Preparing for the remote Cyber Essentials Plus Test

This guide details the tests that are to be conducted and tips on how to prepare for remote assessments.

Revision History

Removed mention of Nessus Essentials as this is now website stated this is for Educational and Personal use	TW	13/05/2020
Reflects the present Nessus website and warns that users should check their website to clarify current terms of use before installing.	TW	15/06/2020
Reflects mobile phone requirements.	TW	25/9/2020
Created remote testing document	AW	22/10/2020
Updated project timeline	GR	20/05/2021
Added extra notes to the Android testing to clarify how to check for app that can install other apps. Removed hyperlinks to test site	TW	11/08/2021
Updated project timeline	GR	02/09/2021
Updated to include Evendine requirements	TW	31/01/2022
Updated project timeline	GR	04/04/2023
Updated to include Cloud Scanning Agent Option	TW	26/01/2024
Update of mobile device pin requirements from eight to six and updated project timeline	GRM	07/08/2024

Contents

INDELIBLE DATA

CYBER ESSENTIALS PLUS TIMELINE

1 Quote

- Online Scoping form to be complete via our website.
- Proposal sent for digital signature. This includes; quote, Vulnerability Authorisation Form and contract.
- Upon receipt of signed proposal, an initial invoice for 50% of quoted fee is issued for immediate payment.
- Once initial payment is received the project will commence.

2 Cyber Essentials Basic

- If Cyber Essentials Basic is required a portal login will be sent to the client's technical point of contact.
  - Assessment includes complimentary login to our exclusive online guide for passing Cyber Essentials Basic first time.
- Cyber Essentials Basic must be submitted on the portal before a Cyber Essentials Plus assessment date can be agreed.

3 Preperation

- Date agreed for assessment and supporting documentation sent.
- Client to download and install the appropriate scanning software (please see Preparing for the remote test document).
- Provide contract details for the assessment and technical lead at your company and agree date for prep call.
- Grant permission for external scans to be conducted on an agreed date.

4 Documentation

- A date can be agreed for the assessment.
- Complete the Asset Declaration Form
  - To be uploaded to our secure upload at least two weeks before the assessment date.
- Prepare an Asset Register
  - During the prep call, the assessor will select a sample for the assessment.
  - Read and act upon the Preparing for the test document.

5 External Scans & Prep Call

- External scans conducted on an agreed date up to one week before the assessment.
- Prep call with assessor up to one week before assessment, this is to check you have everything in place for the assessment to go ahead.

6 Assessment

Assessment day

- Remaining invoice balance will be sent

In the event of a failure

- You will be permitted one free retest which must be of the initial assessment.
- Further retests will be chargeable at £480+VAT.

7 Certificate Issued

- The Basic and Plus certificate will be sent via Blockmark in PDF form. You will be able to set up an account to download a digital copy.

Show Stopper Information

If the following is not in place by the day of your assessment, we will not be able to proceed.

- The latest version of the Asset Declaration Form (https://www.indelibledata.co.uk/asset-declaration-spreadsheet/) and Asset Register must be completed and shared with us before assessment day in order for a random test sample to be selected by the assessor. This must include mobile devices.
- Cyber Essentials Basic must be achieved or has been deemed as ready to pass by your assessor.
- If you have any unsupported firewalls or end point operating systems, please do not schedule an assessment. More information can be found in the 'End of Life Information' document.
- A member of staff with administrative rights must be available for the duration of the assessment.
    - They must have network knowledge and authority to access all devices in scope
    - they must be able to start and stop services on devices (Nessus requires certain services to be running)
- The assessor must be able to see the screen of this administrator/ end users
- Our preferred methods are Teamviewer, Quick Assist or Microsoft Teams but other options can be discussed.
- The administrator must be able to see or take control of the required sample of machines whether on single or multiple sites. Ideally, the assessor might view one machine which in turn can access all other sample machines in scope for both vulnerability scanning and screen sharing.
- Ensure that the Nessus scanner is fully installed (see below).

If any of the above are not possible, then we **MUST** know ahead of time so that we can discuss further.

Nessus Essentials

Our assessor must be able to perform a detailed scan of the in-scope devices.

If you do not have a copy of Nessus already installed, we request that you attempt to install Nessus Essentials in the first instance by getting an activation code from here: https://www.tenable.com/products/nessus/nessus-essentials

The Nessus Software versions for each build can be found here: https://www.tenable.com/downloads/nessus

It may be difficult to identify, but a typical installation for Windows 10 is:

Ensure that the Nessus scanner is fully installed, you can tell if this is the case as the scanner will prompt for the username and password created during installation (or ask to create a scan), this is after the registration key entry and the "compiling plugins" loading screen, please note that this can take multiple hours to fully complete.

Any download issues must be addressed ***before*** the day of assessment. ***The username and password that was created during the installation of Nessus should be remembered and used on the day.***

We ask that you are comfortable with the Terms and Conditions of the Nessus Essentials Software. Currently, this software can be used commercially for up to 16 IP addresses – but this may be subject to change without notification.

Please also be aware that, on the day of the test, there must be spare capacity within Nessus to conduct a scan of the sample. i.e. if you have scanned 10 IP addresses already, this would only allow six further IPs to be scanned during the audit – though existing IP numbers can be scanned as many times as you wish.

If you have any concerns about the use of the software being downloaded, please let us know and we will discuss alternative options.

It is not always possible to install the Nessus software in a location where it can access all devices over the network, for example, it may be infeasible to install it in a location where it can scan machines where the user is working from (unless there is a VPN in place).

Again, if this is likely to be an issue, please let us know as soon as possible so we can discuss other remote scanning options.

Remote Access Software

It is also important that, before the day of assessment, the remote access software is downloaded on the computer on which the scans are to run.

TeamViewer can be downloaded from the following website:
https://download.teamviewer.com/full

Or, we may have organised a screenshare via Teams or Microsoft Windows' built-in Quick Assist tool.

An assessor will call 1-3 days ahead of the test and will expect Nessus Essentials to have been downloaded on a designated machine, or discuss other viable means of scanning if you don't believe all machines can be scanned from a single place.

Device Sampling

The sample is calculated as follows:

Number of devices of each OS Build	Sample Size
1	1
2-5	2
6-19	3
20-60	4
61+	5

So, for example, if your organisation has 5xMicrosoft Windows 10 Pro (20H2), 20xMicrosoft Windows 10 Pro (21H1), 30xMacbook pro (Big Sur) and 8 Linux end-user devices (Ubuntu), this would equate to 6 Windows 10, 4 Macs and 3 Linux devices being tested on the day.

If you change operating system versions on devices after submitting the Asset Declaration form, please advise us before assessment as this will affect the sample size.

Windows 10 versions are separated by edition and feature version ie. Windows 10 Pro v21H2. So, if the company has 6 Windows 10 Pro 21H2 versions and 6 Windows 10 Pro 22H2, then this would require 3 of each Windows version to be tested on the day (3x Windows 10 Pro 21H2 and 3x Windows 10 Pro 22H2). In this example, if all Windows devices were at the same version only 3 would need to be tested rather than 6.

If the company uses the Windows 10 Operating System, we recommend having a single edition and version throughout the company, wherever possible, as this can vastly reduce the number of devices required to be tested.

Please remember that mobile phones (that access company information, such as emails) are also in scope. The assessor will ask to see the relevant number of Android OS variants and iOS devices following guidelines in the above table.

Remember if you are using Virtual Desktops (also known as Remote Desktops), we will ask how many users are licensed to use this method of connection, and they will also be added to the sample (even if the same operating system is already part of the endpoint sample).

What the assessor will be testing

Test 1 – External scanning

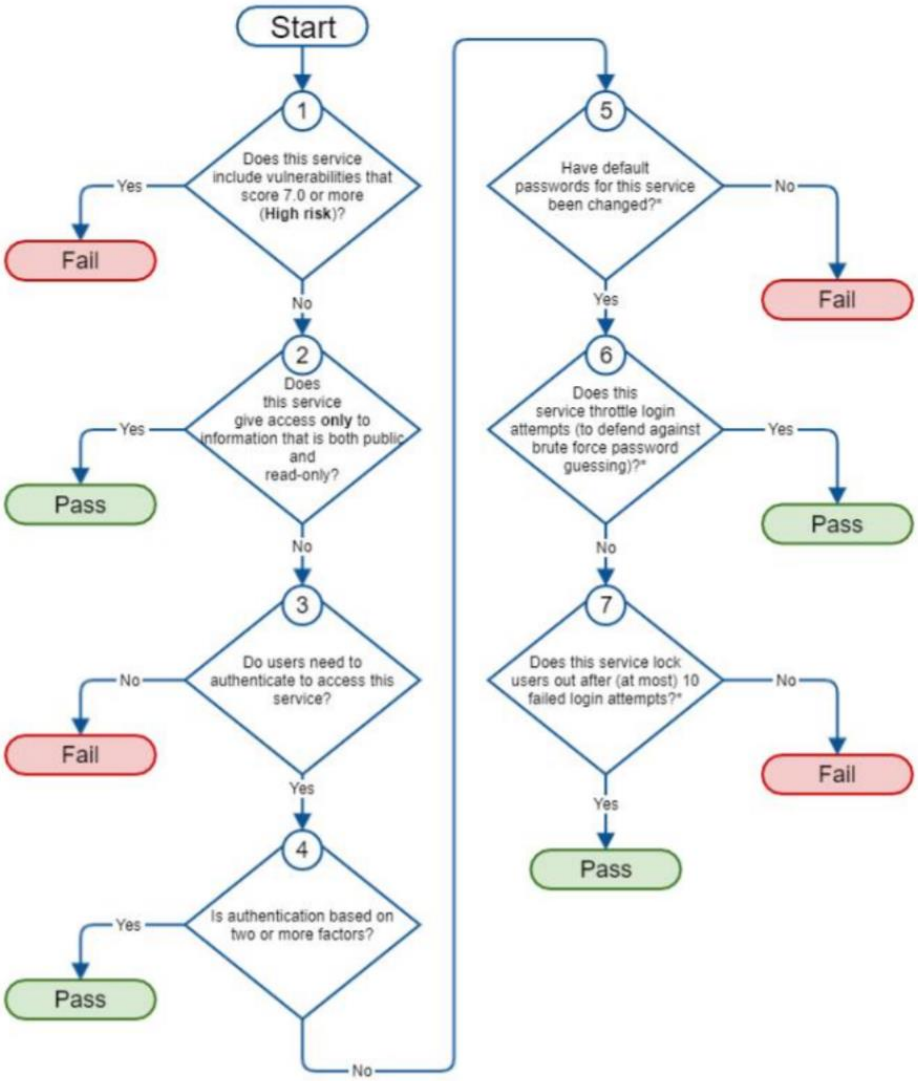
Before the assessment you will have received an "Asset Declaration" form where you must list any protections that are in place to prevent password guessing of any login prompts that are accessible via the internet.

On the day of the test, we may require you to evidence your answers.

Access controlled to a limited range of computers (certificates or IP whitelisted)	Login prompt?	Login protection			Data requiring protection	
		2FA	Lockout after 10 attempts?	Throttling	Public and read-only	Commercial / Personal sensitive
N	*Y*	*N*	*N*	*Y*	*Y*	*Y*
Y	*Y*	*Y*	*N*	*N*	*Y*	*Y*

We will conduct technical tests but cannot always identify such controls as 2FA or Throttling, so please have at hand any configuration pages that can help demonstrate that the stated controls have been implemented.

The assessor will use the following flow diagram when conducting the external test:



Test 2 – Email Tests

We will send a mixture of binary, script and files masquerading as viruses (don't worry, we have written the executable files and "virus" files are internationally recognised test files).

The following files will be sent:

Executables	Macros	Containers
.bat	.docm	.zip
.exe	.xlsm	.7z
.pif		.rar
.ps1		.tar.
.sh		gz
.py		.tar
.dmg		.gz

The hope is that none of the benign virus files should reach your inbox, but if they do, your virus checker should catch them.

The same applies to the binary and script files except, as they are **not** known viruses, the Anti-Virus software may not step in. This is ok, but the email software, or the computer operating system should not allow these files to run on open (there should be a prompt or opportunity to cancel after attempted execution).

Typically, in an Office 365 environment, binary files and the benign viruses are blocked at the server. Script files (such as .py and .sh) often make it through to the inbox and cause issues with companies that develop software – as software developers' computers are often set up to run such files. This means that the test .py and .sh files will execute. Measures must be taken to, at least, warn the user that the file may cause problems if they run it.

Container files (these are files that have been "zipped up" using applications such as winzip, 7zip and WinRar etc) have also been found to cause problems as the operating system may not be aware that the file inside the container originated from the internet.

Remember – we are not asking you to block "Zip" files as we know that companies rely on sending many such files every day as they are an important way of grouping a folder-worth of files together as attachments. We do, however, expect your email server, or computer's operating system, to act upon any executable files contained within "Zip" files. It is very unlikely that users will receive executable files in the course of their day-to-day duties.

Typical actions that we would expect to find are either:

- that the container files are blocked
- there is an opportunity to cancel execution after opening the container file

We will also send relevant files to email accounts to be accessed by mobile devices. Currently these are the .py and .sh files, but are subject to change.

Please arrange, ahead of time, for us to send a sample of our files to you to ensure that our site is not being blacklisted.

Test 3 – URL Checks

The aim of this test is to ensure that computers are configured not to execute files via web browsers without sufficient warning.

All browsers found within the sample set of devices are checked and must show, at least, a warning, or opportunity to cancel before execution.

Test 4 – Check that Users are not Administrators for day-to-day duties (this is at computer, network and Cloud level)

The assessor will ask users to open certain configuration files that cannot normally be accessed by standard users. So, for example, if a user can start and stop system services without needing to enter administrative credentials, it is likely they have administrative privileges and will fail this test.

When testing Cloud accounts (for example, Office 365) the user's day-to-day account must not be able to add/remove users in the Cloud tenant.

Test 5 – Check that Multi-Factor Authentication is implemented for Administrators of Cloud accounts

An administrative user for all the cloud accounts mentioned on the questionnaire will be required to log-in via a browser incognito window and demonstrate the receipt of a second authentication factor.

Please be aware that if the company has answered "Yes" to *A7.14 Have you enabled Multi Factor Authentication for all users of cloud systems?* Then users in the sample will be asked to log into their cloud systems (via a browser incognito window) and demonstrate the receipt of a second authentication Factor.

Test 6 – Patch scanning

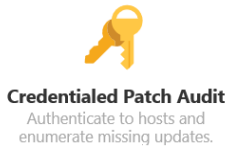
This is generally the most involved and challenging aspect of the test. Remember that the assessor has a limited knowledge of the network they are about to attach to, so it is important that a representative of the company is on-hand to help navigate around.

This test is to identify known weaknesses in devices that, if left unresolved, could cause them to become exploited by malware.

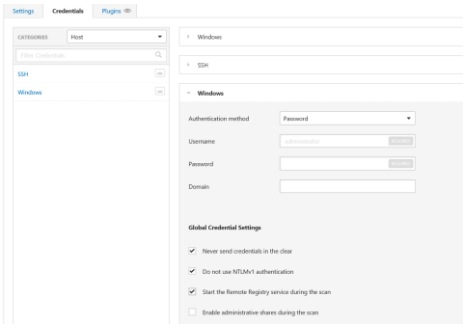
So, for example, if the assessor cannot access your device and an unpatched service goes unreported, that device could become compromised at a later date, so please ensure you have the following ready for the assessor:

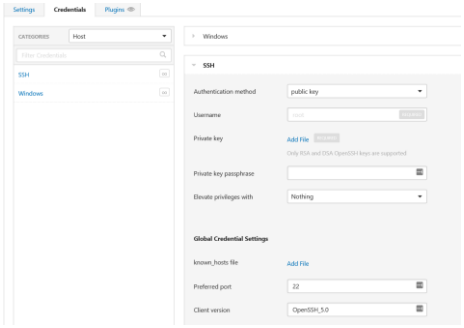
- Temporary ***administrative*** credentials (domain level preferred)
- The ***remote registry*** service enabled on all machines in the sample set
- The **server** service enabled
- ***File and print*** services enabled
- The onboard ***firewall*** disabled for the duration of the scan (or set to allow ports 445/tcp and 139/tcp from the scanning machine)

For your information, we will be conducting a "Credentialed Patch Audit"



For this we must know windows or mac/linux (SSH) connectivity details:





<u>Please ensure all credentials have been tested.</u>

Sometimes the scanner will simply not work as intended – this could be due to network protection controls or device controls that cannot be changed.

If your environment is not conducive to on-site scanning, just let us know and we will send installation instructions to interact with our Cloud Based scanner.

If the assessment overruns due to technical issues, then additional costs are likely to be incurred so it is highly recommended that you, at least, check the services are running following the guidance in the above article before the assessment.

Gap Analysis

The optional Gap Analysis is a less intensive run through of the Cyber Essentials Plus assessment to identify areas that could cause a failure **without officially recording any results**.

We run a full external scan on in-scope IP addresses to find any vulnerabilities and unexpected open ports.

We run an internal vulnerability scan and check a sample of machine browsers and machines' capability to run untrusted programs/applications.

We also help clients with their Cyber Essentials Basic submission if required by evaluating the responses and highlighting areas that may need to be addressed.

A Gap Analysis and report can be completed in one day and it is recommended to be conducted at least two weeks before the assessment.

Please read through and implement points 1-20 ahead of the Gap Analysis.

Assessment day

1. A start time and screenshare method will have been agreed in the prep call
2. Indelible Data will ask for the email address from the Client to which test emails and a screen share link will be sent to.
3. Indelible Data will send the test emails (without attachments) whilst the Client is on the phone
4. Indelible Data will talk you through the screen sharing session and send all the remaining test emails.
5. Once Indelible Data is able to see the screen, with the Clients help, Indelible Data will need to ensure the user is not an administrator (the Client should not be able to run the **secpol** program).
6. The assessor will type "what is my IP" into Google and check it is in range of the IPs that were declared in the Asset Declaration Form ahead of the test.
7. Indelible Data may ask the Client to start the steps recorder and set the number of recordings to 100
8. Indelible Data will ask the Client to click through the emails and it will record the findings in the Evidence spreadsheet (the Client may be asked to make a screen recording via the in-built steps recorder).
9. Indelible Data will then ask the Client to click through the links on each browser and Indelible Data will record the findings in the Evidence spreadsheet (the Client may be

asked to make a screen recording via the in-built steps recorder). Be sure not to forget the Virus test file links on the page. Administrative checks and MFA checks will also be conducted here.

10. Indelible Data will then ask the Client to bring up the anti-virus screen and check it is up to date.
11. Indelible Data will create a new tab on the spreadsheet for every different build / use identified.
12. Indelible Data will check that Nessus plugins are up to date (look at the settings page)
13. Indelible Data will ensure the correct sample of machines are in the Nessus target box (these may actually be different to those identified in the Evidence spreadsheet if the Client wishes – just as long as they represent the different uses of devices in the company) -The following guide is also used for the email and URL tests:
14. Indelible Data will tick the ***enable remote registry*** and ***enable administrative shares*** boxes.
15. The client must ensure the account has sufficient credentials for the scan (Credentialed Scan) – we recommend a test Domain Admin account is used (there maybe a requirement on the day to amend a registry key or create a local admin user). On a Mac, a representative of the company should be confident in privilege escalation where required.
16. Indelible Data will request sight of the mobile devices in scope – this may be via web cam or a Team Viewer session (if installed).
17. The devices will be checked for no sign of Rooting / Jailbreaking / Developer mode and certificates will be checked to ensure untrusted applications cannot run. ***Screen lock will be checked for the required minimum six character pin length.***
18. Indelible Data will remain on the line to ensure the scan is logging in correctly then ask the Client to call back when the scan has finished.
19. To check the scan, Indelible Data ensures the Plugin ID 20811 has fired correctly.
20. Indelible Data will ask the Client to upload the results using our secure upload site or password protected and emailed

How you can help make the Cyber Essentials Plus assessment run smoothly

Disclaimer – all files and applications mentioned in this document are run at the user's own risk.

The external scan

Please list, in the Asset Declaration Form, all the IP addresses that you know to be in scope.

Each IP address will likely have known ports and services associated with it.

If you are a home or small office user, you may not even know the IP address. To get this please go to a google search page and type ***what is my IP address?*** and record the number (e.g.72.66.78.22).

Typical ports that may be open could be Port 80 (if you are hosting a web service) or Port 25 (if your email server is on your company's premise).

Please do not simply guess the ports/services that can be accessed from the internet – the ports that you declare should be taken from your company's up-to-date documentation or from the firewall's configuration page.

Typical ports/services that company's fail to accurately declare include:

- VPN and associated ports (such as 500/udp)
- VOIP Services for companies that use Internet Telephone Services (VOIP)
- Web based ports to administer the firewall – should these be open, then further security controls must be in place (such as 2-Factor Authentication or access only permitted from trusted locations)
- SNMP. If this is open then ensure that the community string is not public (unless this can be justified)

We will conduct a full port scan of the IP address supplied and compare the results with those ports and services which you've declared. If there are discrepancies, the assessor is likely to issue a fail – so please take this part seriously and research the open ports fully ahead of the test.

If any of the services provide a login prompt, then we will check against a known list of default and well-known credentials.

Typical services that we will password-guess against include:

- SSH
- FTP

- SMTP
- MySQL / SQL
- Web forms (we will also try basic methods of authentication bypass)

As well as checking the behaviour of executable files, we also test that virus checkers are up to date and configured for on-access scanning.

Mobile devices

We will ask you to click the .py and .sh files on mobile devices.

Further checks on mobile devices will be conducted to ensure they are not able to run applications not found in their app/play store:

iPhone:

- Take a screengrab of the OS Version (Settings -> General -> About)
- Scroll down the page until “Certificate Trust Settings” and examine any trusted root certificates. For example, for devices managed by InTune, we would expect to find Software Centre (SC_) issued certificates.
- Look for the presence of “Device Management” (Settings -> General) and investigate which certificates are associated with his.

Android:

- Take a screengrab of the OS Version
- Search within settings for “Build Number” Then choose Build number and scroll to the bottom of the screen and double tap on the word “Build Number” again to see if we are invited to proceed into Developer Mode.
- Search within settings for apps with “special app access” and ensure the device cannot install apps from unknown sources by looking at “Install unknown apps” – apps should all say “not allowed”
- Search within settings for “Certificates” – then look at User Certificates to see what are installed. If that is not there try “User Credentials”

Patch Scanning

The following resources are useful for those users who have Nessus and are unable to successfully conduct scans themselves.

- https://docs.tenable.com/nessus/Content/NessusCredentialedChecks.htm
- https://docs.tenable.com/nessus/Content/EnableWindowsLoginsForLocalAndRemoteAudits.htm

- https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm
- https://docs.tenable.com/nessus/Content/CredentialedChecksOnLinux.htm
- https://docs.tenable.com/nessus/Content/Credentials.htm?Highlight=remote%20registry
- https://docs.tenable.com/nessus/Content/Windows.htm?Highlight=remote%20registry