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

Installation Guide and Release Notes

27 February 2017
Revision: 1.7 Gold

Contents:

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

1 Introduction

This document provides system requirements, installation instructions, 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	1.7.100.35600
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 Intel® SGX Platform Services Operation Enclave	1.6.101.32775
Intel® SGX Application Enclave Service (AESM)	1.7.100.35600
Intel® SGX Windows* 7/8.1/10 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 1.6 release:

- New Intel® SGX Launcher Enclave to support 2048 enclave launch white-list entries
- Enclave launch white-list file version 10 is now used by default
- Updated Intel® SGX Platform Service Dal applet (PSDA) to support longer operation latency

- Released Intel SGX PSW installation executable file (EXE)
- Updated Intel® Platform Service Initialization Enclave to fix bugs
- Ability to query the Intel SGX PSW version string
- Intel SGX device driver is used for Windows 8.1 64-bit version
- Updated Intel® SGX Platform Service Dal applet (PSDA) to handle exceptions when the SGX platform service is used in a platform without a coin battery.
- Bug fixes

3 System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor (Intel® microarchitecture code name Skylake)
- 7th Generation Intel® Core™ Processor (Intel® microarchitecture code name KabyLake)

Firmware Requirements

- The 6th Generation Intel® Core™ Processor (Intel® microarchitecture code name Skylake) BIOS RC 0.7 or newer if the system is using an Intel reference BIOS.
- The 7th Generation Intel® Core™ Processor (Intel® microarchitecture code name KabyLake) BIOS RC 1.0.5 (BIOS 52.2) or newer if the system is using an Intel reference BIOS

Software Requirements

- Supported operating systems for the Intel® SGX PSW installer:
    - Microsoft Windows* 7/Threshold2/Redstone1/Redstone2 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 Installation Notes

Before installing Intel® SGX PSW, enable Intel® SGX in the BIOS.

For example, if the system is using an Intel reference BIOS, you may configure the BIOS options according to the following steps:

Go to **Intel Advanced Menu → CPU Configuration → SW Guard Extensions (SGX)**. Set **SW Guard Extensions (SGX)** as **Enabled** or **Software Controlled**.

- If you set Software Controlled for the **SW Guard Extensions (SGX)** option, you need to enable Intel® SGX using **Intel® SGX Enabling Functions** after installing Intel® SGX PSW. See the *Intel® SGX SDK User's Guide for Windows* OS* for more details.
- If you set Enabled for the **SW Guard Extensions (SGX)** option, you may need to configure **Intel Advanced Menu → CPU Configuration → PRMRR**. You can set it to 32MB, 64MB or 128MB. The default option is 128MB.

This step may be only applicable to Intel reference BIOS and may be not applicable to OEM BIOS.

You need administrator privilege to run the installer. Once installed, you can see **Intel® Software Guard Extensions Platform Software** in the **Control Panel\Programs\Programs and Features** list.

The Intel® SGX PSW installer does not uninstall the Intel SGX device driver after the uninstallation of the platform software. Subsequent installations of the Intel® SGX PSW will update the driver to a newer version only (no downgrade is allowed).

To use Intel® SGX platform service, you need to install full set of Intel® Management Engine (ME) software components which includes Intel® Dynamic Application Loader(DAL) Host Interface Service. If you install Intel® ME driver only, Intel® SGX platform service is not available.

Default Installation Folders

The default top-level installation folder for this product is:

- `C:\Program Files\Intel\IntelSGXPSW`

5 Known Issues and Limitations

- Intel® Software Guard Extensions 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 is through 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.
- The legacy Intel SGX PSW installation entry cannot be removed from "Programs and Features" in Windows Control Panel if you install a legacy Intel SGX PSW installer with ".exe" as file name extension and upgrade with the 1.7 version installer. To work around the issue, manually uninstall Intel SGX PSW (.exe) before installing the 1.7 version. If you install legacy Intel SGX PSW installer with ".msi" as file name extension and upgrade with 1.7 installer, the issue is not observed.
- When installing the Intel SGX PSW installer on Windows 7, you may see a dialog "Windows can't verify the publisher of this driver software". To fix this, install Microsoft Security Advisory 3033929, more details are available at https://technet.microsoft.com/en-us/library/security/3033929.

6 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.

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