ManageEngine

A quick guide to the Essential Eight Maturity Model

The Essential Eight Maturity Model is published by the Australian Signals Directorate (ASD) to support the implementation of the Essential Eight, the baseline set of eight mitigation strategies drawn from ASD's Strategies to Mitigate Cyber Security Incidents and designed to protect internet-connected IT networks. The model defines four maturity levels, Maturity Level Zero through Maturity Level Three, with Levels One to Three based on mitigating increasing levels of adversary strategies and targeting. Organizations are assessed against each of the eight strategies individually, and overall maturity is equal to the least-mature strategy. Maturity Level Two is mandated for non-corporate Commonwealth entities under the Protective Security Policy Framework.

Core principles of the Essential Eight Maturity Model

Sl.no	Focus area	What is it?	Key requirements
1	Multi-factor authentication	Requires a second authentication factor for users of online services, systems, and data repositories, with factor strength increasing by maturity level.	• MFA for organizational online services. • MFA for third-party services. • MFA for privileged users of systems. • MFA for unprivileged users of systems. • Phishing-resistant authentication methods. • Central logging of MFA events.
2	Restrict administrative privileges	Governs how privileged access is requested, validated, scoped, separated from ordinary use, and withdrawn over time.	• Validate privileged access on request. • Revalidate privileged access every 12 months. • Disable after 45 days inactivity. • Dedicated privileged user accounts. • Separate privileged and unprivileged environments. • Central logging of privileged access.
3	Application control	Restricts which executables, software libraries, scripts, and installers are permitted to execute on workstations and servers.	• Restrict executables, libraries, and scripts. • Extend control to internet-facing servers. • Apply the Microsoft-recommended blocklist. • Validate rulesets annually. • Central logging of allowed and blocked events.
4	User application hardening	Removes or disables the application features most commonly abused by adversaries to execute malicious code.	• Block browser Java and web advertisements. • Harden Microsoft Office and PDF software. • Block PowerShell from the internet. • Central logging of PowerShell events. • Central logging of command-line process
5	Central logging, monitoring, and response	Requires event logs to be centrally collected, protected from tampering, and analyzed in time to detect events and act on incidents.	• Protect logs from modification and deletion. • Analyze logs to detect cybersecurity events. • Identify incidents from analyzed events. • Enact the incident response plan.
6	Regular backups	Requires backups of important data, software, and configuration settings to be performed, retained, tested, and shielded from tampering.	• Restrict access to backups. • Prevent modification and deletion of backups. • Extend restrictions to privileged accounts. • Test restoration during disaster recovery.

Source: www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model

The Essential Eight Maturity Model and ManageEngine

ManageEngine offers solutions that help you enforce identity controls, govern privileged access, and monitor security events across on-premises, cloud, and hybrid environments. AD360, ManageEngine's IAM solution, addresses MFA, privileged access validation, access governance, and the permissions that protect backup repositories, while Log360, its SIEM solution, addresses central log collection, tamper-evident retention, threat detection, and incident response. With both deployed together, you can implement the controls required under the Essential Eight Maturity Model.

How can ManageEngine help you implement the Essential Eight Maturity Model?

Adaptive MFA

Enforce a second factor at machine logon, VPN, RDP, Outlook on the web, cloud applications, and Windows UAC, and vary the requirement by time, geolocation, IP address, and device.

Helps with Multi-factor

Phishing-resistant authentication

Mandate FIDO2 passwordless keys, YubiKey and smart cards, or biometrics for users of online services, systems, and data repositories.

Helps with Multi-factor authentication, ML2–ML3.

Privileged access approval workflows

Route requests for privileged access and management actions through multi-level review before execution, and retain the request record for audit.

Helps with Restrict administrative privileges, ML1–ML3.

Access certification and review

Schedule periodic revalidation of privileged access, and disable entitlements automatically when they are not reconfirmed or when accounts fall inactive.

Helps with Restrict administrative privileges, ML2–ML3.

Role-based access governance

Limit technicians to the rights their role requires through granular delegation scoped by OU, group, tenant, or object attribute, preventing privilege creep.

Helps with Restrict administrative privileges, ML1–ML3.

Privileged activity and change auditing

Consolidate Domain Admin and Enterprise Admin actions, security group changes, and Local Administrator Password Solutions (LAPS) password retrievals into one searchable trail with before-and-after values.

Helps with Restrict administrative privileges, ML2–ML3.

For more information, contact sales@manageengine.com

Application control event logging

Centrally collect the allow and block events produced by Windows Defender Application Control and AppLocker, and onboard non-standard sources through the custom log parser.

Helps with Application control, ML2–ML3.

PowerShell and process-creation auditing

Collect PowerShell module, script block, and transcription events alongside command-line process-creation events, and make them searchable and available to correlation.

Helps with User application hardening, ML2–ML3.

Tamper-evident log archiving

Store collected logs in a compressed, encrypted, and time-stamped archive held away from originating hosts, with role-based console access and configurable retention.

Helps with Central logging, monitoring, and response, ML2–ML3.

Threat detection and behavior analytics

Analyze logs from servers and workstations in real time, apply correlation rules and threat intelligence feeds, and surface anomalies through AI-driven behavior baselining and risk scoring.

Helps with Central logging, monitoring, and response, ML2–ML3.

Incident response automation

Execute predefined SOAR playbooks on detection to contain incidents, and support case management and forensic review through incident timelines and ITSM integration.

Helps with Central logging, monitoring, and response, ML2–ML3.

Backup access control and monitoring

Manage the NTFS and share permissions governing who can reach backup files, and alert in real time on access, modification, or deletion by unauthorized accounts.

Helps with Regular backups, ML1–ML3.