Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# Essential Eight Maturity Model Changes

**First published:** November 2023
**Last updated**:

# Introduction

The following are the changes for the November 2023 update of the Australian Signals Directorate (ASD)'s *Essential Eight Maturity Model*.

# Overview of changes

## Patch applications and operating systems

In response to an ASD assessment of the average time taken by malicious actors to exploit vulnerabilities, additional focus has been placed on higher priority patching scenarios. Specifically, when vendors assess a vulnerability to be of a critical nature (e.g. it facilitates authentication bypasses that grant privileged access or facilitates remote code execution without user interaction). In such circumstances, organisations should patch, update or otherwise mitigate vulnerabilities within 48 hours. This change impacts Maturity Level One through Maturity Level Three.

In providing prioritised patching guidance, increased emphasis has been placed on patching applications that routinely interact with untrusted content from the internet, such as office productivity suites, web browsers, email clients, PDF software and security software. In doing so, the patching timeframe for these applications has been strengthened from within one month to within two weeks. This has also resulted in an associated strengthening in vulnerability scanning activities from at least fortnightly to at least weekly for these applications. This change impacts Maturity Level One.

To counter-balance changes made to strengthening patching timeframes for higher risk scenarios, patching of operating systems for less important devices, such as workstations, non-internet-facing servers and non-internet-facing network devices, have been rebalanced from within two weeks to within one month. This has also resulted in an associated rebalancing of the required frequency of vulnerability scanning activities for such devices from at least weekly to at least fortnightly. This change impacts Maturity Level Two and Maturity Level Three.

Finally, a requirement to apply patches, updates or other vendor mitigations for vulnerabilities in drivers and firmware has been added to mitigate known vulnerabilities. This change impacts Maturity Level Three.

## Multi-factor authentication

Previously, Maturity Level One did not specify the types of authentication factors that could be used for multi-factor authentication (MFA). This led to the adoption of weaker forms of MFA that used biometrics, security questions or 'Trusted Signals', none of which are recognised as valid authentication factors within standards. In response, a new minimum standard that requires 'something users have', in addition to 'something users know', has been adopted. This change impacts Maturity Level One.

In responding to ongoing attacks against citizens that continue to rely on just passwords for online customer services, the requirement for organisations to enforce the use of MFA for protecting web portals that store sensitive customer data (e.g. personal, health or identity-related data) has been adopted. In doing so, this change amends the existing requirement that allowed customers to easily opt-out of using MFA and instead use very weak password-based authentication. Furthermore, an approach of providing the option of phishing-resistant MFA for customers at lower maturity levels, while requiring its use for customers at higher maturity levels, has also been adopted. This change impacts Maturity Level One through Maturity Level Three.

In response to greater MFA adoption, international standards that are increasingly becoming business-as-usual (e.g. FIDO2/WebAuthn), the rise of attacks against weaker MFA implementations (e.g. those susceptible to real-time phishing attacks or social engineering attacks), and cyber policy changes being made by ASD's international partners, MFA requirements have been bolstered to require the use of phishing-resistant MFA by organisations at a lower maturity level. This impacts Maturity Level Two.

Finally, a requirement has been added for users to authenticate to their workstations using a form of phishing-resistant MFA (e.g. smart cards, security keys or Windows Hello for Business). This change impacts Maturity Level Two and Maturity Level Three.

## Restrict administrative privileges

Due to the absence of governance processes for granting, controlling and rescinding privileged access to data repositories, requirements have been added to ensure consistency with governance processes for granting, controlling and rescinding privileged access to systems and applications. This change impacts Maturity Level One through Maturity Level Three.

Requirements preventing access to the internet by privileged user accounts have been amended in a measured manner to support the management of cloud services. In doing so, such user accounts will need to be explicitly identified and strictly limited to required accesses and duties. This change impacts Maturity Level One through Maturity Level Three.

Requirements ensuring that credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed have been expanded to include break glass accounts as these user accounts are the most powerful user accounts for systems. This change impacts Maturity Level Two and Maturity Level Three.

Finally, additional requirements focused on the hardening of administrative infrastructure used by privileged users have been added. This includes the use of Secure Admin Workstations as well as enabling both memory isolation and Local Security Authority protection functionality within Microsoft Windows. This change impacts Maturity Level Three.

## Application control

In response to malicious actors increasingly using living off the land techniques, and insights gained from Essential Eight implementation assessments, application control changes have focused on performing annual reviews of application control rulesets and implementing Microsoft's recommended application blocklist at a lower maturity level. This change impacts Maturity Level Two.

## Restrict Microsoft Office macros

Due to a lack of native support for macro execution event logging in Microsoft Windows, associated implementation challenges with attempting to capture such events, and advice from incident responders and threat hunters that such events provide limited benefit, the requirement to collect and analyse these events for signs of compromise has been removed. This change impacts Maturity Level Two and Maturity Level Three.

Due to a vulnerability in digitally-signed macros that allows for tampering of macro code without invalidating a file's digital signature, a requirement has been added to enforce the use of newer, and more secure, V3 digital signatures for macros. This change impacts Maturity Level Three.

## User application hardening

As Internet Explorer 11 is no longer supported by Microsoft, and does not receive updates for any identified vulnerabilities, organisations are now required to either disable its use or uninstall it from operating systems. This change impacts Maturity Level One and Maturity Level Two.

The requirement to implement either ASD or vendor hardening guidance has been amended to require the implementation of both where available, with the more stringent requirements taking precedence when conflicts occur. This change impacts Maturity Level Two and Maturity Level Three.

Finally, the PowerShell logging requirement was amended to avoid duplicating application control logging and instead focus on leveraging native PowerShell logging functionality. Supporting this, a requirement to log command line process creation events has been added. This covers both shells a malicious actor can use to execute commands on compromised devices. This change impacts Maturity Level Two and Maturity Level Three.

## Regular backups

While no significant changes have been made to this mitigation strategy, organisations are now encouraged to consider the business criticality of their data when prioritising backups rather than focusing exclusively on backing up important data. This change impacts Maturity Level One through Maturity Level Three.

## Various

As a cross-cutting measure, the centralised collection, protection and analysis of event logs to detect potential signs of compromise, in addition to reporting and responding to identified cyber security incidents, will now be required at Maturity Level Two. However, given the threat model for Maturity Level Two (which prioritises the protection of internet-facing infrastructure), analysis of event logs at this maturity level should be focused on detecting signs of compromise in internet-facing infrastructure rather than all organisational assets within an ICT environment.

Finally, this update has adopted language from mapped controls within the *Information Security Manual* (ISM). This will ensure consistency between the two publications while also allowing for the ISM's OSCAL baselines for the Essential Eight to be automatically ingested by governance, reporting and compliance tools within organisations for Essential Eight tracking and reporting purposes.

# Changes by maturity level

## Maturity Level One

### Patch applications

- Changing the requirement for 48-hour response timeframes for addressing vulnerabilities in online services from being applicable only when exploits for vulnerabilities exist to when either vulnerabilities are assessed as critical by vendors or working exploits exist.
- Changing the requirement for conducting vulnerability scanning activities for high-risk software from at least fortnightly to at least weekly.

- Changing the requirement for patching vulnerabilities in high-risk software from within one month to within two weeks.

### Patch operating systems

- Changing the requirement for 48-hour response timeframes for addressing vulnerabilities in operating systems of internet-facing servers and internet-facing network devices from being applicable only when exploits for vulnerabilities exist to when either vulnerabilities are assessed as critical by vendors or working exploits exist.

### Multi-factor authentication

- Removing the caveat that customers of online customer services that process, store or communicate sensitive customer data can easily opt-out of using multi-factor authentication.
- Adding a requirement that 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.

### Restrict administrative privileges

- Adding a requirement that requests for privileged access to data repositories are validated when first requested.
- Changing the requirement for the types of privileged user accounts that can access the internet from only privileged service accounts to all privileged user accounts explicitly authorised to do so.
- Adding a requirement that privileged user accounts that have been explicitly authorised to access the internet are strictly limited to only what is required for users and services to undertake their duties.

### Application control

- Changing the requirement for implementation of application control from using NTFS permissions to using an application control solution, either in-built for an operating system or an equivalent third-party vendor solution.

### Restrict Microsoft Office macros

- No significant change.

### User application hardening

- Changing the requirement for Internet Explorer 11 from not processing content from the internet to being disabled or removed.

### Regular backups

- No significant change.

## Maturity Level Two

### Patch applications

- Changing the requirement for 48-hour response timeframes for addressing vulnerabilities in online services from being applicable only when exploits for vulnerabilities exist to when either vulnerabilities are assessed as critical by vendors or working exploits exist.

## Patch operating systems

- Changing the requirement for 48-hour response timeframes for addressing vulnerabilities in operating systems of internet-facing servers and internet-facing network devices from being applicable only when exploits for vulnerabilities exist to when either vulnerabilities are assessed as critical by vendors or working exploits exist.
- Changing the requirement for conducting vulnerability scanning activities for operating systems of workstations, non-internet-facing servers and non-internet-facing network devices from at least weekly to at least fortnightly.
- Changing the requirement for patching vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices from within two weeks to within one month.

## Multi-factor authentication

- Removing the caveat that customers of online customer services that process, store or communicate sensitive customer data can easily opt-out of using multi-factor authentication.
- Adding a requirement that multi-factor authentication be used to authenticate unprivileged users of systems to their devices.
- Adding a requirement that multi-factor authentication used for authenticating users of online services be phishing-resistant.
- Adding a requirement that multi-factor authentication used for authenticating customers of online customer services provide a phishing-resistant option.
- Adding a requirement that multi-factor authentication used for authenticating users of systems to their devices be phishing-resistant.
- Changing the requirement for event log retention from local logged to centralised logging.
- Adding a requirement that event logs are protected from unauthorised modification and deletion.
- Adding a requirement that event logs for internet-facing servers are monitored for signs of compromise.
- Adding a requirement that cyber security incidents are reported to both an organisation's CISO and ASD.
- Adding a requirement that cyber security incident response plans are enacted in response to cyber security incidents.

## Restrict administrative privileges

- Adding a requirement that requests for privileged access to data repositories are validated when first requested.
- Adding a requirement that privileged access to data repositories are disabled after 12 months unless revalidated.
- Changing the requirement for the types of privileged user accounts that can access the internet from only privileged service accounts to all privileged user accounts explicitly authorised to do so.
- Adding a requirement that privileged user accounts that have been explicitly authorised to access the internet are strictly limited to only what is required for users and services to undertake their duties.
- Adding a requirement that credentials for break glass accounts are long, unique, unpredictable and managed.
- Changing the requirement for event log retention from local logged to centralised logging.
- Adding a requirement that event logs are protected from unauthorised modification and deletion.
- Adding a requirement that event logs for internet-facing servers are monitored for signs of compromise.
- Adding a requirement that cyber security incidents are reported to both an organisation's CISO and ASD.
- Adding a requirement that cyber security incident response plans are enacted in response to cyber security incidents.

### Application control

- Adding a requirement that Microsoft's recommended application blocklist be implemented.
- Adding a requirement that application control rulesets are validated at least annually.
- Changing the requirement for event log retention from local logged to centralised logging.
- Adding a requirement that event logs are protected from unauthorised modification and deletion.
- Adding a requirement that event logs for internet-facing servers are monitored for signs of compromise.
- Adding a requirement that cyber security incidents are reported to both an organisation's CISO and ASD.
- Adding a requirement that cyber security incident response plans are enacted in response to cyber security incidents.

### Restrict Microsoft Office macros

- Removing the requirement for allowed and blocked Microsoft Office macro events to be logged.

### User application hardening

- Changing the requirement for Internet Explorer 11 from not processing content from the internet to being disabled or removed.
- Changing the requirement for implementing hardening guidance from implementing ASD or vendor hardening guidance to implementing ASD and vendor hardening guidance, with the most restrictive requirements taking precedence when conflicts occur.
- Changing the requirement for PowerShell event log collection from application control events associated with blocked PowerShell scripts to PowerShell module logging, script block logging and transcription events.
- Adding a requirement for logging of command line process creation events.
- Changing the requirement for event log retention from local logged to centralised logging.
- Adding a requirement that event logs are protected from unauthorised modification and deletion.
- Adding a requirement that event logs for internet-facing servers are monitored for signs of compromise.
- Adding a requirement that cyber security incidents are reported to both an organisation's CISO and ASD.
- Adding a requirement that cyber security incident response plans are enacted in response to cyber security incidents.

### Regular backups

- No significant change.

## Maturity Level Three

### Patch applications

- Changing the requirement for 48-hour response timeframes for addressing vulnerabilities in online services from being applicable only when exploits for vulnerabilities exist to when either vulnerabilities are assessed as critical by vendors or working exploits exist.

## Patch operating systems

- Changing the requirement for 48-hour response timeframes for addressing vulnerabilities in operating systems of internet-facing servers and internet-facing network devices from being applicable only when exploits for vulnerabilities exist to when either vulnerabilities are assessed as critical by vendors or working exploits exist.
- Changing the requirement for conducting vulnerability scanning activities for operating systems of workstations, non-internet-facing servers and non-internet-facing network devices from at least weekly to at least fortnightly.
- Adding a requirement that a vulnerability scanner be used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.
- Adding a requirement that a vulnerability scanner be used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.
- Changing the requirement for patching vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices from within two weeks to within one month.
- Adding a requirement that patches, updates or other vendor mitigations for vulnerabilities in drivers be applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
- Adding a requirement that patches, updates or other vendor mitigations for vulnerabilities in drivers be applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
- Adding a requirement that patches, updates or other vendor mitigations for vulnerabilities in firmware be applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
- Adding a requirement that patches, updates or other vendor mitigations for vulnerabilities in firmware be applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

## Multi-factor authentication

- Removing the caveat that customers of online customer services that process, store or communicate sensitive customer data can easily opt-out of using multi-factor authentication.
- Adding a requirement that multi-factor authentication be used to authenticate unprivileged users of systems to their devices.
- Changing the requirement for the implementation of multi-factor authentication from important data repositories to all data repositories, with prioritisation of important data repositories being encouraged.

## Restrict administrative privileges

- Adding a requirement that requests for privileged access to data repositories are validated when first requested.
- Adding a requirement that privileged access to data repositories are disabled after 12 months unless revalidated.
- Adding a requirement that privileged access to data repositories are limited to only what is required for users and services to undertake their duties.
- Changing the requirement for the types of privileged user accounts that can access the internet from no privileged user accounts to all privileged user accounts explicitly authorised to do so.
- Adding a requirement that privileged user accounts that have been explicitly authorised to access the internet are strictly limited to only what is required for users and services to undertake their duties.
- Adding a requirement that Secure Admin Workstations are used in the performance of administrative activities.

- Adding a requirement that credentials for break glass accounts are long, unique, unpredictable and managed.
- Adding a requirement that Microsoft Windows's memory integrity functionality be enabled.
- Adding a requirement that Microsoft Windows's Local Security Authority protection functionality be enabled.

### Application control

- No significant change.

### Restrict Microsoft Office macros

- Adding a requirement that Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.
- Adding a requirement that Microsoft Office macros digitally signed by signatures other than V3 signatures are prevented from being enabled via the Message Bar or Backstage View.
- Removing the requirement for allowed and blocked Microsoft Office macro events to be logged.

### User application hardening

- Changing the requirement for implementing hardening guidance from implementing ASD or vendor hardening guidance to implementing ASD and vendor hardening guidance, with the most restrictive requirements taking precedence when conflicts occur.
- Changing the requirement for PowerShell event log collection from application control events associated with blocked PowerShell scripts to PowerShell module logging, script block logging and transcription events.
- Adding a requirement for logging of command line process creation events.

### Regular backups

- No significant change.

# Contact details

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

**Disclaimer**

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

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



## For more information, or to report a cyber security incident, contact us:

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


**Australian Government**

**Australian Signals Directorate**