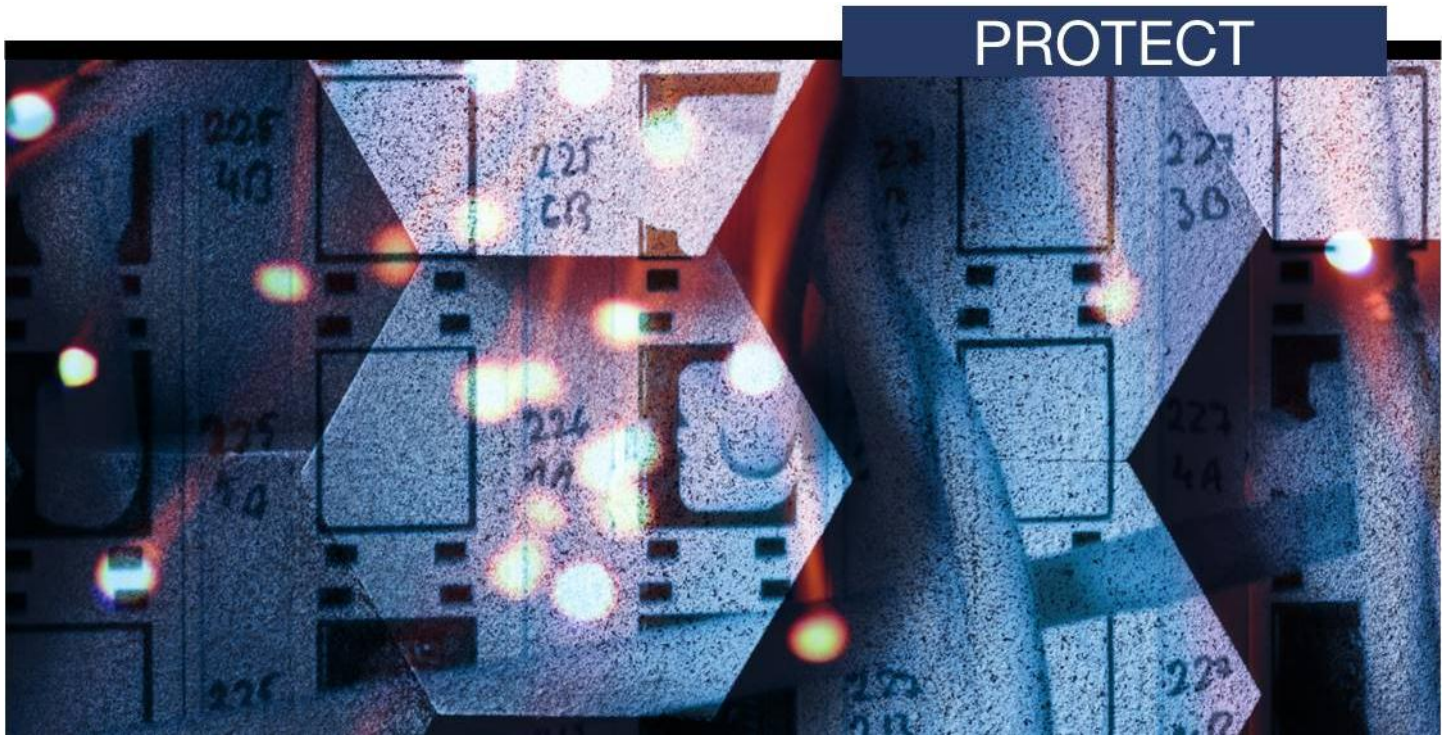
Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

Hardening Microsoft Windows 8.1 Update Workstations

May 2018



CONTENTS

Introduction

1. Workstations are often targeted by an adversary using malicious webpages, emails with malicious attachments and removable media with malicious content in an attempt to extract sensitive information. Hardening workstations is an important part of reducing this risk.
2. This document provides guidance on hardening workstations using Enterprise editions of Microsoft Windows 8.1 Update. Some Group Policy settings used in this document may not be available or compatible with Professional, Core or RT editions of Microsoft Windows 8.1 Update.
3. While this document refers to workstations, most Group Policy settings are equally applicable to servers (with the exception of Domain Controllers) using Microsoft Windows Server 2012 R2. The names and locations of Group Policy settings used in this document are taken from Microsoft Windows 8.1 Update; some differences may exist for earlier versions of Microsoft Windows.
4. Before implementing recommendations in this document, thorough testing should be undertaken to ensure the potential for unintended negative impacts on business processes is reduced as much as possible.
5. This document is intended for information technology and information security professionals within organisations looking to undertake risk assessments or vulnerability assessments as well as those wishing to develop a hardened Standard Operating Environment for workstations.

High priorities

6. The following security controls, listed in alphabetical order, are considered to have an excellent effectiveness and should be treated as high priorities when hardening Microsoft Windows 8.1 Update workstations.

Address Space Layout Randomization

7. An adversary may attempt to compromise a workstation by accessing the location of important information in memory such as an executable's base address and the position of the heap, stack and libraries in a process' address space. To reduce this risk, Address Space Layout Randomization (ASLR) should be enabled for all applications that support it. By default, ASLR is enabled from Microsoft Windows Vista onwards and can mitigate some forms of attacks by randomising the location of important information in memory. The use of ASLR can be confirmed by using the Enhanced Mitigation Experience Toolkit from Microsoft[1] to ensure ASLR is set to *Application Opt In*.

Application hardening

8. 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 the *Microsoft Office 2013 Security Guide* as part of the Microsoft Security Compliance Manager tool[2]. In such cases, vendor guidance should be followed to assist in securely configuring their products.

9. The Australian Cyber Security Centre (ACSC) also provides guidance for hardening Microsoft Office. For more information see *Hardening Microsoft Office 2013*[3] and *Hardening Microsoft Office 2016*[4].

Application versions and patches

10. While some vendors may release new application versions to address security vulnerabilities, others may release patches. If new application versions and patches for applications are not installed it can allow an adversary 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

[1] https://technet.microsoft.com/en-au/security/jj653751/

[2] https://technet.microsoft.com/en-au/solutionaccelerators/cc835245.aspx

[3] https://www.acsc.gov.au/publications/protect/Hardening_MS_Office_2013.pdf

[4] https://www.acsc.gov.au/publications/protect/Hardening_MS_Office_2016.pdf

patches for applications should be applied in an appropriate timeframe as determined by the severity of security 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; however, this may be done as soon as practical rather than within two days of release.

11. For more information on determining the severity of security vulnerabilities and timeframes for applying new application versions and patches for applications see *Assessing Security Vulnerabilities and Applying Patches*[5].

Application whitelisting

12. An adversary can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it on their workstation. Such malicious code often aims to exploit security vulnerabilities in existing applications and doesn't need to be installed on the workstation to be successful. To reduce this risk, an application whitelisting solution should be appropriately implemented. Application whitelisting when implemented in its most effective form (e.g. using hashes for executables, dynamic link libraries, scripts, installers and packaged apps) can be an extremely effective mechanism in not only preventing malicious code from executing but also ensuring only authorised applications can be installed on workstations. Less effective implementations of application whitelisting (e.g. using approved paths for installed applications in combination with access controls requiring privileged access to write to these locations) can be used as a first step towards implementing a more comprehensive application whitelisting solution.

13. For more information on application whitelisting and how it can be appropriately implemented see *Implementing Application Whitelisting*[6].

14. If Microsoft AppLocker[7] is used for application whitelisting, the following rules can be used as a sample path-based implementation. In support of this, the rules, enforcement of rules and the automatic starting of the Application Identity service should be set via Group Policy at a domain level[8].

Whitelisting Rule	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\ AppLocker\DLL Rules	
[Path] %ProgramFiles%*	Allow Everyone
[Path] %WinDir%*	Allow Everyone Exceptions: %System32%\Microsoft\ Crypto\RSA\MachineKeys* %System32%\spool\ drivers\color* %System32%\Tasks*

[5] https://www.acsc.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Applying_Patches.pdf

[6] https://www.acsc.gov.au/publications/protect/Application_Whitelisting.pdf

[7] https://technet.microsoft.com/en-us/library/hh831409(v=ws.11).aspx

[8] https://technet.microsoft.com/en-au/library/ee844118.aspx

[Path] %WinDir%* (*continued*)	%WinDir%\debug\WIA* %WinDir%\Tasks* %WinDir%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\ AppLocker\Executable Rules	
[Path] %ProgramFiles%*	Allow Everyone
[Path] %WinDir%*	Allow Everyone Exceptions: %System32%\Microsoft\ Crypto\RSA\MachineKeys* %System32%\spool\ drivers\color* %System32%\Tasks* %WinDir%\debug\WIA* %WinDir%\Tasks* %WinDir%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\ AppLocker\Packaged app Rules	
[Publisher] CN=Microsoft Corporation, O=Microsoft Corporation, L-Redmond, S=Washington, C=US	Allow Everyone
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\ AppLocker\Script Rules	
[Path] %ProgramFiles%*	Allow Everyone
[Path] %WinDir%*	Allow Everyone Exceptions: %System32%\Com\dmp* %System32%\FxsTmp* %System32%\Microsoft\ Crypto\RSA\MachineKeys* %System32%\spool\ drivers\color* %System32%\spool\PRINTERS* %System32%\spool\SERVERS* %System32%\Tasks* %WinDir%\debug\WIA* %WinDir%\Registration\CRMLog* %WinDir%\Tasks* %WinDir%\Temp* %WinDir%\tracing*

Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\ AppLocker\Windows Installer Rules	
[Publisher] CN=Microsoft Corporation, O=Microsoft Corporation, L-Redmond, S=Washington, C=US	Allow Everyone

Credential caching

15. 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 an adversary 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.

16. 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

17. 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 an adversary. To reduce this risk, WDigest authentication should be disabled. In addition, additional protections for the LSASS process available in Microsoft Windows 8.1 should be implemented[9].

18. The following Group Policy settings can be implemented to disable WDigest authentication and provide additional protection to credentials stored in LSASS process memory.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
LSA Protection	Enabled
WDigest Authentication	Disabled

Credential entry

19. 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.

20. The following Group Policy settings can be implemented to ensure credentials are entered in a secure manner as well as prevent the disclosure of usernames of previous users.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not display network selection UI	Enabled

[9] https://technet.microsoft.com/en-au/library/dn408187.aspx

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
Sign-in last interactive user automatically after a system-initiated restart	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Do not require CTRL+ALT+DEL	Disabled

Data Execution Prevention

21. Data Execution Prevention (DEP) is a security function that can help protect workstations by monitoring applications to ensure they use memory safely. If DEP notices an application attempting to execute instructions from a portion of memory used for data it will close the application and notify the user. The default setting for desktop lines of Microsoft Windows is *Turn on DEP for essential Windows programs and services only*. This default setting does not cover non-Windows programs and will fail to block malicious code that would otherwise be blocked if DEP was applied to it. To reduce this risk, DEP, preferably hardware-based, should be enabled for all applications and services except those that need to be explicitly excluded for compatibility reasons. To enable DEP for all applications and services, except those that need to be explicitly excluded, the DEP setting within Microsoft Windows can be changed to *Turn on DEP for all programs and services except those I select*. This can be set under the Data Execution Prevention tab within the Performance Options of System Properties. Additionally, if the CPU supports hardware-based DEP, the text *Your computer's processor supports hardware-based DEP* will be displayed. Should there be a need to force the use of DEP for all applications and services, the Enhanced Mitigation Experience Toolkit[10] from Microsoft can be used to set DEP to *Always On*. This toolkit can also be used to determine the DEP status of running processes at any given time. The Process Explorer tool[11] in the Windows Sysinternals suite[12] can also display this information.

22. The following Group Policy setting can be implemented to ensure DEP is used in File Explorer.

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

Early Launch Antimalware

23. Another key security feature of Trusted Boot supported by Microsoft Windows 8.1 Update and motherboards with an UEFI is Early Launch Antimalware (ELAM) support. Used in conjunction

[10] https://technet.microsoft.com/en-au/security/jj653751/

[11] https://docs.microsoft.com/en-au/sysinternals/downloads/process-explorer

[12] https://docs.microsoft.com/en-au/sysinternals/

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 drivers should be allowed to be initialised during the boot process.

24. The following Group Policy setting can be implemented to ensure only known good 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 and unknown

Elevating privileges

25. 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 an adversary that gains 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.

26. 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: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
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	Prompt for credentials on the secure desktop
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: Switch to the secure desktop when prompting for elevation	Enabled

User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Enhanced Mitigation Experience Toolkit

27. An adversary that develops exploits for Microsoft Windows or 3rd party applications will have a higher success rate when measures designed by Microsoft to help prevent security vulnerabilities from being exploited are not implemented. The Enhanced Mitigation Experience Toolkit (EMET)[13] was designed by the Microsoft Security Research Center (MSRC) engineering team to provide additional system-wide and application-specific mitigation measures for Microsoft Windows operating systems and 3rd party applications.

28. To reduce the risk of an adversary exploiting security vulnerabilities in Microsoft Windows or 3rd party applications, the latest version of EMET should be implemented using system-wide and application-specific mitigation measures.

29. The Group Policy Administrative Templates for EMET are provided in the EMET installation directory. The ADMX and associated en-us ADML file for EMET 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. Of note, each time changes are made to EMET Group Policy settings on the Domain Controller, the *emet_conf --refresh* command will need to be run via a script or scheduled task on workstations to import the changes to the EMET configuration.

30. The following Group Policy settings can be implemented to ensure EMET is appropriately implemented.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\EMET	
Default Action and Mitigation Settings	Enabled Deep Hooks: Enabled Anti Detours: Enabled Banned Functions: Enabled Exploit Action: Stop Program
Default Protections for Internet Explorer	Enabled
Default Protections for Popular Software	Enabled
Default Protections for Recommended Software	Enabled
EMET Agent Visibility	Enabled Start Agent Hidden: Disabled

[13] https://technet.microsoft.com/en-au/security/jj653751/

Reporting	Enabled Event Log: Enabled Tray Icon: Enabled Early Warning: Disabled
System ASLR	Enabled ASLR Setting: Application Opt-In
System DEP	Enabled DEP Setting: Always On
System SEHOP	Enabled SEHOP Setting: Application Opt-Out

Local administrator accounts

31. When built-in administrator accounts are used with common account names and passwords it can allow an adversary that compromises 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, an adversary can still identify these accounts based on their security identifier (i.e. S-1-5-21-*domain*-500[14]) 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, built-in administrator accounts should be disabled. Instead, domain accounts with local administrative privileges, but without domain administrative privileges, should be used for workstation management.

32. The following Group Policy setting can be implemented to disable built-in administrator accounts.

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

33. If a common local administrator account absolutely must be used for workstation management then Microsoft's Local Administrator Password Solution (LAPS)[15] 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[16].

[14] https://support.microsoft.com/en-au/help/243330/well-known-security-identifiers-in-windows-operating-systems

[15] https://www.microsoft.com/en-au/download/details.aspx?id=46899

[16] https://support.microsoft.com/en-au/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\MS Security Guide	
Apply UAC restrictions to local accounts on network logons	Enabled

Measured Boot

34. The third key security feature of Trusted Boot supported by Microsoft Windows 8 and motherboards with both an UEFI and a Trusted Processing 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.

Multi-factor authentication

35. 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, an adversary that brute forces 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 users as they perform a privileged action or access any important or sensitive data repositories.

36. For more information on how to effectively implement multi-factor authentication see *Multi-factor authentication*[17].

Operating system architecture

37. 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

38. Patches are released either in response to previously disclosed security vulnerabilities or to proactively address security vulnerabilities that have not yet been publicly disclosed. In the case of disclosed security vulnerabilities, it is possible that exploits have already been developed and are freely available in common hacking tools. In the case of patches for security vulnerabilities that have not yet been publically disclosed, it is relatively easy for an adversary to use freely available tools to identify the security 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 and deployed in an appropriate timeframe as determined by the severity of the security vulnerability and any mitigating measures already in place. This can be achieved using Microsoft System Center Configuration Manager (SCCM)[18]. Microsoft Windows Server Update Services (WSUS)[19] can also centrally deploy patches but only for Microsoft applications.

[17] https://www.acsc.gov.au/publications/protect/Multi_Factor_Authentication.pdf

[18] https://www.microsoft.com/en-au/cloud-platform/system-center-configuration-manager

[19] https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

39. For more information on determining the severity of security vulnerabilities and timeframes for applying patches see *Assessing Security Vulnerabilities and Applying Patches*[20].

40. 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	
Allow Automatic Updates immediate installation	Enabled
Configure Automatic Updates	Enabled Configure automatic updating: 4 - Auto download and schedule the install Schedule install day: 0 - Every day
No auto-restart with logged on users for scheduled automatic updates installations	Enabled
Turn on recommended updates via Automatic Updates	Enabled

41. 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	
Specify intranet Microsoft update service location	Enabled Set the intranet update service for detecting updates: *<server:port>*

42. Alternatively, if System Centre Configuration Manager (SCCM) is used instead of Microsoft update servers or a WSUS server, equivalent settings can be implemented to achieve a similar outcome.

Operating system version

43. Microsoft Windows 10 Anniversary Update has introduced improvements in security functionality over Microsoft Windows 8.1 Update. This has made it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discovered. Using older versions of Microsoft Windows exposes organisations to exploit techniques that have since been mitigated in newer versions of Microsoft Windows. To reduce this risk, workstations should use Microsoft Windows 10 Anniversary Update or later.

Password policy

44. 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. In addition, having no maximum password age can allow an adversary to maintain extended access to a workstation or network once a password has been compromised while having no

[20] https://www.acsc.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Applying_Patches.pdf

minimum password age can allow an adversary to recycle passwords if forced to change them due to maximum password ages. To reduce this risk, a secure password policy should be implemented.

45. The following Group Policy settings can be implemented to achieve a secure password policy.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Logon	
Turn off picture password sign-in	Enabled
Turn on PIN sign-in	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy	
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
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

Restricting privileged accounts

46. 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.

47. For more information on the use of privileged accounts and minimising their usage see *Restricting Administrative Privileges*[21].

Secure Boot

48. 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 new security feature supported by Microsoft Windows 8.1 Update and motherboards with an Unified Extensible Firmware Interface (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.

[21] https://www.acsc.gov.au/publications/protect/Restricting_Admin_Privileges.pdf

Structured Exception Handling Overwrite Protection

49. Without Structured Exception Handling Overwrite Protection (SEHOP) an adversary can use Structured Exception Handler overwrite techniques to execute malicious code on a workstation. By default, SEHOP is disabled in the desktop line of Microsoft Windows. To reduce this risk, SEHOP should be enabled for all applications.

50. SEHOP can be enabled by using the Enhanced Mitigation Experience Toolkit from Microsoft[22] to set SEHOP to *Always On* or by implementing the following registry entry using Group Policy preferences.

Registry Entry	Recommended Value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel	
DisableExceptionChainValidation	REG_DWORD 0x00000000 (0)

[22] https://technet.microsoft.com/en-au/security/jj653751/

Medium priorities

51. The following security controls, listed in alphabetical order, are considered to have a very good effectiveness and should be treated as medium priorities when hardening Microsoft Windows 8.1 Update workstations.

Account lockout policy

52. Allowing unlimited attempts to access workstations will fail to prevent an adversary's 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.

53. 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
Reset account lockout counter after	15 minutes

Anonymous connections

54. An adversary 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.

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

Group Policy Setting	Recommended Option
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 security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access this computer from the network	Administrators Remote Desktop Users

Deny access to this computer from the network	Guests NT AUTHORITY\Local Account

Antivirus software

56. An adversary can develop malicious code to exploit security 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, an adversary 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.

57. 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. An adversary 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 (using heuristics to identify and block malicious behaviour) should also be implemented. In doing so, heuristic functionality should be set at the highest level available.

Attachment Manager

58. 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 an adversary 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.

59. 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

60. Failure to capture and analyse security related audit events from workstations can result in intrusions going unnoticed. In addition, the lack of such information can significantly hamper investigations following a security incident. To reduce this risk, security related audit events from workstations should be captured and routinely analysed.

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

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\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

62. 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	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	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

Autoplay and AutoRun

63. 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 an adversary to automatically execute malicious code. To reduce this risk, Autoplay and AutoRun functionality should be disabled.

64. 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

BIOS and UEFI passwords

65. An adversary with access to a workstation's BIOS or 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 BIOS and UEFI passwords should be used for all workstations to prevent unauthorised access.

Boot devices

66. By default, workstations are often configured to boot from optical media, or even USB media, in preference to hard drives. An adversary 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, an adversary 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

67. 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 an adversary 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 an adversary 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.

68. 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 installation and configuration of Network Bridge on your DNS domain network	Enabled
Route all traffic through the internal network	Enabled Select from the following states: Enabled State
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

69. When built-in guest accounts are used, it can allow an adversary 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.

70. 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

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Deny log on locally	Guests

Case locks

71. Without the use of case locks an adversary can gain physical access to the insides of a workstation. An adversary with this access can install or remove hardware, remove and replace the CMOS battery to reset the BIOS or UEFI to default settings (i.e. no password), or temporarily remove hard drives to create copies for offline analysis at a later date. To reduce this risk, case locks should be used on workstations to prevent an adversary from gaining unauthorised access.

CD burner access

72. If CD burning functionality is enabled, and CD burners are installed in workstations, an adversary 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.

73. 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 3rd 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

74. Storing audit event logs on workstations poses a risk that an adversary 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 security incidents. To reduce this risk, audit event logs from workstations should be transferred to a secure central logging server.

Command Prompt

75. An adversary who gains access to a workstation can use the Command Prompt to execute in-built Microsoft Windows tools such as *net* and *schtasks* 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.

76. 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

77. Communications interfaces that use Direct Memory Access (DMA) can allow an adversary 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[23] (e.g. disabling the functionality in the Basic Input/Output System (BIOS) or UEFI; removing the SBP-2 driver and disabling the Thunderbolt controller; or using an end point protection solution).

78. The following Group Policy settings can be implemented to remove the SBP-2 driver and disable the Thunderbolt controller.

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_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.

Endpoint device control

79. An adversary 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

[23] https://support.microsoft.com/en-au/help/2516445/blocking-the-sbp-2-driver-and-thunderbolt-controllers-to-reduce-1394-d

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.

80. 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

81. 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.

82. The following Group Policy settings provide a sample implementation that allows data to be read from but not executed from or written to all 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
Custom Classes: Deny read access	Disabled
Custom Classes: Deny write access	Enabled
Floppy Drives: Deny execute access	Enabled
Floppy Drives: Deny read access	Disabled
Floppy Drives: 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

83. 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.

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

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup	
Prevent the computer from joining a homegroup	Enabled
User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing	
Prevent users from sharing files within their profile.	Enabled

Group Policy processing

85. 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, an adversary 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.

86. The following Group Policy settings can be implemented to ensure only domain-based Group Policy settings are applied to workstations.

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 Process even if the Group Policy objects have not changed
Configure security policy processing	Enabled Process even if the Group Policy objects have not changed
Turn off background refresh of Group Policy	Disabled
Turn off Local Group Policy Objects processing	Enabled

Hard drive encryption

87. An adversary 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, an adversary that gains access to a stolen or unsanitised hard

drive 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, 256-bit AES full disk encryption should be used to protect the contents of hard drives from unauthorised access.

88. 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	Enabled Select the encryption method: AES 256-bit
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 use of passwords for fixed data drives *(continued)*	Configure password complexity for fixed data drives: Require password complexity Minimum password length for fixed data drive: 10
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 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: Backup 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: 13

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: 10
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 Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive) 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

Choose how BitLocker-protected removable drives can be recovered *(continued)*	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: 10
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

Installing applications

89. While the ability to install applications may be a business requirement for users, this privilege can be exploited by an adversary. An adversary 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, an adversary 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. To reduce this risk, all application installations should be strictly controlled.

90. 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 SmartScreen	Enabled Require approval from an administrator before running downloaded unknown software
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

Internet printing

91. Microsoft Windows has the ability to print to internet printers over HTTP. If not disabled, this functionality could result in the accidental or intentional release of sensitive information into the public domain. To reduce this risk, internet printing should be disabled.

92. The following Group Policy settings can be implemented to prevent the use of internet printing.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off downloading of print drivers over HTTP	Enabled
Turn off printing over HTTP	Enabled

Legacy and run once lists

93. Once malicious code has been copied to a workstation, an adversary 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.

94. 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

95. A new feature of Microsoft Windows 8.1 Update 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 Microsoft Windows 8.1 Update workstation (e.g. corporate workstation, home PC, Internet café) 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.

96. 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\OneDrive	
Prevent the usage of OneDrive for file storage	Enabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts

MSS settings

97. By failing to specify MSS specific registry values an adversary may be able to exploit weaknesses in a workstation's security posture to gain access to sensitive information. To reduce this risk, MSS specific registry values that are still relevant to modern versions of Microsoft Windows should be specified using Group Policy settings.

98. The Group Policy Administrative Templates for MSS specific registry values are available from the Microsoft Security Guidance blog[24]. The ADMX and associated en-us ADML file 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.

99. The following Group Policy settings can be implemented to configure MSS specific registry values 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

[24] https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/

MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled

NetBIOS over TCP/IP

100. NetBIOS over TCP/IP facilitates a number of intrusion methods. To reduce this risk, NetBIOS over TCP/IP should be disabled. 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

101. Using insecure network authentication methods may permit an adversary 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.

102. 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

103. 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.

104. 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

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

Power management

106. 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. An adversary 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.

107. 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

108. 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.

109. For more information on how to effectively implement PowerShell see *Securing PowerShell in the Enterprise*[25].

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

Group Policy Setting	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on PowerShell Script Block Logging	Enabled
Turn on Script Execution	Enabled Execution Policy: Allow only signed scripts

Registry editing tools

111. 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).

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

[25] https://www.acsc.gov.au/publications/protect/Securing_PowerShell.pdf

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

113. 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 an adversary manages 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 an adversary. While Remote Assistance only grants access to the privileges of the user that generated the request, an adversary 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.

114. 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

115. While remote desktop access may be convenient for legitimate users to access workstations across a network, it also allows an adversary to access other workstations once they have compromised an initial workstation and user's credentials. This risk can be compounded if an adversary can compromise domain administrator credentials or common local administrator credentials. To reduce this risk, Remote Desktop Services should be disabled.

116. The following Group Policy settings can be implemented to disable Remote Desktop Services.

Group Policy Setting	Recommended Option
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	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Allow log on through Remote Desktop Services	*<blank>*
Deny log on through Remote Desktop Services	Administrators Guests NT AUTHORITY\Local Account

117. Alternatively, if it is an essential business requirement to use Remote Desktop Services, it should be configured in a manner that is as secure as possible and only on workstations and for users for which it is explicitly required.

118. 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\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
Deny logoff of an administrator logged in to the console session	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
Do not allow local administrators to customize permissions	Enabled
Require secure RPC communication	Enabled
Require use of specific security layer for remote (RDP) connections	Enabled Security Layer: SSL (TLS 1.0)
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 Guests

Remote Procedure Call

119. 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.

120. 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

121. 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 an adversary, this information could expose potentially sensitive information on workstations. This information could also subsequently be used by an adversary 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.

122. 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\System\Troubleshooting and Diagnostics\ Microsoft Support Diagnostic Tool	
Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Application Compatibility	
Turn off Inventory Collector	Enabled
Turn off Steps Recorder	Enabled

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

123. An adversary 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 such as application whitelisting solutions. To reduce this risk, users with standard credentials should be prevented from using Safe Mode options to log in.

124. 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

125. Periodically, workstations connected to a domain will communicate with the domain controllers. If an adversary has 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.

126. 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

127. By failing to comprehensively specify security policies, an adversary 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.

128. The following Group Policy settings can be implemented, in addition to those specifically mentioned in other areas of this document, 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\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\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
Network security: Force logoff when logon hours expire	Enabled
Network security: LDAP client signing requirements	Negotiate signing
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

Server Message Block sessions

129. An adversary that has 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 an adversary 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.

130. The following Group Policy settings can be implemented to ensure communications between SMB clients and servers are secure.

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: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Session locking

131. An adversary with physical access to an unattended workstation may attempt to inappropriately access other users' sessions in order to use their credentials to access sensitive information they don't have access to or to conduct actions on the network 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.

132. 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	
Allow users to select when a password is required when resuming from connected standby	Disabled
Turn off app notifications on the lock screen	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Show lock in the user tile menu	Enabled
Computer Configuration\Policies\Windows 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

Software-based firewalls

133. Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary 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 (from Microsoft Windows 7 onwards) can be used to control both inbound and outbound traffic for specific applications.

Sound Recorder

134. 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. An adversary 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.

135. 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

136. 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 an adversary 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.

System backup and restore

137. An adversary that compromises 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 the adversary has administrative access. From here an adversary 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, an adversary 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.

138. 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

139. By default, when cryptographic keys are stored in Microsoft Windows, users can access them without first entering a password to unlock the certificate store. An adversary that compromises 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.

140. 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

User rights policies

141. By failing to comprehensively specify user rights policies, an adversary 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.

142. The following Group Policy settings can be implemented, in addition to those specifically mentioned in other areas of this document, 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>*
Act as part of the operating system	*<blank>*
Allow log on locally	Administrators Users
Create a pagefile	Administrators
Create a token object	*<blank>*
Create global objects	Administrators LOCAL SERVICE NETWORK SERVICE SERVICE
Create permanent shared objects	*<blank>*
Create symbolic links	Administrators
Debug programs	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
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	*<blank>*
Modify an object label	*<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 and email access

143. An adversary can often deliver malicious code directly to workstations via external web and email access. Once a workstation has been exploited, an adversary can use these same communication paths for bi-directional communications to control their malicious code. To reduce this risk, web and email access on workstations should occur through a non-persistent virtual environment (i.e. using virtual desktops or virtual applications). When using a virtual environment, workstations will receive additional protection against intrusion attempts targeted at exploiting security vulnerabilities in web browsers and email clients as any attempts, if successful, will execute in a non-persistent virtual environment rather than on a local workstation.

Web Proxy Auto Discovery protocol

144. 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 security 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 Remote Management

145. Windows Remote Management (WinRM)[26] is the Microsoft implementation of the WS-Management Protocol[27] 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 an adversary. To reduce this risk, Windows Remote Management should be securely configured.

146. 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

[26] https://msdn.microsoft.com/en-au/library/aa384426(v=vs.85).aspx

[27] https://msdn.microsoft.com/en-au/library/windows/desktop/aa384470(v=vs.85).aspx

Windows Remote Shell access

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

148. 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

149. 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.

150. 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	
Don’t search the web or display web results in Search	Enabled
Don’t search the web or display web results in Search over metered connections	Enabled

Windows To Go

151. A new feature of Microsoft Windows 8.1 Update is Windows To Go. Windows To Go allows users to boot into a Microsoft Windows 8.1 Update workspace stored on USB media from any machine that supports the minimum hardware requirements. While this may be highly beneficial for Bring Your Own Device (BYOD) or remote access initiatives, it can also pose a risk to an organisation’s network. Workstations that allow automatic booting of Windows To Go workspaces do not discriminate between approved workspaces and malicious workspaces developed by an adversary. As such, an adversary may use a malicious workspace they have customised with their desired toolkit to attempt to gain access to sensitive information on the network. To reduce this risk, automatic booting of Windows To Go media should be disabled.

152. The following Group Policy setting can be implemented to disable the automatic booting of Windows To Go media.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Portable Operating System	
Windows To Go Default Startup Options	Disabled

Low priorities

153. The following security controls, listed in alphabetical order, are recommended for consideration and should be treated as low priorities when hardening Microsoft Windows 8.1 Update workstations.

Displaying file extensions

154. When extensions for known file types are hidden, an adversary 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.

155. 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

156. 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. An adversary 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.

157. 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

158. 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 an adversary to determine the location of a specific user. To reduce this risk, location services in the operating system and applications should be disabled.

159. 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

160. 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.

161. 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

Publishing information to the Web

162. Microsoft Windows has the ability to assist users in either directly publishing information to the Web or sending information to publishers for professional publication. If not disabled, this functionality could result in the accidental or intentional release of sensitive information into the public domain. To reduce this risk, the ability to publish information to the Web or send to publishers should be disabled.

163. The following Group Policy setting can be implemented to disable the ability to publish information to the Web or send it to publishers.

Group Policy Setting	Recommended Option
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off Internet download for Web publishing and online ordering wizards	Enabled

Resultant Set of Policy reporting

164. 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 an adversary 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.

165. 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

Contact details

166. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).


acsc.gov.au
PARTNERING FOR A CYBER SECURE AUSTRALIA