secureX7

WINDOWS 11
USER ACCOUNT HARDENING
FOR CYBER ESSENTIALS

Apply least privilege and protect user access

PRACTICAL CYBER SECURITY. POWERED BY AI.

A practical guide for standalone and workgroup Windows 11 PCs

User accounts • Admin rights • Passwords • MFA

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

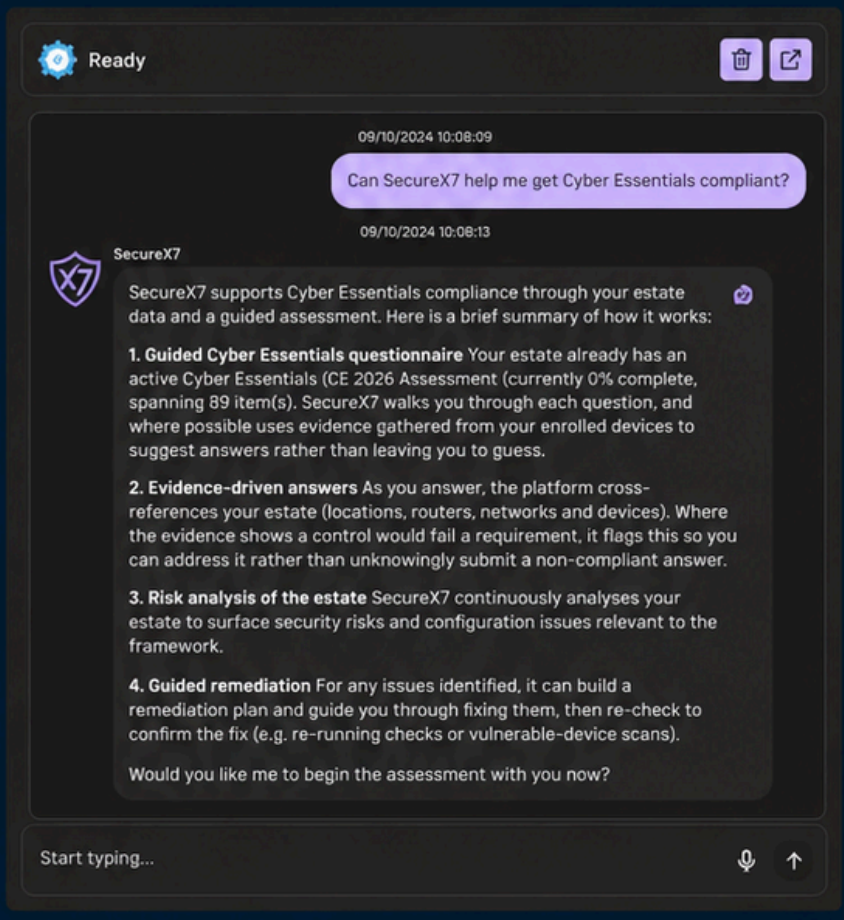
Prioritised remediation

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

Separate standard and admin use

Check account types

Settings > Accounts > Other users shows local account types. For Windows Pro, Computer Management > Local Users and Groups provides additional visibility.

Create separate administrator identity

Use a distinct administrator account for elevated maintenance. Daily activity should use a standard user account.

Inspect administrators

Run Get-LocalGroupMember -Group Administrators in PowerShell. Review every member and investigate unexpected group or account entries.

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

Strengthen authentication

Password policy

For local accounts on supported editions, review secpol.msc > Account Policies. Apply a defensible length and protection against password guessing.

Windows Hello

Configure sign-in options under Settings > Accounts > Sign-in options. Windows Hello is useful where available but does not replace cloud-service MFA requirements.

Cloud MFA

Review Microsoft 365 or other in-scope cloud-service authentication separately. Windows local account settings cannot establish cloud MFA compliance.

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

Manage joiners movers leavers

Joiners

Approve access, create a unique account and grant only required permissions.

Movers

Reassess application access and privileged roles when responsibilities change.

Leavers

Disable access promptly, revoke sessions where relevant and record completion. Review dormant and shared accounts periodically.

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

- ✓ Daily users do not routinely hold administrator rights
- ✓ Administrator accounts separate and restricted
- ✓ Authentication controls protect against guessing
- ✓ Cloud MFA and leaver processes evidenced where relevant

EVIDENCE TO RETAIN

- Local account and Administrators group review
- Password/lockout configuration evidence
- Cloud MFA report and access review records

PRACTICAL NOTE

Windows 11 Home lacks some local management consoles. Use available Settings, PowerShell and provider controls and document limitations.

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