secureX7

MICROSOFT DEFENDER ANTIVIRUS CONFIGURATION FOR CYBER ESSENTIALS

Verify malware protection, exclusions and resilience

PRACTICAL CYBER SECURITY. POWERED BY AI.

A practical guide for standalone and workgroup Windows 11 PCs

Antivirus • Threat protection • Exclusions • 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

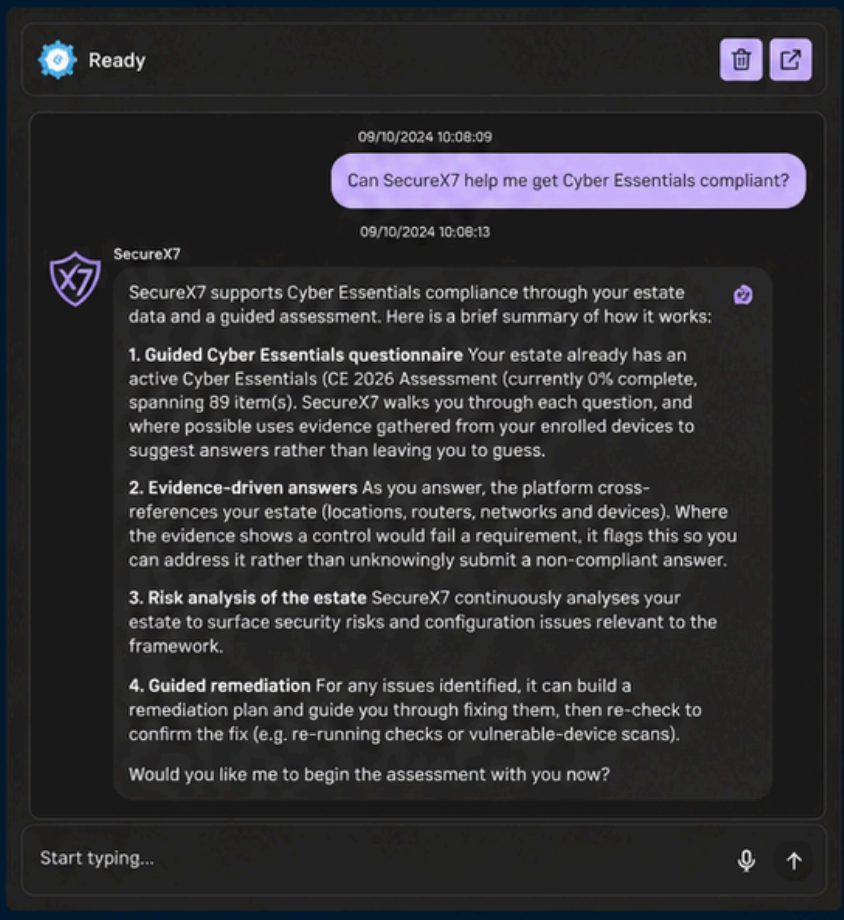
Prioritised remediation

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

Verify antivirus protection

Windows Security

Open Windows Security > Virus & threat protection > Manage settings. Check real-time protection, cloud-delivered protection and tamper protection.

PowerShell status

Use Get-MpComputerStatus and review AntivirusEnabled, RealTimeProtectionEnabled, AMServiceEnabled and AntivirusSignatureLastUpdated. Some properties depend on product mode and device policy.

Third-party antivirus

If another supported product is used, verify it is active and updated. Microsoft Defender may operate in passive mode; avoid assuming its disabled real-time protection means the device is unprotected.

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

Review exclusions and detection

Exclusions

Open Virus & threat protection > Manage settings > Exclusions. Remove obsolete or overly broad file, folder and process exclusions.

Protection updates

Use Windows Security > Virus & threat protection > Protection updates to check intelligence status. Investigate persistent update errors.

Detection and alerts

Review Protection history for unresolved detections and confirm alerts are investigated by an assigned owner.

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 malware resilience

Reputation-based protection

Review Windows Security > App & browser control > Reputation-based protection for SmartScreen and potentially unwanted application blocking.

Controlled folder access

Consider ransomware protection through Controlled folder access, but test approved applications before enforcing it broadly.

Backups and recovery

Maintain separate, recoverable backups and test restoration. Backups are an important resilience measure, although they are not a substitute for the Cyber Essentials malware control.

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

- ✓ Effective malware protection active on every in-scope PC
- ✓ Protection intelligence is current
- ✓ Exclusions justified and reviewed
- ✓ Unresolved malware warnings investigated

EVIDENCE TO RETAIN

- Windows Security protection screenshots
- Get-MpComputerStatus output where appropriate
- Exclusion review and detection-handling records

PRACTICAL NOTE

Cyber Essentials accepts more than one compliant malware-protection approach; confirm the chosen approach and its evidence.

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