

Internet of Things Certified Hardware Coverage for Ubuntu Core 20 / Ubuntu 20.04

Contents

1	Introduction	2
2	Blocking	3
2.1	Firmware	3
2.2	Processors	3
2.3	Real-Time Clock	3
2.4	Memory	3
2.5	Internal Hard Drives	3
2.6	Networking	3
2.7	USB controllers	4
2.8	Mediacard readers	4
2.9	Bluetooth 4.0	4
2.10	Advanced Configuration and Power Interface	4
2.11	I2C	4
2.12	LEDs	4
2.13	USB 3.1 (Type C)	4
2.14	Thunderbolt 3	5
2.15	TPM 2.0	5
2.16	GPIO	5
2.17	Serial Ports	5
2.18	Audio	5
3	Non-blocking	7
3.1	Mediacard readers	7
3.2	CANBus	7
3.3	IoT Communication Protocols	7
3.4	Advanced Configuration and Power Interface	7
3.5	LEDs	8
3.6	TPM 2.0	8
4	Q & A	9
5	Appendix A. FWTS tests	10

1. Introduction

This document lists the coverage for certification of Internet of Things (IoT) devices with Ubuntu images. IoT devices can be certified with the following image types:

- Ubuntu Core 20
- Ubuntu Server 20.04
- Ubuntu Desktop 20.04

The guide applies to devices submitted to Canonical through one of the following programmes:

- IoT Devices Enablement Programme with Certification
- IoT ODM Partner Programme

For each test job, one of the following certification statuses is specified:

Blocking

Features that are required for certification. If any of the blocking tests fails, the certification will fail.

Non-blocking

Features that are tested but not mandatory for certification. Failure in non-blocking tests will not prevent certification. However, a note will be added to the certificate to inform potential customers or users.

Note

Only categories of hardware are tested and not specific types of hardware. For example, tests are run to verify USB controllers work, but the type of peripheral(s) used during those tests are not specified.

Coverage is flexible based on customer requirements (for example, if a device's use cases don't require LEDs, then LEDs can be non-blocking)

Certain test jobs are designed to validate specific hardware capabilities, such as camera and audio playback functionality. To ensure that the required hardware capabilities are present and properly recognised on the machine under test, these features are explicitly defined in *manifest entries* and linked to the relevant test jobs. This prevents test jobs from being skipped due to system deficiencies in automated detection.

Full test descriptions can be found in Canonical certification site for partners:

<https://certification.canonical.com>

2. Blocking

2.1. Firmware

Ubuntu Core 20 is installed using the factory default BIOS or UEFI, with the default options (including SecureBoot, if that's the default setting). Firmware needs to be compliant with Canonical Firmware Test Suite (FWTS).

It is recommended that after running Canonical fwts with the list of tests defined in the [Appendix A](#), ideally, no CRITICAL or HIGH failures should be reported, but those are not automatically certification blockers.

2.2. Processors

x86_64 and ARM processors are tested to ensure proper functionality. We will test specific features as:

- CPU's performance states (frequency up and down in runtime)
- CPU's sleep states (cpu on and off in runtime)
- Running CPU at its maximum frequency

We will also include a general stress test performed for 120 minutes to verify that the system can handle a sustained high load for a period of time. This test uses the tool "stress" available in the Universe repositories.

For Intel CPU's, the IPDT (Intel Processor Diagnostic Tool) test suite will be run. The diagnostic checks for brand identification, verifies the processor operating frequency, tests specific processor features, and performs a stress test on the processor.

2.3. Real-Time Clock

If present on the device, the device must have a working real-time clock. This will be tested by scheduling a wake alarm to bring the system up after a halt.

2.4. Memory

Proper detection of the amount of memory installed is required (the amount of memory installed is the memory seen by the OS).

2.5. Internal Hard Drives

All internal hard drives are tested to be properly detected. On all of them, an in-house performance test is run. All disks need to report at least a read performance of 15MB/s.

2.6. Networking

- Ethernet. Connections are tested for functionality, but not for performance.
- WWAN connections: - 3G/4G/LTE connection
- Wireless: - 802.11 b/g/n/ac/ax connection

2.7. USB controllers

USB controllers are tested using storage devices in all available USB ports. And the USB human interface device, keyboard or mouse, should be working properly with any USB port.

- USB 2.0
- USB 3.0 SuperSpeed mode
- Keyboard or mouse (basic functionality)

2.8. Mediocard readers

Mediocard readers are tested for read and write for the following type or cards:

- SD
- SDHC

2.9. Bluetooth 4.0

Bluetooth LE (Smart and Smart Ready) is tested for device scanning and pairing. Apart from pairing, several profiles are specifically tested and required:

- Eddystone Beacon
- HID Over GATT Profile (HOGP), Low-Energy keyboard or mouse with basic functionality

2.10. Advanced Configuration and Power Interface

Boot/Reboot

Both cold boot and soft boot are tested and required to work.

2.11. I2C

All devices attached to the I2C bus must be found and able to be read, This includes:

- Temperature sensors
- Humidity sensors
- Accelerometers

2.12. LEDs

When LEDs exist, they will be tested by following some basic expectations here. The actual behavior may vary depending on the hardware design. To ensure that the behavior is working as expected, please be sure to test against specifications obtained from OEM, as each OEM may have different defined behavior for LEDs. The following LEDs are tested:

- Power
- Serial Port LEDs (indicating activity)

2.13. USB 3.1 (Type C)

USB Type C (USB3.1) supports various types of devices (e.g. Video, Power) through the use of adapters or peripherals. The following adapters/peripherals should work:

- Type-C to Display Port - Display hot plugging and different modes (mirror, extended, just internal, just external) are required to work. - Audio output needs to be undistorted

over this port.

- Storage devices
- Keyboard or mouse (basic functionality)

2.14. Thunderbolt 3

- Audio output must be undistorted over this port.
- Storage devices with hot plugging capability should work when BIOS is set to “No security” option.
- Monitor hot plugging including different modes (mirrored, extended, internal only, external only) are required to work.
- Daisy-chaining devices should work with a storage device and a monitor chained together.

2.15. TPM 2.0

If a TPM 2.0 device is present it should be able to be activated from the BIOS. - The system will be tested to ensure it is capable of running the Ubuntu Core 20 Full Disk Encryption (FDE) implementation.

2.16. GPIO

We test the functionality of individual GPIO lines when the associated controller driver in the kernel implements a [GPIO Sysfs Interface](#)¹ via the gpiolib implementers framework. In such cases, the GPIO system may be tested in two ways:

- Direct: - GPIO controllers are exposed through sysfs - GPIO lines are accessible by the user
- Indirect: - Communication with device connected via GPIO

2.17. Serial Ports

Tests are carried out on ports that provide access via the Linux tty layer. The exact tests performed depend on the physical characteristics of the driver/receiver hardware. The possible tests include:

- Ensure expected number of devices are available
- Looped tests: - RS232 Ports: perform loopback test to ensure RX/TX - RS422/485 Ports: connect together to ensure RX/TX
- Machine to Machine tests: confirm that a connection can be made to another PC device and RX/TX is operational

2.18. Audio

Output needs to be undistorted between 0%-100%. Output lines tested:

- Internal speakers
- 3.5mm headphones
- HDMI audio output
- DisplayPort audio output

¹ <https://www.kernel.org/doc/Documentation/gpio/sysfs.txt>

Input needs to be recorded undistorted between 0%-100%. Input lines tested:

- Internal microphone
- 3.5mm microphone

Plug detection: when a new audio line input or output is plugged in the system, it needs to be recognized.

3. Non-blocking

3.1. Mediocard readers

Mediocard readers are also tested for read and write for the following type or cards:

- MMC (before and after suspend)

3.2. CANBus

Devices that support the SocketCAN standard are tested to ensure that the adapter is present and can be communicated with via CANBus configuration commands.

3.3. IoT Communication Protocols

The following protocols will be tested to ensure devices can be found and commands can be issued:

- Zigbee
- Z-wave
- Thread

3.4. Advanced Configuration and Power Interface

Suspend/Resume (S3)

For x86 devices, a 30 cycle suspend/resume stress test is performed using the fwts S3 test. The test is passed if all 30 cycles complete without failure. Any errors reported in the fwts log for the 30 cycle suspend/resume stress test are informational only and do not affect the outcome of the test, however, we do recommend examining and fixing any failures noted, as they indicate firmware non-compliance with standards.

Apart from the stress test, a single cycle suspend/resume is performed, if it's a hybrid graphic system, suspend and graphic related functionalities are required to work flawlessly on both Performance mode and Power Saving mode, and the following features and devices are tested and need to work after suspend:

- CPU
- Memory
- Networking (Wifi, Ethernet)
- Audio
- Bluetooth
- USB controllers
- Input devices
- Mediocard

Watchdog Timer

A test will be performed to verify that any kernel module needed for watchdog timers are loaded and working as expected.

3.5. LEDs

- Cloud LED
- Wireless LED
- Bluetooth LED
- WWAN LED

3.6. TPM 2.0

In addition to the testing in the Required section, the following tests will be run to identify compliance with the TPM 2.0 standard:

- All tpm2-tools commands will be tested with the upstream integrations tests (NV, Attestation, Key management, Encryption, Signing and Utilities tests)
- Access to the TPM device for userspace applications will be checked using tests based on the clevis library

4. Q & A

- **Does changing the speed of processors require a new certificate?**

No. Only changing the CPU family would require retesting and issuing a new certificate.

5. Appendix A. FWTS tests

As part of the certification process, we run a series of firmware tests that are part of the Canonical Firmware Test Suite. In general, any HIGH or CRITICAL error found in the fwts log can cause potential errors in the system and should be looked at by OEMs/ODMs.

Category	Test Item	Description
Information	acpidump	Check ACPI table acpidump.
Information	version	Gather kernel system information.
ACPI	acpitables	ACPI table settings confidence checks.
ACPI	apicinstance	Check for single instance of APIC/MADT table.
ACPI	hpet_check	High Precision Event Timer configuration test.
ACPI	mcfg	MCFG PCI Express* memory mapped config space.
ACPI	method	ACPI DSDT Method Semantic Tests.
CPU	mpcheck	Check Multi Processor tables.
CPU	msr	CPU MSR consistency check.
CPU	mtrr	MTRR validation.
System	apicedge	APIC Edge/Level Check.
System	klog	Scan kernel log for errors and warnings.