Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. The products described 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.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel 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.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

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

*Other names and brands may be claimed as the property of others

Copyright © 2021, Intel Corporation. All Rights Reserved.
# Contents

1  **Introduction** ........................................................................................................5  
   1.1  Demo Platform Details ..................................................................................... 5  

2  **Configuring Your Platform for Intel® SGX** ....................................................6  
   2.1  Platform Requirements ...................................................................................... 6  
   2.2  Intel® SGX BIOS menu configuration ................................................................. 7  
   2.3  Installing Platform Software and Drivers ......................................................... 13  
      2.3.1  For Linux* ................................................................................................. 13  
      2.3.2  For Windows* ............................................................................................. 13  

3  **Confirming Your Setup Has Enabled Intel® SGX** .............................................14  
   3.1  For Linux............................................................................................................ 14  
   3.2  For Windows....................................................................................................... 14  

4  **Useful Intel® SGX Links** ....................................................................................16
## Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>• Initial release of the document.</td>
<td>September/2021</td>
</tr>
</tbody>
</table>
1 Introduction

This document is meant to guide customers through the process of enabling and testing Intel® Software Guard Extensions (Intel® SGX) to ensure that it works properly on their platforms.

1.1 Demo Platform Details

This document, while meant to be a general customer guide for setting up Intel® SGX, is based off enabling and testing Intel® SGX on a SuperMicro® 2200U server platform with 3rd Gen Intel® Xeon® Scalable Processor running BIOS Version 1.1. Therefore, keep in mind that the BIOS menu settings, software installation instructions, and so on, may differ for your platform. This document will try and note when the user should pay careful attention to possible differences in the setup.
2 Configuring Your Platform for Intel® SGX

This section describes how to ensure your platform is Intel® SGX-capable and enable Intel® SGX in the BIOS menu.

2.1 Platform Requirements

Supported Hardware:

- 3rd Gen Intel® Xeon® Scalable Processors
- For each memory controller, all channel 0 slots should be populated (8 DIMMS per socket at least), DIMM population should be symmetric across IMCs:

<table>
<thead>
<tr>
<th>IMC#</th>
<th>IMC0</th>
<th>IMC1</th>
<th>IMC2</th>
<th>IMC3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>Chan 0 (A)</td>
<td>Chan 1 (B)</td>
<td>Chan 0 (C)</td>
<td>Chan 1 (D)</td>
</tr>
<tr>
<td>DDR4</td>
<td>Slot0</td>
<td>Slot1</td>
<td>Slot0</td>
<td>Slot1</td>
</tr>
<tr>
<td>8</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
</tr>
<tr>
<td>12</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
</tr>
<tr>
<td>16</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
</tr>
</tbody>
</table>

BIOS Requirements:

- Intel® SGX enabled in BIOS menu (see Section 2.2 for instructions)
- Continue to check for BIOS updates

OS Requirements:

- Windows* Server 2019
- Linux*:
  - Ubuntu* 20.04
  - Ubuntu* 18.04
  - Fedora 31 Server
  - Red Hat* Enterprise Linux* Server 8.2
  - see Intel® Software Guard Extensions SDK for Linux* - Downloads | 01.org for full list
Software Requirements:

- Intel® SGX Platform Software
  - Systems that are shipped with an Intel® SGX application are required to preinstall the Intel® SGX PSW
  - A standalone Intel® SGX PSW for Windows* OS is available, see section 2.3
  - Note: Depending on Windows version, PSW and drivers may already be automatically installed via Windows Update

2.2 Intel® SGX BIOS menu configuration

Intel® SGX requires certain settings in the BIOS to be enabled or disabled. For example, TME (Total Memory Encryption) must be enabled, UMA (Uniform Memory Access) must be disabled, and conflicting RAS (Reliability, Availability and Serviceability) settings such as Mirroring mode must be disabled.

To navigate to these settings, press F11 when prompted on the boot menu to reach the BIOS menu (it may be a different key depending on your platform).

In the BIOS menu, check the following settings below are correct to enable Intel® SGX:

**Note:** Depending on your BIOS Menu Layout, there may be different paths/settings to enable Intel® SGX. If not located under the 'Advanced' tab, try checking the 'Security' tab.

**Note:** If Intel® SGX is not visible or is grayed out in the setup menu, it may be because the proper settings like TME enabling have not been set. Following the steps below should fix this.

Necessary settings (pictures of BIOS menu screens also can be found below):

- Main menu-> Advanced -> CPU Configuration -> Total Memory Encryption (TME) -> Enabled
- Main menu-> Advanced -> Chipset Configuration -> North Bridge -> Memory Configuration -> Memory RAS Configuration Setup -> Mirror Mode -> Disabled
- Main menu-> Advanced -> ACPI Settings -> NUMA -> Enabled
- Main menu-> Advanced -> ACPI Settings -> UMA-Based Clustering -> Disable (A112A11)
- Main menu-> Advanced-> CPU Configuration -> SW Guard Extensions (SGX) -> Enabled
- Main menu-> Advanced-> CPU Configuration -> SGXLEPUBKEYHASHx Write Enable -> Enabled (**this is also known as Flexible Launch Control**
Related settings you may want to change:

Sub-NUMA clustering (SNC):

**Main menu-> Advanced-> Chipset Configuration - North bridge -> Uncore Configuration -> SNC (Sub NUMA) -> “Enable SNC2”**

Specify PRMRR size:

**Main menu -> Advanced-> CPU Configuration -> PRMRR Size -> specify PRMRR size**

**Note:** The Protected Region Memory Range Region (PRMRR) contains the Enclave Page Cache (EPC) for execution of Intel® SGX applications. The maximum EPC (Enclave Page Cache) size is half of the installed memory size up to the max SKU size of 512GB EPC per processor, which bounds the maximum PRMRR size. Therefore, depending on your 3rd Gen Intel® Xeon® Scalable Processor SKU you may not be able to use the maximum PRMRR size.

*In terms of SKUs:* The default EPC size is 64 GB for both Platinum and Gold SKUs. For Silver, the default EPC size is 8 GB. There are exceptions (listed below) for 5 SKUs where the maximum enclave size increases to 512 GB. Additionally, there are also two specific Platinum and Gold SKUs – 8358P and 8352V – that do not follow the default logic of 64 GB EPC size and instead have an EPC size of 8 GB.

The 3rd Gen Xeon Processor SKUs that support Max Intel® SGX Enclave Capacity (512 GB) are:

<table>
<thead>
<tr>
<th>SKU</th>
<th>CORES</th>
<th>BASE (GHz)</th>
<th>SINGLE CORE TURBO (GHz)</th>
<th>ALL CORE TURBO (GHz)</th>
<th>CACHE (MB)</th>
<th>TDP (Watts)</th>
<th>Support for Intel Optane Persistent Memory 200 Series</th>
<th>Intel SGX Enclave Capacity (Per Processor)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8380</td>
<td>40</td>
<td>2.3</td>
<td>3.4</td>
<td>3.0</td>
<td>60</td>
<td>270</td>
<td>Yes</td>
<td>512 GB</td>
</tr>
<tr>
<td>8368Q</td>
<td>38</td>
<td>2.6</td>
<td>3.7</td>
<td>3.3</td>
<td>57</td>
<td>270</td>
<td>Yes</td>
<td>512 GB</td>
</tr>
<tr>
<td>8368</td>
<td>38</td>
<td>2.4</td>
<td>3.4</td>
<td>3.2</td>
<td>57</td>
<td>270</td>
<td>Yes</td>
<td>512 GB</td>
</tr>
<tr>
<td>8352S</td>
<td>32</td>
<td>2.2</td>
<td>3.4</td>
<td>2.8</td>
<td>48</td>
<td>205</td>
<td>Yes</td>
<td>512 GB</td>
</tr>
<tr>
<td>5318S</td>
<td>24</td>
<td>2.1</td>
<td>3.4</td>
<td>2.6</td>
<td>36</td>
<td>165</td>
<td>Yes</td>
<td>512 GB</td>
</tr>
</tbody>
</table>

Here is an example of the BIOS screens on the Supermicro system and the proper settings:

**Main Menu**
From main screen navigate to Advanced menu

**Advanced Menu**

Advanced menu -> CPU Configuration menu
Scroll down to find TME and Intel® SGX enabling settings

**Advanced menu -> Chipset Configuration -> North Bridge**

North bridge configuration menu
North Bridge -> Uncore Configuration

SNC enabling

North Bridge -> Memory Configuration

Memory Configuration menu, RAS settings
Memory RAS Configuration

Mirroring off

ACPI Settings menu

ACPI Settings, NUMA and UMA-based clustering
2.3 Installing Platform Software and Drivers

Now that Intel® SGX has been enabled, you may need to install the platform software and drivers (Note: downloading the Software Developer Kit is not necessary for confirming your setup has correctly enabled Intel® SGX).

*Note:* Depending on your Windows version, the PSW and drivers may already be automatically installed via Windows Update. *Trying to reinstall them may show a fail message if they are already installed.* See Chapter 3 on how to check if they are installed.

2.3.1 For Linux*

See the documentation at [Intel SGX SW Installation Guide for Linux (01.org)](https://www.intel.com/content/www/us/en/architecture-and-technology/intel-software-guard-extensions/intel-sgx-sw-installation-guide-for-linux.html) for downloading the Software Developer Kit (SDK), Platform Software (PSW), and Data Center Attestation Primitives (DCAP).

2.3.2 For Windows*

See [SDK for Intel® Software Guard Extensions](https://www.intel.com/content/www/us/en/architecture-and-technology/intel-software-guard-extensions.html), click on “Download Windows* SDK.” At a later screen it will give you an option to specifically select the Platform Software from a drop-down menu like so:

![Platform Software Download Menu](image)

From here you can choose to install the Software Developer Kit (SDK), Platform Software (PSW), and/or Data Center Attestation Primitives (DCAP). These downloads come with installation guides that you can read for further instruction.
3 Confirming Your Setup Has Enabled Intel® SGX

3.1 For Linux

After enabling Intel® SGX, Linux users can check the EPC (Enclave Page Cache) size in CPUID leaf 0x12 subleaf 0x2 by typing "cupid -l 0x12 -s 0x2". The output would look as follows:

```
[username] > cupid -l 0x12 -s 0x2
CPU 0:
   SGX EPC enumeration (0x12/n):
      section physical address = 0x0000000070200000
      section size = 0x0000000005e00000
      section property = confidentiality & integrity protection
```

If the physical address and size are not equal to 0x0, then Intel® SGX has been enabled correctly.

3.2 For Windows

Windows users can confirm Intel® SGX has been properly enabled by checking the drivers in the Device Manager. You should see a driver under “Software Components” for Intel® SGX:
4 Useful Intel® SGX Links

Main Intel® SGX for Linux Platform Software and SDK repo:
https://github.com/intel/linux-sgx/

ECDSA Remote Attestation/Data Center Attestation Primitives (DCAP) Info:

b. https://01.org/intel-software-guard-extensions/downloads - For downloading pre-built DCAP components for various OSs and distros.
c. https://github.com/intel/SGXDataCenterAttestationPrimitives - Open source Linux DCAP components repo
d. https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_DCAP_Multipackage_SW.pdf - In-depth guide to remote attestation using DCAP

Intel® SGX Remote Attestation API portal: https://api.portal.trustedservices.intel.com/