

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

Installation Guide and Release Notes

27 April 2018

Revision: 2.0.101

---

## 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	2.0.101.44269
Intel® SGX Launcher Enclave	2.0.1.44145
Intel® SGX Platform Services Initialization Enclave	2.0.1.44145
Intel® SGX Quoting Enclave	2.0.1.44145
Intel® SGX Provisioning Enclave	2.0.1.44145
Intel® SGX Provisioning Cert Enclave	2.0.1.44145
Intel® SGX Platform Services Operation Enclave	2.0.1.44145
Intel® SGX Application Enclave Service (AESM)	2.0.101.44269
Intel® SGX device driver for Windows* 7 (64 bit only)	1.9.105.42072
Intel® SGX device driver for Windows* 10 Fall Creators Update (version 1709) 64-bit version	1.9.105.41752

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

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 1.9.105.41752 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 2.0.101.44269.
  - The component INF is also hosted by Windows Update:  
[http://www.catalog.update.microsoft.com/Search.aspx?q=dev\\_0e0c](http://www.catalog.update.microsoft.com/Search.aspx?q=dev_0e0c)
  - In the current implementation, the component INF for Intel® SGX PSW uses a series of INF directives (CopyFile, AddReg, etc), but does NOT use the traditional desktop EXE installer (via AddSoftware, ColnInstaller, or other mechanisms).
  - 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.

### Windows 10 Creators Update (Version 1703) and earlier

The Intel® SGX PSW installer continues to be an EXE installer application.

## 2 What's New

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

- Update the cryptography lib to Intel® Integrated Performance Primitives Cryptography 2018 Update 2.1.
- Update Intel® SGX platform service Dal applet.
- Bug fixes.

## Changes in previous releases

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.
- Bug fixes.

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

- Mitigated security vulnerability CVE-2018-3626 (<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626>). For more details, refer to Security Advisory INTEL-SA-00117 (<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00117&languageid=en-fr>)
- Update Intel® SGX PSW installer to prevent SGX PSW 1.6 and 1.7 version installers to install.

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

- Added an Intel® SGX PSW .inf installer to support Microsoft Windows\* 10 Fall Creators Update (version 1709) 64-bit version and above. Intel® SGX PSW .inf installer installs files to the Microsoft® Windows DriverStore instead of Program Files.
- Intel® SGX PSW installer application (.exe) no longer supports Microsoft Windows\* 10 Fall Creators Update (version 1709) 64-bit version and above
- Removed the DotNetSystemProxy.dll from the Intel® SGX PSW .inf installer.
- Security updates to Intel® SGX Application Enclave Service (AESM) and Intel® SGX Application Enclaves.
- Bug fixes.

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.

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

- 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 Intel® SGX platform service, install the following product:
  - Full set of Intel® Management Engine (Intel® ME) software components 12.0.0.1058 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 returns an error code if a newer version of the PSW installer is already installed.
- Applications using the Intel® SGX PSW in Microsoft Windows 10 Fall Creators Update (Version 1709) that 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. After application loads the enclave, the Intel® SGX AESM service status will be “running”.

## 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