

Intel[®] Software Guard Extensions (Intel[®] SGX) SDK for Linux* 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.

Copyright 2014-2020 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
1.5	Intel® SGX Linux 1.5 release	May 2016
1.6	Intel® SGX Linux 1.6 release	September 2016
1.7	Intel® SGX Linux 1.7 release	December 2016
1.8	Intel® SGX Linux 1.8 release	March 2017
1.9	Intel® SGX Linux 1.9 release	July 2017
2.0	Intel® SGX Linux 2.0 release	November 2017
2.1	Intel® SGX Linux 2.1 release	December 2017
2.1.1	Intel® SGX Linux 2.1.1 release	March 2018
2.1.2	Intel® SGX Linux 2.1.2 release	March 2018
2.1.3	Intel® SGX Linux 2.1.3 release	April 2018
2.2	Intel® SGX Linux 2.2 release	July 2018
2.3	Intel® SGX Linux 2.3 release	September 2018
2.4	Intel® SGX Linux 2.4 release	November 2018
2.5	Intel® SGX Linux 2.5 release	March 2019
2.6	Intel® SGX Linux 2.6 release	June 2019
2.7	Intel® SGX Linux 2.7 release	September 2019
2.7.1	Intel® SGX Linux 2.7.1 release	November 2019
2.8	Intel® SGX Linux 2.8 release	January 2020
2.9	Intel® SGX Linux 2.9 release	March 2020
2.9.1	Intel® SGX Linux 2.9.1 release	April 2020
2.10	Intel® SGX Linux 2.10 release	June 2020
2.11	Intel® SGX Linux 2.11 release	August 2020

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® Software Guard Extensions SDK and Platform Software](#)
- [Install Intel\(R\) Software Guard Extensions Eclipse* Plug-in](#)

Install Intel® Software Guard Extensions SDK and Platform Software

The current Linux* OS installation packages include three parts separately:

- Installation package for the Intel® Software Guard Extensions (Intel® SGX) driver
- Installation package for the Intel® SGX platform software (Intel® SGX PSW)
- Installation package for the Intel® SGX SDK.

Hardware Requirements

- 6th Generation Intel® Core™ Processor or newer
- Intel® SGX option enabled in BIOS.

NOTE

This is required when you install the Intel® SGX driver or Intel® SGX PSW, but not required when you install the Intel® SGX SDK installer.

Prerequisites

Ensure that you have one of the following operating systems:

- Ubuntu* 16.04 LTS 64-bit Desktop version
- Ubuntu* 16.04 LTS 64-bit Server version
- Ubuntu* 18.04 LTS 64-bit Desktop version
- Ubuntu* 18.04 LTS 64-bit Server version
- Red Hat* Enterprise Linux Server release 7.6 64bits

- Red Hat* Enterprise Linux Server release 8.2 64bits
- CentOS* 8.1 64bits
- Fedora* 31 Server 64bits
- SUSE* Linux Enterprise Server 15.1 64bits.

To install the Intel® SGX PSW, first install the following tools:

- On Ubuntu* 16.04 and Ubuntu* 18.04

```
$ sudo apt-get install libssl-dev libcurl4-openssl-  
dev libprotobuf-dev
```

- On Red Hat* Enterprise Linux 7.6, Red Hat Enterprise Linux 8.2 and Fedora* 31:

```
$ sudo yum install openssl-devel libcurl-devel pro-  
tobuf-devel yum-utils
```

- On CentOS* 8.1:

```
$ sudo dnf --enablerepo=PowerTools install openssl-  
devel libcurl-devel protobuf-devel yum-utils
```

- On SUSE Linux Enterprise Server* 15.1:

```
$ sudo yum install openssl-devel libcurl-devel pro-  
tobuf-devel yum-utils
```

To install the Intel® SGX SDK, install the following:

- On Ubuntu* 18.04:

```
$ sudo apt-get install build-essential python
```

- On Red Hat* Enterprise Linux 8.2, CentOS* 8.1 and Fedora* 31:

```
$ sudo yum groupinstall 'Development Tools'
```

```
$ sudo yum install python2
```

```
$ sudo alternatives --set python /usr/bin/python2
```

NOTE

Intel® SGX SDK 2.9 release requires GCC 7.3 or above.

The SDK installer will not be provided for below OSes because the native GCC version doesn't meet the requirement:

- Ubuntu* 16.04 LTS Server 64bits
 - Red Hat* Enterprise Linux Server release 7.6 64bits
 - SUSE Linux Enterprise Server* 15.1 64bits
-

Installation

To install the driver, PSW, and SDK packages, you need the root (or sudo) privilege. Install the components in following order:

1. Intel® SGX driver
2. Intel® SGX PSW
3. Intel® SGX SDK

Use the following steps to install these packages:

Intel® SGX Driver Installation

Install the Intel® SGX driver package:

- To install the Intel® SGX driver with ECDSA attestation enabled, see how to [install Intel® Software Guard Extensions Driver for Data Center Attestation Primitives \(Intel® SGX DCAP\)](#).
- To install the Intel® SGX driver without ECDSA attestation:
 1. Download Intel® SGX DCAP driver package.
 2. Run the following command:

```
$ sudo ./sgx_linux_x64_driver.bin
```

The installer also loads the driver and sets it to `auto-load` when the system reboots.

NOTE

Only 64-bit installation packages are available.

NOTE

If Secure Boot is enabled, you need to sign the Intel® SGX. Please refer to the distribution documentation on how to sign drivers for Secure Boot.

Intel® SGX PSW Installation

The Intel® SGX PSW provides 3 services:

- launch
- EPID-based attestation
- algorithm agnostic attestation

Starting from 2.8 release, it is split into multiple packages and users can choose which features and services to install.

Install Intel® SGX PSW Debian packages from the Intel® SGX repository:

1. Connect your system to the network with internet access and open a terminal.

2. Add the repository to your sources.

- On Ubuntu* 16.04:

```
$ echo 'deb [arch=amd64] https://-  
download.01.org/intel-sgx/sgx_repo/ubuntu xenial  
main' | sudo tee /etc/apt/sources.list.d/intel-  
sgx.list
```

- On Ubuntu* 18.04:

```
$ echo 'deb [arch=amd64] https://-  
download.01.org/intel-sgx/sgx_repo/ubuntu bionic  
main' | sudo tee /etc/apt/sources.list.d/intel-sgx.l-  
ist
```

3. Add the key to the list of trusted keys used by the apt to authenticate packages:

```
$ wget -qO - https://download.01.org/intel-sgx/sgx_  
repo/ubuntu/intel-sgx-deb.key | sudo apt-key add -
```

4. Update the apt and install the packages:

```
$ sudo apt-get update
```

- Install launch service:

```
$ sudo apt-get install libsgx-launch libsgx-urts
```

- Install EPID-based attestation service:

```
$ sudo apt-get install libsgx-epid libsgx-urts
```


- Install algorithm agnostic attestation service:

```
$ sudo apt-get install libsgx-quote-ex libsgx-urts
```

NOTE

Optionally, you can install `*-dbgsym` packages to get the debug symbols, and install `*-dev` packages to get the header files for development.

Upgrade from a legacy installation:

Before the Intel® SGX 2.8 release, Intel® SGX PSW is installed as a single package named `libsgx-enclave-common`. Starting with the Intel® SGX 2.8 release, Intel® SGX PSW is split into multiple packages (`libsgx-enclave-common` is one of them). As a result, a simple upgrade will end up with a subset of the Intel® SGX PSW being installed on the system. To enable the required feature, you need to install additional packages. At the same time, you will encounter several error messages when you try to upgrade to the Intel® SGX 2.8 release from an old installation. To address the issue, choose any of the methods below:

- Uninstall the old installation and install new packages.
- Add `-o Dpkg::Options::="--force-overwrite"` option to overwrite existing files and use "dist-upgrade" instead of "upgrade" to install new packages when upgrading. To perform these actions, use the following command:

```
$ sudo apt-get dist-upgrade -o Dpkg::Options::="--force-overwrite"
```

Configure the installation:

Several packages are configured with recommended dependency on other packages that are not required for certain usage. For instance, the background daemon is not required for container usage. It is installed by default but you can drop it by using the additional option during the installation:

- On Ubuntu 16.04 and Ubuntu 18.04:

```
--no-install-recommends
```

NOTE

On .rpm-based system, `rpm-build` ≥ 4.12 is required to enable similar features.

Install the Intel® SGX PSW RPM packages using the Intel® SGX RPM local repository:

1. Download the Intel® SGX RPM local repository from <https://download.01.org/intel-sgx/>.

2. Add the RPM local repository to your repository list.

- On Red Hat* Enterprise Linux 7.6, Red Hat* Enterprise Linux 8.2, CentOS* 8.1 and Fedora* 31:

```
$ sudo yum-config-manager --add-repo file://PATH_TO_LOCAL_REPO
```

- On SUSE Linux Enterprise Server* 15.1:

```
$ sudo zypper addrepo PATH_TO_LOCAL_REPO LOCAL_REPO_ALIAS
```

NOTE

Replace `PATH_TO_LOCAL_REPO` and `LOCAL_REPO_ALIAS` with proper path and name on your system.

3. Install the RPM packages:

- On Red Hat* Enterprise Linux 7.6, Red Hat* Enterprise Linux 8.2, CentOS* 8.1 and Fedora* 31:

- Install launch service:

```
$ sudo yum --nogpgcheck install libsgx-launch libsgx-urts
```

- Install EPID-based attestation service:

```
$ sudo yum --nogpgcheck install libsgx-epid libsgx-urts
```

- Install algorithm agnostic attestation service:

```
$ sudo yum --nogpgcheck install libsgx-quote-ex libsgx-urts
```

- On SUSE Linux Enterprise Server* 15.1:

- Install launch service:

```
$ sudo zypper --no-gpg-checks install libsgx-launch libsgx-urts
```

- Install EPID-based attestation service:

```
$ sudo zypper --no-gpg-checks install libsgx-epid libsgx-urts
```

- Install algorithm agnostic attestation service:

```
$ sudo zypper --no-gpg-checks install libsgx-quote-ex libsgx-urts
```

NOTE

The Intel® SGX RPM local repository is not signed with GPG. Ignore gpgcheck when installing the packages.

NOTE

Optionally, you can install `*-debuginfo` packages to get the debug symbols, and install `*-devel` packages to get the header files for development.

The Intel® SGX platform software package includes user space libraries such as uRTS and AESM. After installation, the libraries are installed to the directory `/usr/lib` or `/usr/lib/x86_64-linux-gnu` or `/usr/lib64`.

The AESM service executable and the AE libraries are installed to the directory:

- If Intel® SGX PSW is installed with Debian or RPM packages

```
/opt/intel/sgx-aesm-service
```

The installer also configures the AESM service as a system daemon, which starts with the user ID `aesmd`. The default home directory of the AESM service is `/var/opt/aesmd`.

After installing the platform software, you may need to setup an http proxy server for the AESM service. For instructions on setting up the proxy, refer to the file `/etc/aesmd.conf`. The setup example is commented out.

Intel® SGX SDK Installation

Download Intel® SGX SDK package: `sgx_linux_<os>_x64_sdk_<version>.bin`.

NOTE

Only 64-bit installation packages are available.

Install the Intel® SGX SDK using the following command:

```
$ ./sgx_linux_<os>_x64_sdk_<version>.bin
```

This command starts the setup program in the interactive mode on the command line. When the question **Do you want to install in current directory? [yes/no]** appears, type **yes** and press **Enter** to install into the current directory or type **no** and press **Enter** to enter another path for installation.

After the installation, the Intel® SGX SDK package is installed into the directory [User Input Path]/sgxsdk. Run the command `source [User Input Path]/sgxsdk/environment` to set all environment variables.

NOTE

The default installation directories for Intel® SGX PSW and Intel® SGX SDK are different:

- The Intel® SGX PSW binary package installs the user space libraries in `/usr/lib`.
- The Intel® SGX PSW Debian packages install the user space libraries in `/usr/lib/x86_64-linux-gnu`.
- The Intel® SGX PSW RPM packages install the user space libraries in `/usr/lib64`.
- The Intel® SGX SDK package installs the corresponding shell libraries in `[User Input Path]/sgxsdk/lib64`.

Shell libraries contain the declaration of the public APIs and are only needed for building Intel® SGX applications. At runtime, the standard user-space libraries in `/usr/lib` or `/usr/lib/x86_64-linux-gnu` or `/usr/lib64` are loaded automatically.

NOTE

Sample code is installed under `[User Input Path]/sgxsdk/SampleCode` directory with read-only permissions for normal users. Each user can make separate copies to modify, build, and experiment with the sample codes.

On Ubuntu* 18.4, Red Hat* Enterprise Linux 8.2, CenOS* 8.1 and Fedora* 31, download the mitigation tools that are named as `as.ld.objdump.gold.r2.tar.gz` from [here](#), unzip them and copy the tools from the directory that corresponds to current OS distribution to the directory of `/usr/local/bin`. Make sure that these tools have execute permission.

See <https://nvd.nist.gov/vuln/detail/CVE-2020-0551> and <https://software.intel.com/security-software-guidance/software-guidance/load-value-injection> for information related to these mitigation tools.

Uninstallation

To uninstall the driver, PSW, and SDK packages, you need the root (or sudo) privilege. Uninstall the components in the following order:

1. Intel® SGX driver
2. Intel® SGX PSW
3. Intel® SGX SDK.

Use the following steps to uninstall these packages:

1. Uninstall the Intel® SGX driver package:
After the installation, a generated script `uninstall.sh` appears in the `/opt/intel/sgxdriver` directory. You can use this script to uninstall the driver.
2. Uninstall the Intel® SGX PSW package:
 - Intel® SGX PSW is installed with `sgx_linux_<os>_x64_psw_<version>.bin`:
After the installation, a generated script `uninstall.sh` appears in the `/opt/intel/sgxpsw` directory. You can use this script to uninstall the platform software.
 - Intel® SGX PSW is installed with Intel® SGX Debian repo:

```
$ sudo apt-get remove *sgx*
```


To uninstall the Intel® SGX PSW Debian debug symbol package if installed, run the following command:

```
$ sudo apt-get remove libsgx-enclave-common-dbg-sym
```
 - Intel® SGX PSW is installed with Intel® SGX RPM local repository.
To uninstall the Intel® SGX PSW debian package, run the following

command with the root privilege:

- On Red Hat* Enterprise 7.6, Red Hat* Enterprise Linux 8.2, CentOS* 8.1 Fedora* 31:

```
$ sudo yum remove *sgx*
```

- On SUSE Linux Enterprise Server* 15.1:

```
$ sudo zypper remove *sgx*
```

3. Uninstall the Intel® SGX SDK package:

After installation, a generated script `uninstall.sh` appears in the `[User Input Path]/sgxsdk` directory. You can use it to uninstall the Intel® SGX SDK.

ECDSA attestation

To enable ECDSA attestation:

- 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):
 - Install the required components that support the Intel® SGX PSW installation, because the Intel SGX Driver is built from the driver package.

```
sudo apt-get install build-essential ocaml auto-  
make autoconf libtool wget python libssl-dev
```

NOTE

This command line contains modules needed beyond the Intel® SGX Driver installation.

- Download the latest Intel® SGX Driver binary file from the Intel® SGX DCAP download directory: <https://download.01.org/intel-sgx/latest/linux-latest/distro/>

For example, to download the driver for Ubuntu* server 18.04, use the following command:

```
sudo wget - https://download.01.org/intel-sgx/latest/linux-  
latest/distro/ubuntu18.04-server/sgx_linux_x64_driver_1.32.bin
```

- Set the protections to allow for the .bin file execution:

```
chmod 777 sgx_linux_x64_driver_1.32.bin
```

- Install the driver using the following command:

```
sudo ./sgx_linux_x64_driver_1.32.bin
```

The installer also loads the Intel® SGX Driver and sets it to be auto-load when the system reboots.

After the Intel® SGX Driver installation, you can see a generated script `uninstall.sh` under the `/opt/intel/sgxdriver` directory. You can use this script to uninstall the 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](#).
- Install Platform Quote Provider Library. Follow [Intel® Software Guard Extensions Data Center Attestation Primitives Installation Guide For Linux* OS](#) to install Intel® SGX DCAP Default Quote Provider Library
- Ensure the PCCS is setup correctly by local administrator or data center administrator. Please also setup `/etc/sgx_default_qcml.conf` for Default Quote provider library according to your real environment:
`USE_SECURE_CERT=TRUE`
`PCCS_URL=https://your_pccs_server:8081/sgx/certification/v2/`
- `PCCS_URL` is the URL of your PCCS caching service. Set `USE_SECURE_CERT` to `FALSE` if PCCS uses self-signed certificates, and `TRUE` for a production PCCS with authenticated certificates.

Install Intel(R) Software Guard Extensions Eclipse* Plug-in

The Intel(R) Software Guard Extensions Eclipse* Plug-in for Linux* OS helps the enclave developer to maintain enclaves and untrusted related code inside Eclipse* C/C++ projects.

This section contains steps to set up your Intel(R) Software Guard Extensions Eclipse* Plugin on a Linux* system, including necessary softwares, steps to install the product, and steps to configure your preferred product directory.

- [Prerequisites](#)
- [Installation](#)
- [Configuration](#)

Prerequisites

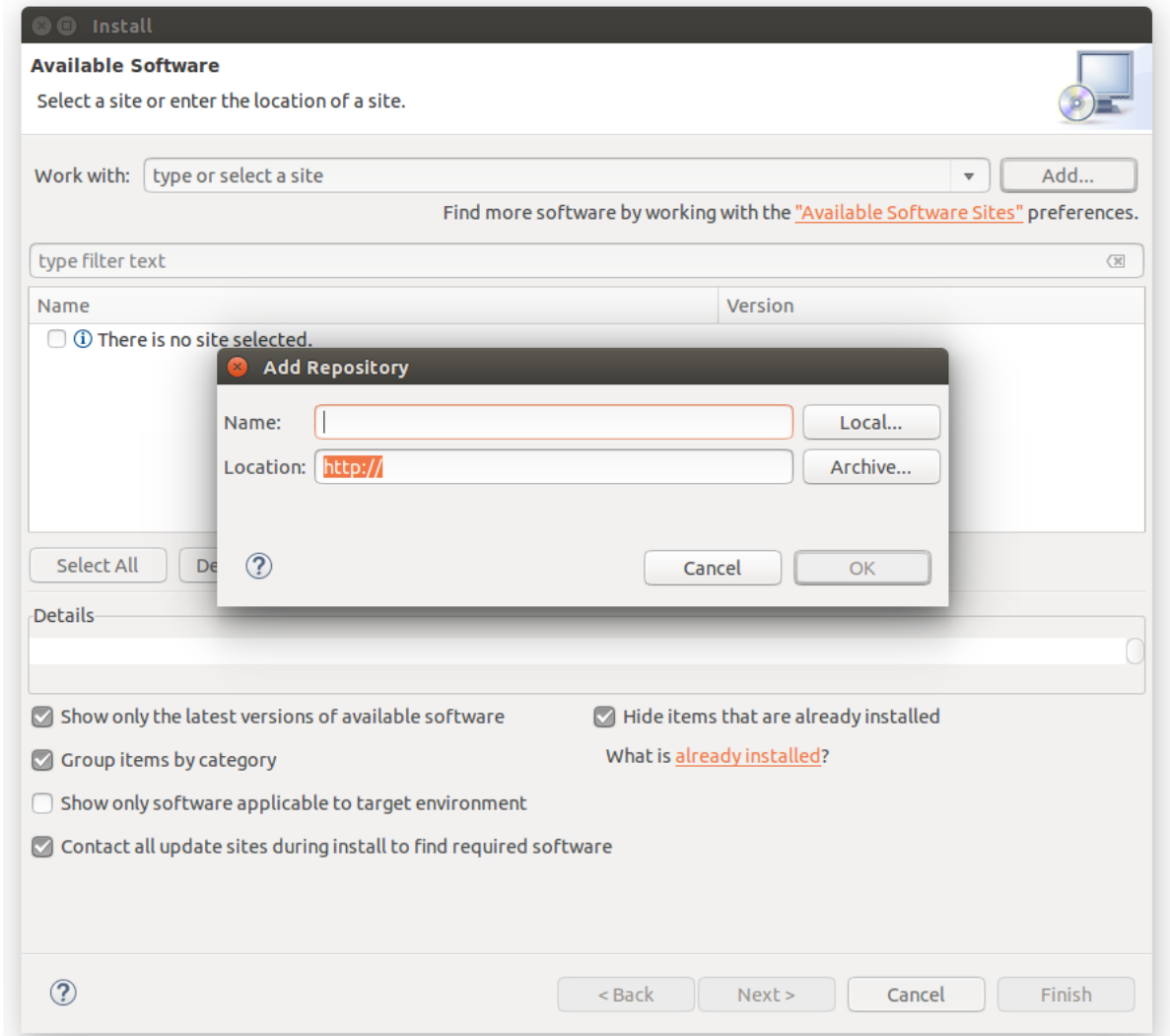
To use Intel(R) Software Guard Extensions Eclipse Plug-in, install the following softwares:

- Eclipse* Mars 1 with CDT IDE for C/C++ Developers (version 4.5.1). To use this version, install Java* Development Kit (JDK) or Java* Runtime Environment (JRE) version 1.8 or above.
- gcc*/g++ tools
- OpenSSL*
- Intel(R) SGX SDK for Linux* OS

Installation

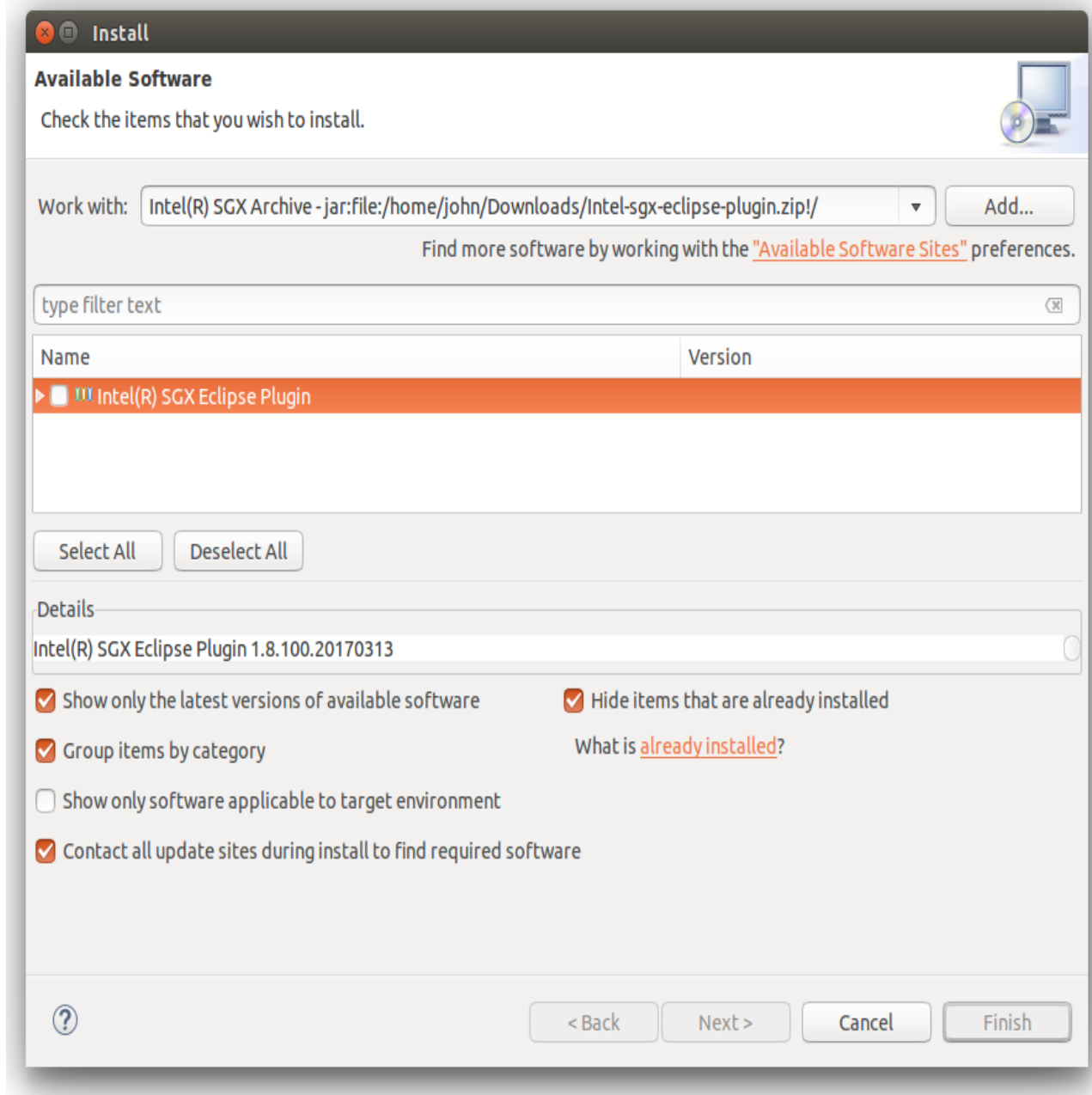
Install the Intel® Software Guard Extensions Eclipse* Plug-in as a regular Eclipse Plugin:

1. Download the .zip archive of Intel® Software Guard Extensions Eclipse Plug-in from [\[Intel Site\]](#)
2. Open Eclipse and go to **Help menu -> Install New Software**. Click the **Add** button for the **Work with** field to open the **Add Repository** dialog as shown in the following graphic:



Add Repository Dialog

3. Enter Intel(R) SGX Archive in the **Name** field . Click the **Archive...** button and select the location of the downloaded archive as shown in the following graphic:



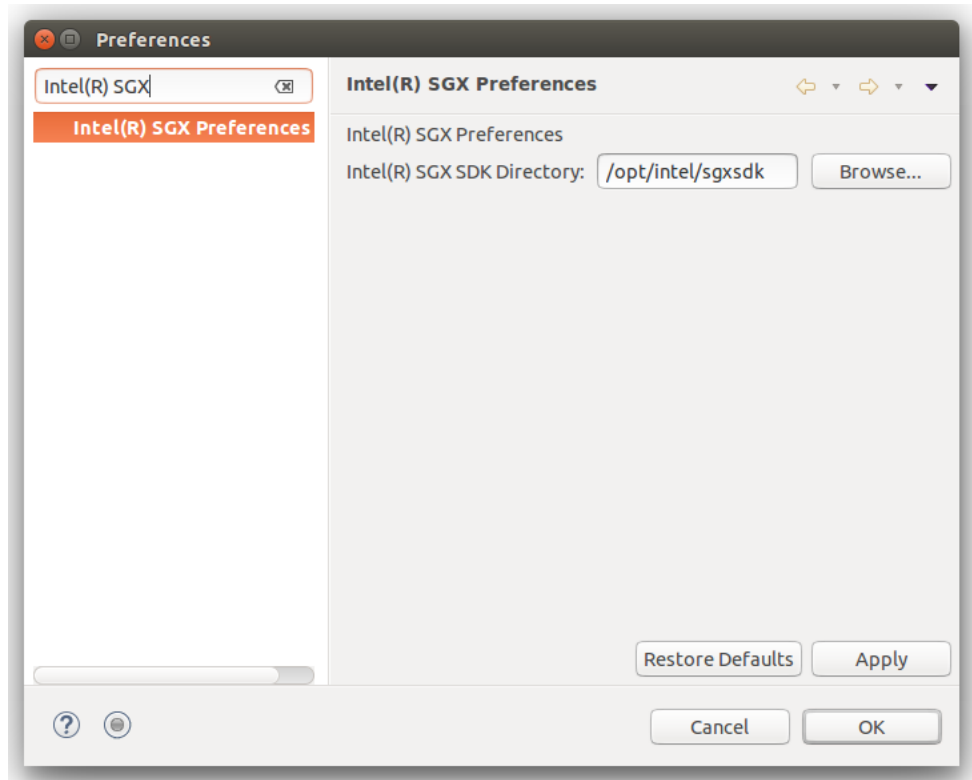
The Location of the Plugin zip Archive

4. Press **OK** to add the archive as a repository.
5. In the **Install** dialog, select the **Intel(R) Software Guard Extensions Plugin** check-box and proceed with the usual steps.

Configuration

If you do not install Intel(R) SGX SDK for Linux* OS in the default location, you need to specify the path for Intel(R) SGX SDK using the following steps:

1. Go to **Window menu ->Preferences**. Enter Intel(R) SGX in the filter text field to quickly locate the **Intel(R) SGX Preferences** page.



Intel(R) SGX Preference Page

2. Enter the path for Intel(R) SGX SDK for Linux OS in the **Intel(R) SGX SDK Directory** field.