secureX7

WINDOWS SERVICES HARDENING
FOR CYBER ESSENTIALS

Reduce unnecessary services and network exposure

PRACTICAL CYBER SECURITY. POWERED BY AI.

A practical guide for standalone and workgroup Windows 11 PCs

Services • Remote access • Network exposure • 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

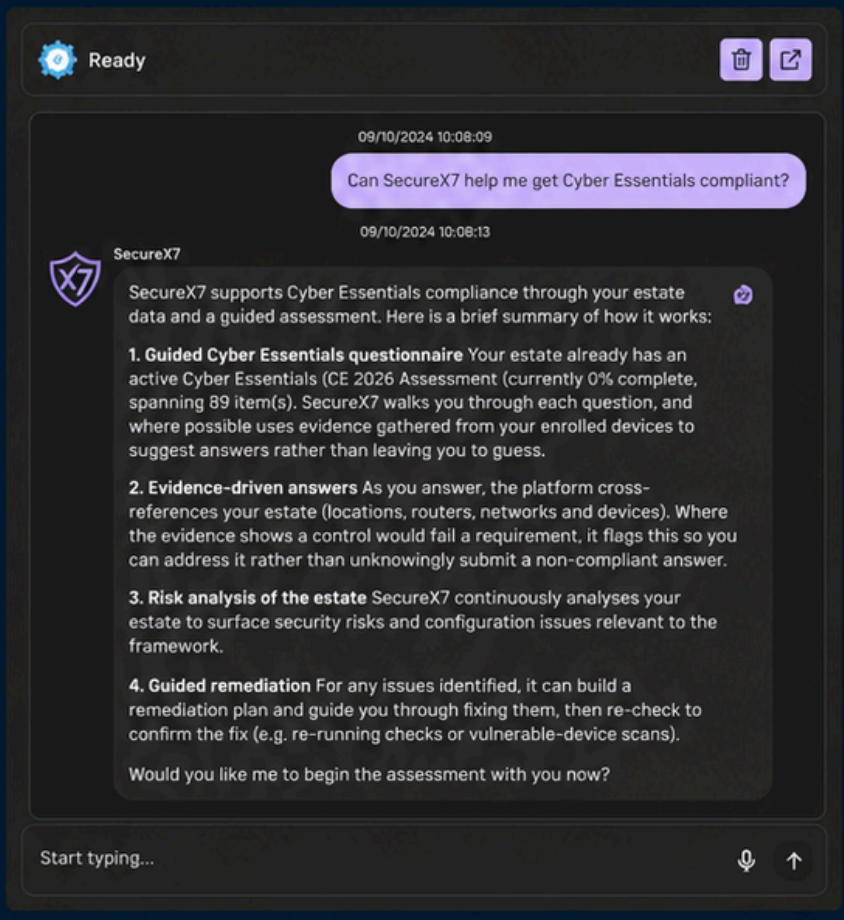
Prioritised remediation

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

Establish a baseline

Inventory services

Open services.msc and identify services with automatic startup. Use Get-Service | Sort Name for a scriptable list.

Inspect listening ports

Use Get-NetTCPConnection -State Listen | Select LocalAddress,LocalPort,OwningProcess to identify TCP listeners. Map process IDs to applications before making changes.

Document business need

Record the purpose, owner and exposure of remote management, file sharing and third-party agents.

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

Remove avoidable exposure

Remote Desktop

Disable RDP if not needed: Settings > System > Remote Desktop. If needed, restrict access and protect the route.

File sharing

Review advanced sharing settings and SMB use. Do not disable necessary file services without understanding operational dependencies.

Unnecessary applications

Remove unsupported or unused remote access tools, trialware and obsolete software before disabling their services.

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

Change services safely

Test before disabling

Service dependencies and Windows edition differences matter. Do not indiscriminately disable Windows Update, Defender or core networking services.

Prefer removal or policy

Uninstall unneeded applications or use approved policy rather than ad hoc registry modifications.

Recheck exposure

After changes, confirm application function, service state and listening ports, then update the approved baseline.

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

- ✓ Unnecessary remote services disabled or removed
- ✓ Listening network services have owners and purposes
- ✓ Core security services remain operational
- ✓ Exceptions documented and periodically reviewed

EVIDENCE TO RETAIN

- Service inventory and network listener review
- Approved change record with before/after evidence
- Remote access and sharing exception register

PRACTICAL NOTE

Service hardening recommendations are risk-based. Cyber Essentials does not prescribe disabling every optional Windows service.

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