Device check report

ACME-DT-01

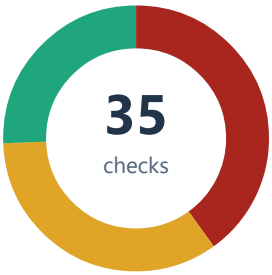
Microsoft Windows 10 Pro 22H2

Client	Checked on	Run as
Acme Ltd	27 October 2026	Administrator

! The short version

14 things need fixing on this computer, and 12 more are worth checking.

9 checks look good. Fixing everything listed should take about 7.5 hours of hands-on time, and 5 of the 26 items can be fixed automatically with Blackdown Digital's fix tool.



! Action needed	14
? Worth checking	12
✓ Looks good	9
– Not checked	0

The five Cyber Essentials controls

Firewalls — ! Action needed

1 item to fix

Secure configuration — ! Action needed

2 items to fix

User access control — ! Action needed

2 items to fix

Malware protection — ! Action needed

1 item to fix

Security updates — ! Action needed

8 items to fix

Fix these first

1. **Firewall is switched off.** Windows Firewall is turned off for: Public networks, and no other firewall product was found.
2. **Old file-sharing protocol (SMBv1) is on.** The old SMBv1 file-sharing protocol is switched on.
3. **An account has no password.** Windows does not require a password for this account and has no record of one being set:...

11 more items to fix in *What to do next*, on the following pages.

BLACKDOWN DIGITAL · SAMPLE DATA

What to do next

Start with the items marked **Action needed**. Each one explains what was found, why it matters, and what to do. Most can be fixed in a few minutes.

How to read this report. Each check is marked ! Action needed (commonly causes a Cyber Essentials question to be answered "No"), ? Worth checking (may be fine, but needs a person to confirm), ✓ Looks good or – Not checked. This is a readiness check of one computer, not a Cyber Essentials certificate or pass mark.

1 Firewall is switched off

! Action needed

Firewalls · About 5 minutes · **Fix tool can do this**

What we found	Windows Firewall is turned off for: Public networks, and no other firewall product was found.
Why it matters	A firewall stops other devices and the internet connecting to this computer without permission. Cyber Essentials requires one on every device.
What to do	Open Windows Security, choose Firewall and network protection, and turn the firewall on for each network type.

2 Old file-sharing protocol (SMBv1) is on

! Action needed

Secure configuration · About 10 minutes · **Fix tool can do this**

What we found	The old SMBv1 file-sharing protocol is switched on.
Why it matters	SMBv1 is obsolete and was used by the WannaCry ransomware. It should not be used on any modern network.
What to do	Turn it off: in "Turn Windows features on or off", untick "SMB 1.0/CIFS File Sharing Support", then restart.

3 An account has no password

! Action needed

User access control · About 10 minutes

What we found	Windows does not require a password for this account and has no record of one being set: reception.
Why it matters	Every account must be protected by a password, PIN or other sign-in method, or anyone could sign in as that user.
What to do	Set a strong password on each of these accounts, or disable the accounts if they are not used. If a password is already set, the account was probably set to change it at next sign-in: check, then sign in once to set it.

BLACKDOWN DIGITAL · SAMPLE DATA

4 Office macros are not controlled

! Action needed

Secure configuration · About 10 minutes

What we found	Microsoft Office is set to run all macros without asking in: Excel.
Why it matters	Macros in documents are one of the most common ways malware gets onto a computer. Cyber Essentials requires files not to run automatically without the user agreeing (A5.8).
What to do	In each program, go to File, Options, Trust Center, Trust Center Settings, Macro Settings, and choose "Disable VBA macros with notification".

5 Day-to-day account has admin rights

! Action needed

User access control · About 30 minutes

What we found	The person signed in when this check ran (reception) was able to run this tool as Administrator without another account, so their account has administrator rights.
Why it matters	Cyber Essentials expects separate accounts for admin tasks (A7.6), so that everyday work such as email and web browsing is done without admin rights (A7.7). Malware that reaches an admin account can take over the whole computer.
What to do	Give each person a standard account for everyday work, and a separate admin account used only when installing software or changing settings. (If this computer was checked while signed in to an admin account specially, check the day-to-day users instead.)

6 Virus definitions are out of date

! Action needed

Malware protection · About 5 minutes · **Fix tool can do this**

What we found	Virus definitions are 15 days old (last updated 12 October 2026).
Why it matters	New threats appear every day. Cyber Essentials expects antivirus definitions to update automatically, in line with the vendor's advice (daily for Defender).
What to do	Open Windows Security, Virus and threat protection, Protection updates, and choose Check for updates. If it keeps falling behind, check Windows Update is working.

7 This version of Windows is no longer supported

! Action needed

Security updates · About 1.5 hours

What we found	This computer runs Windows 10, which reached the end of standard support on 14 October 2025.
Why it matters	Cyber Essentials requires the operating system to be supported. Windows 10 is only acceptable while it is enrolled in, and receiving, Microsoft's paid Extended Security Updates.
What to do	Upgrade to Windows 11 if the hardware allows (the TPM and Secure Boot details are under Details of this computer), replace the computer, or confirm it is enrolled in Extended Security Updates and check with your certification body.

BLACKDOWN DIGITAL · SAMPLE DATA

8 Microsoft Office is no longer supported

! Action needed

Security updates · About 1 hour

What we found	Installed: Microsoft Office Professional Plus 2016 (support ended 14 October 2025).
Why it matters	Cyber Essentials requires all software to be supported by its maker and receiving security fixes, and unsupported software to be removed (A6.2, A6.6). One-off purchase versions of Office stop receiving updates on a fixed date.
What to do	Move to Microsoft 365 Apps (included in most Microsoft 365 business plans) or Office 2024, then uninstall the old version.

9 .NET runtimes are no longer supported

! Action needed

Security updates · About 10 minutes

What we found	Out-of-support or soon-to-end versions installed: .NET 6 (support ended 12 November 2024): Microsoft Windows Desktop Runtime - 6.0.36 (x64).
Why it matters	.NET is used by other programs to run. Cyber Essentials requires all software to be supported by its maker and receiving security fixes, and unsupported software to be removed (A6.2, A6.6).
What to do	Uninstall .NET versions that no program needs (Settings, Apps). Each entry listed is a separate item in the Installed apps list, so remove each one (search the list for ".NET", "Desktop Runtime" and "ASP.NET Core"). If a program still needs one, update that program or ask its supplier. Use .NET 10 where a newer version is needed.

10 Google Chrome is out of date

! Action needed

Security updates · About 5 minutes

What we found	Google Chrome version 129.0.6668.90 is installed. Around version 156 was current when this computer was checked, so it is about 27 versions behind and missing security fixes.
Why it matters	Web browsers are the software attackers target most. Cyber Essentials requires critical updates within 14 days (A6.5).
What to do	Open Google Chrome, go to Settings, About, let it update, then restart it. If it will not update, reinstall it from the official website, or uninstall it if it is not used.

11 Microsoft Edge is out of date

! Action needed

Security updates · About 5 minutes

What we found	Microsoft Edge version 130.0.2849.56 is installed. Around version 155 was current when this computer was checked, so it is about 25 versions behind and missing security fixes.
Why it matters	Web browsers are the software attackers target most. Cyber Essentials requires critical updates within 14 days (A6.5).
What to do	Open Microsoft Edge, go to Settings, About, let it update, then restart it. If it will not update, reinstall it from the official website, or uninstall it if it is not used.

BLACKDOWN DIGITAL · SAMPLE DATA

12 Mozilla Firefox is out of date

! Action needed

Security updates · About 5 minutes

What we found	Mozilla Firefox version 115.0.2 is installed. Around version 159 was current when this computer was checked, so it is about 44 versions behind and missing security fixes.
Why it matters	Web browsers are the software attackers target most. Cyber Essentials requires critical updates within 14 days (A6.5).
What to do	Open Mozilla Firefox, go to Settings, About, let it update, then restart it. If it will not update, reinstall it from the official website, or uninstall it if it is not used.

13 7-Zip needs a security update

! Action needed

Security updates · About 5 minutes

What we found	7-Zip 23.01 is installed. It has a vulnerability that attackers are known to be exploiting (CVE-2025-0411), fixed in version 24.09. Version 25.00 also fixes further high-severity vulnerabilities (CVE-2025-11001 and CVE-2025-11002).
Why it matters	This vulnerability is on the US government's list of flaws being actively used by attackers. Cyber Essentials requires critical fixes to be installed within 14 days (A6.5).
What to do	Install the latest 7-Zip from 7-zip.org (or uninstall it: Windows can open zip files on its own).

14 Retired software is installed

! Action needed

Security updates · About 10 minutes

What we found	Installed: Adobe Flash Player (retired December 2020).
Why it matters	These programs no longer get any security fixes from their makers. Cyber Essentials requires all software to be supported by its maker and receiving security fixes, and unsupported software to be removed (A6.2, A6.6).
What to do	Uninstall them (Settings, Apps, Installed apps). If something still depends on one, ask its supplier for a supported alternative.

15 Firewall openings need checking

? Worth checking

Firewalls · About 15 minutes

What we found	2 custom rules let any device connect to this computer on a specific port, for example: TeamViewer Remote Control Service; Sage 50 Data Service.
Why it matters	Programs often add these rules when installed. Each opening should have a business reason, and anything no longer needed should be removed.
What to do	Look through the rules in Appendix A and remove any for software that is no longer used.

BLACKDOWN DIGITAL · SAMPLE DATA

16 No automatic screen lock

? Worth checking

Secure configuration · About 5 minutes · **Fix tool can do this**

What we found	No automatic lock was found: there is no screen-lock policy or secure screen saver, and Windows does not ask for a sign-in when it wakes from sleep (the screen turns off after 10 minutes, but that alone does not lock it).
Why it matters	Cyber Essentials requires a password, PIN or fingerprint to unlock a device (A5.9, A5.10). Locking automatically stops someone using a computer that has been left unattended.
What to do	Set the computer to lock after 10 to 15 minutes: Settings, System, Power, "Screen and sleep" (turn off the screen and sleep after 10 to 15 minutes), and Settings, Accounts, Sign-in options, "If you have been away, when should Windows require you to sign in again?" set to "When PC wakes up from sleep".

17 Remote Desktop is switched on

? Worth checking

Secure configuration · About 10 minutes

What we found	Remote Desktop is turned on (with Network Level Authentication).
Why it matters	Remote Desktop is a common target for attackers, so it should only be on if it is needed, and never reachable directly from the internet.
What to do	Turn it off if nobody uses it. If it is needed, confirm the office router does not forward port 3389 to this computer.

18 Drive encryption needs checking

? Worth checking

Secure configuration · About 30 minutes

What we found	BitLocker is not protecting the main drive (C:).
Why it matters	Not required for Cyber Essentials, but strongly recommended, especially for laptops. It stops data being read if the device is lost or stolen.
What to do	Turn on BitLocker (or Device encryption on Windows Home) and keep a copy of the recovery key somewhere safe.

19 Admin rights need checking

? Worth checking

User access control · About 15 minutes

What we found	3 accounts or groups have administrator rights on this computer: Administrator, acmeadmin, sarah@acme.co.uk.
Why it matters	Cyber Essentials expects admin rights to be given only to people who need them, and used only for admin tasks, not for everyday work such as email and web browsing.
What to do	Confirm each one is needed. People who use this computer day to day should sign in with a standard account and use a separate admin account only when needed.

BLACKDOWN DIGITAL · SAMPLE DATA

20 Local password length needs checking

? Worth checking

User access control · About 5 minutes · **Fix tool can do this**

What we found	The minimum length for local account passwords on this computer is 0 characters.
Why it matters	Where multi-factor authentication is not used, Cyber Essentials expects passwords of at least 12 characters (or at least 8 with a block on common passwords). This does not apply if people sign in with Microsoft 365 / Entra ID accounts protected by multi-factor authentication.
What to do	If people sign in with local accounts, set the minimum password length to 12 (Local Security Policy, Account Policies, Password Policy).

21 Security updates may be overdue

? Worth checking

Security updates · About 30 minutes

What we found	2 updates are waiting to be installed, all released within the last 14 days or not marked critical.
Why it matters	These are not overdue yet, but need installing within 14 days of release to meet Cyber Essentials.
What to do	Open Settings, Windows Update, install the updates and restart the computer.

22 Updates are not installing regularly

? Worth checking

Security updates · About 30 minutes

What we found	The last Windows update (not counting antivirus definitions) was installed 40 days ago, on 16 September 2026.
Why it matters	Microsoft releases security updates every month, so a gap of more than a month usually means updates are not installing.
What to do	Open Settings, Windows Update, choose Check for updates, and fix any errors shown.

23 Not restarted recently

? Worth checking

Security updates · About 5 minutes

What we found	Windows is waiting for a restart to finish installing updates.
Why it matters	Many updates only take effect after a restart, so a computer that is never restarted can stay unprotected.
What to do	Restart the computer, ideally at least once a week.

24 Adobe Acrobat may be out of date

? Worth checking

Security updates · About 10 minutes

What we found	Adobe Acrobat Reader version 24.002.20759 is installed, which appears to be more than a year out of date.
Why it matters	PDF readers are a common target for attackers, and Adobe releases security fixes most months.
What to do	Open it, choose Help, Check for updates, and install any updates.

BLACKDOWN DIGITAL · SAMPLE DATA

25 Oracle Java may need a paid licence

? Worth checking

Security updates · About 20 minutes

What we found	Oracle Java is installed: Java 8 Update 401 (64-bit).
Why it matters	Most Oracle Java versions released since 2019 need a paid licence for business use (it depends on the version and how it is used), and Cyber Essentials requires software to be licensed and supported (A6.3). Old copies are also a common security risk.
What to do	Uninstall it if nothing needs it. If a program needs Java, check you have an Oracle licence, or switch to a free build such as Eclipse Temurin or Microsoft Build of OpenJDK, and keep it updated.

26 Remote access software is installed

? Worth checking

Security updates · About 15 minutes

What we found	Remote access software is installed: TeamViewer 15.40.8.
Why it matters	Remote access tools are a favourite way in for attackers, and are often left installed after a one-off support session. Cyber Essentials expects software that is not needed to be removed (A5.1), and accounts that can reach the computer from the internet to be well protected.
What to do	Uninstall any that are not needed. For those that are, keep them updated, protect the account with multi-factor authentication, and turn off unattended access if it is not used.

Beyond this computer. The installed software was checked against Blackdown Digital's list of commonly unsupported, retired or known-vulnerable programs (last updated 14 November 2026), but not every program can be checked automatically, so look through Appendix B too: everything must be supported and updated within 14 days. Your other devices, your router or firewall, and your cloud services are assessed separately.

BLACKDOWN DIGITAL · SAMPLE DATA

Results by control

Firewalls

! Action needed

Stops unwanted connections reaching this computer from other devices and the internet.

Result	Check	What we found
! Action needed	**Firewall is switched on**	Windows Firewall is turned off for: Public networks, and no other firewall product was found.
? Worth checking	**No extra openings from any address**	2 custom rules let any device connect to this computer on a specific port, for example: TeamViewer Remote Control Service; Sage 50 Data Service.
✓ Looks good	**Unexpected incoming connections are blocked**	Incoming connections are blocked unless a rule specifically allows them.

Secure configuration

! Action needed

Removes or turns off things that are not needed, and switches on sensible protective settings.

Result	Check	What we found
! Action needed	**Old file-sharing protocol (SMBv1) is off**	The old SMBv1 file-sharing protocol is switched on.
! Action needed	**Office macros are controlled**	Microsoft Office is set to run all macros without asking in: Excel.
? Worth checking	**Screen locks when left unattended**	No automatic lock was found: there is no screen-lock policy or secure screen saver, and Windows does not ask for a sign-in when it wakes from sleep (the screen turns off after 10 minutes, but that alone does not lock it).
? Worth checking	**Remote Desktop is controlled**	Remote Desktop is turned on (with Network Level Authentication).
? Worth checking	**Main drive is encrypted**	BitLocker is not protecting the main drive (C:).
✓ Looks good	**User Account Control is on**	User Account Control (UAC) is turned on.
✓ Looks good	**USB drives cannot run files automatically**	AutoPlay is on with its normal setting: Windows asks what to do when a USB drive or disc is inserted, and does not run programs from it by itself. Cyber Essentials accepts this (question A5.8). Turning AutoPlay off is a little tighter.

BLACKDOWN DIGITAL · SAMPLE DATA

User access control

Makes sure only the right people can sign in, and admin rights are kept to those who need them.

! Action needed

Result	Check	What we found
! Action needed	**Every account needs a password**	Windows does not require a password for this account and has no record of one being set: reception.
! Action needed	**Day-to-day account is a standard account**	The person signed in when this check ran (reception) was able to run this tool as Administrator without another account, so their account has administrator rights.
? Worth checking	**Admin rights are limited**	3 accounts or groups have administrator rights on this computer: Administrator, acmeadmin, sarah@acme.co.uk.
? Worth checking	**Local passwords are long enough**	The minimum length for local account passwords on this computer is 0 characters.
✓ Looks good	**Guest account is disabled**	The built-in Guest account is disabled.
✓ Looks good	**Built-in Administrator account is disabled**	The built-in Administrator account is disabled.
✓ Looks good	**Password guessing is limited**	Accounts lock after 10 wrong password attempts.

Malware protection

Stops viruses and other harmful software running on this computer.

! Action needed

Result	Check	What we found
! Action needed	**Virus definitions are up to date**	Virus definitions are 15 days old (last updated 12 October 2026).
✓ Looks good	**Antivirus is running**	Microsoft Defender is installed with real-time protection switched on.
✓ Looks good	**Antivirus cannot be switched off by malware**	Defender tamper protection is switched on.

BLACKDOWN DIGITAL · SAMPLE DATA

Security updates

! Action needed

Keeps Windows supported and patched, so known security holes are closed quickly.

Result	Check	What we found
! Action needed	**Windows is still supported**	This computer runs Windows 10, which reached the end of standard support on 14 October 2025.
! Action needed	**Microsoft Office is supported**	Installed: Microsoft Office Professional Plus 2016 (support ended 14 October 2025).
! Action needed	**.NET runtimes are supported**	Out-of-support or soon-to-end versions installed: .NET 6 (support ended 12 November 2024): Microsoft Windows Desktop Runtime - 6.0.36 (x64).
! Action needed	**Google Chrome is up to date**	Google Chrome version 129.0.6668.90 is installed. Around version 156 was current when this computer was checked, so it is about 27 versions behind and missing security fixes.
! Action needed	**Microsoft Edge is up to date**	Microsoft Edge version 130.0.2849.56 is installed. Around version 155 was current when this computer was checked, so it is about 25 versions behind and missing security fixes.
! Action needed	**Mozilla Firefox is up to date**	Mozilla Firefox version 115.0.2 is installed. Around version 159 was current when this computer was checked, so it is about 44 versions behind and missing security fixes.
! Action needed	**7-Zip is patched**	7-Zip 23.01 is installed. It has a vulnerability that attackers are known to be exploiting (CVE-2025-0411), fixed in version 24.09. Version 25.00 also fixes further high-severity vulnerabilities (CVE-2025-11001 and CVE-2025-11002).
! Action needed	**No retired software is installed**	Installed: Adobe Flash Player (retired December 2020).
? Worth checking	**Security updates installed within 14 days**	2 updates are waiting to be installed, all released within the last 14 days or not marked critical.
? Worth checking	**Updates are installing regularly**	The last Windows update (not counting antivirus definitions) was installed 40 days ago, on 16 September 2026.
? Worth checking	**Recently restarted**	Windows is waiting for a restart to finish installing updates.
? Worth checking	**Adobe Acrobat is up to date**	Adobe Acrobat Reader version 24.002.20759 is installed, which appears to be more than a year out of date.
? Worth checking	**Oracle Java is licensed and kept updated**	Oracle Java is installed: Java 8 Update 401 (64-bit).
? Worth checking	**Remote access software is controlled**	Remote access software is installed: TeamViewer 15.40.8.
✓ Looks good	**Automatic updates are switched on**	Automatic updates are switched on and not delayed.

BLACKDOWN DIGITAL · SAMPLE DATA

Details of this computer

Computer

Computer name	ACME-DT-01
Windows	Microsoft Windows 10 Pro
Version and build	22H2 (build 19045.4946)
Make and model	Dell Inc. OptiPlex 7010
Processor	13th Gen Intel(R) Core(TM) i5-1345U
Memory	15.7 GB
Windows installed	2 November 2024
Last restarted	14 Sep 2026, 08:02 UTC

Management

Domain or workgroup	WORKGROUP
Joined to Microsoft Entra ID	Yes
Joined to a local domain	No
Device management (MDM)	Not enrolled
TPM security chip	Present (version 2.0)
Secure Boot	Yes

Antivirus

Microsoft Defender mode	Normal
Real-time protection	Yes
Tamper protection	Yes
Definitions updated	12 Oct 2026, 03:00 UTC
Last quick scan	26 Oct 2026, 12:40 UTC
Scan exclusions	0

Antivirus products registered with Windows: Windows Defender

Windows Update

Update service	Running now (starts automatically when needed)
Managed update server (WSUS)	No
Security updates delayed	No
Last Windows update installed	16 September 2026
Updates waiting	2

Software the questionnaire asks you to list

Web browsers (A6.2.1)	Google Chrome 129.0.6668.90; Microsoft Edge 130.0.2849.56; Mozilla Firefox 115.0.2
Malware protection (A6.2.2)	Microsoft Defender Antivirus 4.18.24090.11
Email applications (A6.2.3)	Microsoft 365 Apps for business 16.0.18025.20140; Microsoft Office Professional Plus 2016 16.0.4266.1001
Office applications (A6.2.4)	Microsoft 365 Apps for business 16.0.18025.20140; Microsoft Office Professional Plus 2016 16.0.4266.1001

Local user accounts

Account	Status	Type	Admin rights	Last sign-in
Administrator	Disabled	Built-in administrator	Yes	Not available

BLACKDOWN DIGITAL · SAMPLE DATA

Account	Status	Type	Admin rights	Last sign-in
Guest	Disabled	Built-in guest	No	Not available
DefaultAccount	Disabled	User	No	Not available
acmeadmin	Enabled	User	Yes	11 June 2026
reception	Enabled	User	No	20 October 2026

Updates waiting to be installed

Update	Severity	Available for
2026-10 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5066835)	Critical	13 days
Windows Malicious Software Removal Tool x64 - v5.130 (KB890830)	Not rated	13 days

Most recent updates installed

Update	Date	Result
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.419.230.0)	27 October 2026	Installed
2026-09 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5065426)	16 September 2026	Installed
2026-08 Cumulative Update for Windows 11 Version 24H2 for x64-based Systems (KB5063878)	14 August 2026	Installed

BLACKDOWN DIGITAL · SAMPLE DATA

Appendix A: Firewall openings

46 rules allow incoming connections. 43 are standard Windows rules; the 3 other rules, usually added by installed software, are listed here.

Rule	Program	Protocol	Port	From
TeamViewer Remote Control Service	TeamViewer_Service.exe	TCP	5938	Any
Sage 50 Data Service	Sage.DataService.exe	TCP	2638	Any
Zoom Video Meeting	Zoom.exe	UDP	Any	Any

Appendix B: Installed software

18 programs were found. Remove anything that is no longer needed, and check that the rest is still supported by its maker and kept up to date.

Program	Version	Publisher
7-Zip 23.01 (x64)	23.01	Igor Pavlov
Adobe Acrobat Reader	24.002.20759	Adobe
Google Chrome	129.0.6668.90	Google LLC
Microsoft 365 Apps for business - en-gb	16.0.18025.20140	Microsoft Corporation
Microsoft Edge	130.0.2849.56	Microsoft Corporation
Microsoft OneDrive	24.201.1006.0005	Microsoft Corporation
Microsoft Teams	24243.1309.3132.617	Microsoft Corporation
Mozilla Firefox (x64 en-GB)	115.0.2	Mozilla
Sage 50 Accounts	30.1.105.0	Sage (UK) Ltd
TeamViewer	15.40.8	TeamViewer
VLC media player	3.0.18	VideoLAN
Zoom Workplace	6.2.5	Zoom Video Communications, Inc.
Dell SupportAssist	4.0.3.4	Dell Inc.
Microsoft Visual C++ 2015-2022 Redistributable (x64)	14.40.33810.0	Microsoft Corporation
Microsoft Office Professional Plus 2016	16.0.4266.1001	Microsoft Corporation
Microsoft Windows Desktop Runtime - 6.0.36 (x64)	6.0.36.34217	Microsoft Corporation
Java 8 Update 401 (64-bit)	8.0.4010.10	Oracle Corporation
Adobe Flash Player 32 NPAPI	32.0.0.465	Adobe

Appendix C: Programs accepting network connections

Programs that other devices on the network could connect to. Many are normal parts of Windows.

Program	Port	Address
svchost	135	0.0.0.0
System	445	0.0.0.0
svchost	3389	0.0.0.0

BLACKDOWN DIGITAL · SAMPLE DATA

Program	Port	Address
TeamViewer_Service	5938	0.0.0.0

About this report

Produced by the Blackdown Digital Cyber Essentials device check, version 1.10.0.0 (fingerprint 2CCAFAD7CE44EB83), on 27 Oct 2026, 09:38 UTC, run by ACME-DT-01\reception. The tool only reads settings and made no changes to this computer. The same results are attached inside this PDF as a data file, so they can be combined with results from other computers into a business report. The support end dates, current browser versions and known-exploited software list this check uses were last reviewed on 14 November 2026. Results reflect this computer at the time of the check. This report lists account names, so please treat it as confidential, send it securely and delete copies when no longer needed. Blackdown Digital provides readiness support and does not issue Cyber Essentials certificates.

BLACKDOWN DIGITAL · SAMPLE DATA