secureX7

WINDOWS 11
SECURITY UPDATE MANAGEMENT
FOR CYBER ESSENTIALS

Maintain supported software and timely security fixes

PRACTICAL CYBER SECURITY. POWERED BY AI.

A practical guide for standalone and workgroup Windows 11 PCs

Windows Update • Applications • 14-day rule • Evidence

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

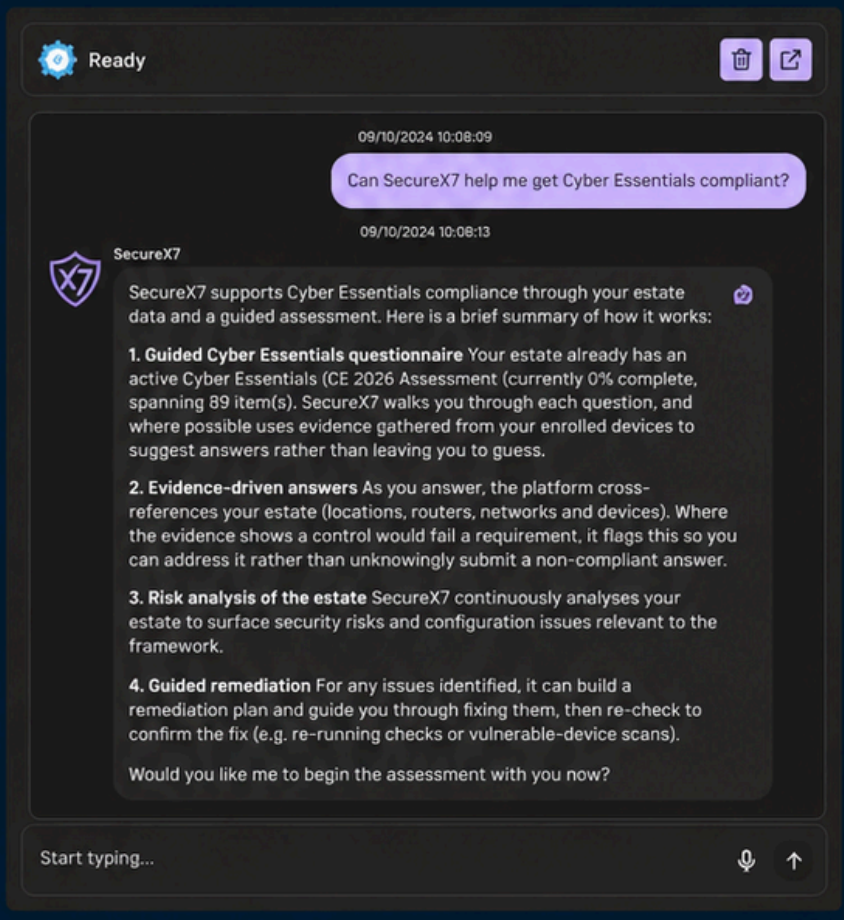
Prioritised remediation

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

Inventory supported releases

Identify Windows release

Use Settings > System > About and winver to record Windows edition, version and build for each device.

Confirm vendor support

Check that each Windows release and installed application remains supported and receives security fixes. Windows 11 feature versions have different support dates.

Find installed software

Use Settings > Apps > Installed apps and an asset inventory to identify browsers, PDF readers, conferencing tools and remote access utilities.

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

Configure and verify updates

Windows Update

Open Settings > Windows Update. Enable appropriate automatic update behaviour and review update history and failures.

PowerShell inspection

Use Get-ComputerInfo | Select WindowsProductName,WindowsVersion,OsBuildNumber for context. Windows Update history may require management tooling or the Settings UI.

Third-party updates

Verify each application’s own updater or centrally managed deployment process. Windows Update alone does not patch all applications.

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

Apply the 14-day rule

Start the clock at fix release

Qualifying high/critical vendor-rated vulnerabilities or CVSS v3 base score 7.0+ require vendor-approved fixes within 14 days of release, not 14 days after discovery.

Track exceptions and failures

Log the fix release date, affected assets, deployment date and validation result. Escalate unsuccessful deployments promptly.

Unsupported products

Remove, replace or otherwise bring unsupported in-scope products into a supported state; isolation alone is not a general exemption.

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

- ✓ All in-scope Windows releases supported
- ✓ Software inventory includes third-party applications
- ✓ Qualifying security fixes deployed within 14 days of release
- ✓ Update failures and exceptions tracked

EVIDENCE TO RETAIN

- Asset and software inventory with versions
- Dated Windows Update and application update evidence
- Patch tracking record showing release and deployment dates

PRACTICAL NOTE

A vendor-approved configuration fix can sometimes meet the requirement; check the current Cyber Essentials technical specification.

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