



Hardening Microsoft Windows 11 Workstations

January 2026 changes

Last updated: January 2026

Executive Summary

Malicious actors often target workstations through malicious websites, emails, or removable media to extract sensitive information. Hardening workstations plays a critical role in reducing this risk.

This document summarises the changes introduced in the January 2026 update to the [Hardening Microsoft Windows 11 workstations](#) publication.

The update aligns guidance with Windows 11 version 25H2 and introduces new security recommendations, revised Group Policy settings, and updated terminology.

We added new hardening measures for auditing, printers, widgets, app installations, and SMB sessions. We also replaced references to Internet Explorer with Microsoft Edge, updated guidance for Windows Copilot, and included new options for operating system patching during OOBE.

Overall, the structure remains similar, but security posture is strengthened with additional controls and auditing capabilities.

Our goal is to help organisations quickly identify what has changed since the previous version (24H2) and understand the impact of these updates on their security posture.

Detailed Change Log

Section	Change type	Detail
Front-matter	Changed	Update: 24H2 Sep 2025 → 25H2 Jan 2026; Version baseline updated to Windows 11 25H2
Windows Copilot	Changed	GPO deprecated; now disable via PowerShell/AppLocker
Operating System Patching	Added	New GPO: Allow Updates in OOBE
Audit Event Management	Added	Enable CLFS log file authentication
Network Authentication	Added	NTLM Enhanced Logging and Domain-wide NTLM Logs
Printers	Added	Require IPPS for IPP printers; Set TLS/SSL policy for IPP printers
App Install Controls	Added	MSIX streaming install domain restrictions; Allowed package family names for non-admin installs
SMB Sessions	Added	Audit SMB client SPN support
Widgets	Added	Disable Widgets on lock screen and Widgets Board
Microsoft Store	Added	Remove default Microsoft Store packages

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2025

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>).

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/legalcode.en>).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>).



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre