

Cyber Essentials Plus Sampling



[Download PDF](#)

Cyber Essentials Plus Sampling

Internal tests are carried out against a sample of end-user devices (including tablets and smartphones) that can connect to organisational services or data, a sample of internal and cloud hosted servers (including hypervisors they are hosted on), as well as a sample of accounts that must include at least one administrator and one user of cloud services used by the organisation. Cloud services will be sampled based on those in use by the user of the sampled device. One of the devices sampled must be an admin user device.

Choosing a representative samples per test

For Test 2 'Check patching, by authenticated vulnerability scan of devices', end-user devices, IaaS instances and ALL servers (including virtual) and hypervisors must be sampled and scanned. Where a scan can not be carried out manual checks can be conducted.

For Test 3 'Check malware protection' end-user devices, IaaS instances and only servers that allow users to access an interactive desktop environment need to be sampled. An "interactive desktop environment" means a graphical interface such as an X server, Windows or macOS. It does not include a text-based environment such as an SSH or telnet session or a bash / DOS / PowerShell command line.

For Test 4 'Check Multi-factor authentication configuration', cloud services will be tested based on the random sample selection. The random sample is taken from the normal every day users of each sampled end-user device. At least one administrator and one normal user account for each service must be tested.

For Test 5 'Check account separation' all end-user devices, servers that allow users to access an interactive desktop environment must be sampled.

When deciding the scope for the internal audit as part of Cyber Essentials Plus certification, a knowledge of the organisation's infrastructure is needed.

You must test a representative sample of the common devices in use at the organisation. This means that if the organisation has a couple of obscure devices (say a particular Raspberry Pi configuration), then these devices are unlikely to require testing.

The devices to be tested must be declared by the Assessor to the applicant not more than 72 hours or 3 working days prior to the test being carried out.

Applicants must not be allowed to choose their own samples.

Where a machine selected for sampling is not available, a different machine must be selected by the Assessor

For the common devices that you decide are in scope for testing, you must select a random sample of a certain quantity of each. The table below shows the minimum quantities required for each build or version of each Operating System:

Number of devices of each type/build	Sample size
1	1
2-5	2
6-19	3
20-60	4
61+	5

The sample table above dictates the minimum required sample for each OS type. It is up to the Assessor to be confident that they are testing a sample that is representative of the whole of the applicant's scoped infrastructure.

For Microsoft products the scope should be broken down by Version and Edition.

An organisation has:

Example 1

- 100 Microsoft Windows 11 Enterprise 26H1 desktops
- 60 Microsoft Windows 11 Pro 25H2 laptops
- 30 MacBook Pro Tahoe laptops
- 80 Apple smartphones iOS26
- 15 Samsung Smartphones Android 16
- 1 x ESXi 8 hypervisor hosting the following servers:
 - 3 Windows Server 2025 servers (virtual) offering 250 Windows 11 Enterprise 25H2 desktops
 - 5 Windows Server 2025 servers (virtual) used for other services

In this example the Assessor will test:

- 5 x Microsoft Windows 11 Enterprise 26H1 desktops
- 4 x Microsoft Windows 11 Pro 25H2 laptops
- 4 x MacBook Pro Tahoe laptops
- 5 x Apple smartphones iOS26

- 3 x Samsung Smartphones Android 16
- 1 x ESXi 8 hypervisor
 - 3 x Windows Server 2025 (virtual)
 - 5 x Windows 11 Enterprise 25H2 desktops

Example 2

An organisation has:

- 60 Microsoft Windows 11 Home 25H2 desktops
- 40 Microsoft Windows 11 Pro 26H1 laptops
- 30 MacBook Pro Tahoe laptops
- 50 Apple smartphones iOS26
- 10 Samsung Smartphones Android 16
- Cloud-hosted servers in Azure:
 - 3 Windows Server 2025 servers offering 100 Windows 11 Enterprise 26H1 desktops
 - 10 Red Hat Enterprise Linux 9 servers

In this example the Assessor will test:

- 4 x Microsoft Windows 11 Home 25H2 desktops
- 4 x Microsoft Windows 11 Pro 26H1 laptops
- 4 x MacBook Pro Tahoe laptops
- 5 x Apple smartphones iOS26
- 3 x Samsung Smartphones Android 16
- Azure cloud-hosted servers:
 - 2 Windows Server 2025 servers (virtual)
 - 3 Red Hat Enterprise Linux 9 servers (virtual)

© The IASME Consortium Ltd 2026 All rights reserved.

