Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Hardening Microsoft Windows 10 and Windows 11 workstations

First published: May 2017
Last updated: July 2024

Table of contents

Introduction

Workstations are often targeted by malicious actors using malicious websites, emails or removable media in an attempt to extract sensitive information. Hardening workstations is an important part of reducing this risk.

This publication provides recommendations on hardening workstations using Enterprise and Education editions of Microsoft Windows 10 and Windows 11. Before implementing recommendations in this publication, thorough testing should be undertaken to ensure the potential for unintended negative impacts on business processes is reduced as much as possible.

While this publication refers to workstations, most recommendations are equally applicable to servers (with the exception of Domain Controllers) using Microsoft Windows Server.

Security features discussed in this publication, along with the names and locations of Group Policy settings, are taken from Microsoft Windows 10 version 22H2 and Windows 11 version 23H2 – some differences will exist for earlier versions.

For cloud-based device managers, such as Microsoft Endpoint Manager, equivalents can be found for many of the Group Policy settings. Alternatively, there is often a function to import Group Policy settings into cloud-based device managers.

High priorities

The following recommendations, listed in alphabetical order, should be treated as high priorities when hardening Microsoft Windows 10 and Windows 11 workstations.

Application hardening

When applications are installed they are often not pre-configured in a secure state. By default, many applications enable functionality that isn't required by any users while in-built security functionality may be disabled or set at a lower security level. For example, Microsoft Office by default allows untrusted macros in Office documents to automatically execute without user interaction. To reduce this risk, applications should have any in-built security functionality enabled and appropriately configured along with unrequired functionality disabled. This is especially important for key applications such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .NET Framework). In addition, vendors may provide guidance on configuring their products securely. For example, Microsoft provides security baselines for their products on the Microsoft Security Baselines Blog. In such cases, vendor guidance should be followed to assist in securely configuring their products.

The Australian Signals Directorate also provides guidance for hardening Microsoft Office. For more information see the *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

Application versions and patches

While some vendors may release new application versions to address vulnerabilities, others may release patches. If new application versions and patches for applications are not installed it can allow malicious actors to easily compromise workstations. This is especially important for key applications that interact with content from untrusted sources such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash),

email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .NET Framework). To reduce this risk, new application versions and patches for applications should be applied in an appropriate timeframe as determined by the severity of vulnerabilities they address and any mitigating measures already in place. In cases where a previous version of an application continues to receive support in the form of patches, it still should be upgraded to the latest version to receive the benefit of any new security functionality.

For more information on determining the severity of vulnerabilities and timeframes for applying new application versions and patches for applications see the *Patching applications and operating systems* publication.

Application control

Malicious actors can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it. Such malicious code often aims to exploit vulnerabilities in existing applications and does not need to be installed to be successful. Application control can be an extremely effective mechanism in not only preventing malicious code from executing, but also ensuring only approved applications can be installed.

When developing application control rules, starting from scratch is a more secure method than relying on a list of executable content currently residing on a workstation. Furthermore, it is preferable that organisations define their own application control ruleset rather than relying on rulesets from application control vendors. This application control ruleset should then be regularly assessed to determine if it remains fit for purpose.

For more information on application control and how it can be appropriately implemented see the *Implementing application control* publication.

Attack surface reduction

Attack surface reduction (ASR), a security feature of Microsoft Windows 10 and Windows 11, forms part of Microsoft Defender Exploit Guard. It is designed to combat the threat of malware exploiting legitimate functionality in Microsoft Office applications. In order to use ASR, Microsoft Defender Antivirus must be configured as the primary real-time antivirus scanning engine on workstations. ASR offers a number of rules which are included below.

ASR Rule Name	Globally Unique Identifier
Block abuse of exploited vulnerable signed drivers	56a863a9-875e-4185-98a7-b882c64b5ce5
Block Adobe Reader from creating child processes	7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c
Block all Office applications from creating child processes	d4f940ab-401b-4efc-aadc-ad5f3c50688a
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
Block executable content from email client and webmail	be9ba2d9-53ea-4cdc-84e5-9b1eeee46550
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	01443614-cd74-433a-b99e-2ecdc07bfc25
Block execution of potentially obfuscated scripts	5beb7efe-fd9a-4556-801d-275e5ffc04cc

Block JavaScript or VBScript from launching downloaded executable content	d3e037e1-3eb8-44c8-a917-57927947596d
Block Office applications from creating executable content	3b576869-a4ec-4529-8536-b80a7769e899
Block Office applications from injecting code into other processes	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
Block Office communication application from creating child processes	26190899-1602-49e8-8b27-eb1d0a1ce869
Block persistence through WMI event subscription	e6db77e5-3df2-4cf1-b95a-636979351e5b
Block process creations originating from PSExec and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c
Block untrusted and unsigned processes that run from USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
Block Win32 API calls from Office macros	92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b
Use advanced protection against ransomware	c1db55ab-c21a-4637-bb3f-a12568109d35

Organisations should either implement ASR using Microsoft Defender Antivirus or use third-party antivirus solutions that offer similar functionality to those provided by ASR. For older versions of Microsoft Windows, alternative measures will need to be implemented to mitigate certain threats addressed by ASR, such as the likes of Dynamic Data Exchange (DDE) attacks.

For organisations using Microsoft Defender Antivirus, the following Group Policy settings can be implemented to enforce the above ASR rules.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction	
Configure Attack Surface Reduction rules	Enabled Set the state for each ASR rule: 56a863a9-875e-4185-98a7-b882c64b5ce5 1 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c 1 d4f940ab-401b-4efc-aadc-ad5f3c50688a 1 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 1 be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 1 01443614-cd74-433a-b99e-2ecdc07bfc25 1 5beb7efe-fd9a-4556-801d-275e5ffc04cc 1 d3e037e1-3eb8-44c8-a917-57927947596d 1 3b576869-a4ec-4529-8536-b80a7769e899 1

75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	1
26190899-1602-49e8-8b27-eb1d0a1ce869	1
e6db77e5-3df2-4cf1-b95a-636979351e5b	1
d1e49aac-8f56-4280-b9ba-993a6d77406c	1
b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	1
92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b	1
c1db55ab-c21a-4637-bb3f-a12568109d35	1

Credential protection

Cached credentials are stored in the Security Accounts Manager (SAM) database and can allow a user to log onto a workstation they have previously logged onto even if the domain is not available. Whilst this functionality may be desirable from an availability of services perspective, this functionality can be abused by malicious actors who can retrieve these cached credentials (potentially Domain Administrator credentials in a worst-case scenario). To reduce this risk, cached credentials should be limited to only one previous logon.

The following Group Policy settings can be implemented to disable credential caching.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	1 logons
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled

Within an active user session, credentials are cached within the Local Security Authority Subsystem Service (LSASS) process (including the user's passphrase in plaintext if WDigest authentication is enabled) to allow for access to network resources without users having to continually enter their credentials. Unfortunately, these credentials are at risk of theft by malicious actors. To reduce this risk, WDigest authentication should be disabled.

Credential Guard, a security feature of Microsoft Windows 10 and Windows 11, is also designed to assist in protecting the LSASS process.

The following Group Policy settings can be implemented to disable WDigest authentication as well as enable memory integrity and Credential Guard functionality, assuming all software, firmware and hardware prerequisites are met. Note, the MS Security Guide Group Policy settings are available as part of the *Microsoft Security Compliance Toolkit*.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
WDigest Authentication (disabling may require KB2871997)	Disabled
Computer Configuration\Policies\Administrative Templates\System\Device Guard	

Turn On Virtualization Based Security	Enabled Select Platform Security Level: Secure Boot and DMA Protection Virtualization Based Protection of Code Integrity: Enabled with UEFI lock Credential Guard Configuration: Enabled with UEFI lock Secure Launch Configuration: Enabled Kernel-mode Hardware-enforced Stack Protection: Enabled in enforcement mode
Computer Configuration\Policies\Administrative Templates\System\Local Security Authority	
Allow Custom SSPs and APs to be loaded into LSASS	Disabled
Configure LSASS to run as a protected process	Enabled Configure LSA to run as a protected process: Enabled with UEFI Lock

Controlled Folder Access

Controlled Folder Access, a security feature of Microsoft Windows 10 and Windows 11, forms part of Microsoft Defender Exploit Guard. It is designed to combat the threat of ransomware.

In order to use Controlled Folder Access, Microsoft Defender Antivirus must be configured as the primary real-time antivirus scanning engine on workstations. Other third-party antivirus solutions may offer similar functionality as part of their offerings.

The following Group Policy settings can be implemented to implement Controlled Folder Access.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Controlled Folder Access	
Configure allowed applications	Enabled Enter the applications that should be trusted: *<organisation defined>*
Configure Controlled folder access	Enabled Configure the guard my folders feature: Block
Configure protected folders	Enabled Enter the folders that should be guarded: *<organisation defined>*

Credential entry

When users enter their credentials on a workstation it provides an opportunity for malicious code, such as a key logging application, to capture the credentials. To reduce this risk, users should be authenticated by using a trusted path to enter their credentials on the Secure Desktop.

The following Group Policy settings can be implemented to ensure credentials are entered in a secure manner.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not display network selection UI	Enabled
Enumerate local users on domain-joined computers	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface	
Do not display the password reveal button	Enabled
Enumerate administrator accounts on elevation	Disabled
Require trusted path for credential entry	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options	
Disable or enable software Secure Attention Sequence	Disabled
Enable MPR notifications for the system	Disabled
Sign-in and lock last interactive user automatically after a restart	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Do not require CTRL+ALT+DEL	Disabled

Early Launch Antimalware

Another key security feature of Trusted Boot, supported by Microsoft Windows 10 and Windows 11 in combination with motherboards with an Unified Extensible Firmware Interface (UEFI), is Early Launch Antimalware (ELAM). Used in conjunction with Secure Boot, an ELAM driver can be registered as the first non-Microsoft driver that will be initialised on a workstation as part of the boot process, thus allowing it to verify all subsequent drivers before they are initialised. The ELAM driver is capable of allowing only known good drivers to initialise; known good and unknown drivers to initialise; known good, unknown and bad but critical drivers to initialise; or all drivers to initialise. To reduce the risk of malicious drivers, only known good and unknown drivers should be allowed to be initialised during the boot process.

The following Group Policy setting can be implemented to ensure only known good and unknown drivers will be initialised at boot time.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware	
Boot-Start Driver Initialization Policy	Enabled Choose the boot-start drivers that can be initialized: Good, unknown and bad but critical

Elevating privileges

Microsoft Windows provides the ability to require confirmation from users, via the User Access Control (UAC) functionality, before any sensitive actions are performed. The default settings allow privileged users to perform sensitive actions without first providing credentials and while standard users must provide privileged credentials they are not required to do so via a trusted path on the Secure Desktop. This provides an opportunity for malicious actors that gain access to an open session of a privileged user to perform sensitive actions at will or for malicious code to capture any credentials entered via a standard user when attempting to elevate their privileges. To reduce this risk, UAC functionality should be implemented to ensure all sensitive actions are authorised by providing credentials on the Secure Desktop.

The following Group Policy settings can be implemented to configure UAC functionality effectively.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Exploit protection

Malicious actors that develop exploits for Microsoft Windows or third-party applications will have a higher success rate when security measures designed by Microsoft to help prevent vulnerabilities from being exploited are not

implemented. Microsoft Defender's exploit protection functionality, a security feature of Microsoft Windows 10 and Windows 11, provides system-wide and application-specific security measures. Exploit protection is designed to replace the Enhanced Mitigation Experience Toolkit (EMET) that was used on earlier versions of Microsoft Windows 10.

System-wide security measures configurable via exploit protection include: Control Flow Guard (CFG), Data Execution Prevention (DEP), mandatory Address Space Layout Randomization (ASLR), bottom-up ASLR, Structured Exception Handling Overwrite Protection (SEHOP) and heap corruption protection.

Many more application-specific security measures are also available, however, they will require testing (either within a test environment or using audit mode) beforehand to limit the likelihood of any unintended consequences. As such, a staged approach to implementing application-specific security measures is prudent. In doing so, applications that ingest arbitrary untrusted data from the internet should be prioritised.

The following Group Policy settings can be implemented to define exploit protection settings and to prevent users from modifying these settings on their devices.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Exploit Guard\Exploit Protection	
Use a common set of exploit protection settings	Enabled Type the location (local path, UNC path, or URL) of the mitigation settings configuration XML file: *<organisation defined>*
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Security\App and browser protection	
Prevent users from modifying settings	Enabled

In addition, the following Group Policy setting can be implemented to ensure DEP is not disabled for File Explorer.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Turn off Data Execution Prevention for Explorer	Disabled

Furthermore, the following Group Policy setting can be implemented to force the use of SEHOP. Note, the MS Security Guide Group Policy settings are available as part of the *Microsoft Security Compliance Toolkit*.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Enabled Structured Exception Handling Overwrite Protection (SEHOP)	Enabled

Local administrator accounts

When built-in administrator accounts are used with common account names and passwords it can allow malicious actors that compromise these credentials on one workstation to easily transfer across the network to other workstations. Even if built-in administrator accounts are uniquely named and have unique passwords, malicious actors can still identify these accounts based on their security identifier (i.e. *S-1-5-21-domain-500*) and use this information to focus any attempts to brute force credentials on a workstation if they can get access to the SAM database. To reduce this risk, Microsoft's Local Administrator Password Solution (LAPS) needs to be used to ensure unique passphrases are used for each workstation. In addition, User Account Control restrictions should be applied to remote connections using such accounts. Note, the MS Security Guide Group Policy settings are available as part of the *Microsoft Security Compliance Toolkit*.

The following Group Policy settings can be implemented to secure the use of built-in administrator accounts.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Administrator account status	Enabled
Computer Configuration\Policies\Administrative Templates\Windows\LAPS	
Configure password backup directory	Enabled Backup directory: Active Directory *or* Backup directory: Azure Active Directory
Enable password encryption	Enabled
Name of administrator account to manage	Disabled
Password Settings	Enabled Password Complexity: Large letters + small letters + numbers + specials Password Length: 30 Password Age (Days): 365
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Apply UAC restrictions to local accounts on network logons	Enabled

Measured Boot

The third key security feature of Trusted Boot, supported by Microsoft Windows 10 and Windows 11 in combination with motherboards with both an UEFI and a Trusted Platform Module (TPM), is Measured Boot. Measured Boot is used to develop a reliable log of components that are initialised before the ELAM driver. This information can then be scrutinised by antimalware software for signs of tampering of boot components. To reduce the risk that malicious changes to boot components go unnoticed, Measured Boot should be used on workstations that support it.

Microsoft Edge

Microsoft Edge is a web browser that was first introduced in Microsoft Windows 10 to replace Internet Explorer 11. As Microsoft Edge contains enhanced security functionality (being based on the Chromium project) it should be used wherever possible.

For organisations using Microsoft Edge instead of third-party web browsers, a number of Group Policy settings can be configured (once the supporting Group Policy Administrative Templates have been installed) to harden the web browser, including Microsoft Defender SmartScreen. Recommended hardening guidance for Microsoft Edge is available from the Microsoft Security Baselines Blog.

Multi-factor authentication

As privileged credentials often allow users to bypass security functionality put in place to protect workstations, and are susceptible to key logging applications, it is important that they are appropriately protected against compromise. In addition, malicious actors that brute force captured password hashes can gain access to workstations if multi-factor authentication hasn't been implemented. To reduce this risk, hardware-based multi-factor authentication should be used for privileged users, remote access and any access to important or sensitive data repositories.

Organisations may consider whether Windows Hello for Business (WHfB) is suitable for their environment. Notably, WHfB can be configured with a personal identification number (PIN) or face/fingerprint recognition to unlock the use of asymmetric cryptography stored in a TPM in order to authenticate users. Note, the use of TPMs places additional importance on patching TPMs for vulnerabilities and decommissioning those devices that are not able to be patched. Organisations may also choose to enforce the use of the latest versions of TPMs when using WHfB. Finally, Microsoft has issued guidance on the use of FIDO2 security tokens as part of multi-factor authentication for Microsoft Windows logons.

The following Group Policy settings can be implemented to enable WHfB with either the use of biometrics or PINs.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\PIN Complexity	
Expiration	Enabled PIN Expiration: 365
Minimum PIN length	Enabled Minimum PIN length: 6
Computer Configuration\Policies\Administrative Templates\Windows Components\Biometrics\Facial Features	
Configure enhanced anti-spoofing	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Hello for Business	
Use a hardware security device	Enabled Do not use the following security devices: TPM 1.2
Use biometrics	Enabled

Use Windows Hello for Business	Enabled

For more information on how to effectively implement multi-factor authentication see the *Implementing multi-factor authentication* publication.

Operating system architecture

The x64 (64-bit) versions of Microsoft Windows include additional security functionality that the x86 (32-bit) versions lack. This includes native hardware-based Data Execution Prevention (DEP) kernel support, Kernel Patch Protection (PatchGuard), mandatory device driver signing and lack of support for malicious 32-bit drivers. Using x86 (32-bit) versions of Microsoft Windows exposes organisations to exploit techniques mitigated by x64 (64-bit) versions of Microsoft Windows. To reduce this risk, workstations should use the x64 (64-bit) versions of Microsoft Windows.

Operating system patching

Patches are released either in response to previously disclosed vulnerabilities or to proactively address vulnerabilities that have not yet been publicly disclosed. In the case of disclosed vulnerabilities, it is possible that exploits have already been developed and are freely available in common hacking tools. In the case of patches for vulnerabilities that have not yet been publically disclosed, it is relatively easy for malicious actors to use freely available tools to identify the vulnerability being patched and develop an associated exploit. This activity can be undertaken in less than one day and has led to an increase in 1-day attacks. To reduce this risk, operating system patches and driver updates should be centrally managed, deployed and applied in an appropriate timeframe as determined by the severity of the vulnerability and any mitigating measures already in place.

Previously, operating system patching was typically achieved by using Microsoft Endpoint Configuration Manager, or Microsoft Windows Server Update Services (WSUS), along with Wake-on-LAN functionality to facilitate patching outside of core business hours. However, Windows Update for Business may replace or supplement many WSUS functions. Configuration of Windows Update for Business can be applied through Group Policy settings or the equivalent settings in Microsoft Endpoint Manager. Microsoft has also issued guidance on common misconfigurations relating to Windows updates.

For more information on determining the severity of vulnerabilities and timeframes for applying patches see the *Patching applications and operating systems* publication.

The following Group Policy settings can be implemented to ensure operating systems remain appropriately patched.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage end user experience	
Configure Automatic Updates	Enabled Configure automatic updating: 4 - Auto download and schedule the install Scheduled install day: 0 - Every day Scheduled install time: *<organisation defined>* Install updates for other Microsoft products
Remove access to “Pause updates” feature	Enabled

Remove access to use all Windows Update features	Disabled

Furthermore, if a Windows Server Update Services (WSUS) server is used, the following Group Policy setting can be implemented.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Manage updates offered from Windows Server Update Service	
Specify intranet Microsoft update service location	Enabled Set the intranet update service for detecting updates: *<server:port>*

Operating system version

Microsoft Windows 10 and Windows 11 have introduced improvements in security functionality over previous versions of Microsoft Windows. This has made it more difficult for malicious actors to craft reliable exploits for vulnerabilities they discovered. Using older versions of Microsoft Windows, including previous versions of Microsoft Windows 10 and Windows 11, exposes organisations to exploit techniques that have since been mitigated in newer versions of Microsoft Windows. To reduce this risk, workstations should use the latest version of Microsoft Windows 10 or Windows 11.

Restricting privileged accounts

Providing users with a privileged account for day to day usage poses a risk that they will use this account for external web and email access. This is of particular concern as privileged users have the ability to execute malicious code with privileged access rather than standard access. To reduce this risk, users that don't require privileged access should not be granted privileged accounts while users that require privileged access should have separate standard and privileged accounts with different credentials. In addition, any privileged accounts used should have external web and email access blocked.

For more information on the use of privileged accounts and minimising their usage see the *Restricting administrative privileges* publication.

Secure Boot

Another method for malicious code to maintain persistence and prevent detection is to replace the default boot loader for Microsoft Windows with a malicious version. In such cases the malicious boot loader executes at boot time and loads Microsoft Windows without any indication that it is present. Such malicious boot loaders are extremely difficult to detect and can be used to conceal malicious code on workstations. To reduce this risk, motherboards with Secure Boot functionality should be used. Secure Boot, a component of Trusted Boot, is a security feature of Microsoft Windows 10 and Windows 11 in combination with motherboards with an UEFI. Secure Boot works by checking at boot time that the boot loader is signed and matches a Microsoft signed certificate stored in the UEFI. If the certificate signatures match the boot loader is allowed to run, otherwise it is prevented from running and the workstation will not boot.

Medium priorities

The following recommendations, listed in alphabetical order, should be treated as medium priorities when hardening Microsoft Windows 10 and Windows 11 workstations.

Account lockout policy

Allowing unlimited attempts to access workstations will fail to prevent malicious actors' attempts to brute force authentication measures. To reduce this risk, accounts should be locked out after a defined number of invalid authentication attempts. The threshold for locking out accounts does not need to be overly restrictive in order to be effective. For example, a threshold of 5 incorrect attempts, with a reset period of 15 minutes for the lockout counter, will prevent any brute force attempt while being unlikely to lock out a legitimate user who accidently enters their password incorrectly a few times.

The following Group Policy settings can be implemented to achieve a reasonable lockout policy.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	
Account lockout duration	0
Account lockout threshold	5 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	15 minutes

Anonymous connections

Malicious actors can use anonymous connections to gather information about the state of workstations. Information that can be gathered from anonymous connections (i.e. using the *net use* command to connect to the IPC$ share) can include lists of users and groups, SIDs for accounts, lists of shares, workstation policies, operating system versions and patch levels. To reduce this risk, anonymous connections to workstations should be disabled.

The following Group Policy settings can be implemented to disable the use of anonymous connections.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation	
Enable insecure guest logons	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network access: Allow anonymous SID/Name translation	Disabled

Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	O:BAG:BAD:(A;;RC;;;BA)
Network security: Allow LocalSystem NULL session fallback	Disabled

Antivirus software

Malicious actors can develop malicious code to exploit vulnerabilities in software not detected and remedied by vendors during testing. As significant time and effort is often involved in the development of functioning and reliable exploits, malicious actors will often reuse their exploits as much as possible before being forced to develop new exploits. To reduce this risk, endpoint security applications with signature-based antivirus functionality should be implemented. In doing so, signatures should be updated at least on a daily basis.

Whilst using signature-based antivirus functionality can assist in reducing risk, they are only effective when a particular piece of malicious code has already been profiled and signatures are current. Malicious actors can create variants of known malicious code, or develop new unseen malicious code, to bypass traditional signature-based detection mechanisms. To reduce this risk, endpoint security applications with host-based intrusion prevention functionality, or equivalent functionality leveraging cloud-based services, should also be implemented. In doing so, such functionality should be set at the highest level available.

If using Microsoft Defender Antivirus, the following Group Policy settings can be implemented to optimally configure it.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus	
Configure detection for potentially unwanted applications	Enabled Block
Configure local administrator merge behaviour for lists	Disabled
Control whether or not exclusions are visible to Local Admins	Enabled

Turn off Microsoft Defender Antivirus	Disabled
Turn off routine remediation	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MAPS	
Configure local setting override for reporting to Microsoft MAPS	Disabled
Configure the 'Block at First Sight' feature	Enabled
Join Microsoft MAPS	Enabled Join Microsoft MAPS: Advanced MAPS
Send file samples when further analysis is required	Enabled Send file samples when further analysis is required: Send all samples
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine	
Configure extended cloud check	Enabled Specify the extended cloud check time in seconds: 50
Enable file hash computation feature	Enabled
Select cloud protection level	Enabled Select cloud blocking level: High blocking level *or* Select cloud blocking level: High+ blocking level
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Quarantine	
Configure removal of items from Quarantine folder	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-time Protection	
Monitor file and program activity on your computer	Enabled
Scan all downloaded files and attachments	Enabled
Turn off real-time protection	Disabled
Turn on behavior monitoring	Enabled

Turn on process scanning whenever real-time protection is enabled	Enabled
Turn on script scanning	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Scan	
Allow users to pause scan	Disabled
Check for the latest virus and spyware security intelligence before running a scheduled scan	Enabled
Scan archive files	Enabled
Scan packed executables	Enabled
Scan removable drives	Enabled
Turn on e-mail scanning	Enabled
Turn on heuristics	Enabled

Attachment Manager

The Attachment Manager within Microsoft Windows works in conjunction with applications such as the Microsoft Office suite and Internet Explorer to help protect workstations from attachments that have been received via email or downloaded from the internet. The Attachment Manager classifies files as high, medium or low risk based on the zone they originated from and the type of file. Based on the risk to the workstation, the Attachment Manager will either issue a warning to a user or prevent them from opening a file. If zone information is not preserved, or can be removed, it can allow malicious actors to socially engineer a user to bypass protections afforded by the Attachment Manager. To reduce this risk, the Attachment Manager should be configured to preserve and protect zone information for files.

The following Group Policy settings can be implemented to ensure zone information associated with attachments is preserved and protected.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager	
Do not preserve zone information in file attachments	Disabled
Hide mechanisms to remove zone information	Enabled

Audit event management

Failure to capture and analyse security-related audit events from workstations can result in cybersecurity intrusions going unnoticed. In addition, the lack of such information can significantly hamper investigations following a

cybersecurity incident. To reduce this risk, security-related audit events from workstations should be captured and routinely analysed.

The following Group Policy settings can be implemented to ensure security-related audit events are appropriately captured and synchronised.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation	
Include command line in process creation events	Enabled
Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers	
Configure Windows NTP Client	Enabled NtpServer: *<organisation defined>*
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\ Application	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 65536
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 2097152
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 65536
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Manage auditing and security log	Administrators

Furthermore, the following Group Policy settings can be implemented to enable a comprehensive auditing strategy.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Audit Policies\Account Management	
Audit Computer Account Management	Success and Failure
Audit Other Account Management Events	Success and Failure

Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Audit Policies\Detailed Tracking	
Audit Process Creation	Success
Audit Process Termination	Success
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Audit Policies\Logon/Logoff	
Audit Account Lockout	Failure
Audit Group Membership	Success
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Audit Policies\Object Access	
Audit File Share	Success and Failure
Audit File System	Success and Failure
Audit Kernel Object	Success and Failure
Audit Other Object Access Events	Success and Failure
Audit Registry	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Audit Policies\Policy Change	
Audit Audit Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Audit Policies\System	

Audit System Integrity	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Change the system time	Administrators LOCAL SERVICE

Autoplay and AutoRun

When enabled, Autoplay will automatically begin reading from a drive or media source as soon as it is used with a workstation, while AutoRun commands, generally in an autorun.inf file on the media, can be used to automatically execute any file on the media without user interaction. This functionality can be exploited by malicious actors to automatically execute malicious code. To reduce this risk, Autoplay and AutoRun functionality should be disabled.

The following Group Policy settings can be implemented to disable Autoplay and AutoRun functionality.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies	
Disallow Autoplay for non-volume devices	Enabled
Set the default behavior for AutoRun	Enabled Default AutoRun Behavior: Do not execute any autorun commands
Turn off Autoplay	Enabled Turn off Autoplay on: All drives

Boot devices

By default, workstations are often configured to boot from optical media, or even USB media, in preference to hard drives. Malicious actors with physical access to such workstations can boot from their own media in order to gain access to the content of the hard drives. With this access, malicious actors can reset local user account passwords or gain access to the local SAM database to steal password hashes for offline brute force cracking attempts. To reduce this risk, workstations should be restricted to only booting from the designated primary system drive.

Bridging networks

When workstations have multiple network interfaces, such as an Ethernet interface and a wireless interface, it is possible to establish a bridge between the connected networks. For example, when using an Ethernet interface to connect to an organisation's wired network and a wireless interface to connect to another non-organisation controlled network such as a public wireless hotspot. When bridges are created between such networks malicious actors can directly access the wired network from the wireless network to extract sensitive information. To reduce

this risk, the ability to install and configure network bridges between different networks should be disabled. This won't prevent malicious actors from compromising a workstation via the wireless network and then using malicious software as a medium to indirectly access the wired network. This can only be prevented by manually disabling all wireless interfaces when connecting to wired networks.

The following Group Policy settings can be implemented to disable the ability to install and configure network bridges.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\Network Connections	
Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled
Minimize the number of simultaneous connections to the Internet or a Windows Domain	Enabled Minimize Policy Options: 3 = Prevent Wi-Fi when on Ethernet
Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager	
Prohibit connection to non-domain networks when connected to domain authenticated network	Enabled

Built-in guest accounts

When built-in guest accounts are used, it can allow malicious actors to log onto a workstation over the network without first needing to compromise legitimate user credentials. To reduce this risk, built-in guest accounts should be disabled.

The following Group Policy settings can be implemented to disable and rename built-in guest accounts.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Guest account status	Disabled

CD burner access

If CD burning functionality is enabled, and CD burners are installed in workstations, malicious actors may attempt to steal sensitive information by burning it to CD. To reduce this risk, users should not have access to CD burning functionality except when explicitly required.

The following Group Policy setting can be implemented to prevent access to CD burning functionality, although as this Group Policy setting only prevents access to native CD burning functionality in Microsoft Windows, users should also be prevented from installing third-party CD burning applications. Alternatively, CD readers can be used in workstations instead of CD burners.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Remove CD Burning features	Enabled

Centralised audit event logging

Storing audit event logs on workstations poses a risk that malicious actors could attempt to modify or delete these logs during an intrusion to cover their tracks. In addition, failure to conduct centralised audit event logging will reduce the visibility of audit events across all workstations, prevent the correlation of audit events and increase the complexity of any investigations after cybersecurity incidents. To reduce this risk, audit event logs from workstations should be transferred to a secure central logging server.

Command Prompt

Malicious actors who gain access to a workstation can use the Command Prompt to execute in-built Microsoft Windows tools to gather information about the workstation or domain as well as schedule malicious code to execute on other workstations on the network. To reduce this risk, users should not have Command Prompt access or the ability to execute batch files and scripts. Should a legitimate business requirement exist to allow users to execute batch files (e.g. cmd and bat files); run logon, logoff, startup or shutdown batch file scripts; or use Remote Desktop Services, this risk will need to be accepted.

The following Group Policy setting can be implemented to prevent access to the Command Prompt and script processing functionality.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\System	
Prevent access to the command prompt	Enabled Disable the command prompt script processing also: Yes

Direct Memory Access

Communications interfaces that use Direct Memory Access (DMA) can allow malicious actors with physical access to a workstation to directly access the contents of a workstation's memory. This can be used to read sensitive contents such as cryptographic keys or to write malicious code directly into memory. To reduce this risk, communications interfaces that allow DMA (e.g. FireWire and Thunderbolt) should be disabled. This can be achieved either physically (e.g. using epoxy) or by using software controls (e.g. disabling the functionality in the UEFI, disabling the FireWire and Thunderbolt controllers, removing the SBP-2 driver, or using an end point protection solution).

The following Group Policy settings can be implemented to disable the FireWire and Thunderbolt controllers, remove the SBP-2 driver, and enable Kernel DMA Protection (a security feature of Microsoft Windows 10 and Windows 11).

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions	

Prevent installation of devices that match any of these device IDs	Enabled Prevent installation of devices that match any of these Device IDs: PCI\CC_0C0010, PCI\CC_0C0A Also apply to matching devices that are already installed.
Prevent installation of devices using drivers that match these device setup classes	Enabled Prevent installation of devices using drivers for these device setup classes: {d48179be-ec20-11d1-b6b8-00c04fa372a7} Also apply to matching devices that are already installed.
Computer Configuration\Policies\Administrative Templates\System\Kernel DMA Protection	
Enumeration policy for external devices incompatible with Kernel DMA Protection	Enabled Enumeration policy: Block All

Drive encryption

Malicious actors with physical access to a workstation may be able to use a bootable CD/DVD or USB media to load their own operating environment. From this environment, they can access the local file system to gain access to sensitive information or the SAM database to access password hashes. In addition, malicious actors that gain access to a stolen or unsanitised hard drive, or other removable media, will be to recover its contents when connected to another machine on which they have administrative access and can take ownership of files. To reduce this risk, AES-based full disk encryption should be used to protect the contents of hard drives from unauthorised access. The use of full disk encryption may also contribute to streamlining media sanitisation during decommissioning processes.

If Microsoft BitLocker is used, the following Group Policy settings should be implemented.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption	
Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)	Enabled Select the encryption method for operating system drives: XTS-AES 128-bit (default) Select the encryption method for fixed data drives: XTS-AES 128-bit (default) Select the encryption method for removable data drives: XTS-AES 128-bit
Disable new DMA devices when this computer is locked	Enabled
Prevent memory overwrite on restart	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\ Fixed Data Drives	

Choose how BitLocker-protected fixed drives can be recovered	Enabled Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for fixed data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives
Configure use of passwords for fixed data drives	Enabled Require password for fixed data drive Configure password complexity for fixed data drives: Require password complexity Minimum password length for fixed data drive: 14
Deny write access to fixed drives not protected by BitLocker	Enabled
Enforce drive encryption type on fixed data drives	Enabled Select the encryption type: Full encryption
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\ Operating System Drives	
Allow devices compliant with InstantGo or HSTI to opt out of pre-boot PIN.	Disabled
Allow enhanced PINs for startup	Enabled
Allow network unlocked at startup	Enabled
Allow Secure Boot for integrity validation	Enabled
Choose how BitLocker-protected operating system drives can be recovered	Enabled Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard

	Save BitLocker recovery information to AD DS for operating system drives Configure storage of BitLocker recovery information to AD DS: Store recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for operating system drives
Configure minimum PIN length for startup	Enabled Minimum characters: 14
Configure use of passwords for operating system drives	Enabled Configure password complexity for operating system drives: Require password complexity Minimum password length for operating system drive: 14
Disallow standard users from changing the PIN or password	Disabled
Enforce drive encryption type on operating system drives	Enabled Select the encryption type: Full encryption
Require additional authentication at startup	Enabled Settings for computers with a TPM Configure TPM startup: Do not allow TPM Configure TPM startup PIN: Allow startup PIN with TPM Configure TPM startup key: Allow startup key with TPM Configure TPM startup key and PIN: Allow startup key and PIN with TPM
Reset platform validation data after BitLocker recovery	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\ Removable Data Drives	
Choose how BitLocker-protected removable drives can be recovered	Enabled Allow data recovery agent Configure user storage of BitLocker recovery information: Allow 48-digit recovery password Allow 256-bit recovery key Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for removable data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages

	Do not enable BitLocker until recovery information is stored to AD DS for removable data drives
Configure use of passwords for removable data drives	Enabled Require password for removable data drive Configure password complexity for removable data drives: Require password complexity Minimum password length for removable data drive: 14
Control use of BitLocker on removable drives	Enabled Allow users to apply BitLocker protection on removable data drives
Deny write access to removable drives not protected by BitLocker	Enabled
Enforce drive encryption type on removable data drives	Enabled Select the encryption type: Full encryption
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Machine account lockout threshold	10

Endpoint device control

Malicious actors with physical access to a workstation may attempt to connect unauthorised USB media or other devices with mass storage functionality (e.g. smartphones, digital music players or cameras) to facilitate malicious code infections or the unauthorised copying of sensitive information. To reduce this risk, endpoint device control functionality should be appropriately implemented to control the use of all removable storage devices.

The following Group Policy setting can be implemented to disable the use of removable storage devices.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access	
All Removable Storage classes: Deny all access	Enabled

Alternatively, if specific classes of removable storage devices are required to meet business requirements, the execute, read and write permissions should be controlled on a class by class basis.

The following Group Policy settings provide a sample implementation that allows data to be read from but not executed from or written to common classes of removable storage devices.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access	

CD and DVD: Deny execute access	Enabled
CD and DVD: Deny read access	Disabled
CD and DVD: Deny write access	Enabled
Removable Disks: Deny execute access	Enabled
Removable Disks: Deny read access	Disabled
Removable Disks: Deny write access	Enabled
Tape Drives: Deny execute access	Enabled
Tape Drives: Deny read access	Disabled
Tape Drives: Deny write access	Enabled
WPD Devices: Deny read access	Disabled
WPD Devices: Deny write access	Enabled

File and print sharing

Users sharing files from their workstations can result in a lack of appropriate access controls being applied to sensitive information and the potential for the propagation of malicious code should file shares have read/write access. To reduce this risk, local file and print sharing should be disabled. Ideally, sensitive information should be centrally managed (e.g. on a network share with appropriate access controls). Disabling file and print sharing will not affect a user's ability to access shared drives and printers on a network.

The following Group Policy settings can be implemented to prevent users from sharing files.

Group Policy Setting	Recommended Option
User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing	
Prevent users from sharing files within their profile.	Enabled

Group Policy processing

Relying on users to set Group Policy settings for their workstations creates the potential for users to inadvertently misconfigure or disable security functionality without consideration of the impact on the security posture of the workstation. Alternatively, malicious actors could exploit this to disable any Local Group Policy settings that are hampering their efforts to extract sensitive information. To reduce this risk, all audit, user rights and security related Group Policy settings should be specified for workstations at an organisational unit or domain level. To ensure these policies aren't weakened, support for Local Group Policy settings should also be disabled.

The following Group Policy settings can be implemented to ensure only domain-based Group Policy settings are obtained and applied to workstations in a secure manner.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\Network Provider	
Hardened UNC Paths	Enabled Hardened UNC Paths: *\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 *\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1
Computer Configuration\Policies\Administrative Templates\System\Group Policy	
Configure registry policy processing	Enabled Do not apply during periodic background processing = False Process even if the Group Policy objects have not changed = Enabled
Configure security policy processing	Enabled Do not apply during periodic background processing = False Process even if the Group Policy objects have not changed = Enabled

Installing applications

While the ability to install applications may be a business requirement for users, this privilege can be exploited by malicious actors. Malicious actors can email a malicious application, or host a malicious application on a compromised website, and use social engineering techniques to convince users into installing the application on their workstation. Even if privileged access is required to install applications, users will use their privileged access if they believe, or can be convinced that, the requirement to install the application is legitimate. Additionally, if applications are configured to install using elevated privileges, malicious actors can exploit this by creating a Windows Installer installation package to create a new account that belongs to the local built-in administrators group or to install a malicious application.

The following Group Policy settings can be implemented to control application installations.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Configure Windows Defender SmartScreen	Enabled Pick one of the following settings: Warn and prevent bypass

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender SmartScreen\Explorer	
Configure Windows Defender SmartScreen	Enabled Pick one of the following settings: Warn and prevent bypass
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	
Allow user control over installs	Disabled
Always install with elevated privileges	Disabled
User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	
Always install with elevated privileges	Disabled

Legacy and run once lists

Once malicious code has been copied to a workstation, malicious actors with registry access can remotely schedule it to execute (i.e. using the run once list) or to automatically execute each time Microsoft Windows starts (i.e. using the legacy run list). To reduce this risk, legacy and run once lists should be disabled. This may interfere with the operation of legitimate applications that need to automatically execute each time Microsoft Windows starts. In such cases, the *Run these programs at user logon* Group Policy setting can be used to perform the same function in a more secure manner when defined at a domain level; however, if not used this Group Policy setting should be disabled rather than left in its default undefined state.

The following Group Policy settings can be implemented to disable the use of legacy and run once lists.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not process the legacy run list	Enabled
Do not process the run once list	Enabled
Run these programs at user logon	Disabled

Microsoft accounts

A feature of Microsoft Windows 10 and Windows 11 is the ability to link Microsoft accounts (formerly Windows Live IDs) to local or domain accounts. When this occurs, a user's settings and files are stored in the cloud using OneDrive rather than locally or on a domain controller. While this may have the benefit of allowing users to access their settings and files from any workstation (e.g. corporate workstation, home PC, internet cafe) it can also pose a risk to an organisation as they lose control over where sensitive information may be accessed from. To reduce this risk, users should not link Microsoft accounts with local or domain accounts.

The following Group Policy settings can be implemented to disable the ability to link Microsoft accounts to local or domain accounts.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime	
Allow Microsoft accounts to be optional	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft account	
Block all consumer Microsoft account user authentication	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive	
Prevent the usage of OneDrive for file storage	Enabled

MSS settings

MSS settings are registry values previously identified by Microsoft security experts that can be used for increased security. While many of these registry values are no longer applicable in modern versions of Microsoft Windows, some still provide a security benefit. By failing to specify these MSS settings, malicious actors may be able to exploit weaknesses in a workstation's security posture to gain access to sensitive information. To reduce this risk, MSS settings that are still relevant to modern versions of Microsoft Windows should be specified using Group Policy settings.

The Group Policy Administrative Templates for MSS settings are available from the Microsoft Security Guidance blog. The ADMX and ADML files can be placed in *%SystemDrive%\Windows\SYSVOL\domain\Policies\PolicyDefinitions* on the Domain Controller and they will automatically be loaded in the Group Policy Management Editor.

The following Group Policy settings can be implemented to configure MSS settings that are still relevant to modern versions of Microsoft Windows.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MSS (Legacy)	
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	Enabled DisableIPSourceRoutingIPv6: Highest protection, source routing is completely disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Enabled DisableIPSourceRouting: Highest protection, source routing is completely disabled
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled

NetBIOS over TCP/IP

NetBIOS over TCP/IP facilitates a number of intrusion methods. To reduce this risk, NetBIOS over TCP/IP should be disabled for all network interfaces. As NetBIOS over TCP/IP is only used to support legacy Microsoft Windows

operating systems, such as those prior to Microsoft Windows 2000, there shouldn't be a business requirement for its use except in very rare circumstances. NetBIOS over TCP/IP can be disabled by setting the NetBIOS settings under the IPv4 WINS settings on each network interface to *Disable NetBIOS over TCP/IP*. NetBIOS over TCP/IP is not supported by IPv6.

Network authentication

Using insecure network authentication methods may allow malicious actors to gain unauthorised access to network traffic and services. To reduce this risk, only secure network authentication methods, ideally Kerberos, should be used for network authentication.

The following Group Policy settings can be implemented to configure Kerberos, and if required for legacy purposes, the use of NTLMv2.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Configure encryption types allowed for Kerberos	AES128_HMAC_SHA1 AES256_HMAC_SHA1
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption

NoLMHash policy

When Microsoft Windows hashes a password that is less than 15 characters, it stores both a LAN Manager hash (LM hash) and Windows NT hash (NT hash) in the local SAM database for local accounts, or in Activity Directory for domain accounts. The LM hash is significantly weaker than the NT hash and can easily be brute forced. To reduce this risk, the NoLMHash Policy should be implemented on all workstations and domain controllers. As the LM hash is designed for authentication of legacy Microsoft Windows operating systems, such as those prior to Microsoft Windows 2000, there shouldn't be a business requirement for its use except in very rare circumstances.

The following Group Policy setting can be implemented to prevent the storage of LM hashes for passwords. All users should be encouraged to change their password once this Group Policy setting has been set as until they do they will remain vulnerable.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Do not store LAN Manager hash value on next password change	Enabled

Operating system functionality

Leaving unneeded functionality in Microsoft Windows enabled can provide greater opportunities for potentially vulnerable or misconfigured functionality to be exploited by malicious actors. To reduce this risk, unneeded functionality in Microsoft Windows should be disabled or removed.

Password and logon authentication policy

The use of weak passwords, such as eight character passwords with no complexity, can allow them to be brute forced within minutes using applications freely available on the web. To reduce this risk, a secure password policy should be implemented.

The following Group Policy settings can be implemented to achieve a secure single-factor password policy. Note, Group Policy settings for passwords used as part of multi-factor authentication may not need to be as stringent (e.g. they can be a length of 6 characters without complexity).

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Turn off picture password sign-in	Enabled
Turn on convenience PIN sign-in	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy	
Maximum password age	365 days
Minimum password length	14 characters
Relax minimum password length limits	Enabled
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Power management

One method of reducing power usage by workstations is to enter a sleep, hibernation or hybrid sleep state after a pre-defined period of inactivity. When a workstation enters a sleep state it maintains the contents of memory while powering down the rest of the workstation; with hibernation or hybrid sleep, it writes the contents of memory to the hard drive in a hibernation file (hiberfil.sys) and powers down the rest of the workstation. When this occurs, sensitive information such as encryption keys could either be retained in memory or written to the hard drive in a hibernation file. Malicious actors with physical access to the workstation and either the memory or hard drive can recover the

sensitive information using forensic techniques. To reduce this risk, sleep, hibernation and hybrid sleep states should be disabled.

The following Group Policy settings can be implemented to ensure that sleep, hibernation and hybrid sleep states are disabled.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings	
Allow standby states (S1-S3) when sleeping (on battery)	Disabled
Allow standby states (S1-S3) when sleeping (plugged in)	Disabled
Require a password when a computer wakes (on battery)	Enabled
Require a password when a computer wakes (plugged in)	Enabled
Specify the system hibernate timeout (on battery)	Enabled System Hibernate Timeout (seconds): 0
Specify the system hibernate timeout (plugged in)	Enabled System Hibernate Timeout (seconds): 0
Specify the system sleep timeout (on battery)	Enabled System Sleep Timeout (seconds): 0
Specify the system sleep timeout (plugged in)	Enabled System Sleep Timeout (seconds): 0
Specify the unattended sleep timeout (on battery)	Enabled Unattended Sleep Timeout (seconds): 0
Specify the unattended sleep timeout (plugged in)	Enabled Unattended Sleep Timeout (seconds): 0
Turn off hybrid sleep (on battery)	Enabled
Turn off hybrid sleep (plugged in)	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Show hibernate in the power options menu	Disabled
Show sleep in the power options menu	Disabled

PowerShell

Allowing any PowerShell script to execute exposes a workstation to the risk that a malicious script may be unwittingly executed by a user. To reduce this risk, users should not have the ability to execute PowerShell scripts; however, if using PowerShell scripts is an essential business requirement, only signed scripts should be allowed to execute. Ensuring that only signed scripts are allowed to execute can provide a level of assurance that a script is trusted and has been endorsed as having a legitimate business purpose.

For more information on how to effectively implement PowerShell see the *Securing PowerShell in the enterprise* publication.

The following Group Policy settings can be implemented to control the use of PowerShell scripts.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on Module Logging	Enabled Module Names: *
Turn on PowerShell Script Block Logging	Enabled
Turn on PowerShell Transcription	Enabled Transcript output directory: *<organisation defined>*
Turn on Script Execution	Enabled Execution Policy: Allow only signed scripts

Printers

Malicious actors may attempt to install malicious printer drivers in order to introduce vulnerabilities to systems. Alternatively, malicious actors may look to exploit weaknesses in the Print Spooler. To reduce this risk, all printer driver installations should be strictly controlled and the Print Spooler hardened.

The following Group Policy settings can be implemented to secure the use of printers.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Configure RPC packet level privacy setting for incoming connections	Enabled
Computer Configuration\Policies\Administrative Templates\Printers	
Configure Redirection Guard	Enabled Redirection Guard Options: Redirection Guard Enabled

Configure RPC connection settings	Enabled Protocol to use for outgoing RPC connections: RCP over TCP Use authentication for outgoing RPC connections: Default
Configure RPC listener settings	Enabled Protocol to use for outgoing RPC connections: RCP over TCP Use authentication for outgoing RPC connections: Negotiate
Configure RPC over TCP port	Enabled RCP over TCP port: 0
Limits printer driver installation to Administrators	Enabled
Manage Print Driver signature validation	Enabled Select the driver signature mechanism for this computer: Allow all validly signed drivers
Manage processing of Queue-specific files	Enabled Manage processing of Queue-Specific files: Limit Queue-specific files to Color profiles
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\ Internet Communication settings	
Turn off downloading of print drivers over HTTP	Enabled

Registry editing tools

One method for malicious code to maintain persistence (i.e. remain after a workstation is rebooted) is to use administrative privileges to modify the registry (as standard privileges only allow viewing of the registry). To reduce this risk, users should not have the ability to modify the registry using registry editing tools (i.e. regedit) or to make silent changes to the registry (i.e. using .reg files).

The following Group Policy setting can be implemented to prevent users from viewing or modifying the registry using registry editing tools.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\System	
Prevent access to registry editing tools	Enabled Disable regedit from running silently: Yes

Remote Assistance

While Remote Assistance can be a useful business tool to allow system administrators to remotely administer workstations, it can also pose a risk. When a user has a problem with their workstation they can generate a Remote Assistance invitation. This invitation authorises anyone that has access to it to remotely control the workstation that issued the invitation. Invitations can be sent by email, instant messaging or saved to a file. If malicious actors manage to intercept an invitation they will be able to use it to access the user's workstation. Additionally, if network traffic on port 3389 is not blocked from reaching the internet, users may send Remote Assistance invitations over the internet which could allow for remote access to their workstation by malicious actors. While Remote Assistance only grants access to the privileges of the user that generated the request, malicious actors could install a key logging application on the workstation in preparation of a system administer using their privileged credentials to fix any problems. To reduce this risk, Remote Assistance should be disabled.

The following Group Policy settings can be implemented to disable Remote Assistance.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Remote Assistance	
Configure Offer Remote Assistance	Disabled
Configure Solicited Remote Assistance	Disabled

Remote Desktop Services

While remote desktop access allows for the remote administration of workstations across a network, it also allows malicious actors to access other workstations once they have compromised an initial workstation and user's credentials. This risk can be compounded if malicious actors can compromise domain administrator credentials or common local administrator credentials. To reduce this risk, Remote Desktop Services should be configured in a manner that is as secure as possible and only for users for which it is explicitly required.

The following Group Policy settings can be implemented to use Remote Desktop Services in as secure a manner as possible.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation	
Encryption Oracle Remediation	Enabled Protection Level: Force Updated Clients
Remote host allows delegation of non-exportable credentials	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client	
Configure server authentication for client	Enabled Authentication setting:

	Do not connect if authentication fails
Do not allow passwords to be saved	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections	
Allow users to connect remotely by using Remote Desktop Services	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection	
Do not allow Clipboard redirection	Enabled
Do not allow drive redirection	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security	
Always prompt for password upon connection	Enabled
Require secure RPC communication	Enabled
Require use of specific security layer for remote (RDP) connections	Enabled Security Layer: SSL
Require user authentication for remote connections by using Network Level Authentication	Enabled
Set client connection encryption level	Enabled Encryption Level: High Level
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Allow log on through Remote Desktop Services	Remote Desktop Users
Deny log on through Remote Desktop Services	Administrators NT AUTHORITY\Local Account

Remote Procedure Call

Remote Procedure Call (RPC) is a technique used for facilitating client and server application communications using a common interface. RPC is designed to make client and server interaction easier and safer by using a common library to handle tasks such as security, synchronisation and data flows. If unauthenticated communications are allowed between client and server applications, it could result in accidental disclosure of sensitive information or the failure to take advantage of RPC security functionality. To reduce this risk, all RPC clients should authenticate to RPC servers.

The following Group Policy setting can be implemented to ensure RPC clients authenticate to RPC servers.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call	
Restrict Unauthenticated RPC clients	Enabled RPC Runtime Unauthenticated Client Restriction to Apply: Authenticated

Reporting system information

Microsoft Windows contains a number of in-built functions to, often automatically and transparently, report system information to Microsoft. This includes system errors and crash information as well as inventories of applications, files, devices and drivers on the system. If captured by malicious actors, this information could expose potentially sensitive information on workstations. This information could also subsequently be used by malicious actors to tailor malicious code to target specific workstations or users. To reduce this risk, all in-built functions that report potentially sensitive system information should be directed to a corporate Windows Error Reporting server.

The following Group Policy settings can be implemented to prevent potentially sensitive system information being reported to Microsoft.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Application Compatibility	
Turn off Inventory Collector	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds	
Allow Diagnostic Data	Enabled Diagnostic data off (not recommended)
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\ Advanced Error Reporting Settings	
Configure Corporate Windows Error Reporting	Enabled Corporate server name: *<organisation defined>* Connect using SSL Server port: *<organisation defined>*

Safe Mode

Malicious actors with standard user credentials that can boot into Microsoft Windows using Safe Mode, Safe Mode with Networking or Safe Mode with Command Prompt options may be able to bypass system protections and security functionality. To reduce this risk, users with standard credentials should be prevented from using Safe Mode options to log in.

The following registry entry can be implemented using Group Policy preferences to prevent non-administrators from using Safe Mode options.

Registry Entry	Recommended Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	
SafeModeBlockNonAdmins	REG_DWORD 0x00000001 (1)

Secure channel communications

Periodically, workstations connected to a domain will communicate with the domain controllers. If malicious actors have access to unprotected network communications, they may be able to capture or modify sensitive information communicated between workstations and the domain controllers. To reduce this risk, all secure channel communications should be signed and encrypted with strong session keys.

The following Group Policy settings can be implemented to ensure secure channel communications are appropriately signed and encrypted.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Require strong (Windows 2000 or later) session key	Enabled

Security policies

By failing to comprehensively specify security policies, malicious actors may be able to exploit weaknesses in a workstation's Group Policy settings to gain access to sensitive information. To reduce this risk, security policies should be comprehensively specified.

The following Group Policy settings can be implemented, in addition to those specifically mentioned in other areas of this publication, to form a comprehensive set of security policies.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Network\DNS Client	
Turn off multicast name resolution	Enabled
Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings	

Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content	
Turn off Microsoft consumer experiences	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Turn off heap termination on corruption	Disabled
Turn off shell protocol protected mode	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds	
Prevent downloading of enclosures	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Search	
Allow indexing of encrypted files	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Game Recording and Broadcasting	
Enables or disables Windows Game Recording and Broadcasting	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Disabled (on-premises AD) *or* Enabled (hybrid and Azure AD)
Network security: LDAP client signing requirements	Negotiate signing
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

Server Message Block sessions

Malicious actors that have access to network communications may attempt to use session hijacking tools to interrupt, terminate or steal a Server Message Block (SMB) session. This could potentially allow malicious actors to modify

packets and forward them to a SMB server to perform undesirable actions or to pose as the server or client after a legitimate authentication has taken place to gain access to sensitive information. To reduce this risk, all communications between SMB clients and servers should be signed, with any passwords used appropriately encrypted.

The following Group Policy settings can be implemented to ensure communications between SMB clients and servers are secure. Note, the MS Security Guide Group Policy settings are available as part of the *Microsoft Security Compliance Toolkit*.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Configure SMB v1 client driver	Enabled Configure MrxSmb10 driver: Disable driver (recommended)
Configure SMB v1 server	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Digitally sign communications (always)	Enabled

Session locking

Malicious actors with physical access to an unattended workstation with an unlocked session may attempt to inappropriately access sensitive information or conduct actions that won't be attributed to them. To reduce this risk, a session lock should be configured to activate after a maximum of 15 minutes of user inactivity. Furthermore, be aware that information or alerts may be displayed on the lock screen. To reduce the risk of unauthorised information disclosure, minimise the amount of information that the lock screen is permitted to display.

The following Group Policy settings can be implemented to set session locks.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	
Prevent enabling lock screen camera	Enabled
Prevent enabling lock screen slide show	Enabled
Computer Configuration\Policies\Administrative Templates\System\Logon	

Turn off app notifications on the lock screen	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy	
Let Windows apps activate with voice while the system is locked	Enabled Default for all apps: Force Deny
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace	
Allow Windows Ink Workspace	Enabled Choose one of the following actions: On, but disallow access above lock
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Machine inactivity limit	900 seconds
User Configuration\Policies\Administrative Templates\Control Panel\Personalization	
Enable screen saver	Enabled
Password protect the screen saver	Enabled
Screen saver timeout	Enabled Seconds: 900
User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications	
Turn off toast notifications on the lock screen	Enabled
User Configuration\Policies\Administrative Templates\Windows Components\Cloud Content	
Do not suggest third-party content in Windows spotlight	Enabled

Software-based firewalls

Network firewalls often fail to prevent the propagation of malicious code on a network, or malicious actors from extracting sensitive information, as they generally only control which ports or protocols can be used between segments on a network. Many forms of malicious code are designed specifically to take advantage of this by using common protocols such as HTTP, HTTPS, SMTP and DNS. To reduce this risk, software-based firewalls that filter both incoming and outgoing traffic should be appropriately implemented. Software-based firewalls are more effective than network firewalls as they can control which applications and services can communicate to and from workstations. The in-built Windows firewall can be used to control both inbound and outbound traffic for specific applications.

Sound Recorder

Sound Recorder is a feature of Microsoft Windows that allows audio from a device with a microphone to be recorded and saved as an audio file on the local hard drive. Malicious actors with remote access to a workstation can use this

functionality to record sensitive conversations in the vicinity of the workstation. To reduce this risk, Sound Recorder should be disabled.

The following Group Policy setting can be implemented to disable the use of Sound Recorder.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Sound Recorder	
Do not allow Sound Recorder to run	Enabled

Standard Operating Environment

When users are left to setup, configure and maintain their own workstations it can very easily lead to an inconsistent and insecure environment where particular workstations are more vulnerable than others. This inconsistent and insecure environment can easily allow malicious actors to gain an initial foothold on a network. To reduce this risk, workstations should connect to a domain using a Standard Operating Environment that is centrally controlled and configured by experienced information technology and information security professionals. However, in some cases, cloud-based domain services may be more effective in deploying workstation configurations to a mobile and disparate workforce. In particular, security objectives may be achieved without the need to create 'gold' images and can offer more flexible enrolment processes. However, enrolment methods, such as Microsoft Intune self-enrolment, may introduce their own security risks, such as leaving behind local administrator accounts.

System backup and restore

Malicious actors that compromise a user account with privileges to backup files and directories can use this privilege to backup the contents of a workstation. This content can then be transferred to a non-domain connected workstation where malicious actors have administrative access. From here malicious actors can restore the contents and take ownership, thereby circumventing all original access controls that were in place. In addition, if a user has privileges to restore files and directories, malicious actors could exploit this privilege by using it to either restore previous versions of files that may have been removed by system administrators as part of malicious code removal activities or to replace existing files with malicious variants. To reduce this risk, the ability to use backup and restore functionality should be limited to administrators.

The following Group Policy settings can be implemented to control the use of backup and restore functionality.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Back up files and directories	Administrators
Restore files and directories	Administrators

System cryptography

By default, when cryptographic keys are stored in Microsoft Windows, users can access them without first entering a password to unlock the certificate store. Malicious actors that compromise a workstation, or gains physical access to an unlocked workstation, can use these user keys to access sensitive information or resources that are cryptographically protected. To reduce this risk, strong encryption algorithms and strong key protection should be used on workstations.

The following Group Policy settings can be implemented to ensure strong encryption algorithms and strong key protection is used.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled

UEFI passwords

Malicious actors with access to a workstation's UEFI can modify the hardware configuration of the workstation to introduce attack vectors or weaken security functionality within the workstation's operating system. This can include disabling security functionality in the CPU, modifying allowed boot devices and enabling insecure communications interfaces such as FireWire and Thunderbolt. To reduce this risk, strong UEFI passwords should be used for all workstations to prevent unauthorised access.

User rights policies

By failing to comprehensively specify user rights policies, malicious actors may be able to exploit weaknesses in a workstation's Group Policy settings to gain access to sensitive information. To reduce this risk, user rights policies should be comprehensively specified.

The following Group Policy settings can be implemented, in addition to those specifically mentioned in other areas of this publication, to form a comprehensive set of user rights policies.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access Credential Manager as a trusted caller	*<blank>*
Access this computer from the network	Remote Desktop Users
Act as part of the operating system	*<blank>*
Allow log on locally	Users
Create a pagefile	Administrators
Create a token object	*<blank>*
Create global objects	Administrators LOCAL SERVICE

	NETWORK SERVICE SERVICE
Create permanent shared objects	*<blank>*
Debug programs	Administrators
Deny access to this computer from the network	Administrators NT AUTHORITY\Local Account
Deny log on as a batch job	Administrators
Deny log on locally	Administrators
Deny log on as a service	Administrators
Enable computer and user accounts to be trusted for delegation	*<blank>*
Force shutdown from a remote system	Administrators
Impersonate a client after authentication	Administrators LOCAL SERVICE NETWORK SERVICE SERVICE
Load and unload device drivers	Administrators
Lock pages in memory	*<blank>*
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Take ownership of files or other objects	Administrators

Virtualised web access

Malicious actors can often deliver malicious code directly to workstations via external web access. Once a workstation has been exploited, malicious actors can use these same communication paths for bi-directional communications to control their malicious code. To reduce this risk, web access on workstations should occur through a non-persistent virtual environment (e.g. using Windows Defender Application Guard for Microsoft Edge). When using a virtual environment, workstations will receive additional protection against intrusion attempts targeted at exploiting vulnerabilities in web browsers as any attempts, if successful, will execute in a non-persistent virtual environment rather than on a local workstation.

Web Proxy Auto Discovery protocol

The Web Proxy Auto Discovery (WPAD) protocol assists with the automatic detection of proxy settings for web browsers. Unfortunately, WPAD has suffered from a number of severe vulnerabilities. Organisations that do not rely on the use of the WPAD protocol should disable it. This can be achieved by modifying each workstation's host file at *%SystemDrive%\Windows\System32\Drivers\etc\hosts* to create the following entry: *255.255.255.255 wpad*.

Windows Copilot

As part of the in-built artificially intelligence functionality of Microsoft Windows 11, users can use Windows Copilot (with either Bing Chat or Bing Chat Enterprise as the chat platform provider). Notably, however, this functionality, if used, could result in the accidental disclosure of sensitive information when sensitive terms or topics are searched for on the web, especially if Bing Chat is used as the chat platform provider (as it lacks the data protection measures of Bing Chat Enterprise). To reduce this risk, the ability to use Windows Copilot should be disabled until such time that organisations have made a risk-based decision on its use. Even then, only Windows Copilot configured with Bing Chat Enterprise as the chat platform provider should be considered for business and corporate environments.

The following Group Policy settings can be implemented to turn off Windows Copilot.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\Windows Components\Windows Copilot	
Turn off Windows Copilot	Enabled

Windows Remote Management

Windows Remote Management (WinRM) is the Microsoft implementation of the WS-Management Protocol which was developed as a public standard for remotely exchanging management data between devices that implement the protocol. If appropriate authentication and encryption is not implemented for this protocol, traffic may be subject to inception by malicious actors. To reduce this risk, Windows Remote Management should be securely configured.

The following Group Policy settings can be implemented to secure the use of the Windows Remote Management.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client	
Allow Basic authentication	Disabled
Allow unencrypted traffic	Disabled
Disallow Digest authentication	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service	
Allow Basic authentication	Disabled

Allow unencrypted traffic	Disabled
Disallow WinRM from storing RunAs credentials	Enabled

Windows Remote Shell access

When Windows Remote Shell is enabled it can allow malicious actors to remotely execute scripts and commands on workstations. To reduce this risk, Windows Remote Shell should be disabled.

The following Group Policy setting can be implemented to disable Windows Remote Shell access.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell	
Allow Remote Shell Access	Disabled

Windows Search and Cortana

As part of the in-built search functionality of Microsoft Windows, users can search for web results in addition to local workstation results. This functionality if used could result in the accidental disclosure of sensitive information if sensitive terms are searched for automatically on the web in addition to the local workstation. To reduce this risk, the ability to automatically search the web should be disabled.

The following Group Policy settings can be implemented to prevent web search results being returned for any user search terms.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Search	
Allow Cortana	Disabled
Don’t search the web or display web results in Search	Enabled

Low priorities

The following recommendations, listed in alphabetical order, should be treated as low priorities when hardening Microsoft Windows 10 and Windows 11 workstations.

Displaying file extensions

When extensions for known file types are hidden, malicious actors can more easily use social engineering techniques to convince users to execute malicious email attachments. For example, a file named *vulnerability_assessment.pdf.exe* could appear as *vulnerability_assessment.pdf* to a user. To reduce this risk, hiding extensions for known file types should be disabled. Showing extensions for all known file types, in combination with user education and awareness of dangerous email attachment file types, can help reduce the risk of users executing malicious email attachments.

The following registry entry can be implemented using Group Policy preferences to prevent extensions for known file types from being hidden.

Registry Entry	Recommended Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	
HideFileExt	REG_DWORD 0x00000000 (0)

File and folder security properties

By default, all users have the ability to view security properties of files and folders. This includes the security properties associated with files and folders as well as users and groups that they relate to. Malicious actors could use this information to target specific accounts that have access to sensitive information. To reduce this risk, users should not have the ability to view security properties of files and folders.

The following Group Policy setting can be implemented to disable users' access to the security tab in file and folder properties in File Explorer.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Remove Security tab	Enabled

Location awareness

When users interact with the internet their workstations often automatically provide geo-location details to websites or online services to assist them in tailoring content specific to the user's geographical region (i.e. the city they are accessing the internet from). This information can be captured by malicious actors to determine the location of a specific user. To reduce this risk, location services in the operating system and applications should be disabled.

The following Group Policy settings can be implemented to disable location services within the operating system.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors	
Turn off location	Enabled
Turn off location scripting	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\ Windows Location Provider	
Turn off Windows Location Provider	Enabled

Microsoft Store

Whilst applications in the Microsoft Store are vetted by Microsoft, there is still a risk that users given access to the Microsoft Store could download and install potentially malicious applications or applications that cause conflicts with other endorsed applications on their workstation. To reduce this risk, access to the Microsoft Store should be disabled.

The following Group Policy settings can be implemented to prevent Microsoft Store access.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\ Internet Communication settings	
Turn off access to the Store	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Store	
Turn off the Store application	Enabled

Resultant Set of Policy reporting

By default, all users have the ability to generate Resultant Set of Policy (RSOP) reports which allows them to view the Group Policy settings being applied to their workstation and user account. This information could be used by malicious actors to determine misconfigurations or weaknesses in Group Policy settings being applied to the workstation or the user account. To reduce this risk, users should not have the ability to generate RSOP reports.

The following Group Policy setting can be implemented to disable users' ability to generate RSOP reports.

Group Policy Setting	Recommended Option
User Configuration\Policies\Administrative Templates\System\Group Policy	
Determine if interactive users can generate Resultant Set of Policy data	Enabled

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate