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

Installation Guide and Release Notes

24 May 2016
Revision: 1.6

Contents:

1 Introduction

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

Product Contents

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

Ingredient Binary	Version String
Intel® SGX Windows* 7/8.1/10 driver (64 bit only)	1.6.80.31049
Intel® SGX Runtime System Library	1.6.100.32132
Intel® SGX Application Enclaves	1.6.101.32775
Intel® SGX Application Enclave Service (AESM)	1.6.101.32869

2 What's New

Intel® Software Guard Extensions PSW includes the following changes in this version

- Apply the following updates for the Intel® SGX PSW installer:
    - Install production architecture enclave (AE) and support flexible provisioning in production environment
    - Install production the platform configuration data (PCD) file
    - Install in Windows* 10 RTM when Hyper-V* is enabled even though you cannot load an enclave in this setting
    - Use Intel® SGX Production Platform Provisioning Service backend server by default
    - Bug fix for the power management support
- Support for manual proxy set-up in Windows10* Network and internet setting
- Support to query platform provisioning status

- Support to query platform service status
- Support to query enclave launch whitelist file

3 System Requirements

Hardware Requirements

- The 6th Generation Intel® Core™ Processor (Intel® microarchitecture code name Skylake)
- A platform that uses Intel® microarchitecture code name Kabylake processor with H0 stepping

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 latest version of Intel® microarchitecture code name Kabylake mobile platform

Software Requirements

- Supported operating systems for the Intel® SGX PSW installer:
    - Microsoft Windows* 7/8.1/10/Threshold2/Redstone1 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 11.5.0.1000 or newer
      Note: To install 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 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 *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 maybe only applicable to Intel reference BIOS and may be not applicable to OEM BIOS.

You need administrator privilege to run the installer. From an Administrator command prompt, run the following:

```
msiexec /i SGX_PSW.msi
```

To force Intel® SGX PSW installation with administrative account, use the following command:

```
msiexec /i SGX_PSW.msi FORCE_INSTALL=1
```

Silent/unattended installations can be done by adding the `/qn` or `/quiet` switch:

```
msiexec /i SGX_PSW.msi /qn
```

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 update the driver to newer versions 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 cannot install Intel® SGX PSW by double-clicking the Intel® SGX PSW installer MSI file. To avoid this issue, use one of the following approaches:
    - Run the Intel® SGX PSW installer as an administrator
    - Run the installer from within a command console which was started by **run as administrator**
- Intel SGX platform service fails for DAL communication failure if you repeatedly use the service over 40 hours.
- If you have installed Intel SGX PSW 1.6.100.32132, and you upgrade Intel® SGX PSW to version 1.6.101.32869 through the **Upgrade** option of Intel® SGX PSW installer, Intel SGX PSW does not communicate with Intel® SGX Product Platform Provisioning Service backend server. To avoid this issue, uninstall Intel SGX PSW 1.6.100.32132, then install Intel SGX PSW 1.6.101.32869.

6 Disclaimer and Legal Information

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.