Install SGX (new DCAP)

Got problems with using DCAP in your system? Please ask in the Telegram or Discord for help. For Validators, you can also ask in the SN Validators chat. Ensure your hardware isHardware Compliance .

If you're running a local machine and not a cloud-based VM -

1. Go to your BIOS menu
2. Enable SGX (Set to "YES", it's not enough to set it to "software controlled")
3. Disable Secure Boot
4. Disable Hyperthreading
5.

During this brief testing phase for the SGX hardware, if feasible, please shut down your active node to avoid any potential app-hashing crashes.

To shutdown your node temporarily, use:

sudo systemctl stop secret-node

To restart your node after the SGX test, run:

sudo systemctl restart secret-node

Check latest SGX DCAP driver

Make sure the SGX driver is installed. The following devices should appear:

```

Copy /dev/sgx_enclave /dev/sgx_provision

```

If your kernel version if5.11 or higher, then you probably already have the SGX driver installed. Otherwise - please update the kernel version to5.11 or higher to ensure that these two devices appear. Also make sure that the user under which the node is supposed to run has privileges to access SGX:

```

Copy sudogroupaddsgx_prv sudousermod-a-Gsgx_prvUSER

# Check if the above has effect, by the following command

groups

```

Thesgx_prv should appear.

If it does not - Logout and re-login may be needed, for the change to take effect.

Install the DCAP runtime and AESM service

First, you need to add the Intel repository to APT:

For Ubuntu 20.04, use this:

```

Copy curl-fsSLhttps://download.01.org/intel-sgx/sgx_repo/ubuntu/intel-sgx-deb.key|sudoapt-keyadd- sudoadd-apt-repository"deb https://download.01.org/intel-sgx/sgx_repo/ubuntu focal main"

```

For Ubuntu 22.04, use this repository:

```

Copy curl-fsSLhttps://download.01.org/intel-sgx/sgx_repo/ubuntu/intel-sgx-deb.key|sudoapt-keyadd- sudoadd-apt-
```

repository"deb https://download.01.org/intel-sgx/sgx_repo/ubuntu jammy main"

```

Next, install the necessary SGX libraries:

```

Copy sudoapt-getupdate sudoapt-getinstall-y\ libsgx-aesm-launch-plugin\ libsgx-enclave-common\ libsgx-epid\ libsgx-launch\ libsgx-quote-ex\ libsgx-uae-service\ libsgx-qe3-logic\ libsgx-pce-logic\ libsgx-aesm-pce-plugin\ libsgx-dcap-ql\ libsgx-dcap-quote-verify\ libsgx-urts\ sgx-aesm-service\ libsgx-aesm-ecdsa-plugin\ libsgx-aesm-quote-ex-plugin\ libsgx-dcap-default-qpl

sudoaptupgrade

```

If your system has 5th Gen Intel® Xeon® Scalable Processor(s)

For the DCAP attestation to work, you'll need to register your platform with Intel. This is achieved by the following:

```

Copy sudoapt-getinstall-ysgx-ra-service

```

You can check the file/var/log/mpa_registration.log , to see if the platform is registered successfully.

Configure Quote Provider

The Quote Provider library is needed to provide the data for DCAP attestation.The configuration file for it should can be found here:

/etc/sgx_default_qcnl.conf

1. Running a baremetal/physical machine
2.

The simplest would be to use the PCCS run by SCRTLabs. Modify the following parameters in the file:

```

Copy //PCCSserveraddress "pccs_url":"https://pccs.scrtlabs.com/sgx/certification/v4/"

```

You can set those parameters by the following command:

```

Copy sudocp/etc/sgx_default_qcnl.conf/etc/sgx_default_qcnl.conf.BKP sudosed-s-i's/localhost:8081/pccs.scrtlabs.com/'/etc/sgx_default_qcnl.conf

```

1. Running on Cloud VPS providers
2.

For cloud VPS providers, the cloud service providers may provide their own PCCS. Please see their documentation for more infomation.

Note: You'll need to restart the AESMD service each time the configuration is changed Next, restart your aesmd service for the changes to take effect.

```

Copy sudosystemctlrestartaesmd.service

```

Use check-hw to test the DCAP attestation
```

Download and run the check-hw tool (included in the Release package here). You should see the following:

```

Copy DCAPattestationok Platformverificationsuccessful!YouareabletorunamainnetSecretnode

```

That would mean all the above steps are ok, and you're good to go.

In case you see some error messages, but at the end the following:

```

Copy PlatformOkay! Platformverificationsuccessful!YouareabletorunamainnetSecretnode

```

That would mean there's a problem with DCAP attestation.

However the EPID attestation still works. Although you may technically run the node, it's strongly recommended to fix this. The EPID will be phased-out by Intel on April 2025.

To get a more detailed error info, runcheck-hw --testnet

Last updated5 hours ago On this page * Check latest SGX DCAP driver * Install the DCAP runtime and AESM service * Configure Quote Provider * Use check-hw to test the DCAP attestation

Was this helpful? Edit on GitHub Export as PDF