# Essential Eight Maturity Model FAQ

Content complexity

**Moderate**

## Content written for

- Small & medium business
- Large organisations & infrastructure
- Government

## Attachments

**PROTECT - Essential Eight Maturity Model FAQ (February 2023)**
1.13MB .pdf

This publication was developed to answer frequently asked questions on the Australian Cyber Security Centre (ACSC)'s *Essential Eight Maturity Model* (E8MM).

# Frequently asked questions

## General questions

### What is the Essential Eight?

- While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC's *Strategies to Mitigate Cyber Security Incidents* as a baseline. This baseline, known as the Essential Eight, makes it much harder for malicious actors to compromise systems.
- The mitigation strategies that constitute the Essential Eight are: application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication and regular backups.

### Why should I implement the Essential Eight?

- Implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber incident.

### What is the *Essential Eight Maturity Model*?

- The E8MM is designed to assist organisations to implement the Essential Eight in a graduated manner based upon different levels of tradecraft and targeting.
- The different maturity levels can also be used to provide a high-level indication of an organisation's cyber security maturity.

### Why update the *Essential Eight Maturity Model*?

- The ACSC is committed to providing cyber security advice that is contemporary, contestable and actionable. This includes regular updates to the E8MM.

through its cyber threat intelligence and cyber incident response functions.

- The ACSC also learns of how our cyber security advice is implemented within organisations as part of Essential Eight assessment and uplift activities.
- Updates to the E8MM follow a thorough review by the ACSC, which includes consultation with government and industry partners.

## *Essential Eight Maturity Model* update (November 2022)

### What were the updates?

- Organisations are recommended to use an automated method of asset discovery at least fortnightly to detect what assets reside on their network (to assist with follow-on vulnerability scanning activities).
- Organisations are recommended to ensure their vulnerability scanners are using an up-to-date vulnerability database before conducting vulnerability scanning activities.
- Minor grammar amendments were made throughout for increased clarity (these changes have not changed the intent of existing requirements).

## *Essential Eight Maturity Model* update (October 2021)

### What were the updates?

- Minor formatting updates to increase the usability of the publication in PDF and HTML formats.

## *Essential Eight Maturity Model* update (July 2021)

### What were the updates?

- Redefining the number of maturity levels and what they represent.
- Moving to a stronger risk-based approach to implementation.
- Implementing the mitigation strategies as a package.

### How were the maturity levels updated?

### Why was Maturity Level Zero reintroduced?

- Maturity Level Zero has been reintroduced to the *Essential Eight Maturity Model* to provide a broader range of maturity level ratings for assessors to consider when evaluating Essential Eight implementations.

## How is the maturity model moving to a stronger risk-based approach to implementation?

- There will be circumstances (such as legacy systems and technical debt) that may prevent immediate or full implementation of requirements within the *Essential Eight Maturity Model*. In such cases, risk management processes may adequately address this.

## How can the mitigation strategies be implemented as a package?

- Organisations previously implemented each of the mitigation strategies individually. This approach was seen as leading to an imbalanced cyber security posture when resources were used implementing a few mitigation strategies to higher maturity levels while other mitigation strategies were not addressed, or addressed at a lower maturity level.
- Achieving a maturity level as a package will provide a more secure baseline than achieving higher maturity levels in a few mitigation strategies to the detriment of others. This is due to the Essential Eight being designed to complement each other and to provide broad coverage of various cyber threats.
- Organisations are now advised to achieve a consistent maturity level across all eight mitigation strategies before moving onto a higher maturity level.

## What changes were made to 'application control'?

- Additional executable content types (i.e. compiled HTML, HTML applications and control panel applets) were introduced for all maturity levels.
- Maturity Level One was updated to focus on using file system access permissions to prevent malware executing from user profiles and temporary folders used by operating systems, web browsers and email clients.
- Maturity Level One was updated to remove the use of application control for servers.

- Maturity Level Three introduced an annual (or more frequent) validation of application control rules.
- Maturity Level Three introduced monitoring to support identification and response to cyber events.

## What changes were made to 'patch applications'?

- Patching requirements were updated for all maturity levels to remove the need for every vulnerability to be individually risk-assessed to determine patching timeframes.
- The patching of internet-facing services within 48 hours if an exploit exists, otherwise within two weeks of release, was introduced for all maturity levels.
- The use of vulnerability scanners was introduced for all maturity levels to identify missing patches. The use and frequency of vulnerability scanners differs depending on the maturity level and was generally set at double the frequency of patching timeframes.
- Maturity Level One was updated to focus on internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products rather than all applications and drivers. This included the removal of unsupported versions.
- Maturity Level One introduced patching office productivity suites, web browsers and their extensions, email clients, PDF software, and security products within one month of release.
- Maturity Level Two introduced patching office productivity suites, web browsers and their extensions, email clients, PDF software, and security products within two weeks of release.
- Maturity Level Two introduced patching all other applications within one month of release.
- Maturity Level Two was updated to recommend removing unsupported versions of internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products rather than all applications.
- Maturity Level Three introduced patching office productivity suites, web browsers and their extensions, email clients, PDF software, and security products within 48 hours if an exploit exists, otherwise within two weeks of release.

- To lower an organisation's attack surface, all maturity levels were updated to recommend that macros are disabled for all users who do not have a demonstrated business requirement for their use.
- Maturity Level One introduced the use of virus scanning for macros, and blocking any macros in files received over the internet, in recognition that macro warning banners for users provide no tangible security benefit.
- Maturity Level Two was updated to remove only allowing digitally signed macros to execute.
- Maturity Level Two introduced the blocking of Win32 API calls by macros, as this functionality is commonly used by malicious macros.
- Maturity Level Two introduced logging to support cyber incident response activities.
- Maturity Level Three was updated to allow for either macros running from within a sandboxed environment, a Trusted Location or that that are digitally signed by a trusted publisher to execute.
- Maturity Level Three introduced preventing digitally signed macros signed by an untrusted publisher from being enabled via the Message Bar or Backstage View in Microsoft Office applications.
- Maturity Level Three introduced an annual (or more frequent) validation of trusted publishers.
- Maturity Level Three introduced monitoring to support identification and response to cyber events.

## What changes were made to 'user application hardening'?

- As Adobe Flash Player reached end of life on 31 December 2020, it is now considered an unsupported application and addressed by the 'patch applications' mitigation strategy instead.
- Maturity Level One introduced web browsers not processing Java and web advertisements from the internet.
- Maturity Level One introduced Internet Explorer 11 not processing content from the internet. This includes either by browsing the web or opening email attachments or other files from the internet within Internet Explorer 11.

- Maturity Level Two introduced blocking OLE package use by Microsoft Office.
- Maturity Level Two introduced the use of ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software.
- Maturity Level Two introduced preventing users from changing Microsoft Office and PDF software security settings.
- Maturity Level Two introduced logging to support cyber incident response activities.
- Maturity Level Three introduced disabling or removing Internet Explorer 11, .NET Framework 3.5 (includes .NET 2.0 and 3.0), and Windows PowerShell 2.0 features from Microsoft Windows.
- Maturity Level Three introduced the use of PowerShell in Constrained Language Mode.
- Maturity Level Three introduced monitoring to support identification and response to cyber events.

## What changes were made to 'restrict administrative privileges'?

- Requirements relating to policy controls were removed. Instead, emphasis was placed on separating privileged and unprivileged operating environments, and the accounts associated with them, for all maturity levels. This included preventing unprivileged accounts from logging into privileged operating environments and vice versa (except for local administrator accounts).
- Maturity Level One was updated to remove references to validating requests for access to information, while retaining validation for access to systems and applications.
- Maturity Level Two introduced the prevention of using a virtualised privileged operating environment from within an unprivileged operating environment.
- Maturity Level Two introduced the use of jump servers for administrative activities.
- Maturity Level Two was updated from revalidating privileged access to systems and applications annually to automatic disabling privileged access after 12 months if not revalidated.
- Maturity Level Two introduced automatically disabling privileged access after 45 days of inactivity.
- Maturity Level Two introduced local administrator and service account credentials being unique, unpredictable and managed.

- Maturity Level Three introduced the use of Windows Defender Credential Guard and Windows Defender Remote Credential Guard.
- Maturity Level Three introduced monitoring to support identification and response to cyber events.

## What changes were made to 'patch operating systems'?

- Patching requirements were updated for all maturity levels to remove the need for every vulnerability to be individually risk-assessed to determine patching timeframes.
- The patching of operating systems of internet-facing services within 48 hours if an exploit exists, otherwise within two weeks of release, was introduced for all maturity levels.
- References to patching or updating of non-operating system related firmware was removed for all maturity levels.
- The use of vulnerability scanners was introduced for all maturity levels to identify missing patches. The use and frequency of vulnerability scanners differs depending on the maturity level and was generally set at double the frequency of patching timeframes.
- Maturity Level One introduced patching operating systems of workstations, servers and network devices within one month of release.
- Maturity Level Two introduced patching operating systems of workstations, servers and network devices within two weeks of release.
- Maturity Level Three introduced patching operating systems of workstations, servers and network devices within 48 hours if an exploit exists, otherwise within two weeks of release.
- Maturity Level Three introduced using the latest release, or the previous release, of operating systems for workstations, servers and network devices.
- Maturity Level Three removed using an automated mechanism to confirm and record the deployment of patches.

## What changes were made to 'multi-factor authentication'?

- Multi-factor authentication requirements were updated to focus on the use of different types of authentication factors (e.g. something you know, something you have and something you are)

  - access by remote workers to an organisation's internet-facing services (e.g. remote desktop clients)
  - access by on-site or remote workers to third-party internet-facing services involving sensitive data (e.g. webmail)
  - access by on-site or remote workers to third-party internet-facing services involving non-sensitive data (e.g. social media).

- Maturity Level One introduced enabling multi-factor authentication by default (but allowing for opt-out) for all non-organisational users (e.g. customers and citizens) if an organisation operates a web portal that requires user authentication.
- Maturity Level One was updated to allow for any two different authentication factors, including the use of Trusted Signals.
- Maturity Level Two was updated to focus on one authentication factor being a physical item (such as a security key, smartcard or mobile phone).
- Maturity Level Two introduced logging to support cyber incident response activities.
- Maturity Level Three was updated to focus on the use of cryptography to protect against real-time phishing attacks and machine-in-the-middle attacks.
- Maturity Level Three introduced monitoring to support identification and response to cyber events.

## What changes were made to 'regular backups'?

- Backup requirements were updated to focus on performing and retaining backups in accordance with an organisation's own business continuity requirements, as opposed to specifying backup frequencies and backup retention timeframes.
- Emphasis was placed on performing and retaining backups in a coordinated and resilient manner.
- Emphasis was placed on the restoration of systems, software and important data from backups being regularly tested in a coordinated manner as part of disaster recovery exercises.

(excluding backup administrators) from accessing backups other than their own, or modifying or deleting those backups.

- Maturity Level Three introduced preventing unprivileged accounts and privileged accounts (excluding backup administrators) from accessing any backups.
- Maturity Level Three introduced preventing unprivileged accounts and privileged accounts (excluding backup break glass accounts) from modifying or deleting any backups.

# Implementation questions – General

## What maturity level should I target?

- Generally, Maturity Level One may be suitable for small to medium enterprises, Maturity Level Two may be suitable for large enterprises, and Maturity Level Three may be suitable for critical infrastructure providers and other organisations that operate in high threat environments.

## Can I implement compensating controls instead of specific Essential Eight requirements?

- Yes. However, system owners will need to demonstrate that their compensating controls provide an equivalent level of protection to the specific Essential Eight requirements they are compensating for. This will assist in ensuring that an equivalent level of overall protection against a specified level of targeting and tradecraft can be achieved and maintained.
- In cases where compensating controls are implemented, a mitigation strategy will be considered to have been fully implemented when all requirements that form that mitigation strategy have been assessed as either implemented or implemented using suitable compensating controls. However, if compensating controls are assessed as not suitable, the mitigation strategy will be assessed as either the next lowest maturity level it qualifies for or Maturity Level Zero.
- Note, system owners that seek to use risk acceptance without compensating controls, or risk transference (e.g. by sourcing cyber insurance), as justification for not implementing an entire mitigation strategy, such as application control or multi-factor authentication, will be considered to have not protected themselves against a specific class of cyber threat and will subsequently be assessed as Maturity Level Zero for both that mitigation strategy and their overall Essential Eight implementation.

## What is an internet-facing service?

- An internet-facing service is any service that is directly accessible over the internet, including those sitting behind a perimeter firewall. For example, a web portal, a cloud service or a network device (such as a firewall or VPN concentrator).
- An example of an internet-facing service that processes, stores or communicates an organisation's sensitive data is any cloud service that has been authorised for use with OFFICIAL: Sensitive or PROTECTED data (such as GovTeams) or any other sensitive business data.
- Examples of internet-facing services that processes, stores or communicates an organisation's non-sensitive data can include web hosting services (such as GovCMS) or social media platforms (such as Facebook, Twitter, YouTube, LinkedIn and Instagram).

## Does the ACSC provide a list of approved products for implementing the Essential Eight?

- No. Organisations should determine the suitability of particular products based on their own requirements.

## Do I require a Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solution to log, protect, monitor and action signs of compromise?

- The ACSC's *Strategies to Mitigate Cyber Security Incidents* publications recommend the use of SIEM and EDR software to centrally log and analyse system behaviour to detect compromises, while also facilitating cyber incident response activities.
- MITRE's research illustrates how various EDR vendors can detect and respond to compromises of systems by a specific malicious actor.
- Recent industry advances have introduced the concept of XDR which combines SIEM and EDR functionality while adding more advanced log analysis capabilities. This often integrates cloud-based analysis of host-based sensor telemetry to link disparate alerts in order to detect compromises of systems.

## Can my organisation filter out events that are known to be legitimate in order to simplify event log analysis and to reduce event log storage space

log storage space requirements.

# Implementation questions – Application control

## Do I need to use an application control solution for Maturity Level One?

- No. While an application control solution may be used at this maturity level, it may also be achieved using file system access permissions.

## Where can I find Microsoft's recommended block rules?

- Information on Microsoft's recommended block rules is available from Microsoft.

## Where can I find Microsoft's recommended driver block rules?

- Information on Microsoft's recommended driver block rules is available from Microsoft.

# Implementation questions – Patch applications

## My vulnerability scanning tool offers the ability to automatically detect assets on a network, can I use it as an asset discovery tool?

- Yes. Some vulnerability scanning tools offer automatic asset discovery functionality that is equivalent to other tools developed for that sole purpose.

## Can I perform automated asset discovery more frequently than fortnightly?

- Yes. While automated asset discovery should be performed at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect.

## How can I find out if a vulnerability has an exploit or not?

- The ACSC, vendors, news outlets and security researchers often cover exploitable vulnerabilities.

## Do I have 48 hours to patch from when exploits are announced or when exploitation starts occurring?

### I'm unable to perform rapid scanning and patching of internet-facing services, what can I do?

- The ACSC encourages all organisations to consider moving their internet-facing services to mature and trustworthy cloud service providers. Depending on the type of cloud service used, this can result in significant security benefits such as the rapid identification and patching of vulnerabilities.

### How can I remove Adobe Flash Player?

- Information on removing Adobe Flash Player, if installed automatically by Microsoft Windows, is available from Microsoft.
- Information on removing Adobe Flash Player, if installed manually, is available from Adobe.

## Implementation questions – Configure Microsoft Office macro settings

### Can I use Application Guard for Office to execute macros in a sandboxed environment?

- Unfortunately, no. Application Guard for Office disables the execution of macros in Microsoft Office documents.

## Implementation questions – User application hardening

### Where can I find information on using attack surface reduction rules for application hardening?

- Information on using attack surface reduction rules is available from Microsoft.
- Information on using attack surface reduction rules is also available in the ACSC's *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

### Where can I find information on preventing the activation of OLE packages?

- Information on preventing the activation of OLE packages is available in the ACSC's *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

# Implementation questions – Restrict administrative privileges

## What are unprivileged operating environments?

- Unprivileged operating environments are those used for non-administrative activities, such as reading emails and browsing the web.

## What are privileged operating environments?

- Privileged operating environments are those used exclusively for administrative activities.

## What are unprivileged accounts?

- Unprivileged accounts include unprivileged user accounts and unprivileged service accounts.

## What are privileged accounts?

- Privileged accounts include privileged user accounts and privileged service accounts.

## Where can I find information on hardening privileged operating environments?

- Microsoft provides a number of resources on securing privileged access, including the use of Privileged Access Workstations (PAWs), to separate privileged and unprivileged (user) operating environments.

## What are 'long' credentials for local administrator accounts and service accounts?

- Long credentials are a minimum of 30 characters.

# Implementation questions – Patch operating systems

## My vulnerability scanning tool offers the ability to automatically detect assets on a network, can I use it as an asset discovery tool?

### Can I perform automated asset discovery more frequently than fortnightly?

- Yes. While automated asset discovery should be performed at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect.

### How can I find out if a vulnerability has an exploit or not?

- The ACSC, vendors, news outlets and security researchers often cover exploitable vulnerabilities.

### Do I have 48 hours to patch from when exploits are announced or when exploitation starts occurring?

- The requirement to patch within 48 hours 'if an exploit exists' relates to the announcement of an exploit or that exploitation is already occurring, whichever occurs first.

### I'm unable to perform rapid scanning and patching of operating systems for internet-facing services, what can I do?

- The ACSC encourages all organisations to consider moving their internet-facing services to mature and trustworthy cloud service providers. Depending on the type of cloud service used, this can result in significant security benefits such as the rapid identification and patching of vulnerabilities.

### What constitutes the previous release of an operating system?

- This depends on the servicing branch being used for the operating system (i.e. Semi-Annual Channel or Long-Term Servicing Channel).
- Information on Microsoft Windows 10, Microsoft Windows 11 and Microsoft Windows Server operating system releases is available from Microsoft.

## Implementation questions – Multi-factor authentication

### Following multi-factor authentication to a system or service, can I use a single factor for re-authentication?

- For Maturity Level One, biometrics can be used as a primary authenticator factor.
- For Maturity Level Two and higher, biometrics can only be used as a secondary authenticator factor to unlock something you have.

## Can I use Trusted Signals as a primary authentication factor?

- For Maturity Level One, Trusted Signals can be used as a primary authentication factor.
- For Maturity Level Two and higher, Trusted Signals cannot be used as a primary authentication factor. However, organisations may use Trusted Signals in addition to two other suitable authentication factors for added security.
- Information on Trusted Signals is available from Microsoft.

## Can I use Windows Hello for Business for multi-factor authentication?

- Yes. Windows Hello for Business uses biometrics (something users are) or a PIN (something users know) to unlock a key or certificate that is tied to a device's Trusted Platform Module (something users have).
- Information on the use of Windows Hello for Business is available from Microsoft.

## What authentication types can be used for something users know?

- The following authentication types can be used for something users know: memorised secrets.
- Further information can be found in Section 5.1.1 of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*.

## What authentication types can be used for something users have?

- The following authentication types can be used for something users have: look-up secrets, out-of-band devices, single-factor OTP devices, single-factor cryptographic software and single-factor cryptographic devices.

### What authentication types can be used for something users have that is unlocked by something users know or are?

- The following authentication types can be used for something users have that is unlocked by something users know or are: multi-factor OTP devices, multi-factor cryptographic software and multi-factor cryptographic devices.
- Further information can be found in Section 5.1.5, Section 5.1.8 and Section 5.1.9 respectively of NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*.

### Where can I find information on certified multi-factor authentication solutions?

- The FIDO Alliance certifies multi-factor authentication solutions against its UAF, U2F and FIDO2 standards.
- Organisations are encouraged to use multi-factor authentication solutions that have been certified against the FIDO2 standard (preferably Level 2 over Level 1).

## Implementation questions – Regular backups

### Can I delete backup contents to satisfy privacy or legal requirements?

- Yes. Depending on the maturity level, this may be done with either a privileged account, a backup administrator account or a break glass account.
- For Maturity Level Three, break glass accounts should only be used for this purpose.

# Contact details

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

Report a cybercrime, cyber security incident or vulnerability.

Report

Report a cyber security incident for critical infrastructure

Get alerts on new threats
**Alert Service**

Become an
**ACSC Partner**

Report a cybercrime or cyber security incident

Acknowledgement of Country

*We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connections to land, sea and communities. We pay our respects to them, their cultures and their Elders; past, present and emerging. We also recognise Australia's First Peoples' enduring contribution to Australia's national security.*