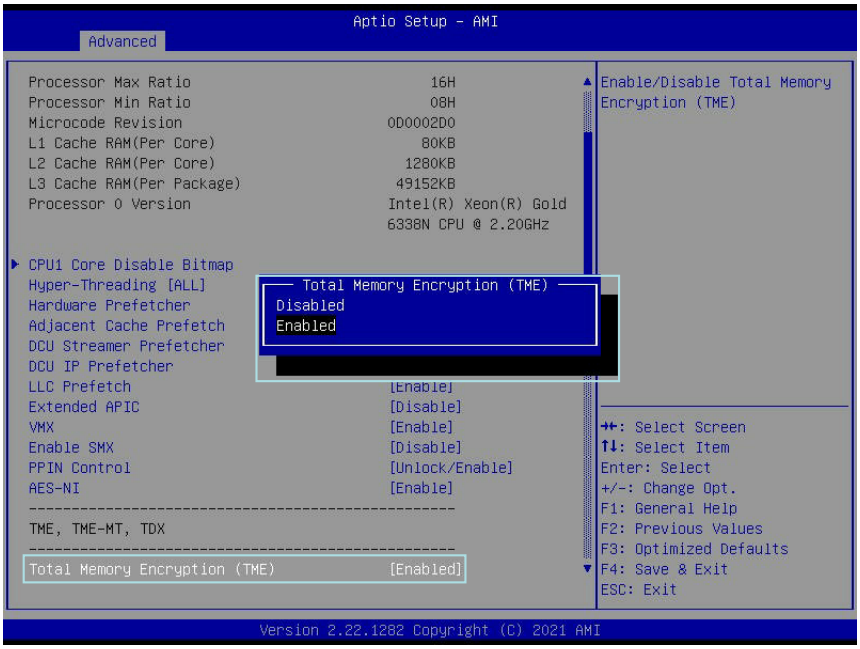
1. Press <Del> during system boot to enter the BIOS Setup utility.



2. Select the Advanced tab from the menu bar on the top of the screen. Using the down arrow key, select *CPU Configuration* and press <Enter> as shown below.

3. When the CPU Configuration submenu displays, scroll down to select *Total Memory Encryption (TME)*.

4. Once Total Memory Encryption (TME) is highlighted, press <Enter>. The TME option dialogue box will display as shown below.



5. From the option dialogue box, select *Enabled* and press <Enter> to enable TME support for your system.

1.3 Step 2: Disabling Mirror Mode, ADDDC Sparing*, and Patrol Scrub Support in the Memory-RAS Configuration Submenu

For Intel SGX to function properly, please disable the following features in the Memory-RAS submenu first:

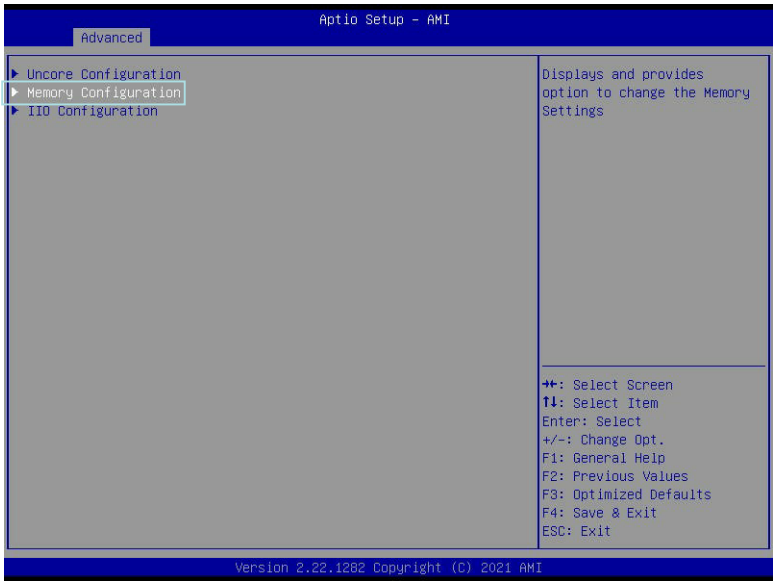
1. Mirror Mode
2. ADDDC (Adaptive Double Device Data Correction) Sparing* (See the notes below.)
3. Patrol Scrub

Note 1: The feature "*ADDDC Sparing*" will only be activated and displayed on the BIOS screen when x4 DRAM DIMMs, which support ADDDC(+1), are installed in the system. Without required DRAMs present, this feature will not be activated but remains dormant, hidden from the user's view. For ADDDC memory support, please refer to the Memory RAS Configuration User's Guide posted on our website at: https://www.supermicro.com/manuals/other/Memory_RAS_Configuration_User_Guide.pdf.

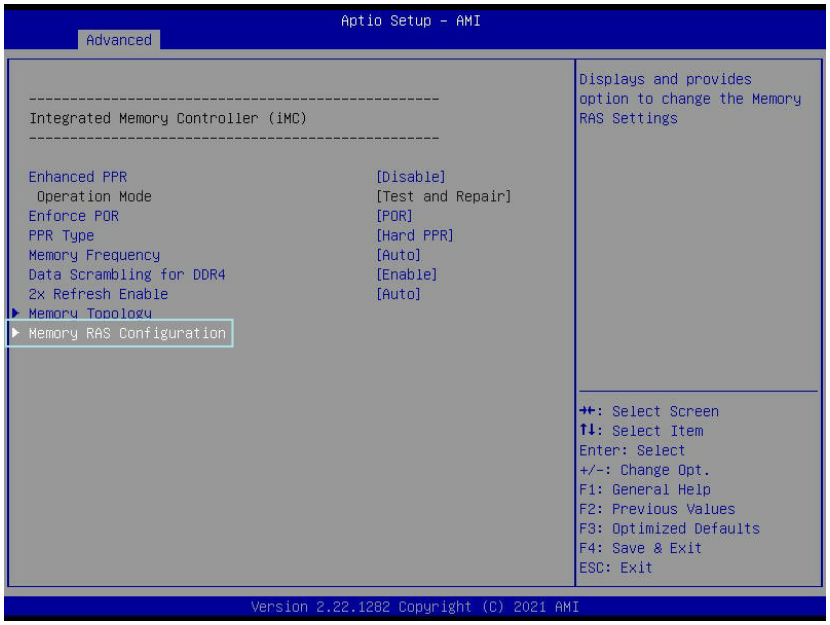
Note 2: If ADDDC Sparing does not appear on your BIOS screen, this feature is inactive and masked off by default, and you will not need to disable it manually.

To properly disable Mirror Mode, Patrol Scrub, and ADDDC Sparing (if needed), please follow the instructions listed below:

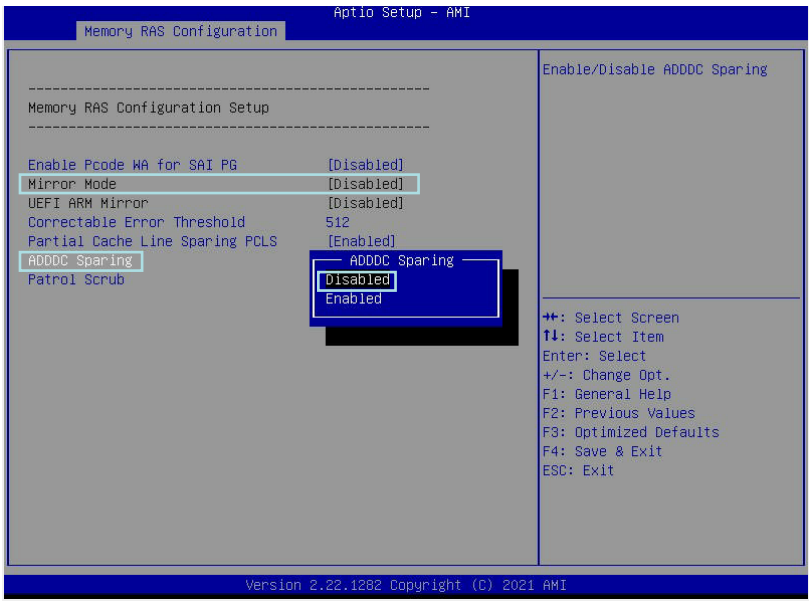
4. From the Advanced menu, select *Chipset Configuration* and press <Enter>.
5. From the Chipset Configuration submenu, select *North Bridge* and press <Enter>.
6. From the North Bridge submenu, select *Memory Configuration* and press <Enter> as shown below.



7. When the Memory Configuration submenu displays, scroll down to select the Memory RAS Configuration submenu as shown below.



8. When *Memory RAS Configuration* is highlighted as shown above, press <Enter>. The Memory RAS Configuration submenu will display. Please check to ensure that Mirror Mode is **Disabled** as shown below.



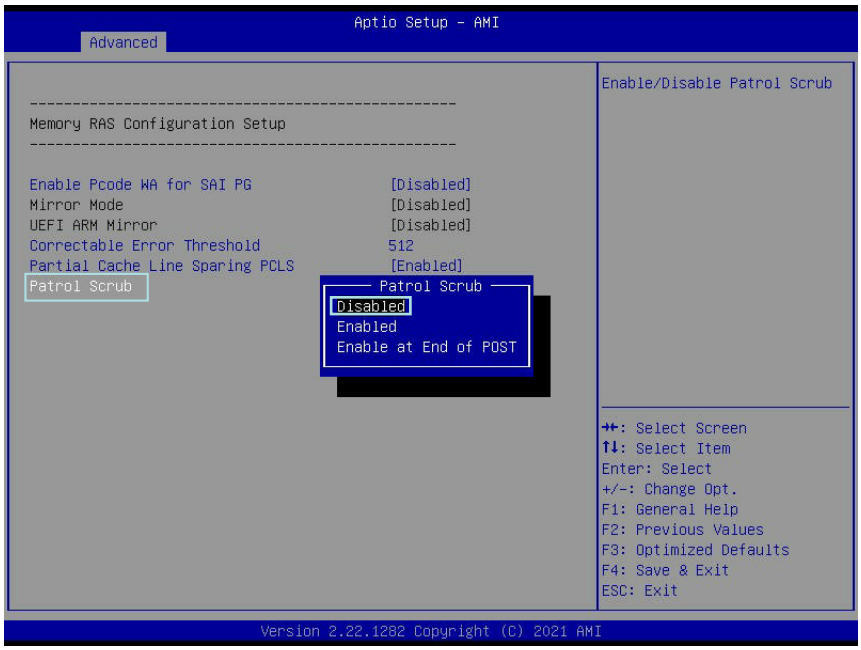
9. With Mirror Mode disabled, scroll down to check if the feature ***ADDDC Sparing*** displays on your screen. If ADDDC Sparing **does not** appear on your screen, this feature is not activated, and you will not need to disable it manually. Please skip this step. (See the notes on the previous page.)

10. If ADDDC Sparing is displayed on your screen, use the arrow keys to select it by highlighting it and press <Enter>.

11. The ADDDC Sparing option dialogue box will display. Select ***Disabled*** from the option box and press <Enter> to disable ADDDC Sparing as shown above.

12. Using the down arrow key, select the feature "*Patrol Scrub"* by highlighting it.

13. With Patrol Scrub highlighted, press <Enter>. From the option dialogue box, select ***Disabled*** and press <Enter> to disable Patrol Scrub support for your system as shown below.

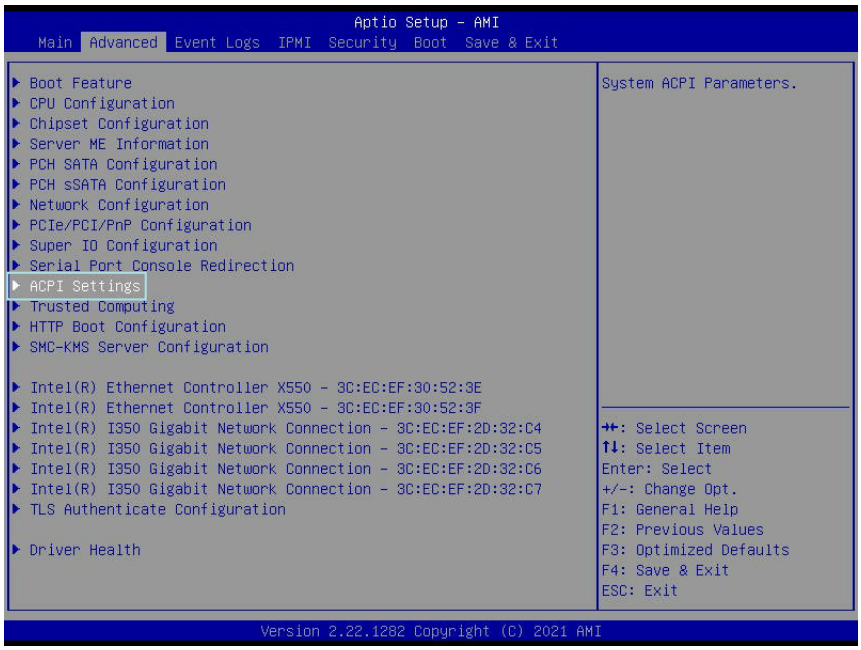


14. Press <F4> to save the settings and reboot the system for the changes you've made to take effect.

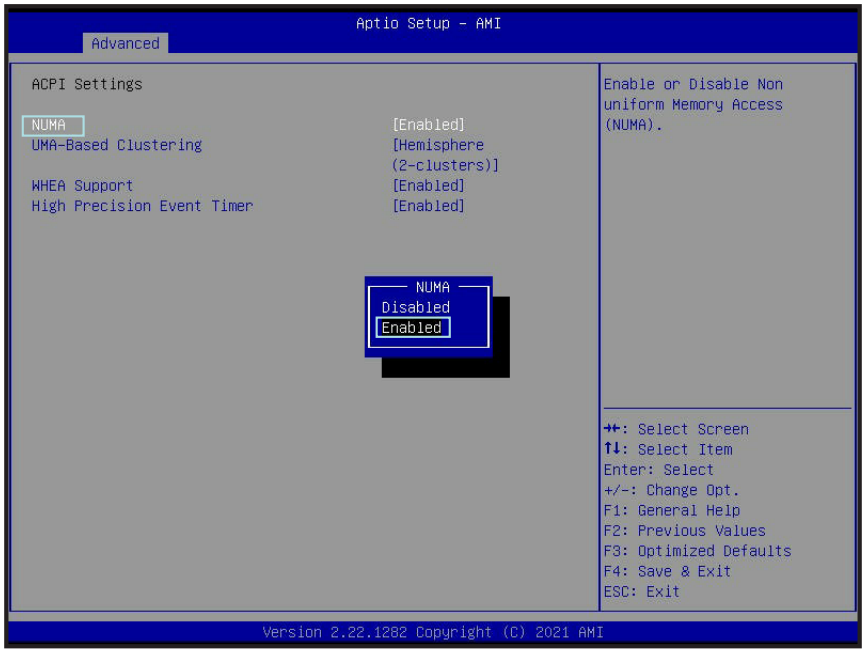
1.4 Step 3: Enabling NUMA and Disabling UMA-Based Clustering Support in the ACPI Submenu

For Intel SGX to function properly, please enable NUMA (Non-Uniform Memory Access) and disable UMA-Based Clustering support in the ACPI submenu by following the instructions below.

1. From the Advanced menu, scroll down to select *ACPI Settings* and press <Enter> as shown below.

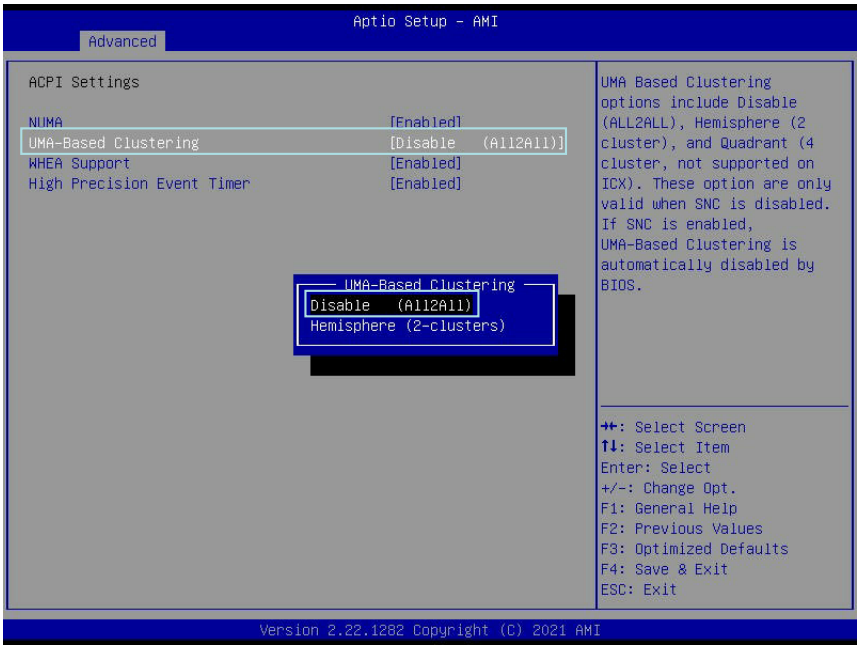


2. From the ACPI submenu, select *NUMA* and press <Enter>.



3. From the NUMA option dialogue box as shown above, select ***Enabled***, and press <Enter> to enable NUMA support.

4. After NUMA is enabled, scroll down to select *UMA-Based Clustering* and press <Enter>. When the option dialogue box displays, select ***Disable (ALL2ALL)*** and press <Enter> to disable UMA-Based Clustering support as show below.

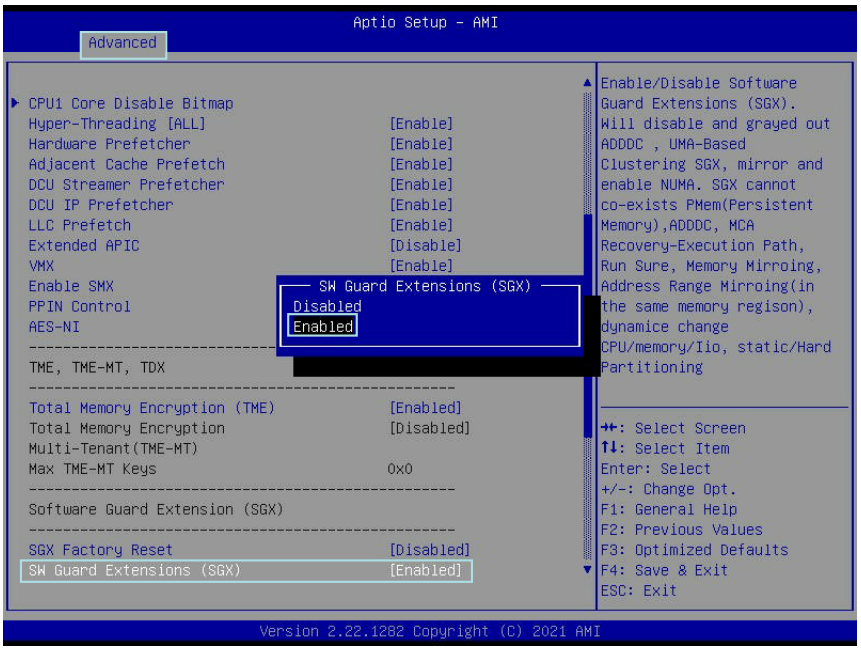


5. After you've enabled NUMA and disabled UMA-Based Clustering support in the ACPI settings, press <F4> to save the settings and reboot the system for the changes you've made to take effect.

1.5 Step 4: Enabling SGX Support in the CPU Configuration Settings

After you've properly configured memory-related features in the UEFI BIOS utility as instructed above, your system is ready to support Intel Software Guard Extensions. To use SGX, please follow the instructions below.

1. After you've saved the changes made from Step 1 to Step 3 by pressing <F4> as instructed in the previous sections, your system will reboot.
2. Press <Del> to enter the BIOS Setup Utility during system boot.
3. Select *Advanced* from the menu bar on top of the screen. From the Advanced menu, select *CPU Configuration* and press <Enter>.
4. When the CPU Configuration submenu displays, scroll down to select *SW Guard Extensions (SGX)* and press <Enter>.
5. From the option dialogue box, select ***Enabled*** to enable SGX support for your system as shown below.



6. After enabling SGX, press <F4> to save all settings and reboot the system. All the changes you've made will take effect after system reboot.