

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

Installation Guide and Release Notes

31 August 2018

Revision: 2.1

---

## 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 the 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	2.1.100.46245
Intel® SGX Launcher Enclave	2.1.100.45833
Intel® SGX Platform Services Initialization Enclave	2.1.100.45833
Intel® SGX Quoting Enclave	2.0.100.45935
Intel® SGX Provisioning Enclave	2.0.100.45833
Intel® SGX Provisioning Cert Enclave	2.0.100.45833
Intel® SGX Platform Services Operation Enclave	2.0.100.45833
Intel® SGX Application Enclave Service (AESM)	2.1.100.46245
Intel® SGX device driver for Windows* 7 (64 bit only)	2.1.100.45644
Intel® SGX device driver for Windows* 10 Fall Creators Update (version 1709) 64-bit version	2.1.100.46245

#### Windows\* 10 Fall Creators Update (Version 1709)

#### Windows\* 10 Spring Creators Update (version 1803)

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:

- Base INF is intended to provide a fundamental driver.
  - It attaches to the Intel® SGX ACPI device when Intel® SGX is enabled on a system: ACPI\INT0E0C
  - Base INF version is 1.9.105.41752 and is hosted by the Windows\* Update. For details, see the Microsoft Update Catalog:  
<http://www.catalog.update.microsoft.com/Search.aspx?q=INT0E0C>
- Extension INFs are used by OEMs to customize and provide additional features.
  - Extension INF attaches to the same hardware device as the base INF. In case of the 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 the base INF.
- Component INFs are typically used by the OEMs and attach to the software device (swc\ven\_int&dev\_0e0c) created by the extension INF.
  - Component INF version is 2.1.100.46245.
  - In the current implementation, the component INF for the Intel® SGX PSW uses a series of INF directives (CopyFile, AddReg, and others), but does NOT use the traditional desktop EXE installer (via AddSoftware, CoInstaller, or other mechanisms).
  - If the SGX AESM, libraries, or something else require update, it is not needed to modify the base INF. The component INF package can be updated independently without modifying the base driver package.

## 2 What's New

Intel® Software Guard Extensions PSW includes the following changes in version 2.1.100.46245:

- Updated the SGX Launcher Enclave and SGX Windows7 device driver to support enclave loading using the Key Separation and Sharing feature if this feature is available. Please refer to the [Intel Software Developer's Manual](#) for details on this new SGX Architecture feature.
- Fixed SGX Quoting enclave bug which causes invalid signature error when user upgrades SGX PSW 1.6 version to later version and does remote attestation.
- Updated SGX Platform Services Operation Enclave to use SGX local attestation library version 2
- Updated SGX Provisioning Cert Enclave and SGX Provisioning Enclave to fix error code bug
- Bug fixes

## Changes in previous releases

Intel® Software Guard Extensions PSW includes the following changes in version 2.0.101.44269:

- Updated the cryptography library to the Intel® Integrated Performance Primitives Cryptography 2018 Update 2.1. Mitigated security vulnerability CVE-2018-3617(<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3617>). For more details, refer to the Intel® Security Advisory INTEL-SA-00106(<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00106&languageid=en-fr>) and INTEL-SA-00135(<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00135&languageid=en-fr>).
- Updated the Intel® SGX platform service Dal applet.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 2.0.100.43647:

- Added support for the Intel® SGX 2.0 instruction set.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 1.9.106.43403:

- Mitigated security vulnerability CVE-2018-3626 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626>). For more details, refer to the Security Advisory INTEL-SA-00117 (<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00117&languageid=en-fr>)

- Updated the Intel® SGX PSW installer to prevent installation of the SGX PSW 1.6 and 1.7 version installers.

Intel® Software Guard Extensions PSW includes the following changes in version 1.9.105.42329:

- Added the Intel® SGX PSW .inf installer to support the Microsoft Windows\* 10 Fall Creators Update (version 1709) 64-bit version and above. Intel® SGX PSW .inf installer stores files to the Microsoft Windows\* DriverStore instead of the Program Files location.
- Intel® SGX PSW installer application (.exe) stopped supporting Microsoft Windows\* 10 Fall Creators Update (version 1709) 64-bit version and above.
- Removed the DotNetSystemProxy.dll from the Intel® SGX PSW .inf installer.
- Updated security for the Intel® SGX Application Enclave Service (AESM) and the Intel® SGX Application Enclaves.
- Fixed bugs.

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

- Added support for the Intel® SGX Platform Services in 8th Generation Intel® Core™ Processor (Intel® microarchitecture code name Coffee Lake) platform.
- Added support for the 3072 bits Intel® SGX provisioning server public key.
- Fixed bugs.

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

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

### 3 System Requirements

#### Hardware Requirements

- 6<sup>th</sup> 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
  - Microsoft Windows\* 10 Spring Creators Update (version 1803) 64-bit version**Note:** Intel® SGX PSW does not support Microsoft Windows\* 32-bit operating system.
- If you need to use the Intel® SGX platform service, install the following product. This is optional, you can skip this if you don't need to use Intel® SGX platform service
  - Full set of Intel® Management Engine (Intel® ME) software components**Note:** To install the full set of Intel® ME software components, you need to perform installation 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 the 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 on the system. To resolve this issue, you can install Windows the Update for Universal CRT (KB2999226) in Windows.
- You cannot install the Intel® SGX PSW when you install Windows\* OS in a legacy mode and the Intel® SGX is set as “Software Controlled” in BIOS. Configure the Intel® SGX as “Enabled” in BIOS before you install the Intel® SGX PSW.
- Legacy (before 1.6 version) Intel® SGX PSW installation entry cannot be removed from “Programs and Features” in the Windows Control Panel if you install the legacy Intel® SGX PSW and upgrade it with a new installer (after 1.7 version). To work around the issue, please manually uninstall the Intel® SGX PSW before installing new version.
- Intel® SGX PSW .exe installer returns an error code if a newer version of the PSW installer is already installed.
- Applications that use the Intel® SGX PSW in Microsoft Windows\* 10 Fall Creators Update (Version 1709) and do not have proxy settings for their users will need a

system proxy setting. Alternatively, the Intel® SGX AESM proxy configuration tool can be used.

- After installing the Intel® SGX PSW .inf installer, the Intel® SGX AESM service status will be “stopped”. It does not impact enclave loading by the Intel® SGX application. When the enclave is loaded, the Intel® SGX AESM service status will be “running”.
- After installing the Intel® SGX PSW .inf installer, it doesn't prevent SGX 1.7 version PSW .exe installer to install. It would prevent SGX 1.8 and later version PSW .exe installer to install.

## 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](http://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