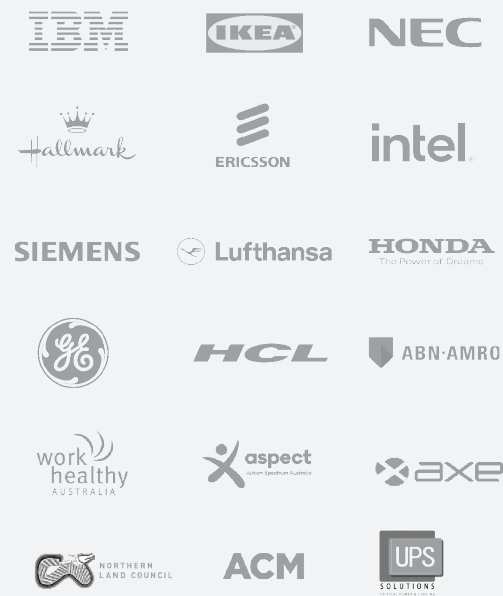


Essential Eight controls for your organisation

Implement the revised and bundled Essential Eight strategies under the Essential Eight Maturity Model, advised by Australian Cyber Security Centre (ACSC), for mitigating common attack vectors in your organisation.

trusted by ManageEngine




For more information:

www.manageengine.com  
sales@manageengine.com  
tech-au@manageengine.com  
in X f o y /ManageEngine

Office 8, Level 4 ,  
194 Varsity Parade,  
Varsity Lakes QLD 4227  
Australia

Are you ready to get started?

Download our free guide and learn how to implement the **Essential Eight Maturity Model!**



or visit our website:  
[mnge.it/essentialeight](https://mnge.it/essentialeight)

Disclaimer:  
The complete implementation of the Essential Eight Maturity Model scheme requires a variety of solutions, processes, people, and technologies. The solutions mentioned in our brochure are some of the ways in which IT management tools can help with implementing the Essential Eight requirements. Coupled with other appropriate solutions, processes, and people, ManageEngine’s solutions help implement the Essential Eight Maturity Model. This material is provided for informational purposes only, and should not be considered as legal advice for the Essential Eight Maturity Model implementation. ManageEngine makes no warranties, expressed, implied, or statutory, as to the information in this material.



Comply with ACSC’s Essential Eight Maturity Model



Essential Eight controls mapping



## Application control

**Achieved Maturity Levels: 3, 2, and 1**  
(Mapped products: [Endpoint Central with Security Addons](#), [Log360](#), [PAM360](#))

- Identify and block applications, and auto-uninstall prohibited software.
- Block executables.
- Allow or block apps on mobile devices running Android, iOS, or Windows, and lock a device to a single application or group of applications.
- Block unsanctioned or malicious cloud application access through CASB.
- Allowed and blocked application control events are centrally logged.
- Protect event logs from unauthorised modification or deletion.
- Manage application allowlist, application blocklist, and endpoint privilege management



## Patch applications

**Achieved Maturity Levels: 3, 2, and 1**  
(Mapped products: [Endpoint Central with Security Addons](#), [Log360](#))

- Detect, approve, download, test, and install Microsoft, non-Microsoft, macOS, and Linux applications patches and service packs..
- Scan for vulnerabilities.
- Mitigate security vulnerabilities by patching or updating systems.
- Remove applications that are no longer supported by vendors.
- Automate mobile app updates using the Mobile Device Management module.

- Manage workstations and servers on a LAN or WAN.
- Gather evidence of previous vulnerability scans with date/time stamp and scope of event logs.



## Restrict Microsoft Office macros

**Achieved Maturity Levels: 3, 2, and 1**  
(Mapped product: [Endpoint Central with Security Addons](#))

- Manage Microsoft Office settings out of the box by disabling macros for users and blocking them in files from the internet.
- Microsoft Office macro security settings cannot be changed by users.
- Allow users to execute macros only in documents from trusted locations with limited write access.



## User application hardening

**Achieved Maturity Levels: 2, and 1**  
(Mapped products: [Endpoint Central with Security Addons](#), [Log360](#))

- Control browser plug-ins, extensions, and allowed sites. Stop processing Java and web advertisements from the internet in web browsers.
- Restrict browsers by providing or restricting access to web applications.
- Collect and examine PowerShell event logs centrally, at regular intervals.



## Restrict administrative privileges

**Achieved Maturity Levels: 3, 2, and 1**  
(Mapped products: [PAM360](#), [AD360](#), [Log360](#))

- Validate requests for privileged access.
- Implement logon restrictions to privileged operating environments.
- Conduct administrative activities through jump servers.
- Create a strong password policy.
- Log changes to privileged accounts and groups.
- Enable just-in-time privilege elevation.
- Delegate role-based access to AD, Exchange, and Microsoft 365.
- Centrally log privileged access events.



## Patch operating systems

**Achieved Maturity Levels: 3, 2, and 1**  
(Mapped products: [Endpoint Central with Security Addons](#), [Network Configuration Manager](#))

- Patch, update, or mitigate security vulnerabilities based on severity in operating systems such as Windows, macOS, and Linux.
- Identify and manage firmware vulnerabilities.
- Scan for vulnerabilities.
- Automate OS updates on mobile devices using the Mobile Device Management module.
- Update Windows legacy EOL systems to avoid a disruption in service.



## Multi-factor authentication

**Achieved Maturity Levels: 3, 2, and 1**  
(Mapped products: [PAM360](#), [AD360](#), [Log360](#))

- Use one or more authentication techniques to verify users' identities during the password reset and account unlock process.
- Use MFA to authenticate privileged users of systems.
- Introduce MFA to manage endpoints.
- Log successful logins for auditing.
- Enable centralised logging of successful and unsuccessful MFA events.
- Analyse event logs from internet-facing servers to detect cybersecurity events.
- Analyse the detected cybersecurity events in timely manner to identify security attacks and incidents



## Regular backups

**Achieved Maturity Levels: 1**  
(Mapped products: [Network Configuration Manager](#), [AD360](#), [Endpoint Central](#))

- Perform comprehensive, scheduled incremental object- and item-level backups in AD, SharePoint Online, on-premises Exchange, and Exchange Online.
- Back up the entire database of application configurations, system settings, and password share permissions through scheduled tasks or live data backup.
- Automate configuration backups for firewalls, routers, switches, and more.