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

Installation Guide and Release Notes

2 October 2017
Revision: 1.8.5

Contents:

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:

Component	Version String
Intel® SGX Runtime System Library	1.8.105.40539
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)	1.8.105.40539
Intel® SGX Windows* 7 driver (64 bit only)	1.6.80.31049

2 What's New

Intel® SGX PSW includes the following changes compared to the Intel® SGX PSW 1.8 release:

- Fixed the “Unknown Device” issue on Windows 10 Fall Creator Update (version 1709).
  Intel SGX now automatically installs the device driver.
  The device driver can also be installed as a Windows update.
- Intel® SGX provisioning backend server now uses port 80.

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
    - Microsoft Windows* 10 Creators Update (version 1703) 64-bit version
    - Microsoft Windows* 10 Fall Creators Update (version 1709) 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).

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.
- 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.
- The legacy (before 1.6 version) Intel® SGX PSW installation entry cannot be removed from "Programs and Features" in Windows Control Panel if you install legacy (before 1.6 version) Intel® SGX PSW and upgrade with new installer (1.7 and newer version). To work around the issue, please manually uninstall Intel® SGX PSW before installing new version.

5 Disclaimer and Legal Information

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.