Hardware Compliance

This is intended to guide you in selecting SGX compliant hardware for Secret Network. This is not a comprehensive list of compliant hardware, but rather a guide for what has been verified to work. This list is often show as SGX compliant, but it does not discriminate against whether SGX is supported via SPS or Intel ME. Only SGX via SPS is supported.

CPU must support SGX via SPS. CPUs that only support SGX via Intel ME will not work.

Supported CPUs

The following are confirmed compliant Intel CPUs:

Brand Family Model Intel XEON E-Series E-2174G E-2176G E-2178G E-2186G E-2188G E-2274G E-2276G E-2278G E-2286G E-2288G E-2334G E-2386G E-2388G XEON Gold-Series *NOT SUPPORTED* AMD *NOT SUPPORTED* Only Intel processors support SGX. AMD processors are *NOT* supported. List of Processors that Support Intel® Software Guard Extensions

Supported Motherboards

The distinguishing factor of these motherboards is that they support Intel SGX.

This is not an exhaustive list of supported motherboards. These are simply motherboards proven supported by community members. Brand Tag Versions Link Supermicro X11SCM-F SYS-5019C-M ,SYS-5019C-MR link X11SCW-F SYS-5019C-WR link X11SCZ-F X11SSL-F Dell Dell R240 BIOS Version2.14.1

Dell R350 BIOS version1.7.3

HP DL20 G10 BIOS version1.80_07-20-2023 DL20 G10 + ASUS ASUS RS100-E10-PI2 BIOS version5601link Asrock E3C246D4U2-2T

link GIGABYTE MX33-BS1-V1 BIOS version F06 link

Last updated2 months ago On this page *Supported CPUs * Supported Motherboards

Was this helpful? Edit on GitHub Export as PDF