Intel® Software Guard Extensions Platform Software for Windows* OS Release Notes

Installation Guide and Release Notes

8 June 2017
Revision: 1.8

Contents:

Introduction
What's New
System Requirements
Known Issues and Limitations
Disclaimer and Legal Information

1 Introduction

This document provides system requirements, limitations and legal information for Intel® Software Guard Extensions (Intel® SGX) platform software (PSW) for Windows*.

Product Contents

Intel® Software Guard Extensions PSW package includes the following software components:

Ingredient Binary	Version String
Intel® SGX Runtime System Library	1.8.100.38701
Intel® SGX Launcher Enclave	1.7.100.34769
Intel® SGX Platform Services Initialization Enclave	1.7.100.35258
Intel® SGX Quoting Enclave Intel® SGX Provisioning Enclave Intel® SGX Provisioning Cert Enclave	1.6.101.32775
Intel® SGX Platform Services Operation Enclave	1.8.100.38323
Intel® SGX Application Enclave Service (AESM)	1.8.100.38701
Intel® SGX Windows* 7 driver (64 bit only)	1.6.80.31049

2 What's New

Intel® Software Guard Extensions PSW includes the following changes compared to the Intel® SGX PSW 1.7 release:

- Support for the `--force-install` option in Intel® SGX PSW installer
- Bug fixes

3 System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor or newer

Software Requirements

- Supported operating systems for the Intel® SGX PSW installer:
    - Microsoft Windows* 7 64-bit version
    - Microsoft Windows* 10 November Update (version 1511) 64-bit version
    - Microsoft Windows* 10 Anniversary Update (version 1607) 64-bit version
      Note: Intel® SGX PSW does not support Microsoft Windows* 32-bit operating system.

- If you need to use Intel® SGX platform service, install the following product:
    - Full set of Intel® Management Engine (ME) software components 11.6.0.1126 or newer
      Note: To install the full set of Intel® Management Engine (ME) software components, you need to install with `SetupMe.exe` instead of `MEISetup.exe` (HECI driver only).

  Note: Intel® SGX PSW communicates with the Intel® SGX backend server, which listens on network port 8080. You should not block port 8080 in the network environment, otherwise you will not be able to use the Intel® SGX remote attestation service or Intel® SGX platform service.

4 Known Issues and Limitations

- Intel® SGX only supports integrated Windows authentication proxy scheme. The Basic and the Digest authenticated proxy schemes are not supported.
- OEM must *not* post Intel® SGX PSW for end-users to download. Any Intel® SGX PSW upgrade for end-users should happen through Intel® SGX applications provided by ISV only.
- You can't load any enclave in Windows 7/8.1 if the Microsoft Universal C Runtime (CRT) isn't installed in the machine. To resolve this issue, you can install Windows Update for Universal CRT (KB2999226) in Windows.
- You can't install Intel® SGX PSW when you install Windows* OS in legacy mode and Intel® SGX is set as "Software Controlled" in BIOS. You need to configure Intel® SGX as "Enabled" in BIOS before you install Intel® SGX PSW.

5 Disclaimer and Legal Information

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

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.

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 forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

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.

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

Optimization Notice

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Notice revision #20110804

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

© Intel Corporation