Intel® Software Guard Extensions (Intel® SGX) SDK for Windows* OS

Installation Guide

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.

This software and the related documents are Intel copyrighted materials, and your use of them is governed by the express license under which they were provided to you (**License**). Unless the License provides otherwise, you may not use, modify, copy, publish, distribute, disclose or transmit this software or the related documents without Intel's prior written permission.

This software and the related documents are provided as is, with no express or implied warranties, other than those that are expressly stated in the License.

Revision History

Revision Number	Description	Revision Date
1.1	Intel® SGX Win 1.1 release	September 2015
1.6	Intel® SGX Win 1.6 release	May 2016
1.7	Intel® SGX Win 1.7 release	November 2016
1.8	Intel® SGX Win 1.8 release	June 2017
1.9	Intel® SGX Win 1.9 release	October 2017
1.9.5	Intel® SGX Win 1.9.5 release	January 2018
1.9.6	Intel® SGX Win 1.9.6 release	March 2018
2.0.0	Intel® SGX Win 2.0.0 release	April 2018
2.0.1	Intel® SGX Win 2.0.1 release	April 2018
2.1	Intel® SGX Win 2.1 release	August 2018
2.2	Intel® SGX Win 2.2 release	November 2018
2.2.3	Intel® SGX Win 2.2.3 release	February 2019
2.3	Intel® SGX Win 2.3 release	March 2019
2.4	Intel® SGX Win 2.4 release	June 2019
2.5	Intel® SGX Win 2.5 release	October 2019
2.5.1	Intel® SGX Win 2.5.1 release	November 2019
2.6	Intel® SGX Win 2.6 release	January 2020
2.7	Intel® SGX Win 2.7 release	March 2020
2.7.1	Intel® SGX Win 2.7.1 release	April 2020
2.8	Intel® SGX Win 2.8 release	June 2020
2.9	Intel® SGX Win 2.9 release	August 2020
2.10	Intel® SGX Win 2.10 release	September 2020
2.11	Intel® SGX Win 2.11 release	November 2020
2.12	Intel® SGX Win 2.12 release	January 2021
2.13	Intel® SGX Win 2.13 release	June 2021
2.14	Intel® SGX Win 2.14 release	September 2021
2.14.1	Intel® SGX Win 2.14.1 release	November 2021
2.15	Intel® SGX Win 2.15 release	March 2022
2.16	Intel® SGX Win 2.16 release	June 2022
2.17	Intel® SGX Win 2.17 release	November 2022
2.18	Intel® SGX Win 2.18 release	March 2023

Intel® Software Guard Extensions SDK and Platform Software Installation

This document provides the instructions on how to install the Intel® SGX SDK and platform software. You can see the details in the following topics:

- Install Intel® SGX SDK
- Install Intel® SGX Platform Software

Install Intel® SGX SDK

Prerequisites

The Intel® Software Guard Extensions SDK package includes components to develop Intel® SGX applications. The main components include:

- Trusted libraries, including standard C library, C++ runtime support, C++11, and so on.

- Development tools including Edger8r application, signing tool, add-ins and wizards for Microsoft Visual Studio* 2017 IDE and Microsoft Visual Studio* 2019 IDE, and EPC measurement tool.
- Sample Projects.

- Visual Studio extensions for creating, modifying, and debugging enclave projects

The following steps describe how to install the Intel(R) SGX SDK when it is distributed via a nuget package.

Using the Nuget package manager

Installers such as the Intel(R)_SGX_Windows_SDK_<version>.exe install packages system-wide. Nuget packages, on the other hand, are typically installed for specific projects from within Visual Studio.

Remove Older Versions - Optional

If you have a previously installed Intel(R)_SGX_Windows_SDK_<version>.exe version of the SDK you can remove it by navigating to the **Control Panel** and uninstalling it from **Apps and Features\Programs and Features**.

Add Local Source - Optional

Nuget packages are normally installed from nuget.org. If you would like to install from a local source, for example `C:\LocalNugetPackages`, you will need to add this directory to the **Package Sources**. In Visual Studio, click on **Tools-> NuGet Package Manager-> Package Manager Settings**.
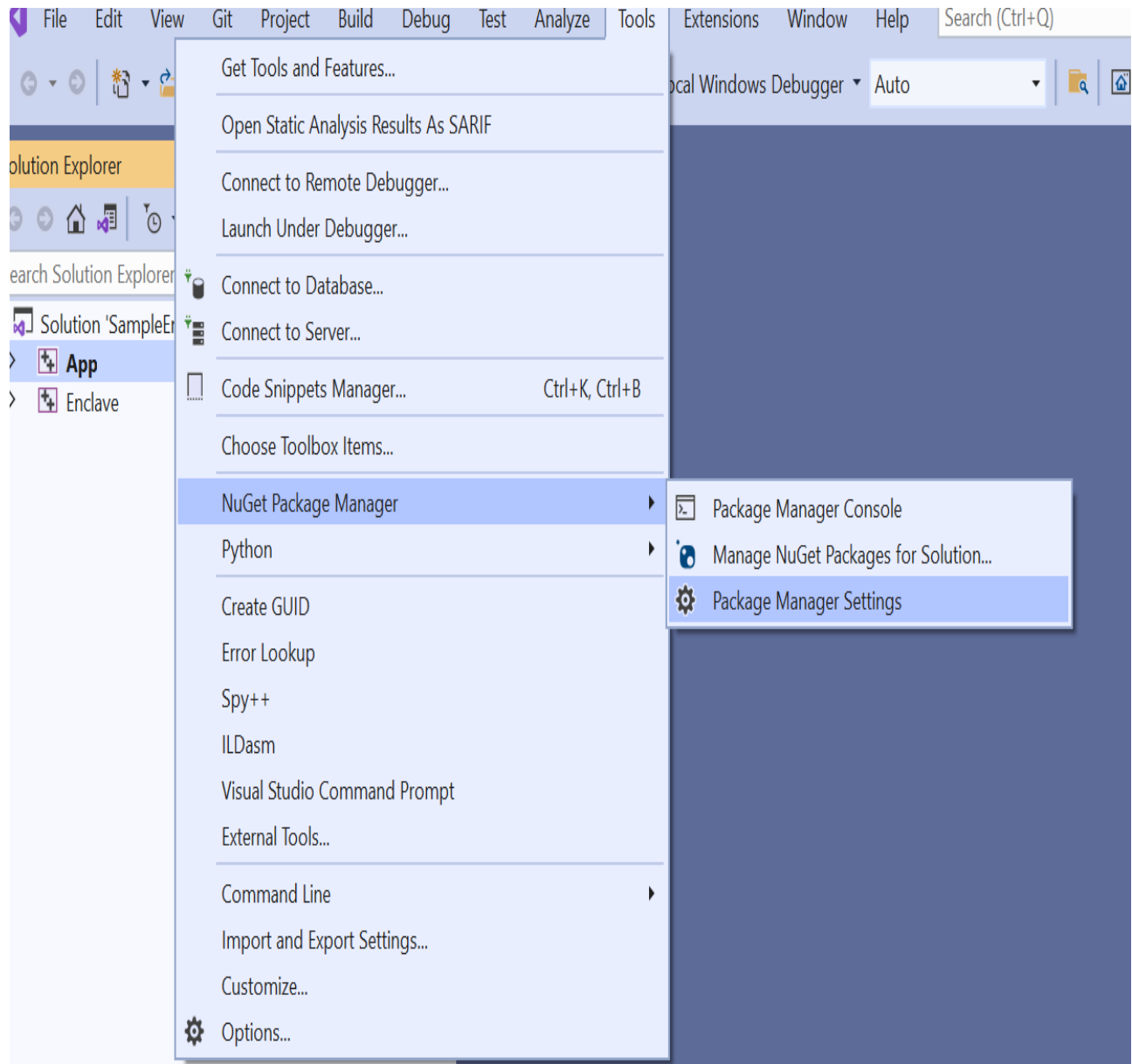
Then, click on the green + button and provide a **Name** and **Source** for the directory that will be used to search for NuGet packages. When you are done, click on **Update** and **OK**.
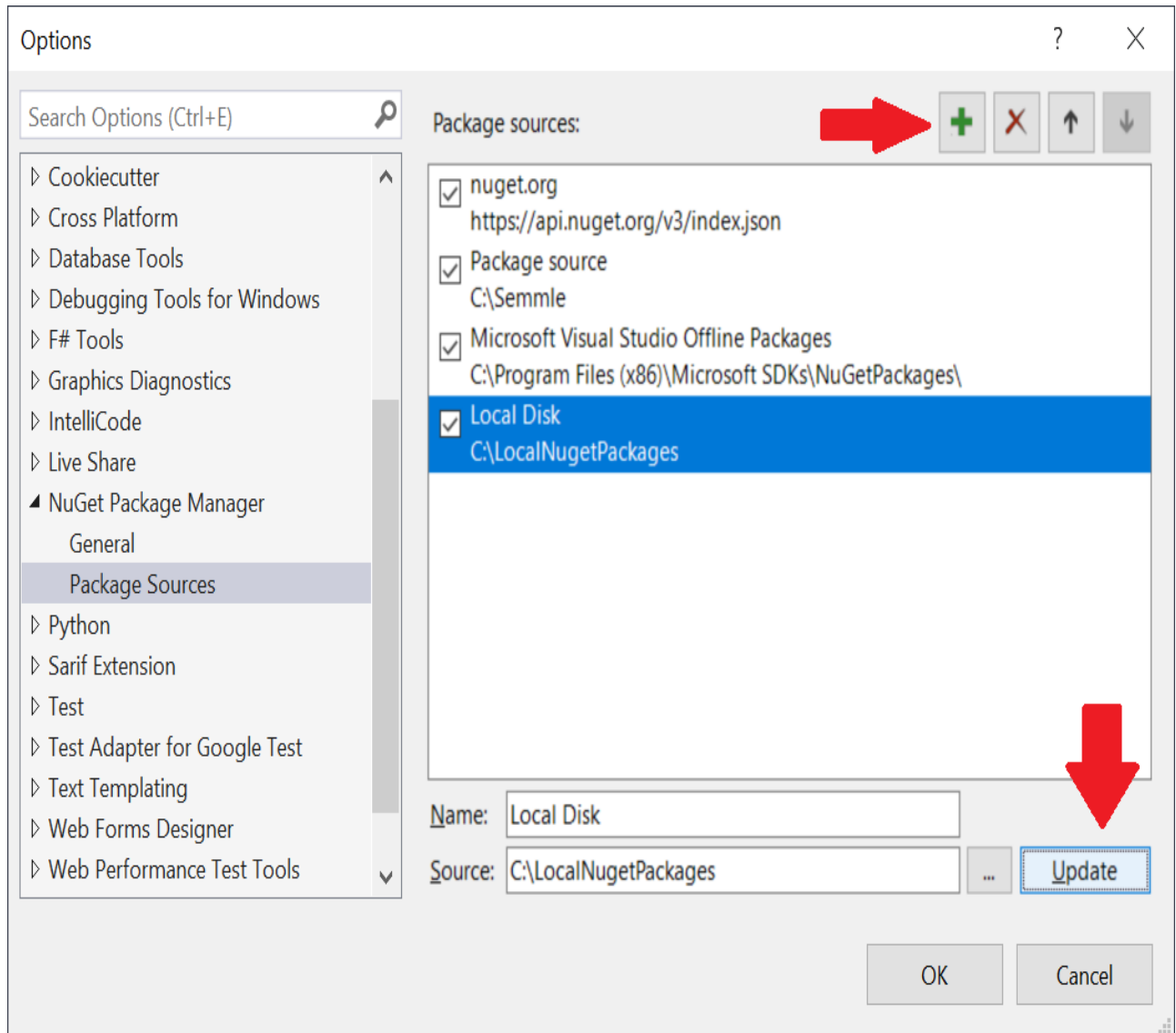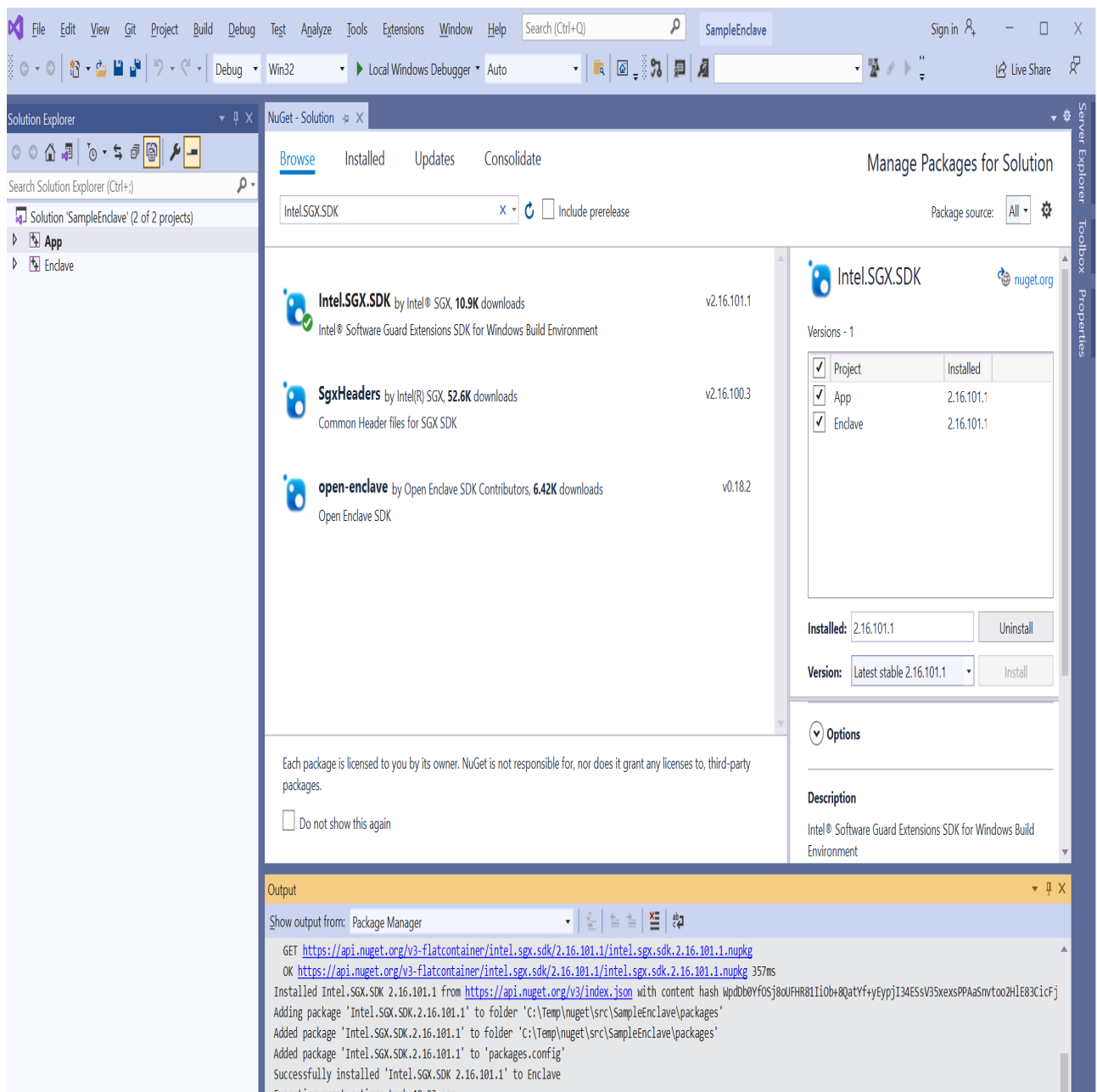

Installation of Intel.SGX.SDK nuget package

In Visual Studio, click on **Tools-> NuGet Package Manager-> Package Manager Settings**. In the Package source drop-down, select whether you want to search nuget.org, a local package source, or all.

In the Browse tab, search for Intel.SGX.SDK and select it and apply it to all the projects in the solution that you wish to use the Intel SGX SDK on. You can then select the **Version** from the drop-down and click on the **Install** button.
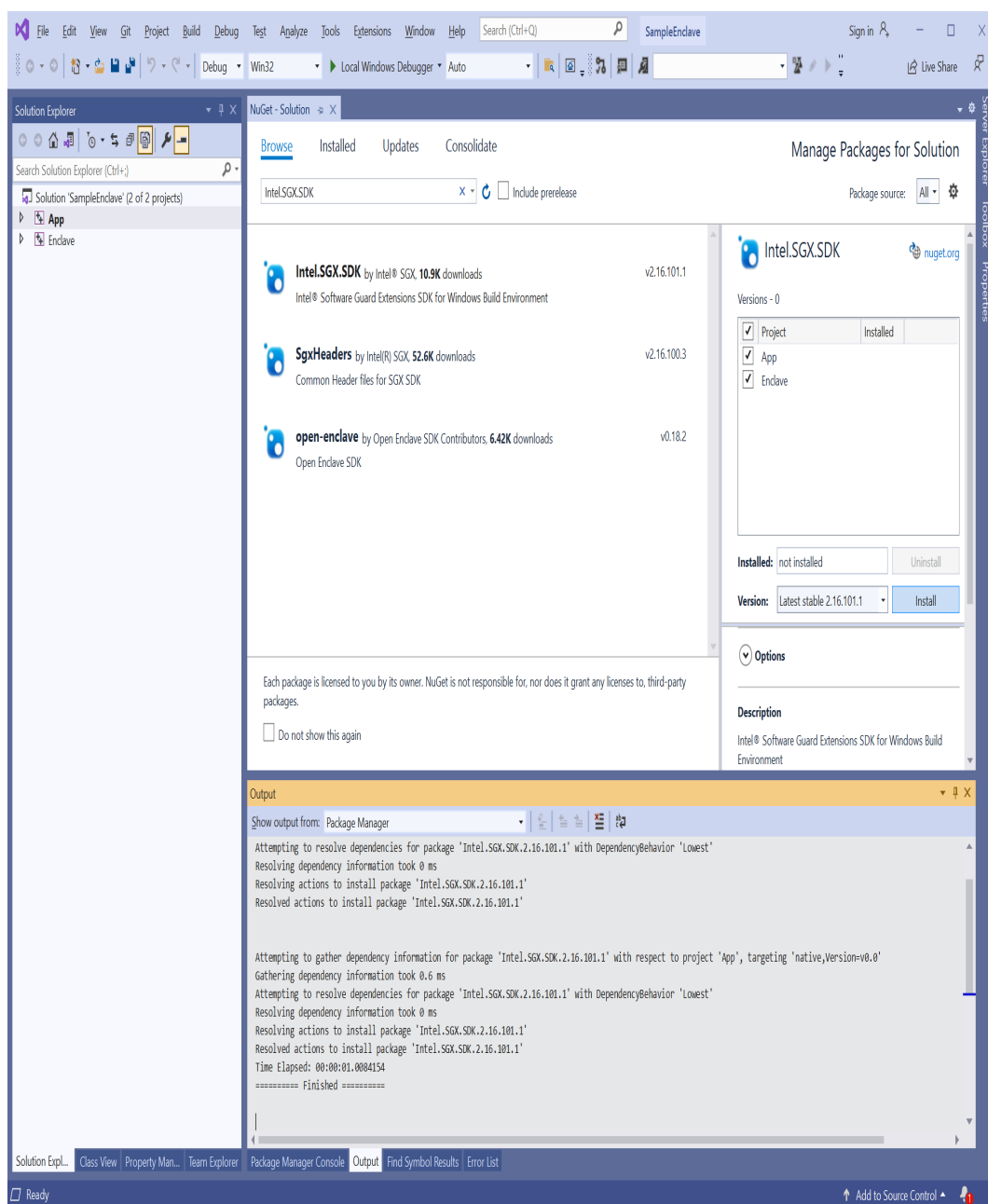
After a successful installation, you will see a message in the output window. The projects selected for this solution will use the Intel SGX SDK provided by the nuget package. No additional projects, solutions, or system-wide settings will be affected. If you want to verify which version of the Intel SGX SDK was used to build an enclave, you can use the `/verbose` flag in the linker options for your project, or execute `dumpbin /all /section:sgxvers Enclave.dll` or `findstr SGX_TRTS_VERSION Enclave.dll`.

Updating Intel.SGX.SDK nuget package

In Visual Studio, click on **Tools-> NuGet Package Manager-> Package Manager Settings**. In the Package source drop-down, select whether you want to search nuget.org, a local package source, or all. You can then select the **Version** from the drop-down you want to install and click on the **Install** button.

Uninstalling Intel.SGX.SDK nuget package

In Visual Studio, click on **Tools-> NuGet Package Manager->
Package Manager Settings**. Click on the **Installed** tab and click on the **Uninstall** button.

Visual Studio add-ins and wizards

The add-in and wizards for Microsoft Visual Studio* 2017 IDE and/or Microsoft Visual Studio* 2019 IDE are also provided separately with `vsix` as an extension name.

Scriptable System-wide Installation of Intel.SGX.SDK nuget package

A nuget package can be thought of as an expandable archive. Users that want to install the Intel.SGX.SDK on the system for the use of all its users can extract the contents of the nuget archive and then set environment variables to point to the extracted file location. For example,

```
PS C:\LocalNugetPackages> mv .\Intel.SGX.SDK.2.16.101.1.nupkg .\Intel.SGX.SDK.2.16.101.1.zip

PS C:\LocalNugetPackages> Expand-Archive .\Intel.SGX.SDK.2.16.101.1.zip

PS C:\LocalNugetPackages> [Environment]::SetEnvironmentVariable('SGXSDKInstallPath',
'C:\LocalNugetPackages\Intel.SGX.SDK.2.16.101.1\build\native\',
'User')
```

If installing as a system administrator for the whole system, the environment variable should be set machine-wide:

```
PS C:\LocalNugetPackages> [Environment]::SetEnvironmentVariable('SGXSDKInstallPath',
'C:\LocalNu-
```

```
getPackages\Intel.SGX.SDK.2.16.101.1\build\native\',
'Machine')
```

Finally, if you need to support simulation or debugging, add `'%SGXSDKIn-stallPath%\bin\x64\Release\; %SGXSDKIn-stallPath%\bin\win32\Release\'` to the PATH environment variable.

Note that precise management of system-wide PATH is beyond the scope of this document, but should be very familiar to system administrators. Users that are not familiar with setting system-wide environment variables can use the nuget package manager if they wish to avoid the possibility of adding an untrusted directory to the PATH environment variable.

Install Intel® SGX Platform Software

The 1.9.5 release of the Intel® SGX Platform Software (Intel® SGX PSW) is the first release that provides an INF-based installation that does not use the traditional desktop EXE installer. However, it does not support this new INF installation mechanism in older versions of the OS. Older OSes can use the traditional desktop EXE installer instead.

Windows 10 Fall Creators Update (version 1709) and later

The Intel® SGX PSW is provided as a Software Component that matches the Software Component device SWC\VEN_INT&DEV_0E0C_PSWDCAP. This Software Component device is created when installing the base driver for the Intel® SGX ACPI device acpi\int0e0c. When Intel® SGX is enabled and the Intel® SGX PSW is installed, **Device Manager** will include **Intel® Software Guard Extensions** in both the **System Devices** and in **Software Components**.

For more information regarding software components, please see the Intel® Software Guard Extensions Platform Software for Windows* OS Release Notes.

Online Installation

If BIOS has been configured to enable Intel® SGX and the system is configured to obtain updates from Windows Update, it will automatically install the Intel® SGX base driver and the Intel® SGX PSW from Windows Update.

Offline Installation

To install the Intel® SGX PSW when not receiving Windows Updates, the base INF and the component INF must both be installed. To achieve this, execute the following commands:

- `pnputil /add-driver sgx_base.inf /install`

- `pnputil /add-driver sgx_psw.inf /install`

Uninstallation

Uninstallation of INF-installed Intel® SGX PSW is not recommended.

Windows* 10 Creators Update (version 1703) and older

Support for lower versions of the OS has been deprecated.

Additional Dependencies

To use Intel® SGX platform services, you need to install a full set of Intel® Management Engine (Intel® ME) software components, which includes Intel® Dynamic Application Loader Host Interface Service (Intel® DAL Host Interface Service). If you install Intel® ME driver only, Intel® SGX platform service is not available.

Typically, the Intel® DAL stack and Intel® ME stack are pre-installed with other Intel software on a platform. However, if you receive an error that Intel® SGX platform services are unavailable, install the appropriate Intel® DAL stack and/or Intel® ME stack.

Please refer install Intel® Software Guard Extensions Driver for Data Center Attestation Primitives (Intel® SGX DCAP) to enable ECDSA attestation.

Logging

Logs are added to help debug configuration errors. By default, the SGX shares libraries output logs to standard output or standard error. The AESM as a system service/daemon outputs the log to the Event Log. Open the `Event Viewer` and check the `Applications and Services Logs -> AESMService -> SGX/Admin` or `Applications and Services Logs -> AESMService -> SGX/Diagnostic` to see the log.

ECDSA attestation

To enable ECDSA attestion:

- Ensure that you have the following required hardware:
    - 8th Generation Intel® Core™ Processor or newer with Flexible Launch Control support*.
    - Intel® Atom™ Processor with Flexible Launch Control support*.

- To use ECDSA attestation, you must install the Intel® Software Guard Extensions Driver for Data Center Attestation Primitives (Intel® SGX DCAP):
  Follow the Intel® SGX DCAP Installation Guide for Windows* OS to install the Intel® SGX DCAP driver.

  ### *NOTE*

  If you already installed Intel® SGX driver without ECDSA attestation, please uninstall this driver, or the newly installed ECDSA attestation enabled Intel® SGX driver will not work.

- Install Provisioning Certificate Caching Service(PCCS). About how to install and configure PCCS, please refer SGXDataCenterAttestationPrimitives.

- Ensure the PCCS is setup correctly by local administrator or data center administrator. Please also setup registry for default Quote Provider library according to your real environment.
  [HKEY_LOCAL_MACHINE\SOFTWARE\Intel\SGX\QCNL]

  "USE_SECURE_CERT"=dword:00000001

  "PCCS_URL"="https://localhost:8081/sgx/certification/v2/"

- PCCS_URL is the URL of your PCCS caching service. Set USE_SECURE_CERT to 0 if PCCS uses self-signed certificates, and 1 for a production PCCS with authenticated certificates.