

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

Installation Guide and Release Notes

14 November 2017

Revision: 1.9

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	1.9.100.41172
Intel® SGX Launcher Enclave	1.7.100.34769
Intel® SGX Platform Services Initialization Enclave	1.9.100.40791
Intel® SGX Quoting Enclave	1.9.100.40585
Intel® SGX Provisioning Enclave	1.9.100.40585
Intel® SGX Provisioning Cert Enclave	1.9.100.39656
Intel® SGX Platform Services Operation Enclave	1.9.100.41109
Intel® SGX Application Enclave Service (AESM)	1.9.100.41172
Intel® SGX device driver for Windows* 7 (64 bit only)	1.9.100.39278
Intel® SGX device driver for Windows* 10 Fall Creators Update (version 1709) 64-bit version	1.9.103.38781

Intel® SGX PSW package conforms to the new driver model that Microsoft* requires on Windows* systems (Universal Windows Driver/UWD – DCH)

Follow the links below to learn more about this driver model:

<https://channel9.msdn.com/Events/WinHEC/WinHEC-Online/Understanding-Extension-INFs-and-Component-INFs>

<https://docs.microsoft.com/en-us/windows-hardware/drivers/install/using-an-extension-inf-file>

The Intel SGX DCH implementation is as follows:

- A Base INF is intended to provide a fundamental driver.
 - It attaches to a hardware device - the Intel SGX ACPI device when Intel SGX is enabled on a system: ACPI\INT0E0C
 - The version of the base INF is 1.9.103.38781 and is hosted by Windows Update.
<http://www.catalog.update.microsoft.com/Search.aspx?q=INT0E0C>
- Extension INFs are used by OEMs to customize and provide additional features.
 - An extension INF also attaches to the same hardware device as the base INF. In the case of Intel® SGX, the hardware device is ACPI\INT0E0C.
 - In addition, the INF creates a new [Software Component device](#):
swc\ven_int&dev_0e0c
 - Due to some current limitations, the extension INF functionality is merged into our base INF.
- Component INFs are typically used by the OEM and attaches to the SW device created (swc\ven_int&dev_0e0c) by their extension INF.
 - The version of our component INF is 1.9.100.41172.
 - The component INF is also hosted by Windows Update:
http://www.catalog.update.microsoft.com/Search.aspx?q=dev_0e0c
 - In our current implementation, the component INF installs the SGX_PSW via the EXE installer. The EXE installer is flexible and currently installs the Intel® SGX AESM, the runtime system library, etc. The EXE installer also includes the base INF as well as the legacy driver package used in older OSes where SGX driver was still managing memory, handling IOCTLs, etc. The EXE installer will install the appropriate driver for the OS version it detects.
 - The SGX_PSW EXE installer version matches the version in the component INF.
 - If there is a need to update SGX AESM, libraries, etc., we do not need to modify the base INF. We can update our component INF package independently and leave the base driver package intact.

2 What's New

Intel® Software Guard Extensions PSW includes the following changes in version 1.9.100.41172:

- Support for Intel® SGX Platform Services in 8th Generation Intel® Core™ Processor (Intel® microarchitecture code name Coffee Lake) platform.
- Support for 3072 bits Intel® SGX provisioning server public key.
- Bug fixes.

Changes in previous releases

Intel® Software Guard Extensions PSW includes the following changes in version 1.8.106.40803:

- 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 (Intel® ME) software components 11.8.50.3399 or newer

Note: To install the full set of Intel® ME software components, you need to install with `SetupMe.exe` instead of `MEISetup.exe` (HECI driver only).

Note: Intel® SGX PSW supports Microsoft Windows Server 2016 on Intel® Xeon® Processor E3 Server V5 and V6 platforms

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 cannot load any enclave in Windows 7/8.1 if the Microsoft Universal C Runtime (CRT) is not installed in the machine. To resolve this issue, you can install Windows Update for Universal CRT (KB2999226) in Windows.
- You cannot 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 Intel® SGX PSW and upgrade with new installer (after 1.7 version). To work around the issue, please manually uninstall Intel® SGX PSW before installing new version.
- Intel® SGX PSW installer would return an error code when a newer version PSW installer is already installed.

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