



WINDOWS 11 HARDENING FOR CYBER ESSENTIALS

Ten practical controls to prepare for audit

PRACTICAL CYBER SECURITY. POWERED BY AI.

A concise guide for standalone and workgroup Windows 11 PCs

Secure configuration • Access control • Updates • Firewall • Malware protection

TEN CONTROLS. ONE CONSISTENT BASELINE.

Cyber Essentials does not require every Windows setting to be maximally restrictive. It requires five fundamental controls to operate consistently across the complete in-scope environment.

THE FIVE CONTROL AREAS

01 FIREWALLS

02 SECURE CONFIGURATION

03 SECURITY UPDATES

04 USER ACCESS CONTROL

05 MALWARE PROTECTION

SCOPE BEFORE SETTINGS

Include every business PC, home-working device and relevant BYOD device. Record the Windows edition, applications, users and security configuration. Audit readiness is a property of the whole estate - not one well-configured laptop.

01 SEPARATE USER AND ADMINISTRATOR ACCOUNTS

Use a standard account every day. Elevate only when necessary.



WINDOWS NAVIGATION

Settings > Accounts > Other users

WHAT TO CONFIGURE

Create a separate local administrator account, then change each everyday account to Standard User. Use the administrator credential only for software installation, security changes and maintenance.

The built-in Administrator account is normally disabled; leave it disabled. If it has been enabled, disable it or rename it through Computer Management > Local Users and Groups > Users. Renaming is extra hardening, not a Cyber Essentials requirement.

PASS CHECK

- Everyday accounts show as Standard User
- A distinct administrator account exists
- Admin credentials are unique and securely stored

AUDIT EVIDENCE

Screenshot of account types, plus the documented admin-account procedure.

02 SET A DEFENSIBLE PASSWORD POLICY

Strong means long, unique and resistant to guessing - not difficult to remember.



WINDOWS NAVIGATION

Win + R > secpol.msc > Account Policies

WHAT TO CONFIGURE

For Windows 11 Pro, set a sensible minimum length and an account lockout threshold of ten attempts or fewer. Prefer a minimum of 12 characters and three random words or password-manager-generated values.

Do not force frequent password expiry without cause. Cyber Essentials focuses on unique passwords, compromised-password changes and protection against automated guessing. Windows 11 Home lacks Local Security Policy, so document the rule and use Windows Hello and Microsoft-account protections.

PASS CHECK

- Minimum 12 characters recommended
- Lockout after 10 or fewer failed attempts
- No password reuse; change suspected compromises

AUDIT EVIDENCE

Screenshots of password and lockout policies, supported by the written password procedure.

03

KEEP WINDOWS SUPPORTED AND PATCHED

Unsupported operating systems cannot meet Cyber Essentials.



WINDOWS NAVIGATION

Settings > System > About | Settings > Windows Update

WHAT TO CONFIGURE

Record the edition, version and build of every PC. Enable automatic updates and use Check for updates to confirm the current state.

Cyber Essentials requires fixes for vulnerabilities rated high or critical by the vendor, and vulnerabilities with a CVSS v3 base score of 7.0 or above, to be installed within 14 days. Replacement or isolation is required when a product is no longer supported.

PASS CHECK

- All Windows releases are vendor-supported
- Automatic updating is enabled
- Qualifying fixes are installed within 14 days

AUDIT EVIDENCE

Asset register with Windows release and support dates; recent update-status screenshots.

04 UPDATE APPLICATIONS AS WELL AS WINDOWS

Browsers and business software are frequent attack routes.



WINDOWS NAVIGATION

Microsoft Store > Profile > Settings > App updates

WHAT TO CONFIGURE

The 14-day update rule applies to in-scope software, including browsers, Microsoft 365, PDF readers, conferencing tools and remote-access utilities. Enable automatic updating wherever possible.

Maintain a software inventory and check applications that update independently. Remove old versions rather than leaving them installed beside the current release.

PASS CHECK

- Store app updates are enabled
- Browsers and productivity tools auto-update
- Unsupported and duplicated applications are removed

AUDIT EVIDENCE

Software inventory, update configuration and dated patch-review records.

05 ENABLE MICROSOFT DEFENDER ANTIVIRUS

Built-in protection is effective when active, current and tamper-resistant.



WINDOWS NAVIGATION

Windows Security > Virus & threat protection > Manage settings

WHAT TO CONFIGURE

Ensure Real-time protection, Cloud-delivered protection, Automatic sample submission and Tamper Protection are enabled. Confirm that security intelligence is current.

A supported third-party antivirus product is also acceptable, but do not run two real-time antivirus engines together. Investigate warnings rather than dismissing them.

PASS CHECK

- Real-time and cloud protection are on
- Tamper Protection is enabled
- Security intelligence is current

AUDIT EVIDENCE

Windows Security status showing no warnings and current protection updates.

06 ENABLE THE FIREWALL EVERYWHERE

Block unsolicited inbound traffic unless a business need is documented.



WINDOWS NAVIGATION

Windows Security > Firewall & network protection

WHAT TO CONFIGURE

Confirm Microsoft Defender Firewall is enabled for every applicable profile: Domain, Private and Public. The normal default is to block unsolicited inbound connections while permitting expected outbound traffic.

Do not disable the firewall to make an application work. Create the narrowest possible inbound exception, restrict it by program, port and network profile, and record the business owner and review date.

PASS CHECK

- Firewall is on for all applicable profiles
- Inbound exceptions are minimal and justified
- No broad allow-all rules are present

AUDIT EVIDENCE

Profile-status screenshots and a reviewed register of inbound firewall exceptions.

07 REMOVE UNNECESSARY SOFTWARE AND SERVICES

What is not installed cannot become an unpatched vulnerability.



WINDOWS NAVIGATION

Settings > Apps > Installed apps

WHAT TO CONFIGURE

Remove trialware, obsolete utilities, redundant browsers, unused remote-access tools and applications no longer supported by their vendors. Remove dormant user accounts at the same time.

Disable Remote Desktop, file sharing and remote administration unless they have a documented business purpose. Secure configuration is primarily about reducing the attack surface consistently, not turning on every available restriction.

PASS CHECK

- Unused applications have been removed
- Dormant accounts are deleted or disabled
- Remote services have documented owners

AUDIT EVIDENCE

Current software and account inventories, with a record of removals and approved exceptions.

08 LOCK UNATTENDED DEVICES

A secured account still fails if an unattended PC remains open.



WINDOWS NAVIGATION

Settings > Accounts > Sign-in options

WHAT TO CONFIGURE

Require sign-in when a device wakes and configure an automatic screen lock - normally after five to ten minutes. Set the screen timeout through Settings > System > Power & battery > Screen and sleep.

Use Windows Hello where available. A Windows Hello PIN is bound to the device and is preferable to repeatedly typing a reusable online password.

PASS CHECK

- Wake-up requires authentication
- Screen locks automatically
- Windows Hello is used where practical

AUDIT EVIDENCE

Screenshots of sign-in and timeout settings from each configuration type in scope.

09

TURN ON REPUTATION-BASED PROTECTION

Stop suspicious applications and downloads before they execute.



WINDOWS NAVIGATION

Windows Security > App & browser control > Reputation-based protection

WHAT TO CONFIGURE

Enable Check apps and files, SmartScreen for Microsoft Edge, phishing protection, potentially unwanted app blocking and SmartScreen for Microsoft Store apps.

These controls complement Defender Antivirus; they do not replace it. If another browser is used, confirm its own safe-browsing and download-protection features are enabled and centrally managed where possible.

PASS CHECK

- SmartScreen checks apps and downloads
- Phishing protection is active
- Potentially unwanted apps are blocked

AUDIT EVIDENCE

Screenshot of reputation-based protection and equivalent settings for other browsers.

10 PROTECT CLOUD ACCESS WITH MFA

Cyber Essentials extends beyond the Windows desktop.



WINDOWS NAVIGATION

Microsoft 365 Admin Centre > Users > Active users

WHAT TO CONFIGURE

Enable multi-factor authentication for accounts accessing cloud services, including Microsoft 365, accounting, backup and remote-support platforms. Administrator accounts must also use MFA.

Prefer authenticator apps, passkeys or physical security keys over SMS where supported. Remove leavers promptly and review administrator roles so privilege is granted only to people who need it.

PASS CHECK

- Cloud-service users have MFA enabled
- Every administrator uses MFA
- Leavers and excess roles are removed promptly

AUDIT EVIDENCE

Exported user and MFA status, administrator-role report and leaver records.

READY?

FINAL PRE-AUDIT CHECK

☐ Every in-scope device is in the asset inventory

☐ Windows and applications are vendor-supported

☐ Qualifying security fixes land within 14 days

☐ Daily users do not hold administrator privileges

☐ Defender and Firewall show no unresolved warnings

☐ Cloud and administrator accounts use MFA

☐ Exceptions are justified, owned and reviewed

☐ Evidence is recent and representative

SEE YOUR ESTATE. PRIORITIZE RISK. ACT WITH CONFIDENCE.

Guidance reflects Cyber Essentials principles; always validate against the question set used for your assessment.



SEE YOUR ESTATE. PRIORITIZE RISK. ACT WITH CONFIDENCE.

SecureX7 is a natively built, AI-driven cyber security platform that helps organizations understand their environment, identify the risks that matter most, and take clear action to improve security and compliance.

FROM ASSESSMENT TO ACTION - WITHOUT COMPLEXITY

Discover assets • Assess posture • Prioritize exposure • Guide remediation

[START YOUR FREE TRIAL](#)[REQUEST A FREE DEMO](#)