

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

16 October 2023

Revision: 2.21.1

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* OS.

Product Contents

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

Ingredient Binary	Version String
Intel® SGX Runtime System Library	2.21.100.3
Intel® SGX Launcher Enclave (LE)	2.21.100.1
Intel® SGX Platform Services Initialization Enclave (PSE-pr)	2.21.100.1
Intel® SGX Quoting Enclave (QE)	2.21.100.1
Intel® SGX ECDSA Quoting Enclave (QE3)	1.19.100.1
Intel® SGX ID Enclave	1.19.100.1
Intel® SGX Provisioning Enclave (PvE)	2.21.100.1
Intel® SGX Provisioning Cert Enclave (PcE)	2.21.100.1
Intel® SGX Platform Services Operation Enclave (PSE-op)	2.21.100.1
Intel® SGX Application Enclave Service (AESM)	2.21.100.3
Intel® SGX Quote Verification Enclave (QVE)	1.19.100.1
Intel® SGX ECDSA Quoting Service (sgx_dcap_ql)	1.19.100.3
Intel® SGX DCAP Quote Verification (sgx_dcap_quoteverify)	1.19.100.3

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

To learn more about the driver model, follow the links below:

<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 provides a fundamental driver:
 - It attaches to the Intel® SGX ACPI device when the Intel® SGX is enabled on a system: ACPI\INTOEOC.
 - Base INF version is 2.14.101.1 and it is hosted by the Windows* Update. For details, see the Microsoft* Update Catalog:
<http://www.catalog.update.microsoft.com/Search.aspx?q=INTOEOC>
- Extension INFs are used by OEMs to customize and provide additional features.
 - Extension INF attaches to the same hardware device as the base INF. For the Intel® SGX, the hardware device is ACPI\INTOEOC.
 - In addition, the INF creates a new [Software Component device](#): swc\ven_int&dev_0e0c_pswdcap.
 - Due to current limitations, the extension INF functionality is merged into the base INF.
- Component INFs are typically used by the OEMs. The component INFs attach to the software device (swc\ven_int&dev_0e0c_pswdcap) created by the extension INF.
 - Component INF version is 2.15.100.
 - 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, ColnStaller, or other mechanisms).
 - If the Intel® SGX Architecture Enclave Services Manager (Intel® SGX AESM), libraries, or something else require update, you do not need 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 Platform Software (Intel® SGX PSW) includes the following changes in version 2.21.100.3:

- Resigned all Intel® SGX Architecture Enclaves
- Upgraded Intel® SGX Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.10
- Added Rust wrapper for low-level Quote Generation APIs
- Enabled 'SE_TRACE' log in release binary
- Updated Rust QVL wrapper to use native Rust structure for quote verification collateral
- Added a limitation in the DCAP QVL to only allow the user to set the QvE load policy once
- Fixed bugs

Changes in previous releases

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.20.100.1:

- Enhanced quote verification performance in multi-thread scenarios
- Upgraded Intel® SGX Quote Verification Enclave to integrate latest OpenSSL/SgxSSL 1.1.1u
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.19.100.3:

- Applied CVE-2023-1255, CVE-2023-0465, and CVE-2023-0466 patches to SgxSSL/OpenSSL 1.1.1t
- Upgraded Intel® SGX Quote Verification Enclave to integrate updated SgxSSL
- Enhanced the attestation local cache functionality by giving users the option to provide their own cache file
- Enabled QPL/QCNL log in DCAP samples
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.18.100.2:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1t
- Upgraded SQLite3 to version 3.40.1
- Added new API in quote verification library to extract FMSPC (Family-Model-Stepping-Platform-CustomSKU) value from ECDSA quote
- Fixed bugs

From this release, we will upload ZIP format release package to IDZ (Intel® Developer Zone).

You can use Powershell to extract the .zip file to %TEMP% (the default location for the previous releases), you can execute, for example:

```
Expand-Archive '.\Intel SGX DCAP for Windows v1.16.100.2.zip' $env:temp
```

To expand the archive in the current directory:

```
Expand-Archive '.\Intel SGX DCAP for Windows v1.16.100.2.zip'
```

Or right click on the zip file and click on "Extract All"

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.17.100.2:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1q
- Upgraded Intel® SGX QE3 to make it backward compatible
- Improved ECDSA quote generation and verification performance by caching PCK certificates and collaterals in memory and disk drive
- Added Java support for quote verification library
- Added new APIs to unify Intel® SGX and TDX quote verification in Quote Verification Library
- Added Advisory ID in ECDSA quote verification supplemental data
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.16.100.3:

- Re-signed all the Intel® SGX Architecture Enclaves (AEs) to address [CVE-2022-21123](#), [CVE-2022-21125](#) and [CVE-2022-21166](#)
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1o
- Introduced Intel® ID enclave for QE identity generation
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.15.100.4:

- Enhanced QPL (Quote Provider Library) to support caching Intel® PCK (Provisioning Certificate Key) certificate chain in local memory, or retrieving Intel® PCK cert chain from local HTTP/S address
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1m
- Removed support for Windows Server 2016
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.14.101.1:

- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1l
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.14.100.3:

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2021 update 3
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library
- Added support in Intel® Quote Provider Library (QPL) to retrieve SGX ECDSA quote verification endorsements from Intel® Provisioning Certificate Service (PCS). User can configure PCCS or PCS in QPL's config file
- Updated SGX ECDSA quote verification library (QVL) and quote verification enclave (QvE) to support CRL in different encoding
- Updated SGX ECDSA quote verification library (QVL) and quote verification enclave (QvE) to hardcode Intel® root public key instead of root certificate
- Added Windows 11 support
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.13.100.2:

- Upgraded Intel® Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1k
- Upgraded SQLite to version 3.35.3
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.12.103.1:

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2020 update 3
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.12.102.1:

- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.12.100.4:

- Merged Intel® DCAP INF driver into PSW INF driver
- Added more Windows event log to help identifying possible issues
- Upgraded OpenSSL and SgxSSL to latest version 1.1.1i in DCAP components
- Fixed bugs

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.11.101.1:

- Intel® SGX BASE INF creates a new device, swc\ven_int&dev_0e0c_pswdcap, instead of swc\ven_int&dev_0e0c.
- Intel® SGX PSW INF for swc\ven_int&dev_0e0c_pswdcap also contains Data Center Attestation Primitives (DCAP) binaries that were previously distributed under swc\ven_int&dev_0e0c_dcap.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.11.100.3:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.10.100.2:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.9.100.1:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.8.100.2:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.7.101.2:

- Support to query supported Intel® SGX remote attestation key id list.
- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.7.100.2:

- Changes to address CVE-2020-0551.
- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.6.100.2:

- Added support for running SGX applications inside Windows containers.
- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.5.101:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.5.100:

- Added support for ECDSA-based Quote and corresponding key exchange library interface.
- Added support for new version Intel® Provisioning Certification Server interfaces.
- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.4.100:

- Added support for ECDSA-based Quote and corresponding key exchange library interface.
- Added support for a new interface to check platform information blob from remote attestation response message.

- Updated SGX Window7 driver to remove 2M EPC size reservation for Intel® Provisioning Certificate Enclave (PCE), Intel® Quoting Enclave (QE) and Intel® Provisioning Enclave (PvE).
- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.3.2:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.3.1:

- Fixed bugs.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.4:

- Updated sgx_psw.inf to fix bug.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.3:

- Intel® SGX PSW version 2.2.3 has been updated to include OpenSSL 1.0.2q in Intel® SGX Application Enclave Service (AESM) and OpenSSL 1.1.1a in the installation framework of the EXE version of Intel® SGX PSW, which includes functional and security updates. Users should update to the latest version of the Intel® SGX PSW.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.102.49005:

- Updated Intel® SGX Platform Service DAL Applet

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.101.48504:

- Support Intel® CSME version 1040 and above

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.100.47975:

- Added support for the Intel® SGX Launch Configuration Service and the Intel® SGX Enclave Common Loader library in Microsoft Windows* 10 Anniversary Update, version 1607 or higher.

- Enhancement to address security vulnerability INTEL-SA-00203 (<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00203.html>)
- Fixed bugs.

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

- Updated the Intel SGX Launcher Enclave and the Intel SGX Windows* 7 device driver to support enclave loading using the Key Separation and Sharing feature if this feature is available. For details on the feature, see the [Intel® Software Developer Manual](#).
- Fixed the Intel SGX Quoting enclave bug that caused the invalid signature error when a user upgraded the Intel SGX PSW 1.6 version and did a remote attestation.
- Updated the Intel SGX Platform Services Operation Enclave to use the Intel SGX local attestation library version 2.
- Updated the Intel SGX Provisioning Cert Enclave and the Intel SGX Provisioning Enclave to fix error code bugs.
- Fixed other bugs.

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 Intel 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. The 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 the Microsoft Windows* 10 Fall Creators Update (version 1709) 64-bit version and higher.
- 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 the 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). The 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

- 6th Generation Intel® Core™ Processor or newer with SGX support
- Intel® Xeon® E processors on V5 and V6 platforms
- 3rd Generation Intel® Xeon® Scalable Processors

Software Requirements

- Supported 64bit operating systems for the Intel® SGX base and component drivers:
 - Microsoft Windows* 10 version 1709 or later, including 1803, 1809, 1903, 1909, 2004, 21H1
 - Microsoft Windows* 11
 - Microsoft Windows Server 2019
 - Microsoft Windows Server 2022

Note:

- Intel® SGX PSW does not support the Microsoft Windows* 32-bit operating system.
 - Microsoft Windows Server editions supported on Intel® Xeon® processors.
 - For more detailed installation instructions, please see *Intel® Software Guard Extensions Installation Guide for Windows* OS*.
- If you need to use the Intel® SGX platform service, install the full set of Intel® Management Engine (Intel® ME) software components.

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

4 Known Issues and Limitations

- Please reboot the system if SGX related event log doesn't appear.
- Intel® SGX PSW 2.7.1 does not include the latest functional and security updates in 3rd part components (SQLite). The next release of the Intel® SGX SDK for Windows is targeted to be released in May 2020 and will include additional functional and security updates. Customers should update to the latest version as it becomes available.
- Intel® SGX PSW 2.7 does not include the latest functional and security updates. The next release of the Intel® SGX PSW is targeted to be released in April 2020 and will

include additional functional and security updates. Customers should update to the latest version as it becomes available.

- Intel® SGX PSW 2.6 does not include the latest functional and security updates. Intel® SGX PSW 2.6.1 is targeted to be released in March 2020 and will include additional functional and security updates. Customers should update to the latest version as it becomes available.
 - SQLite 3.30.1 with unmitigated CVEs ([CVE-2019-19244](#), [CVE-2019-19645](#) and [CVE-2019-19880](#)) is used in untrusted part. The CVEs are not exploitable in SGX software stack.
 - OpenSSL 1.1.1d with an unmitigated CVE ([CVE-2019-1551](#)) is used in untrusted part. The CVE is not exploitable in SGX software stack.
- 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 the Windows Update for the Universal CRT (KB2999226) on 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 resolve the issue, manually uninstall the Intel® SGX PSW before installing a new version.
- Intel® SGX PSW .exe installer returns an error if a higher version of the Intel SGX PSW installer is already installed.
- Applications that use the Intel® SGX PSW in Microsoft Windows* 10 Version 1709/1803/1809 and do not have proxy settings for their users, require 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 is set to “stopped”. It does not impact enclave loading by the Intel® SGX application. When the enclave is loaded, the Intel® SGX AESM service status is set to “running”.
- Installation of the Intel® SGX PSW .inf installer has no impact on the Intel SGX PSW .exe installer of version 1.7 but it can affect the Intel SGX PSW .exe installer of version 1.8 or higher.

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