secureX7

WINDOWS 11 SECURE CONFIGURATION CHECKLIST

Review your endpoint security baseline before assessment

PRACTICAL CYBER SECURITY. POWERED BY AI.

A practical guide for standalone and workgroup Windows 11 PCs

Firewalls • Updates • User access • Malware protection

secureX7

CYBER ESSENTIALS MADE SIMPLE

Why grind through Cyber Essentials manually when SecureX7 can do it for you?

CYBER ESSENTIALS

Built to align with Cyber Essentials v3.3 technical requirements

SecureX7 automatically assesses your environment, identifies potential Cyber Essentials gaps, creates a prioritized workplan and guides you through remediation, so you can achieve Cyber Essentials with confidence.

Please use this guide to manually review and correct your security settings in preparation for a Cyber Essentials audit, but if you prefer to automate the process and save valuable time, ask for a free trial and we'll get you up and running in minutes! You're welcome!

Start Your Free 14-Day Trial >

Book a Demo >

Automated Assessment

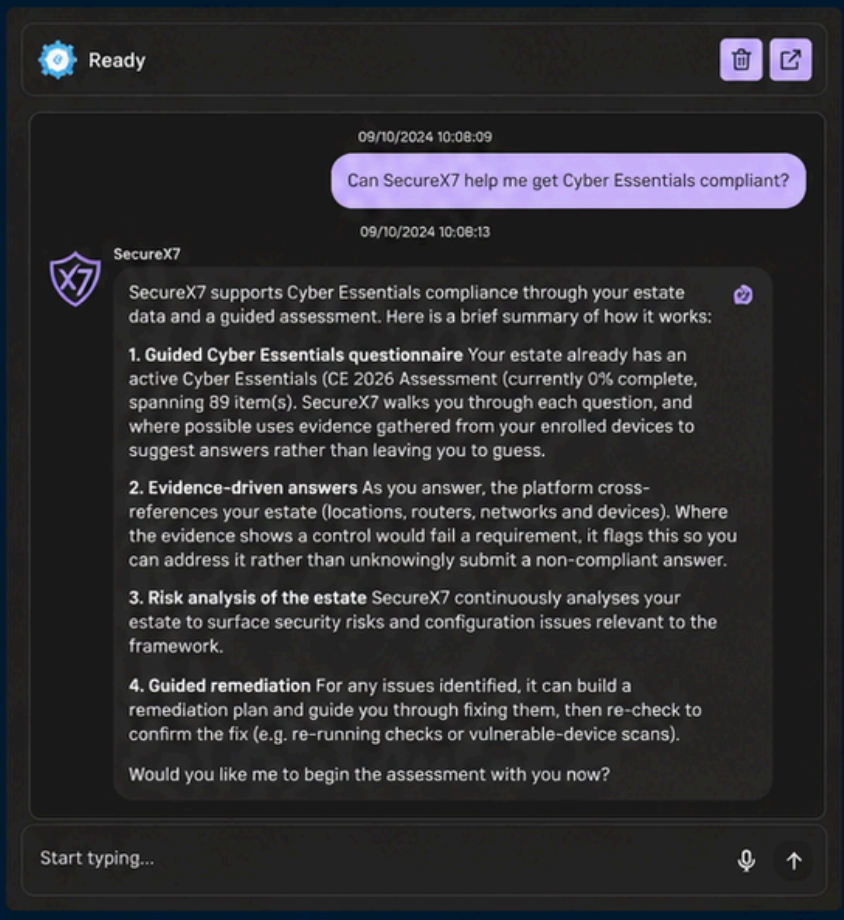
Prioritised remediation

Evidence made easy

Just tell SecureX7 What You Need!

"I need to get Cyber Essentials compliant."

Simply tell SecureX7 your goal and it will guide you through the process.



AUDIT-READY BASELINE

One consistent baseline across your estate

WHY THIS GUIDE MATTERS

Cyber Essentials measures effective implementation of five foundational controls across the complete in-scope environment. These Windows 11 steps support readiness but do not replace the current official technical requirements or an authorised certification assessment.

BEFORE YOU START

Identify the Windows 11 edition, device scope, administrator access, application dependencies and existing management policies. Capture current settings before making changes.

HOW TO USE THE GUIDE

Work through the three configuration areas, confirm the pass checks and retain dated evidence. For centrally managed devices, apply approved settings through Intune, Group Policy or equivalent tooling rather than making conflicting local changes.

SCOPE BEFORE SETTINGS

A compliant test laptop does not establish compliance for the whole organisation. Include in-scope home-working devices, relevant BYOD and applicable cloud services.

CONFIGURATION WALKTHROUGH

Scope and platform

Asset inventory

List all in-scope Windows PCs, home-working devices and relevant BYOD, including edition, version, owner and location.

Supported software

Confirm the Windows release and all installed applications remain supported and unnecessary software is removed.

Secure baseline

Identify the approved Windows configuration for each device type and record deviations or business exceptions.

IMPORTANT

Validate settings against your organisation’s approved baseline and the Cyber Essentials assessment question set in force. Test changes before broad deployment.

CONFIGURATION WALKTHROUGH

Technical control checks

Firewalls

Confirm applicable firewall profiles are enabled, inbound traffic blocked by default and exceptions justified.

Updates

Verify automatic updating and evidence that qualifying fixes are deployed within 14 days of release.

Malware protection

Verify antivirus or other accepted protection approach, current protection data and no unresolved warnings.

IMPORTANT

Validate settings against your organisation’s approved baseline and the Cyber Essentials assessment question set in force. Test changes before broad deployment.

CONFIGURATION WALKTHROUGH

Accounts and final validation

Least privilege

Review local administrators, daily standard-user accounts, dormant accounts and access approvals.

Cloud MFA

Verify in-scope cloud-service users and administrators meet applicable MFA requirements.

Evidence and recheck

Capture representative dated evidence, resolve gaps and reassess before the formal questionnaire or technical audit.

IMPORTANT

Validate settings against your organisation’s approved baseline and the Cyber Essentials assessment question set in force. Test changes before broad deployment.

VERIFICATION AND EVIDENCE

Pass checks and audit records

PASS CHECK

- ✓ Every in-scope device and application recorded
- ✓ Firewalls and malware protection operational
- ✓ Security fixes meet the 14-day requirement
- ✓ Least privilege and cloud MFA verified
- ✓ Exceptions and evidence current

EVIDENCE TO RETAIN

- Dated asset and software inventory
- Firewall, antivirus and update status exports
- Admin group, cloud MFA and exception reviews

PRACTICAL NOTE

A Windows-only checklist cannot prove every Cyber Essentials requirement. Include cloud services, network equipment, organisational processes and assessment scope.

secureX7

SEE YOUR ESTATE.
PRIORITISE RISK.
ACT WITH CONFIDENCE.

SecureX7 helps organisations discover assets, assess supported security configurations, identify vulnerabilities and prioritise remediation.

DISCOVER • ASSESS • PRIORITISE • REMEDIATE • VERIFY

START YOUR FREE TRIAL

REQUEST A DEMO

securex7.com