



Information Security Manual

DECEMBER 2021

Guidelines for System Hardening

Operating system hardening

Standard Operating Environments

Allowing users to setup, configure and maintain their own workstations or servers can create an inconsistent environment where particular workstations or servers are more vulnerable than others. This type of environment can easily allow an adversary to gain an initial foothold on a network.

A Standard Operating Environment (SOE) is a standardised implementation of an operation system and its applications that is designed to ensure a consistent and secure baseline. When SOEs are obtained from third parties, such as service providers, there are additional cyber supply chain risks that should be considered, such as the accidental or deliberate inclusion of malicious content or configurations. To reduce the likelihood of such occurrences, organisations should endeavour to obtain their SOEs from trusted sources while also scanning them for malicious content and configurations before being used.

As the configuration of operating environments will naturally change over time (e.g. patches are applied, configurations are changed, and applications are added or removed) it is essential that SOEs are reviewed and updated at least annually to ensure that an up-to-date baseline is maintained.

Security Control: 1406; Revision: 2; Updated: Aug-20; Applicability: All
SOEs are used for workstations and servers.

Security Control: 1608; Revision: 0; Updated: Aug-20; Applicability: All
SOEs provided by third parties are scanned for malicious content and configurations before being used.

Security Control: 1588; Revision: 0; Updated: Aug-20; Applicability: All
SOEs are reviewed and updated at least annually.

Operating system releases and versions

Newer releases of operating systems often introduce improvements in security functionality. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older releases of operating systems, especially those no longer supported by vendors, exposes organisations to exploitation techniques that have since been mitigated in newer releases. In addition, 64-bit versions of operating systems support additional security functionality that 32-bit versions lack.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security control 1407 is not applicable.

Security Control: 1407; Revision: 4; Updated: Sep-21; Applicability: All

The latest release, or the previous release, of operating systems are used for workstations, servers and network devices.

Security Control: 1408; Revision: 3; Updated: Sep-18; Applicability: All

When developing a Microsoft Windows SOE, the 64-bit version of the operating system is used.

Operating system configuration

When operating systems are deployed in their default state it can lead to an insecure operating environment allowing an adversary to gain an initial foothold on a network. Many settings exist within operating systems to allow them to be configured in a secure state to minimise this security risk. The Australian Cyber Security Centre (ACSC) and vendors often produce hardening guides to assist in securely configuring various operating systems.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1654-1655 are not applicable.

Security Control: 1409; Revision: 1; Updated: Sep-18; Applicability: All

ACSC and vendor guidance is implemented to assist in hardening the configuration of operating systems.

Security Control: 0383; Revision: 6; Updated: Sep-18; Applicability: All

Default operating system accounts are disabled, renamed or have their passphrase changed.

Security Control: 0380; Revision: 8; Updated: Sep-21; Applicability: All

Unneeded operating system accounts, software, components, services and functionality are disabled or removed.

Security Control: 0341; Revision: 4; Updated: Dec-21; Applicability: All

Automatic execution features for removable media are disabled.

Security Control: 1654; Revision: 0; Updated: Sep-21; Applicability: All

Internet Explorer 11 is disabled or removed.

Security Control: 1655; Revision: 0; Updated: Sep-21; Applicability: All

.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.

Security Control: 1584; Revision: 1; Updated: Sep-21; Applicability: All

Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.

Security Control: 1491; Revision: 2; Updated: Sep-21; Applicability: All

Unprivileged users are prevented from running script execution engines in Microsoft Windows, including:

- Windows Script Host (cscript.exe and wscript.exe)
- PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe)
- Command Prompt (cmd.exe)
- Windows Management Instrumentation (wmic.exe)
- Microsoft Hypertext Markup Language (HTML) Application Host (mshta.exe).

Local administrator accounts

When local administrator accounts are used with common account names and passphrases, it can allow an adversary that compromises these credentials on one workstation or server to easily transfer across a network to other workstations or servers.

Security Control: 1410; Revision: 1; Updated: Sep-18; Applicability: All

Local administrator accounts are disabled; alternatively, passphrases that are random and unique for each device's local administrator account are used.

Security Control: 1469; Revision: 1; Updated: Sep-18; Applicability: All

Unique domain accounts with local administrative privileges, but without domain administrative privileges, are used for workstation and server management.

Application management

Users' ability to install any application can be exploited by an adversary using social engineering in order to convince them to install a malicious application. One way to manage this security risk, while also removing burden from system administrators, is to allow users the ability to install approved applications from organisation-managed software repositories or from trusted application marketplaces. Furthermore, to prevent users from removing security functionality, or breaking system functionality, users should not have the ability to uninstall or disable approved software.

Security Control: 1592; Revision: 0; Updated: Aug-20; Applicability: All

Users do not have the ability to install unapproved software.

Security Control: 0382; Revision: 6; Updated: Aug-20; Applicability: All

Users do not have the ability to uninstall or disable approved software.

Application control

Application control mechanisms can be an effective way to not only preventing malicious code from executing on workstations and servers, but also to ensure only approved applications can be installed. When developing application control rulesets, determining approved executables (e.g. .exe and .com files), software libraries (e.g. .dll and .ocx files), scripts (e.g. .ps1, .bat, .cmd, .vbs and .js files), installers (e.g. .msi, .msp and .mst files), compiled HTML (e.g. .chm), HTML applications (e.g. .hta), control panel applets (e.g. .cpl) and drivers based on business requirements is a more secure method than simply approving those currently residing on a workstation or server. Furthermore, it is preferable that organisations define their own application control rulesets, rather than relying on those from application control vendors, and validate them on an annual or more frequent basis.

In implementing application control solutions, organisations should use a reliable method, or combination of methods, such as cryptographic hash rules, publisher certificate rules or path rules. Depending on the method(s) chosen, further system hardening may be required to ensure that application control solutions or application control rulesets cannot be bypassed by an adversary.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1656, 1658, 1582, 1544, 1659 and 1662-1663 are not applicable.

Security Control: 0843; Revision: 9; Updated: Sep-21; Applicability: All

Application control is implemented on workstations.

Security Control: 1490; Revision: 3; Updated: Sep-21; Applicability: All

Application control is implemented on internet-facing servers.

Security Control: 1656; Revision: 0; Updated: Sep-21; Applicability: All

Application control is implemented on non-internet-facing servers.

Security Control: 1657; Revision: 0; Updated: Sep-21; Applicability: All

Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

Security Control: 1658; Revision: 0; Updated: Sep-21; Applicability: All

Application control restricts the execution of drivers to an organisation-approved set.

Security Control: 0955; Revision: 6; Updated: Apr-20; Applicability: All

Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.

Security Control: 1582; Revision: 1; Updated: Sep-21; Applicability: All

Application control rulesets are validated on an annual or more frequent basis.

Security Control: 1471; Revision: 2; Updated: Apr-20; Applicability: All

When implementing application control using publisher certificate rules, both publisher names and product names are used.

Security Control: 1392; Revision: 2; Updated: Apr-20; Applicability: All

When implementing application control using path rules, file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents (including adding new files) and individual files that are approved to execute.

Security Control: 1544; Revision: 2; Updated: Sep-21; Applicability: All

Microsoft's 'recommended block rules' are implemented.

Security Control: 1659; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft's 'recommended driver block rules' are implemented.

Security Control: 0846; Revision: 7; Updated: Apr-20; Applicability: All

All users (with the exception of privileged users when performing specific administrative activities) cannot disable, bypass or be exempted from application control.

Security Control: 1660; Revision: 0; Updated: Sep-21; Applicability: All

Allowed and blocked executions on workstations are logged.

Security Control: 1661; Revision: 0; Updated: Sep-21; Applicability: All

Allowed and blocked executions on internet-facing servers are logged.

Security Control: 1662; Revision: 0; Updated: Sep-21; Applicability: All

Allowed and blocked executions on non-internet-facing servers are logged.

Security Control: 0957; Revision: 8; Updated: Sep-21; Applicability: All

Application control event logs including the name of the file, the date/time stamp and the username of the user associated with the event.

Security Control: 1663; Revision: 0; Updated: Sep-21; Applicability: All

Application control event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Exploit protection

An adversary who develops exploits for Microsoft Windows will be more successful in exploiting security vulnerabilities when exploit protection functional in the operating system hasn't been enabled.

Security Control: 1492; Revision: 1; Updated: Sep-21; Applicability: All

Microsoft's exploit protection functionality is implemented on workstations and servers.

PowerShell

PowerShell is a powerful scripting language developed by Microsoft to provide an integrated interface for automated system administration. As such, it is an important part of system administrator toolkits due to its ubiquity and ease with which it can be used to fully control operating systems; however, it is also a dangerous exploitation tool in the hands of an adversary.

In order to prevent attacks leveraging security vulnerabilities in earlier PowerShell versions, Windows PowerShell 2.0 should be disabled or removed from operating systems. Additionally, PowerShell's language mode should be set to Constrained Language Mode to achieve a balance between security and functionality.

Finally, logging functionality available in PowerShell, such as module logging, script block logging and transcription, can provide invaluable information for incident responders following cyber security incidents that involved PowerShell being used for malicious purposes.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1621-1622 and 1665 are not applicable.

Security Control: 1621; Revision: 1; Updated: Sep-21; Applicability: All
Windows PowerShell 2.0 is disabled or removed.

Security Control: 1622; Revision: 0; Updated: Oct-20; Applicability: All
PowerShell is configured to use Constrained Language Mode.

Security Control: 1623; Revision: 0; Updated: Oct-20; Applicability: All
PowerShell is configured to use module logging, script block logging and transcription functionality.

Security Control: 1624; Revision: 0; Updated: Oct-20; Applicability: All
PowerShell script block logs are protected by Protected Event Logging functionality.

Security Control: 1664; Revision: 0; Updated: Sep-21; Applicability: All
Blocked PowerShell script executions are logged.

Security Control: 1665; Revision: 0; Updated: Sep-21; Applicability: All
PowerShell event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Host-based Intrusion Prevention System

Many security products rely on signatures to detect malicious code. This approach is only effective when malicious code has already been profiled and signatures are available. Unfortunately, an adversary can easily create variants of known malicious code to bypass traditional signature-based detection mechanisms. A Host-based Intrusion Prevention System (HIPS) can use behaviour-based detection to assist in identifying and blocking anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking, as well as detecting malicious code that has yet to be identified by security vendors.

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: All
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: All
A HIPS is implemented on high value servers such as authentication servers, Domain Name System servers, web servers, file servers and email servers.

Software firewall

Traditional network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from exfiltrating data, as they only control which ports or protocols can be used between different network segments. Many forms of malicious code are designed specifically to take advantage of this by using common protocols such as Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Simple Mail Transfer Protocol and Domain Name System. Software firewalls are more effective than traditional network firewalls as they can control which applications and services can communicate to and from workstations and servers. As such, a software firewall should be used to limit both inbound and outbound network connections to approved applications and services that are required by workstations and servers.

Security Control: 1416; Revision: 2; Updated: Sep-18; Applicability: All
A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.

Antivirus software

When vendors develop software they may make coding mistakes that lead to security vulnerabilities. An adversary can take advantage of this by developing malicious code to exploit any security vulnerabilities that have not been detected and remedied by vendors. As significant time and effort is often involved in developing functioning and reliable exploits, an adversary will often attempt to reuse their exploits as much as possible. While exploits may have been previously identified by security vendors, they often remain viable against organisations that do not have antivirus software in place to detect them.

Security Control: 1417; Revision: 3; Updated: Sep-21; Applicability: All

Antivirus software is implemented on workstations and servers and configured with:

- *signature-based detection enabled and set to a high level*
- *heuristic-based detection enabled and set to a high level*
- *ransomware protection measures enabled*
- *detection signatures checked for currency and updated on at least a daily basis*
- *automatic and regular scanning configured for all fixed disks and removable media.*

Security Control: 1390; Revision: 3; Updated: Dec-21; Applicability: All

Antivirus software has reputation rating functionality enabled.

Device access control software

Device access control software can be used to prevent unauthorised removable media and devices (e.g. smartphones, tablets, Bluetooth devices, wireless devices and 4G/5G dongles) from connecting to workstations and servers via external communication interfaces (e.g. Universal Serial Bus, Bluetooth and Near Field Communication). This can assist in preventing the introduction of malicious code or the exfiltration of data. In addition, an adversary can connect devices to locked workstations and servers via an external communication interface that allows Direct Memory Access (DMA). In doing so, the adversary can gain access to encryption keys or write any contents they want to memory (such as malicious code). The best defence against this security vulnerability is to disable access to external communication interfaces that allow DMA (e.g. FireWire, ExpressCard and Thunderbolt).

Security Control: 1418; Revision: 3; Updated: Dec-21; Applicability: All

Unauthorised removable media and devices are prevented from being connected to workstations and servers via the use of device access control software or by disabling external communication interfaces in operating systems.

Security Control: 0345; Revision: 6; Updated: Dec-21; Applicability: All

External communication interfaces that allow DMA are disabled.

Security Control: 0343; Revision: 5; Updated: Dec-21; Applicability: All

Removable media is prevented from being written to via the use of device access control software if there is no business requirement for its use.

Further information

Further information on the use of removable media can be found in the media usage section of the [Guidelines for Media](#).

Further information on patching operating systems can be found in the system patching section of the [Guidelines for System Management](#).

Further information on logging and auditing of operating system events can be found in the event logging and auditing section of the [Guidelines for System Monitoring](#).

Further information on securely configuring Microsoft Windows operating systems can be found in the ACSC's [Hardening Microsoft Windows 10 version 21H1 Workstations](#) publication.

Further information on end of support for Microsoft Windows operating systems can be found in the following ACSC publications:

- [End of Support for Microsoft Windows 10](#)
- [End of Support for Microsoft Windows Server 2008 and Windows Server 2008 R2](#).

Further information on securely configuring Linux workstations and servers can be found in the ACSC's [Hardening Linux Workstations and Servers](#) publication.

Further information on implementing application control can be found in the ACSC's [Implementing Application Control](#) publication.

Further information on Microsoft's [recommended block rules](#) and [recommended driver block rules](#) are available from Microsoft.

Further information on Microsoft's [exploit protection functionality](#) is available from Microsoft.

Further information on the use of PowerShell can be found in the ACSC's [Securing PowerShell in the Enterprise](#) publication.

Further information on [the use of PowerShell by blue teams](#) is available from Microsoft while further information on obtaining [greater visibility through PowerShell logging](#) is available from FireEye.

Further information on independent testing of antivirus software is available from [AV-Comparatives](#) and [AV-TEST](#).

Application hardening

Application selection

When selecting applications it is important that organisations preference vendors that have demonstrated a commitment to secure coding practices and have a strong track record of maintaining the security of their applications. This will assist not only with hardening applications but also increase the likelihood that vendors will release timely patches to remediate any security vulnerabilities found in their applications.

Security Control: 0938; Revision: 4; Updated: Sep-18; Applicability: All

Applications are chosen from vendors that have made a commitment to secure development and maintenance practices.

Application versions

Newer versions of applications often introduce improvements in security functionality. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of applications, especially key business applications such as office productivity suites, web browsers and their extensions, email clients, Portable Document Format (PDF) software, and security products exposes organisations to exploitation techniques that have since been mitigated in newer versions of applications.

Security Control: 1467; Revision: 2; Updated: Sep-21; Applicability: All

The latest releases of office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are used when present within SOEs.

Security Control: 1483; Revision: 0; Updated: Sep-18; Applicability: All

The latest releases of web server software, server applications that store important data, and other internet-accessible server applications are used when present within SOEs.

Hardening application configurations

By default, many applications enable functionality that is not required by users while security functionality may be disabled or set at a low level. This is especially risky for key business applications such as office productivity suites, web browsers and their extensions, email clients, PDF software, and security products that are likely to be targeted by an adversary. To assist in minimising this security risk, the ACSC produces guidance to assist in securely configuring key business applications. Furthermore, to assist in securely configuring their applications, vendors may provide their own security guides.

Security Control: 1486; Revision: 1; Updated: Sep-21; Applicability: All

Web browsers do not process Java from the internet.

Security Control: 1485; Revision: 1; Updated: Sep-21; Applicability: All

Web browsers do not process web advertisements from the internet.

Security Control: 1666; Revision: 0; Updated: Sep-21; Applicability: All

Internet Explorer 11 does not process content from the internet.

Security Control: 1667; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office is blocked from creating child processes.

Security Control: 1668; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office is blocked from creating executable content.

Security Control: 1669; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office is blocked from injecting code into other processes.

Security Control: 1542; Revision: 0; Updated: Jan-19; Applicability: All

Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Security Control: 1670; Revision: 0; Updated: Sep-21; Applicability: All

PDF software is blocked from creating child processes.

Security Control: 1412; Revision: 3; Updated: Sep-21; Applicability: All

ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.

Security Control: 1470; Revision: 4; Updated: Sep-21; Applicability: All

Any unrequired functionality in web browsers, Microsoft Office and PDF software is disabled.

Security Control: 1235; Revision: 3; Updated: Sep-21; Applicability: All

The use of web browser, Microsoft Office and PDF software add-ons is restricted to organisation approved add-ons.

Security Control: 1601; Revision: 0; Updated: Aug-20; Applicability: All

If supported, Microsoft's Attack Surface Reduction rules are implemented.

Security Control: 1585; Revision: 1; Updated: Sep-21; Applicability: All

Web browsers, Microsoft Office and PDF software security settings cannot be changed by users.

Microsoft Office macros

Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications programming language. A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by users to greatly improve their productivity; however, an adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to data. To reduce this security risk, organisations should disable Microsoft Office macros for users that do not have a demonstrated business requirement and secure their use for the remaining users that do.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1674, 1487, 1675-1676 and 1678 are not applicable.

Security Control: 1671; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

Security Control: 1488; Revision: 1; Updated: Sep-21; Applicability: All

Microsoft Office macros in files originating from the internet are blocked.

Security Control: 1672; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office macro antivirus scanning is enabled.

Security Control: 1673; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office macros are blocked from making Win32 API calls.

Security Control: 1674; Revision: 0; Updated: Sep-21; Applicability: All

Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

Security Control: 1487; Revision: 1; Updated: Sep-21; Applicability: All

Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

Security Control: 1675; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.

Security Control: 1676; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.

Security Control: 1489; Revision: 0; Updated: Sep-18; Applicability: All

Microsoft Office macro security settings cannot be changed by users.

Security Control: 1677; Revision: 0; Updated: Sep-21; Applicability: All

Allowed and blocked Microsoft Office macro executions are logged.

Security Control: 1678; Revision: 0; Updated: Sep-21; Applicability: All

Microsoft Office macro event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Further information

Further information on patching applications can be found in the system patching section of the [Guidelines for System Management](#).

Further information on securely configuring Microsoft Office can be found in the ACSC's [Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016](#) publication.

Further information on configuring Microsoft Office macro settings can be found in the ACSC's [Microsoft Office Macro Security](#) publication.

Authentication hardening

Account and authentication types

The guidance within this section is equally applicable to all account types. This includes unprivileged accounts, privileged accounts, break glass accounts and service accounts. In addition, the guidance is equally applicable to interactive authentication and non-interactive authentication.

Authenticating to systems

Before access to a system and its resources is granted to a user, it is essential that they are authenticated. This can be achieved via multi-factor authentication, such as a username along with a passphrase and security key, or via single-factor authentication, such as a username and passphrase.

Security Control: 1546; Revision: 0; Updated: Aug-19; Applicability: All

Users are authenticated before they are granted access to a system and its resources.

Multi-factor authentication

Multi-factor authentication uses two or more authentication factors to confirm a user's identity. This may include:

- something a user knows, such as a password
- something a user has, such as a security key, smart card, mobile phone or physical one-time password token
- something a user is, such as a fingerprint or their facial geometry.

Note, however, that if something a user knows is written down, or typed into a file and stored as plaintext, this becomes something that a user has rather than something a user knows.

Privileged users, users of remote access solutions and users with access to important data repositories are more likely to be targeted by an adversary due to their level of access. For this reason, it is especially important that multi-factor authentication is used for these accounts. In addition, multi-factor authentication is vital to any system administration activities as it can limit the consequences of a compromise by preventing or slowing an adversary's ability to gain unrestricted access to assets. In this regard, multi-factor authentication can be implemented as part of jump server authentication where assets being administered do not support multi-factor authentication themselves.

When implementing multi-factor authentication, several different authentication factors can be implemented. Unfortunately, some authentication factors such as biometrics or codes sent via Short Message Service, Voice over Internet Protocol or email are more susceptible to compromise than others. For this reason, authentication factors that involve something a user has is recommended for use as part of multi-factor authentication. Furthermore, for increased security, the use of verifier impersonation resistant authentication factors are recommended to protect against real-time phishing attacks.

The benefit of implementing multi-factor authentication can be diminished when credentials are reused on other systems. For example, when usernames and passphrases used as part of multi-factor authentication for remote access are the same as those used for corporate workstations. In such circumstances, if an adversary had compromised the device used for remote access, they could capture the username and passphrase for reuse against a corporate workstation that does not require the use of multi-factor authentication.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1505, 1682 and 1684 are not applicable.

Security Control: 0974; Revision: 6; Updated: Sep-21; Applicability: All

Multi-factor authentication is used to authenticate unprivileged users of systems.

Security Control: 1173; Revision: 4; Updated: Sep-21; Applicability: All

Multi-factor authentication is used to authenticate privileged users of systems.

Security Control: 1504; Revision: 1; Updated: Sep-21; Applicability: All

Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.

Security Control: 1679; Revision: 0; Updated: Sep-21; Applicability: All

Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

Security Control: 1680; Revision: 0; Updated: Sep-21; Applicability: All

Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.

Security Control: 1681; Revision: 0; Updated: Sep-21; Applicability: All

Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.

Security Control: 1505; Revision: 1; Updated: Sep-21; Applicability: All

Multi-factor authentication is used to authenticate users accessing important data repositories.

Security Control: 1401; Revision: 5; Updated: Sep-21; Applicability: All

Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

Security Control: 1682; Revision: 0; Updated: Sep-21; Applicability: All

Multi-factor authentication is verifier impersonation resistant.

Security Control: 1559; Revision: 1; Updated: Dec-21; Applicability: All

Passwords used for multi-factor authentication are a minimum of 6 characters, unless more stringent requirements apply.

Security Control: 1560; Revision: 1; Updated: Dec-21; Applicability: S

Passwords used for multi-factor authentication on SECRET systems are a minimum of 8 characters.

Security Control: 1561; Revision: 1; Updated: Dec-21; Applicability: TS

Passwords used for multi-factor authentication on TOP SECRET systems are a minimum of 10 characters.

Security Control: 1357; Revision: 1; Updated: Sep-18; Applicability: All

When multi-factor authentication is implemented, none of the authentication factors on their own can be used for single-factor authentication to another system.

Security Control: 1683; Revision: 0; Updated: Sep-21; Applicability: All

Successful and unsuccessful multi-factor authentications are logged.

Security Control: 1684; Revision: 0; Updated: Sep-21; Applicability: All

Multi-factor authentication event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Single-factor authentication

A significant threat to the compromise of accounts is credential cracking tools. When an adversary gains access to a list of usernames and hashed credential from a system they can attempt to recover username and credential pairs by comparing the hashes of known credentials with the hashed credentials they have gained access to. By finding a match an adversary will know the credential associated with a given username.

In order to reduce this security risk, organisations should implement multi-factor authentication. Note, while single-factor authentication is no longer considered suitable for protecting sensitive or classified data, it may not be possible to implement multi-factor authentication on some systems. In such cases, organisations will need to increase the time on average it takes an adversary to compromise a credential by continuing to increase its length over time. Such increases in length can be balanced against useability through the use of passphrases rather than passwords. In cases where systems don't support passphrases, and as an absolute last resort, the strongest password length and complexity supported by a system will need to be implemented.

Security Control: 0417; Revision: 5; Updated: Oct-19; Applicability: All

When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.

Security Control: 0421; Revision: 8; Updated: Dec-21; Applicability: All

Passphrases used for single-factor authentication are at least 4 random words with a total minimum length of 14 characters, unless more stringent requirements apply.

Security Control: 1557; Revision: 2; Updated: Dec-21; Applicability: S

Passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters.

Security Control: 0422; Revision: 8; Updated: Dec-21; Applicability: TS

Passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters.

Security Control: 1558; Revision: 1; Updated: Apr-20; Applicability: All

Passphrases used for single-factor authentication:

- *are not constructed from song lyrics, movies, literature or any other publicly available material*
- *do not form a real sentence in a natural language*
- *are not a list of categorised words.*

Security Control: 1596; Revision: 0; Updated: Aug-20; Applicability: All

Passphrases used for single-factor authentication cannot be used to authenticate to multiple different systems.

Setting and resetting credentials for user accounts

When credentials for users are set or reset on their behalf, it is important that a user's identity is sufficiently verified beforehand (e.g. by the user physically presenting themselves and their pass to a service desk or known colleague, or by the user answering a set of challenge-response questions). Following the verification of the user's identity, credentials should be randomly generated and provided to the user via a secure communications channel. Subsequently, users should reset their credential on first use to ensure that it is not known by anyone else.

Security Control: 1227; Revision: 4; Updated: Aug-20; Applicability: All

Passwords/passphrases set or reset on users' behalf are randomly generated.

Security Control: 1593; Revision: 0; Updated: Aug-20; Applicability: All

Users provide sufficient evidence to verify their identity when collecting a password/passphrase for their account.

Security Control: 1594; Revision: 0; Updated: Aug-20; Applicability: All

Passwords/passphrases are provided to users via a secure communications channel or, if not possible, split into parts with part being provided to the user and part provided to the user's supervisor.

Security Control: 1595; Revision: 0; Updated: Aug-20; Applicability: All

Users that do not set their own initial password/passphrase are required to change it on first use.

Setting and resetting credentials for service accounts

To provide additional security and credential management functionality for service accounts, Microsoft introduced group Managed Service Accounts in Microsoft Windows Server 2012. In doing so, service accounts that are created as group Managed Service Accounts do not require manual credential management by system administrators, as the operating system automatically manages the credentials. This ensures that service account credentials are not misplaced or forgotten, and that they are automatically changed on a regular basis.

Security Control: 1619; Revision: 0; Updated: Oct-20; Applicability: All

Service accounts are created as group Managed Service Accounts.

Account lockouts

Locking an account after a specified number of failed logon attempts reduces the likelihood of successful credential spraying attacks; however, care should be taken as implementing account lockout functionality can increase the likelihood of a denial of service. Alternatively, some systems may be configured to automatically slowdown repeated failed logon attempts (known as logon rate limiting) rather than locking accounts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful credential spraying attacks.

Security Control: 1403; Revision: 2; Updated: Oct-19; Applicability: All

Accounts are locked out after a maximum of five failed logon attempts.

Security Control: 0431; Revision: 2; Updated: Sep-18; Applicability: All

Repeated account lockouts are investigated before reauthorising access.

Account unlocks

To reduce the likelihood of social engineering being used to compromise accounts, users should provide sufficient evidence to verify their identity when requesting an account unlock.

Security Control: 0976; Revision: 6; Updated: Aug-20; Applicability: All

Users provide sufficient evidence to verify their identity when requesting an account unlock.

Insecure authentication methods

Authentication methods need to resist theft, interception, duplication, forgery, unauthorised access and unauthorised modification. For example, Local Area Network (LAN) Manager and NT LAN Manager authentication methods use weak hashing algorithms. As such, credentials used as part of LAN Manager authentication and NT LAN Manager authentication (i.e. NTLMv1, NTLMv2 and NTLM2) can easily be compromised. Instead, organisations should use Kerberos for authentication within Microsoft Windows environments and ensure all privileged accounts are members of the Protected Users security group.

Security Control: 1603; Revision: 0; Updated: Aug-20; Applicability: All

Authentication methods susceptible to replay attacks are disabled.

Security Control: 1055; Revision: 4; Updated: Oct-20; Applicability: All

LAN Manager and NT LAN Manager authentication methods are disabled.

Security Control: 1620; Revision: 0; Updated: Oct-20; Applicability: All

Privileged accounts are members of the Protected Users security group.

Protecting credentials

Storing credentials with a system that it grants access to increases the likelihood of an adversary gaining access to the system. For example, a credential should never be written down and stuck to a laptop or computer monitor while security keys, smartcards or one-time password tokens should never be left with computers or in laptop bags. Furthermore, obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers.

If storing credentials on a system, sufficient protection should be implemented to prevent them from being compromised. For example, credentials can be stored in a password vault or hardware security module, while credentials stored in a database can be hashed, salted and stretched. In addition, security functionality, such as Windows Defender Credential Guard and Windows Defender Remote Credential Guard, can be enabled to provide additional protection for credentials.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security control 1686 is not applicable.

Security Control: 1685; Revision: 0; Updated: Sep-21; Applicability: All

Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.

Security Control: 0418; Revision: 4; Updated: Oct-19; Applicability: All

Credentials are stored separately from systems to which they grant access.

Security Control: 1597; Revision: 0; Updated: Aug-20; Applicability: All

Credentials are obscured as they are entered into systems.

Security Control: 1402; Revision: 5; Updated: Aug-20; Applicability: All

Stored passwords/passphrases are protected by ensuring they are hashed, salted and stretched.

Security Control: 1686; Revision: 0; Updated: Sep-21; Applicability: All

Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.

Security Control: 1590; Revision: 0; Updated: Aug-20; Applicability: All

Passwords/passphrases are changed if:

- *they are directly compromised*
- *they are suspected of being compromised*
- *they appear in online data breach databases*
- *they are discovered stored in the clear on a network*
- *they are discovered being transferred in the clear across a network*
- *membership of a shared account changes*
- *they have not been changed in the past 12 months.*

Session termination

Implementing measures to automatically terminate user sessions outside of business hours after an appropriate period of inactivity, followed by a workstation reboot, can assist in both system maintenance activities as well as removing any adversaries that may have compromised a system but failed to gain persistence.

Security Control: 0853; Revision: 1; Updated: Aug-20; Applicability: All

Outside of business hours, and after an appropriate period of inactivity, user sessions are terminated and workstations are rebooted.

Session and screen locking

Session and screen locking prevents unauthorised access to a system which a user has already authenticated to.

Security Control: 0428; Revision: 7; Updated: Jun-21; Applicability: All

Systems are configured with a session or screen lock that:

- *activates after a maximum of 15 minutes of user inactivity, or if manually activated by the user*
- *conceals all session content on the screen*
- *ensures that the screen does not enter a power saving state before the session or screen lock is activated*
- *requires the user to reauthenticate to unlock the system*
- *denies users the ability to disable the session or screen locking mechanism.*

Logon banner

Displaying a logon banner to users before access is granted to a system reminds them of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- the user's agreement to abide by abovementioned policies
- legal ramifications of violating the abovementioned policies
- details of monitoring and auditing activities
- a point of contact for any questions.

Security Control: 0408; Revision: 4; Updated: Sep-18; Applicability: All

Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.

Security Control: 0979; Revision: 4; Updated: Sep-18; Applicability: All

Legal advice is sought on the exact wording of logon banners.

Further information

Further information on authorisations, security clearances and briefings for system access can be found in the access to systems and their resources section of the [Guidelines for Personnel Security](#).

Further information on restricting administrative privileges can be found in the ACSC's [Restricting Administrative Privileges](#) publication.

Further information on implementing multi-factor authentication can be found in the ACSC's [Implementing Multi-Factor Authentication](#) publication.

Further information on mitigating the use of stolen credentials can be found in the ACSC's [Mitigating the Use of Stolen Credentials](#) publication.

Further information on [randomly generating passphrases](#) (preferably using five dice rolls and the long word list) is available from the Electronic Frontier Foundation while a [random dice roller](#) is available from RANDOM.ORG.

Virtualisation hardening

Containerisation

Containers allow for versatile deployment of systems, and can be used to quickly scale systems. However, they are still systems that run software and should be treated as any other system. Application of security controls in a containerised environment may take a different form when compared to other types of systems. For example, patching operating systems on workstations may be actioned differently to ensuring that a patched image is being used for a container, however the principle is the same. In general, the same security risks that apply to non-containerised systems would likely apply to containerised systems.

Functional separation between computing environments

Software-based isolation mechanisms are commonly used to share a physical server's hardware among multiple computing environments. The benefits of using software-based isolation mechanisms to share a physical server's hardware include increasing the range of activities that it can be used for and maximising the utilisation of its hardware.

A computing environment could consist of an entire operating system installed in a virtual machine where the isolation mechanism is a hypervisor, as is commonly used in cloud services providing Infrastructure as a Service. Alternatively, a computing environment could consist of an application which uses the shared kernel of the underlying operating system of the physical server where the isolation mechanisms are application containers or application sandboxes, as is commonly used in cloud services providing Platform as a Service. The logical separation of data within a single application, which is commonly used in cloud services providing Software as a Service, is not considered to be the same as multiple computing environments.

An adversary who has compromised a single computing environment, or who legitimately controls a single computing environment, might exploit a misconfiguration or security vulnerability in the isolation mechanism to compromise other computing environments on the same physical server, or compromise the underlying operating system of the physical server.

Security Control: 1460; Revision: 2; Updated: Aug-20; Applicability: All

When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that uses secure coding practices and, when security vulnerabilities have been identified, develops and distributes patches in a timely manner.

Security Control: 1604; Revision: 0; Updated: Aug-20; Applicability: All

When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.

Security Control: 1605; Revision: 0; Updated: Aug-20; Applicability: All

When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system running on the server is hardened.

Security Control: 1606; Revision: 0; Updated: Aug-20; Applicability: All

When using a software-based isolation mechanism to share a physical server's hardware, patches are applied to the isolation mechanism and underlying operating system in a timely manner.

Security Control: 1607; Revision: 0; Updated: Aug-20; Applicability: All

When using a software-based isolation mechanism to share a physical server's hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.

Security Control: 1461; Revision: 4; Updated: Dec-21; Applicability: S, TS

When using a software-based isolation mechanism to share a physical server's hardware for SECRET or TOP SECRET workloads, the physical server and all computing environments running on the physical server are of the same classification and within the same security domain.

Further information

Further information on hypervisor security can be found in National Institute of Standards and Technology Special Publication 800-125A Rev. 1, [Security Recommendations for Server-based Hypervisor Platforms](#).

Further information on container security can be found in National Institute of Standards and Technology Special Publication 800-190, [Application Container Security Guide](#).