secureX7

WINDOWS DEFENDER FIREWALL HARDENING FOR CYBER ESSENTIALS

Configure firewall profiles, inbound rules and exceptions

PRACTICAL CYBER SECURITY. POWERED BY AI.

A practical guide for standalone and workgroup Windows 11 PCs

Firewall • Network profiles • Inbound rules • Audit 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

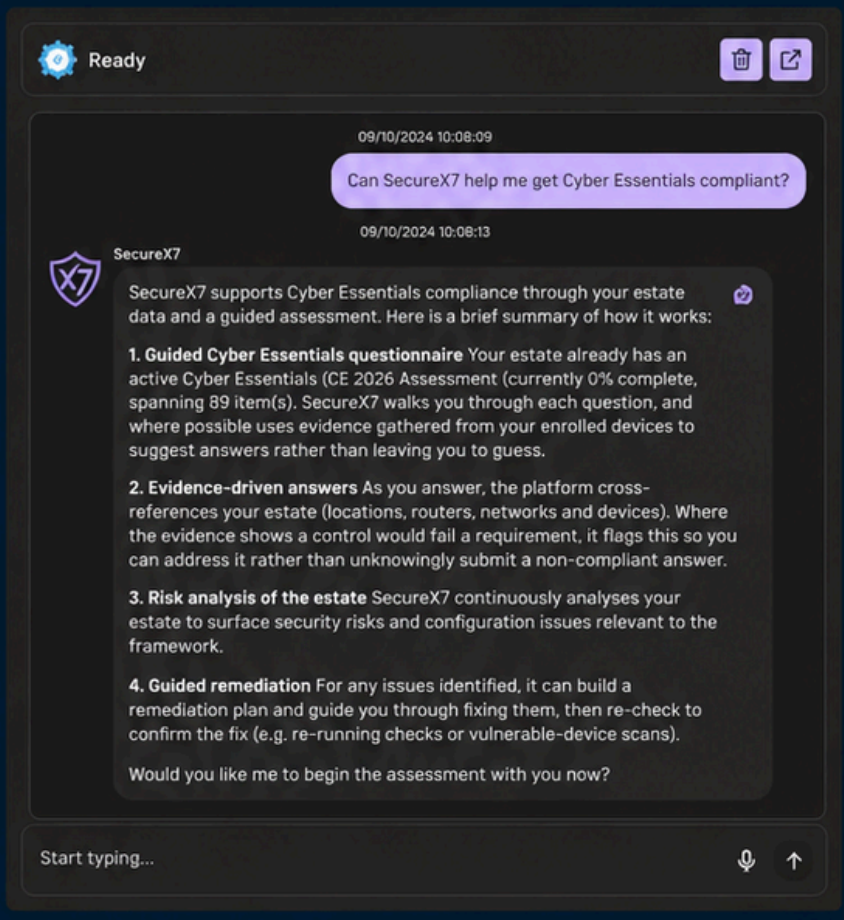
Prioritised remediation

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

Review firewall profiles

Open Windows Security

Windows Security > Firewall & network protection. Review Domain, Private and Public profiles. Confirm Microsoft Defender Firewall is enabled for every applicable profile.

Inspect policy in PowerShell

Run Get-NetFirewallProfile | Select Name,Enabled,DefaultInboundAction,DefaultOutboundAction in an elevated PowerShell window. Expect enabled profiles and a default inbound Block posture.

Avoid disabling protection

Do not disable the firewall to troubleshoot applications. Identify the required traffic and create a narrowly scoped exception instead.

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

Audit inbound rules

Open advanced firewall settings

Run wf.msc > Inbound Rules. Review enabled Allow rules and identify broad rules covering any program, any port or any remote address.

Minimise exceptions

Limit permitted rules by program, protocol, local port, remote address and network profile where possible. Disable obsolete rules after testing.

Record approvals

Maintain a register of rule purpose, system owner, approver, date, exposure and review date.

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

Protect remote and public access

Remote Desktop

If Remote Desktop is unnecessary, disable it under Settings > System > Remote Desktop. If required, restrict source networks and use secure remote access.

Public Wi-Fi

Confirm the Public profile remains enabled and appropriately restrictive. A laptop must be protected even when it is outside the office.

Router and cloud controls

Also review broadband router port forwarding and cloud network firewall rules: host-based firewall checks do not prove these are secure.

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

- ✓ Applicable firewall profiles enabled
- ✓ Unsolicited inbound connections blocked by default
- ✓ Exceptions narrowly scoped, justified and reviewed
- ✓ Remote administration not unnecessarily exposed

EVIDENCE TO RETAIN

- Profile settings and dated PowerShell output
- Exported or reviewed inbound-rule register
- Router or cloud rule evidence where in scope

PRACTICAL NOTE

Firewall protection should be checked on each relevant device configuration, not only one representative workstation.

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