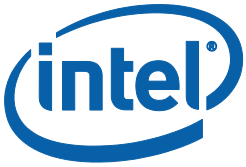


Intel® Software Guard Extensions SDK for Linux* OS

Installation Guide

Legal Information

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

Revision History

Revision Number	Description	Revision Date
1.5	Intel(R) SGX Linux 1.5 release	May 2016
1.6	Intel(R) SGX Linux 1.6 release	September 2016
1.7	Intel(R) SGX Linux 1.7 release	December 2016
1.8	Intel(R) SGX Linux 1.8 release	March 2017
1.9	Intel(R) SGX Linux 1.9 release	July 2017
2.0	Intel(R) SGX Linux 2.0 release	November 2017

Intel(R) Software Guard Extensions SDK and Platform Software Installation

This document provides the instructions on how to install Intel(R) Software Guard Extensions SDK and platform software. You can see the details in the following topics:

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

Install Intel(R) Software Guard Extensions SDK and Platform Software

The current Linux* OS installation packages include three binary installers packaged separately:

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

Download the following installation packages:

- Intel(R) SGX driver: `sgx_linux_x64_driver.bin`
- Intel(R) SGX PSW: `sgx_linux_x64_psw_<version>.bin`
- Intel(R) SGX SDK: `sgx_linux_x64_sdk_<version>.bin`

NOTE

Only 64-bit installation packages are available.

NOTE

The Intel® SGX driver needs to be signed if Secure Boot is enabled. Please consult the distribution documentation on how to sign drivers for Secure Boot.

Hardware Requirements

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

NOTE

This is required when you need to 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* Desktop-16.04-LTS 64bits
- Red Hat* Enterprise Linux Server release 7.4 64bits
- CentOS* 7.3.1611 64bits

To install Intel(R) SGX PSW, first install the following tools: For example:

1. On Ubuntu* 16.04:

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

2. On Red Hat* Enterprise Linux 7.4 and CentOS* 7.3:

```
$ sudo yum install openssl-devel libcurl-devel protobuf-
devel
```

To install Intel(R) SGX SDK, install the following:

1. On Ubuntu* 16.04:

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

2. On Red Hat* Enterprise Linux 7.4 and CentOS* 7.3:

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

To use the trusted platform service, install the following:

- Ensure mei_me driver is enabled and /dev/mei0 exists.

  On Red Hat Enterprise Linux 7.4, update the kernel version to kernel-3.10.0-514.el7 or newer:

  ```
  $ sudo yum update kernel
  ```

- Download [iclsClient] and install it using the following commands:

  On Ubuntu* 16.04:

  ```
  $ sudo apt-get install alien
  ```

  ```
  $ sudo alien --scripts iclsClient-1.45.449.12-1.x86_
  64.rpm
  ```

```
$ sudo dpkg -i iclsclient_1.45.449.12-2_amd64.deb
```

On Red Hat* Enterprise Linux 7.4 and CentOS* 7.3:

```
$ sudo yum install iclsClient-1.45.449.12-1.x86_
64.rpm
```

- Download source code from the[dynamic-application-loader-host-interface] project. In the source code folder build and install the JHI service using the following commands:
  On Ubuntu* 16.04:

```
$ sudo apt-get install uuid-dev libxml2-dev cmake
```

```
$ cmake .;make;sudo make install;sudo systemctl
enable jhi
```

On Red Hat* Enterprise Linux 7.4 and CentOS* 7.3:

```
$ sudo yum install libuuid-devel libxml2-devel cmake
```

```
$ cmake .;make;sudo make install;sudo systemctl
enable jhi
```

Installation

You need the root (or sudo) privilege to install the driver and PSW packages, and install them in following order:

1. Intel(R) SGX driver
2. Intel(R) SGX PSW
3. Intel(R) SGX SDK

Use thefollowing steps to install these packages:

1. Install the Intel(R) SGX driver package using the following command:

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

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

   After the Intel(R) 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.

2. Install the Intel(R) SGX PSW package using the following command:

```
$ sudo ./sgx_linux_x64_psw_<version>.bin
```

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`. The AESM service executable and the AE libraries are installed to the directory `/opt/intel/sgxpsw/aesm`.

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. You can use the file `/etc/aesmd.conf` as a reference. This file shows an example on how to setup the proxy but it is commented out.

After the Intel(R) SGX PSW installation, you can see a generated script `uninstall.sh` under the `/opt/intel/sgxpsw` directory. You can use this script to uninstall the platform software.

3. Install the Intel(R) SGX SDK using the following command:
   ```
   $ ./sgx_linux_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 in the current directory and 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`, which also sets all the environment variables.

   You can also see a generated script `uninstall.sh` under the `[User Input Path]/sgxsdk` directory and use it to uninstall the Intel(R) SGX SDK.

NOTE

The default installation directories for Intel(R) SGX PSW and Intel(R) SGX SDK are different:

- The Intel(R) SGX PSW package installs the user space libraries in `/usr/lib`.

- The Intel(R) 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` 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.

To uninstall Intel(R) SGX, run the corresponding `uninstall.sh` scripts to uninstall the components in the following order. You must have root privileges to uninstall driver and PSW packages.

1. Uninstall the Intel(R) SGX SDK
2. Uninstall the Intel(R) SGX PSW
3. Uninstall the Intel(R) SGX driver

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:

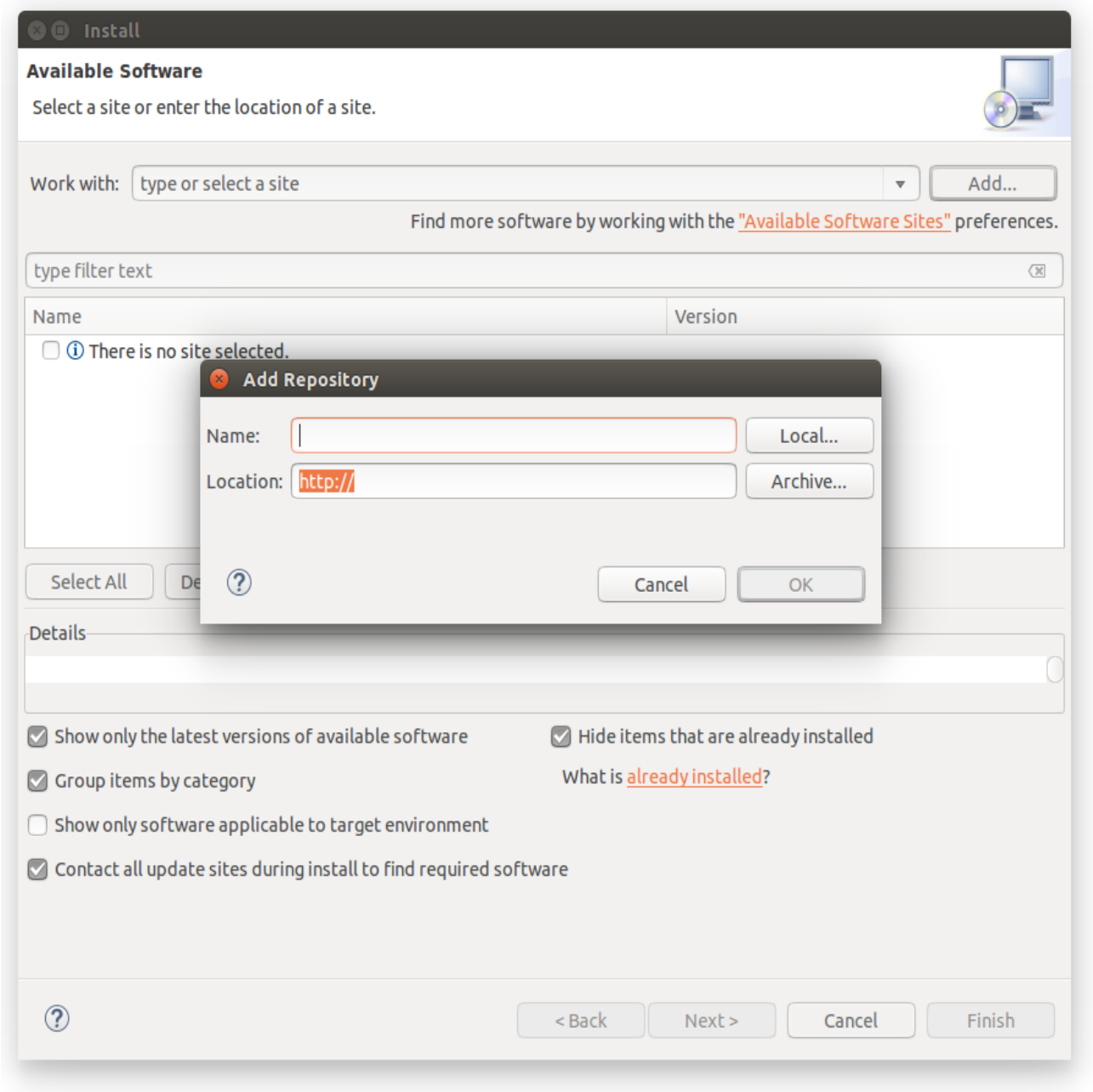
- Eclipse* Mars 1 with CDT IDE for C/C++ Developpers (version 4.5.1). To use this version, install Java* Development Kit (JDK) or Java* Runtime Environment (JRE) version 1.8 or above.

- gcc*/g++ tools
- OpenSSL*
- Intel(R) SGX SDK for Linux* OS

Installation

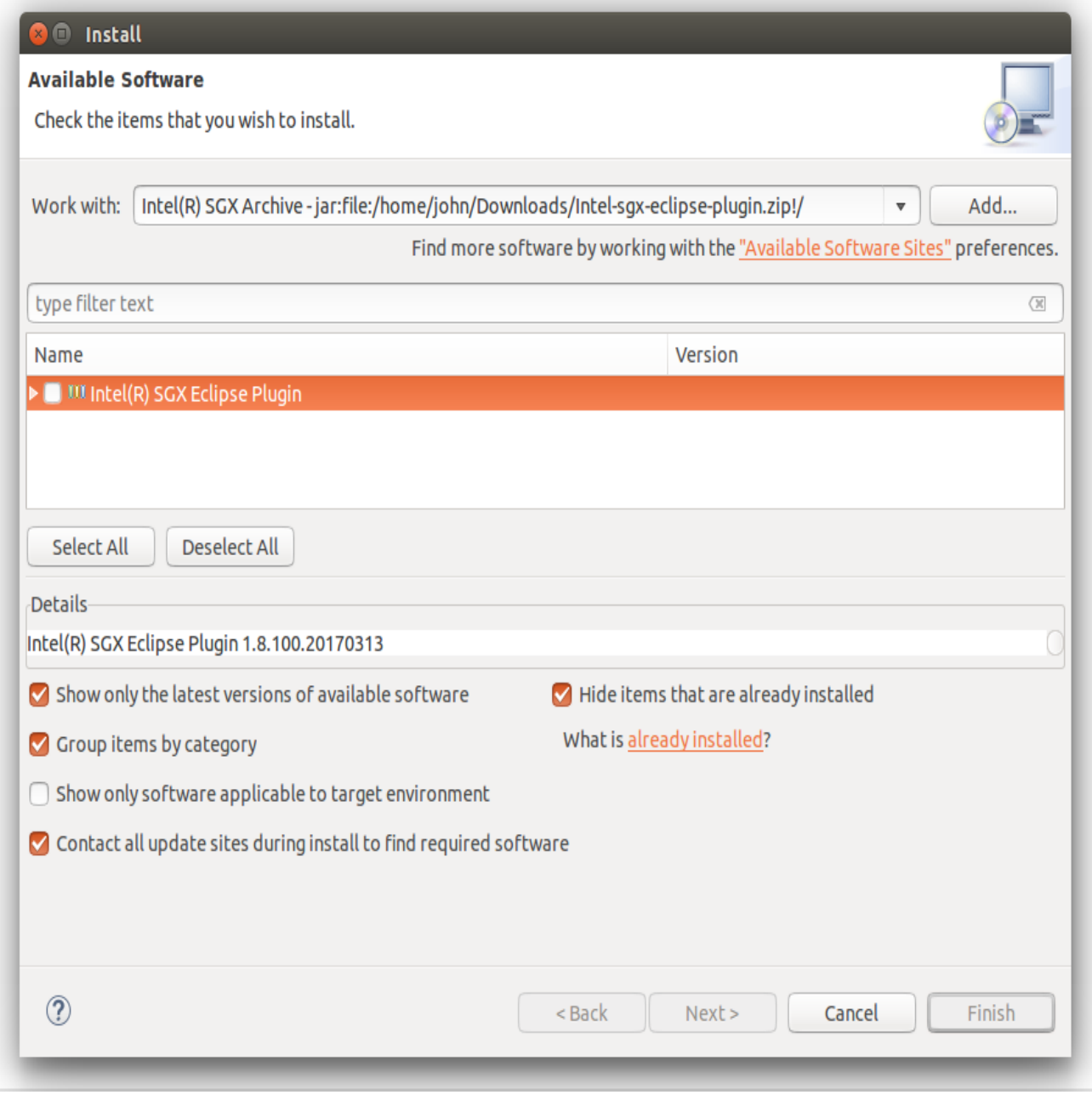
Install Intel(R) Software Guard Extensions Eclipse* Plug-in as a regular Eclipse Plugin:

1. Download the zip archive of Intel(R) Software Guard Extensions Eclipse Plug-in from [Intel Site]
2. 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:



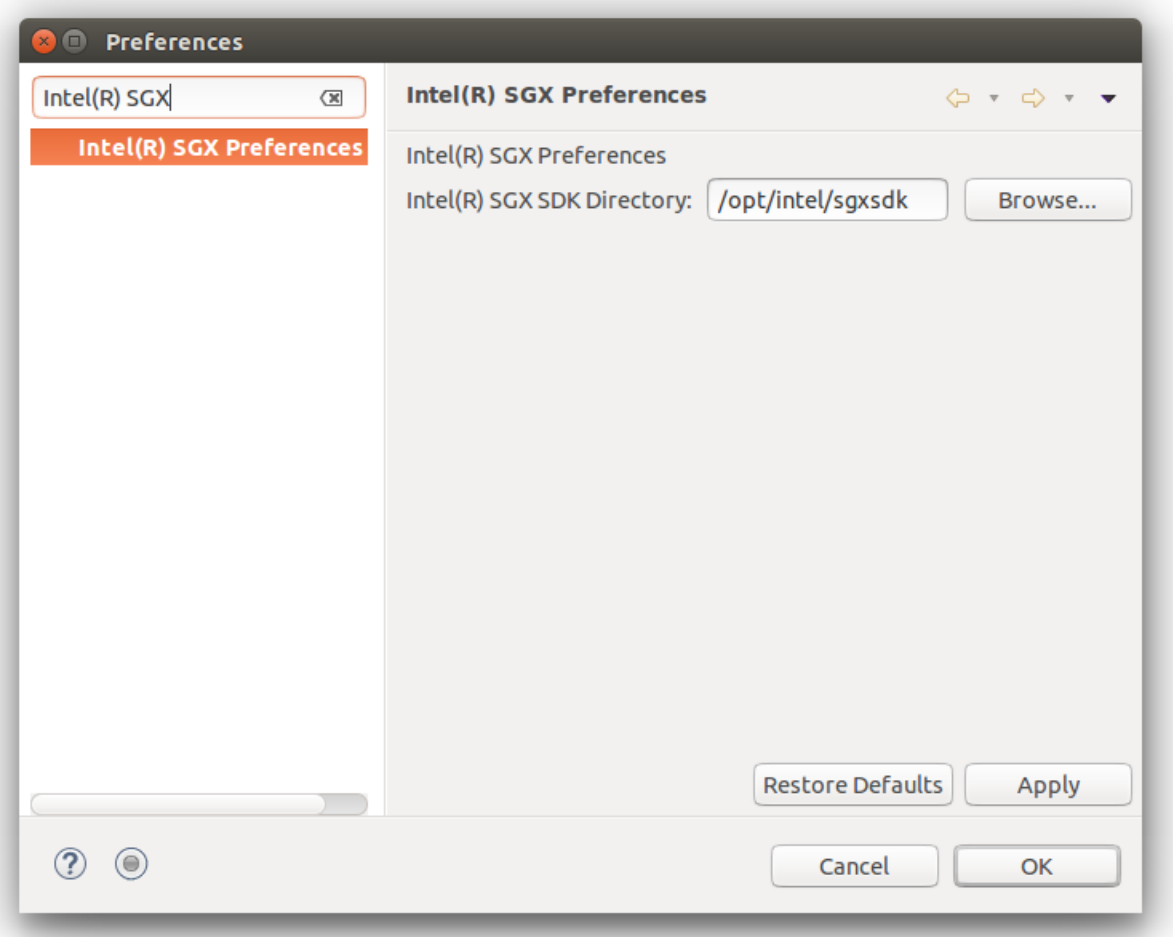
The Location of the Plugin zip Archive

4. Press **OK** to add the archive as a repository.
5. In the **Install** dialog, select the **Intel(R) Software Guard Extensions Plug-in** 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.