ManageEngine's guide to

IMPLEMENTING THE ESSENTIAL EIGHT MATURITY MODEL

Your go-to essentials for a cyber resilient organisation

ManageEngine

Table of
contents

The need to prioritise organisation-wide cybersecurity protection strategies

Cybercrime has been constantly evolving and is a complex issue that affects numerous sectors across the country. Though most organisations have implemented strategic policies and programs to combat security challenges, they are still struggling to keep up with threats posed by rapid advancements in technology.

In 2021, it was reported that over 67,500 cybercrimes occurred in Australia, which is an increase of 13% compared to the previous year. Pandemic-related incidents took a toll too, as threat actors focused their nefarious efforts on exploiting PII issues for financial gain. These examples reiterate that despite implementing strong policies and controls, due diligence is needed to help thwart cybercriminals who continue attempting advanced and sophisticated attacks when given a chance. If organisations can properly understand an adversary's tradecraft, it's easier to invest in the correct policies and solutions.

To combat these rising threats, the Australian government has doubled down on its efforts to secure businesses and individuals across the country, and has increased its focus on nationwide cybersecurity policies. By providing a clear set of policies, organisations and individuals can implement strategies to shield sensitive information from the most common and dangerous attack vectors. The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has developed Strategies to Mitigate Cyber Security Incidents, commonly known as the Essential Eight. These aim to provide prioritised mitigation strategies to help organisations protect themselves from a range of cyberthreats.

This guide will detail the main requirements of the Essential Eight Maturity Model, including what organisations need to consider before and while implementing it, and how organisations can ensure that they are always fully protected.

The Essential Eight explained

The Essential Eight is a cybersecurity-based maturity tool that helps organisations mitigate cybersecurity incidents caused by various cyberthreats and vectors. It is based on the eight mitigation strategies developed by the Australian Signals Directorate that provides guidance to address:

- ***Targeted cyber intrusions and other external adversaries who steal data***
- ***Ransomware attacks that deny access to data for monetary gain, and external adversaries who destroy data and prevent computers and networks from functioning***
- ***Malicious insiders who steal data such as customer details or intellectual property***
- ***Malicious insiders who destroy data and prevent computers and networks from functioning***
- ***Business email compromises***
- ***Industrial control systems***

These are considered to be the foundational security strategies crucial to managing contemporary cybersecurity threats. The objectives of these mitigation strategies, as described in the Essential Eight, are to:

- ***Prevent malware delivery and execution.***
- ***Limit the extent of cybersecurity incidents.***
- ***Recover data and system availability.***

While no single strategy is guaranteed to prevent cyberattacks, it is recommended that organisations implement these eight mitigation strategies as a baseline. These strategies aim to make it harder for attackers to compromise systems and networks.

Moreover, proactively implementing the Essential Eight can be more cost-effective than responding to a large-scale cybersecurity incident. However, as every environment is different and the same set of actions won't apply in every situation or for every company, these mitigation strategies are sought after based on the maturity levels that each organisation would determine through self-assessments. These maturity levels are defined in the Essential Eight as:

0 **Maturity Level Zero:**
Not aligned with the intent of the mitigation strategy

1 **Maturity Level One:**
Partly aligned with the intent of the mitigation strategy

2 **Maturity Level Two:**
Mostly aligned with the intent of the mitigation strategy

3 **Maturity Level Three:**
Fully aligned with the intent of the mitigation strategy

Excluding Maturity Level Zero, the maturity levels are based on mitigating higher levels of adversary tradecraft (i.e., tools, tactics, techniques, and procedures) and targeting. Depending on the adversary's capabilities and intent, different tradecraft can be used on different targets for different operations.

0

Maturity Level Zero:

If an organisation's overall cybersecurity posture is weak, which can compromise the confidentiality of its data or the integrity or availability of its systems and data when exploited, then the maturity level is zero. With its reintroduction, organisations can now assess from a broader range when trying to implement the Essential Eight.

1

Maturity Level One:

If common weaknesses aren't covered, which can become an easy target to adversaries as they seek to leverage available commodity tradecraft like social engineering to manipulate users to fall prey to vicious actions, then the maturity level is one. Depending on the intent of the adversaries, sensitive data might also be destroyed. Adversaries usually look for just any victim in such cases.

2

Maturity Level Two:

If adversaries begin using more effective and well-known tradecraft to increase their chances to gain access to privileged accounts, such as by targeting credentials via phishing attacks to evade multi-factor authentication (MFA), then the maturity level is two. They can be selective in their targets, but conservative in their time, money, and effort. Depending on the intent of the adversaries, data accessible by privileged accounts, when compromised, might be destroyed.

3

Maturity Level Three:

If adversaries are more focused on targets adaptable to the tradecraft used and invested in circumventing policies and controls designed to gain a foothold and exploit weaknesses in the networks, then the maturity level is three. At this level, threat actors exploit old applications or unattended accounts to get into the system, gain access to credentials, pass on crucial and sensitive details over the network, and still manage to cover their tracks and lie low. Depending on the intent of the adversaries, data might also be destroyed.

In all the maturity levels, if the adversaries find an opportunity, they will destroy data as well as backups, if available.

Due to the dynamic nature of the cybersecurity threat landscape, the ACSC regularly updates the maturity model.

Prerequisites, self-assessments, and implementation

To implement the mitigation strategies, an organisation must:

1. Find a reason to upgrade its cybersecurity posture.
2. Identify assets and conduct a risk assessment.
3. Determine the degree of protection necessary to safeguard it from cyberthreats.
4. Follow the steps to implement the Essential Eight in a graduated manner.

Finding a reason to upgrade the cybersecurity posture

The reason to upgrade and choose the Essential Eight Maturity Model could be as simple as achieving compliance, or as important as having experienced a cybersecurity incident. The motivational factor plays a key role as it helps set the target maturity level to reach.

Identifying assets and conducting a risk assessment

There will be instances that might not allow implementing the Essential Eight Maturity Model due to associated risks. In such cases, a prior risk assessment will help with the risk management. Further, a risk-based score will also provide a way to manage and minimise exceptions and reduce impact.

Determining the degree of protection necessary to safeguard from cyberthreats

The next step is to determine the maturity level. This should not be based on how realistically organisations can achieve the target but on the risk of exposure to adversary tradecraft depending on the organisation's data, systems, and industry.

Following the steps to implement all the Essential Eight in a graduated manner

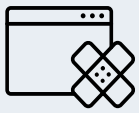
When implementing a mitigation strategy, prioritising it for high-risk users and computers—those with access to sensitive data—could be a good start. Continuous, hands-on testing to check the preventive nature of the strategies will keep the organisation much safer from external or internal malicious acts. The aim should be to implement all eight controls as a bundle until a consistent level of maturity is reached across all the mitigation strategies.

The eight mitigation strategies for your organisation

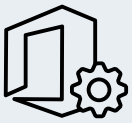
The prioritised mitigation strategies, along with their objectives, as cited in the ACSC Essential Eight report are:

OBJECTIVE 1:
Mitigation strategies to prevent malware delivery and execution.

Application control:
An application control only allows whitelisted and preapproved software to run in your network.



Patch applications:
Regular patching fixes security vulnerabilities in software applications.



Restrict Microsoft Office macros:
Macros from the internet are blocked, and only vetted macros with limited write access or macros that are digitally signed with a trusted certificate are allowed.

User application hardening:
Application hardening involves disabling unsecure and unused services, such as Flash, Java, and web ads from applications, and restricting the use of applications that are known to be vulnerable.

OBJECTIVE 2:

Mitigation strategies to limit the extent of cybersecurity incidents

Restrict administrative privileges:

Restrict administrative privileges to operating systems and applications based on user duties. These should be restricted to only those that need them. Regularly revalidate the need for privileges.

Patch operating systems:

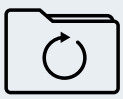
Regular patching fixes security vulnerabilities in operating systems.

Multi-factor authentication:

A user is granted access only after successfully presenting multiple, separate evidences of authenticity.

OBJECTIVE 3:

Mitigation strategies to recover data and system availability



Regular backups:

Regularly back up all data and store it securely offline or at an alternate site such as a secondary data centre or in the cloud.

ManageEngine's solutions to implement the Essential Eight action plan

Mitigation strategies to prevent malware delivery and execution

5.1: Application control

How can ManageEngine help implement this protection strategy?

The Application Control module in Endpoint Central helps you to allow applications that are required for the enterprise and blacklist malicious and untrusted applications. There is additionally an option to greylist applications, and after further analysis, designate them to be blacklisted or whitelisted. Endpoint Central also comes with a built-in ability to block executables and prohibit software.

Log360 Cloud, a cloud-based SIEM solution, comes with built-in CASB capabilities that provide users the option to define allowed and banned cloud applications and services. It monitors the usage of sanctioned, unsanctioned, and blocked applications, and gives insights on the top requested banned application, user who most requested to access un-sanctioned applications, and more. Log360 Cloud also comes with the ability to monitor shadow IT.

Steps to achieve this strategy:

5.1.1 Identify and block applications, and auto-uninstall prohibited software.

5.1.2 Block executables.

5.1.3 Allow or block apps on mobile devices running Android, iOS, or Windows, and lock a device to a single application or group of applications.

5.1.4 Block unsanctioned or malicious cloud application access through CASB.

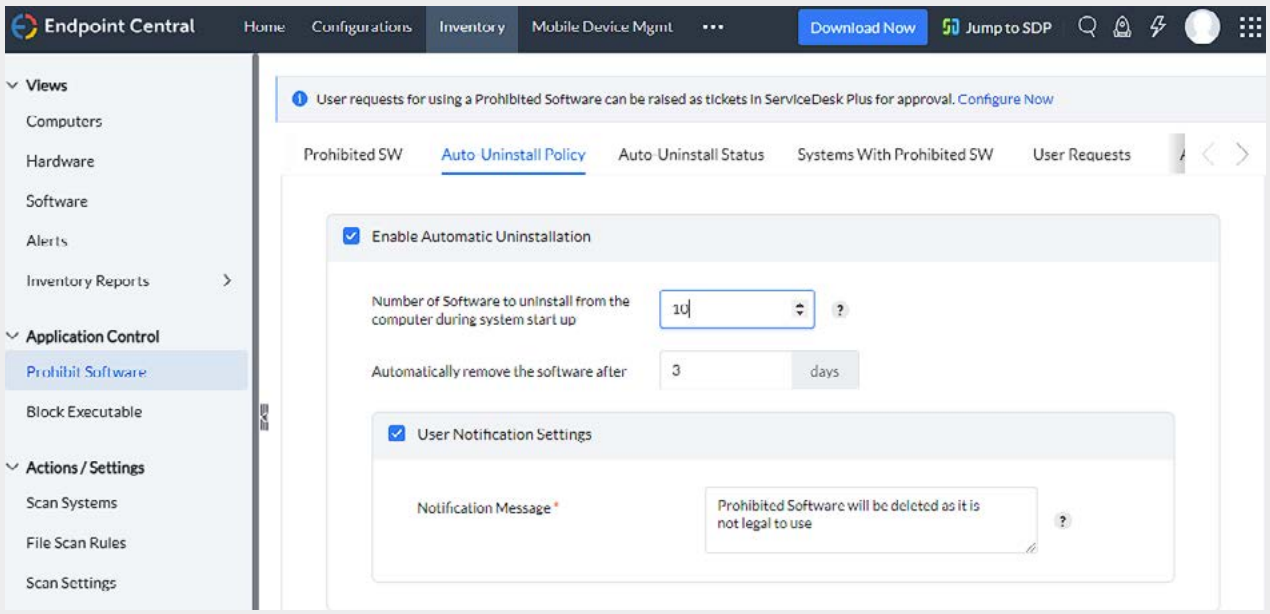
5.1.5 Allowed and blocked application control events are centrally logged.

5.1.6 Protect event logs from unauthorised modification or deletion.

5.1.7 Manage application allowlist, application blocklist, and endpoint privilege management

5.1.1 Identify and block applications, and auto-uninstall prohibited software.

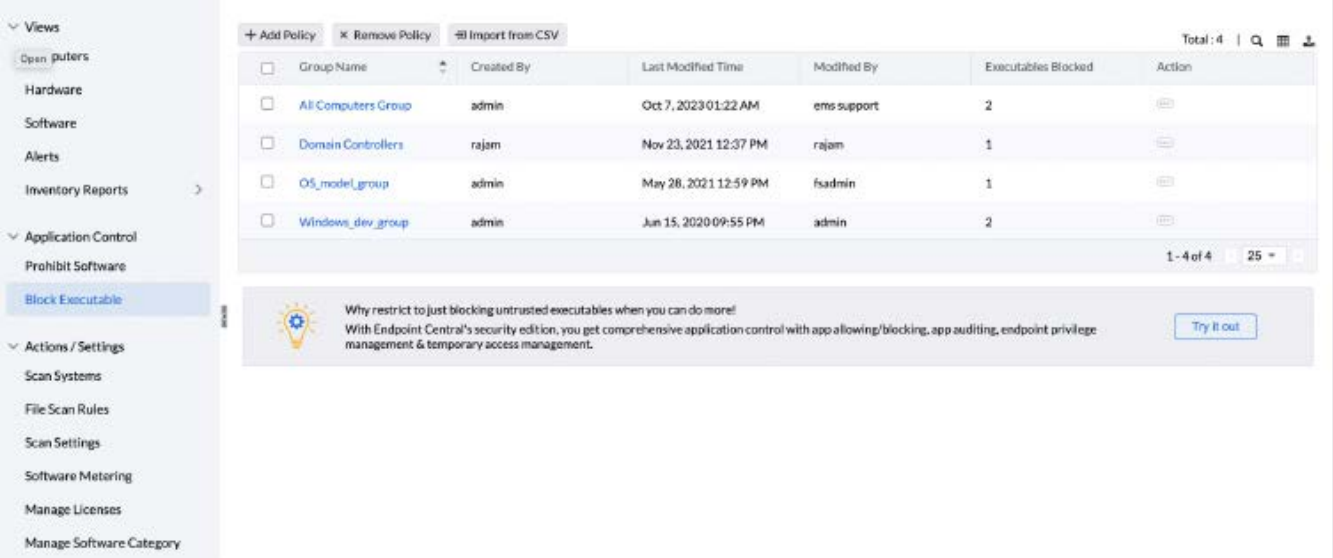
Every organisation prohibits employees from using certain software. Endpoint Central blocks the use of designated software according to your organisation's policies, which helps meet compliance requirements.



Prohibiting software in Endpoint Central → Inventory.

5.1.2 Block executables.

We can prevent the installation of various components on workstations from within the standard user profiles and temporary folders used by the operating system, web browsers, and email clients to enhance security. This is accomplished by blocking the execution of executables.

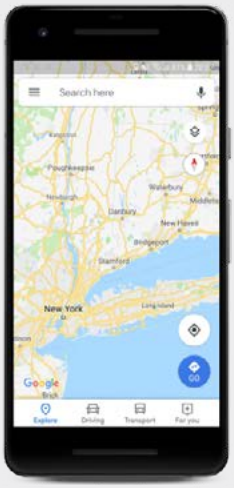


Block executables in Endpoint Central → Inventory.

5.1.3 Allow or block apps on mobile devices running Android, iOS, or Windows, and lock a device to a single application or group of applications.

ManageEngine's MDM solution Mobile Device Manager Plus offers a Kiosk Mode functionality that enables IT admins to lock down devices, restricting them to a single or specific set of apps, and allowing only certain device features, like Wi-Fi and Bluetooth, to be accessible to the user. This ensures they function as single-purpose devices while providing a better user experience, and preventing device misuse.

Single app

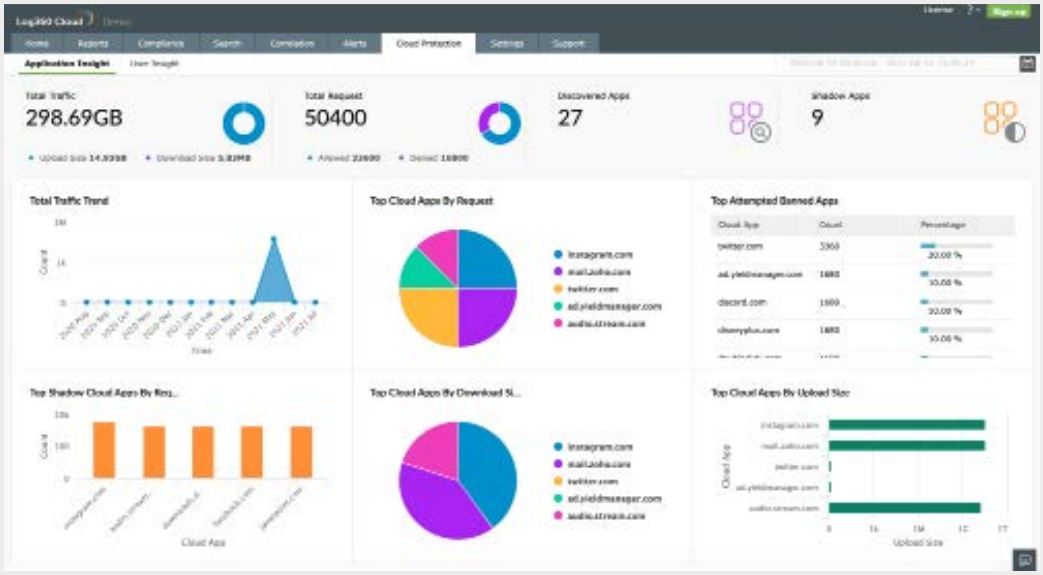


Multi-app

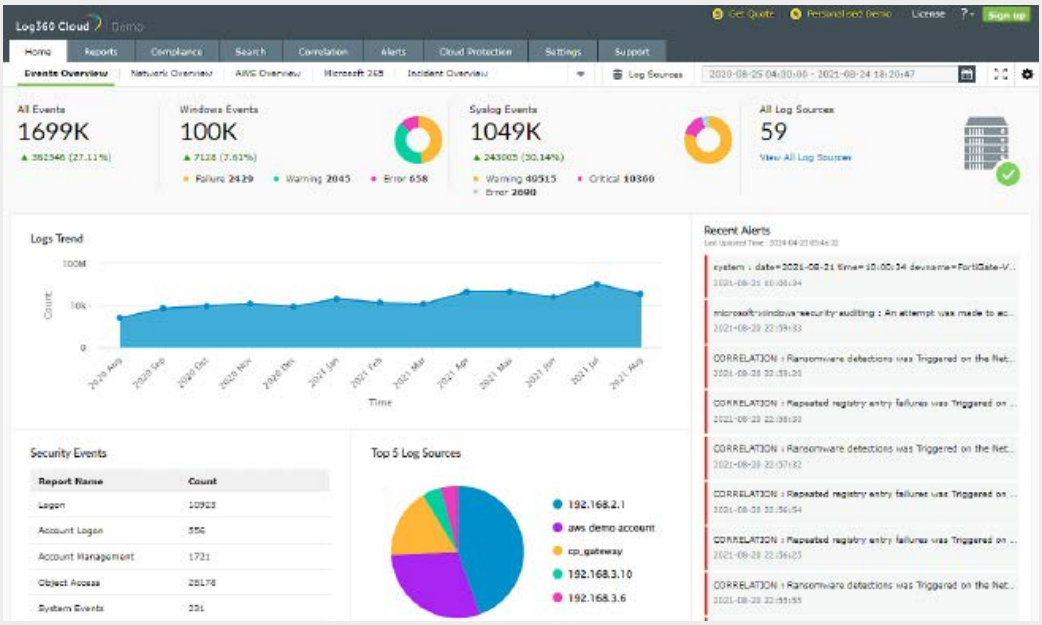
Locking the device to a single app or multiple apps in Kiosk Mode.

5.1.4 Block unsanctioned or malicious cloud application access through CASB.

The CASB feature of Log360 Cloud, enables users to classify applications as "allowed, malicious, and shadow application." Additionally, it offers valuable insights into application usage and shadow IT tracking, including top shadow cloud apps, top banned apps, etc., which plays a crucial role in cloud application management and control.



Viewing the application insights within cloud protection in Log360 Cloud → Cloud Protection.



Viewing the events overview dashboard in Log360 Cloud.

5.1.5 Allowed and blocked application control events are centrally logged.

The centralized logging feature of Log360, allows you to collect, store, and analyze logs from a centralized dashboard. It automatically collect logs from over 750 log sources including firewalls, IDS/IPS, servers, routers, switches, database applications, web servers, proxy servers, and more. This allows you to have a birds-eye view of all the activity in your network.

5.1.6 Protect event logs from unauthorised modification or deletion.

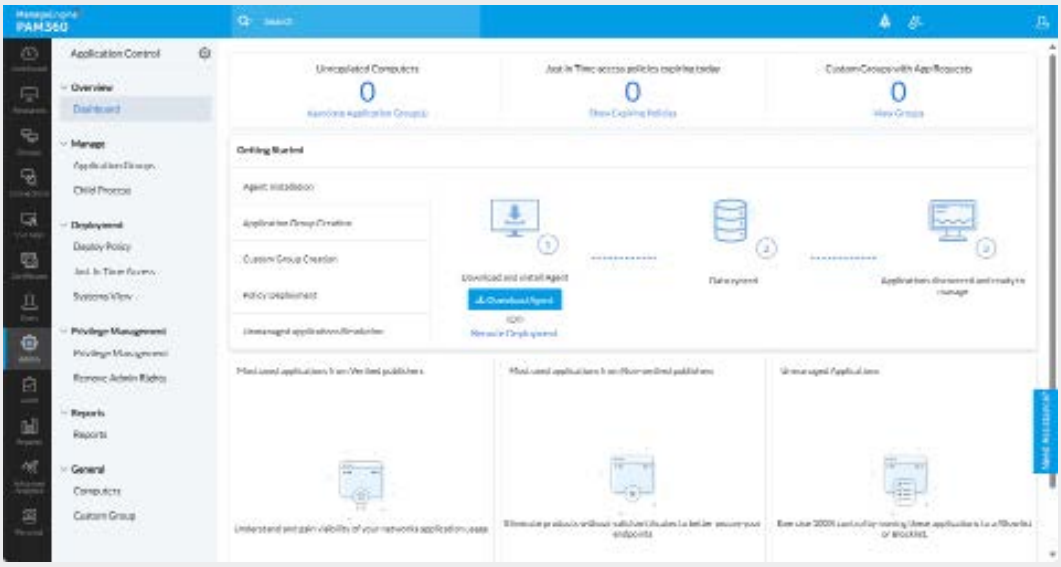
Log360 secures the collected log through hashing, timestamping, and encryption algorithms . Further, the solution provides file integrity monitoring, which can be extended to log archives, to detect tampering of evidence, if any. Log360 can also send alerts for unauthorised modification and/or deletion of the gathered event logs.

Note: The above requirement (Protect event logs from unauthorized modification or deletion) is applicable for the following sections of maturity level two of the Essential 8 maturity model.

- ***Multi-factor authentication***
- ***Restrict administrative privileges***
- ***Application control***
- ***User application hardening***

5.1.7 Manage application allowlist, application blocklist, and endpoint privilege management

PAM360's Application Control module enables administrators to manage application privileges and access on endpoints effectively. By using custom rules, administrators can oversee and control applications, create allowlists and blocklists, and temporarily authorise blocked applications in emergency situations. This feature enhances both security and efficiency in managing application access within the PAM360 environment.



Application management actions within PAM360

Achieved Maturity Levels: 3, 2, and 1
(Endpoint Central with Security Addons, Log360, PAM360)

5.2: Patch applications

How can ManageEngine help implement this protection strategy?

Patching the security vulnerabilities in Microsoft applications and more than 850 third-party applications can be automated and customised using the Patch Management module of Endpoint Central. The Vulnerability Management module in Endpoint Central scans for threats, vulnerabilities, and misconfigurations on endpoints, and suggests relevant patches or mitigations for them.

Security patches are supported by ManageEngine within 12 hours of release, and non-security updates are supported within 24 hours of release. This gives users plenty of time to upgrade within 48 hours of patches being available after a vulnerability is disclosed.

Steps to achieve this strategy:

5.2.1 Detect, approve, download, test, and install Microsoft, non-Microsoft, macOS, and Linux applications patches and service packs.

5.2.2 Scan for vulnerabilities.

5.2.3 Mitigate security vulnerabilities by patching or updating systems.

5.2.4 Remove applications that are no longer supported by vendors

5.2.5 Automate mobile app updates using the Mobile Device Management module.

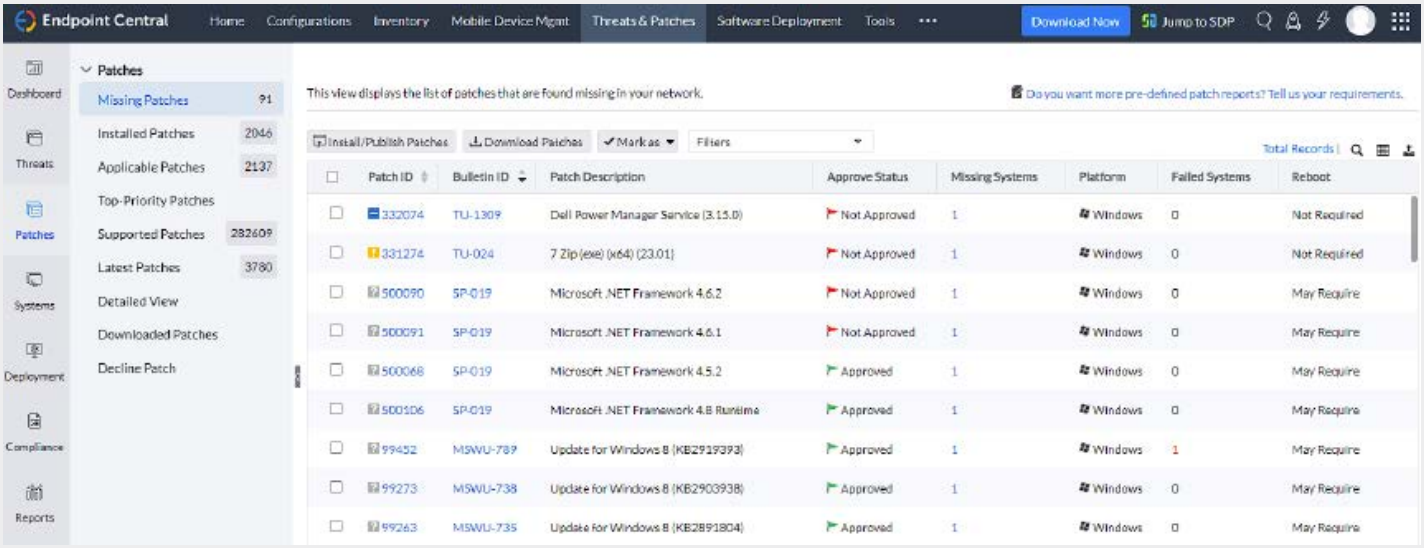
5.2.6 Manage workstations and servers on a LAN or WAN.

5.2.7 Gather evidence of previous vulnerability scans with date/time stamp and scope of event logs.

5.2.1 Detect, approve, download, test, and install Microsoft, non-Microsoft, macOS, and Linux applications patches and service packs.

A top priority for an IT admin is ensuring the latest security patches are in place in all systems. Any significant delays in fixing vulnerabilities in third-party applications can leave endpoints open to attack. Patches need to be deployed to each workstation; ignoring third-party application patches can result in damaging consequences.

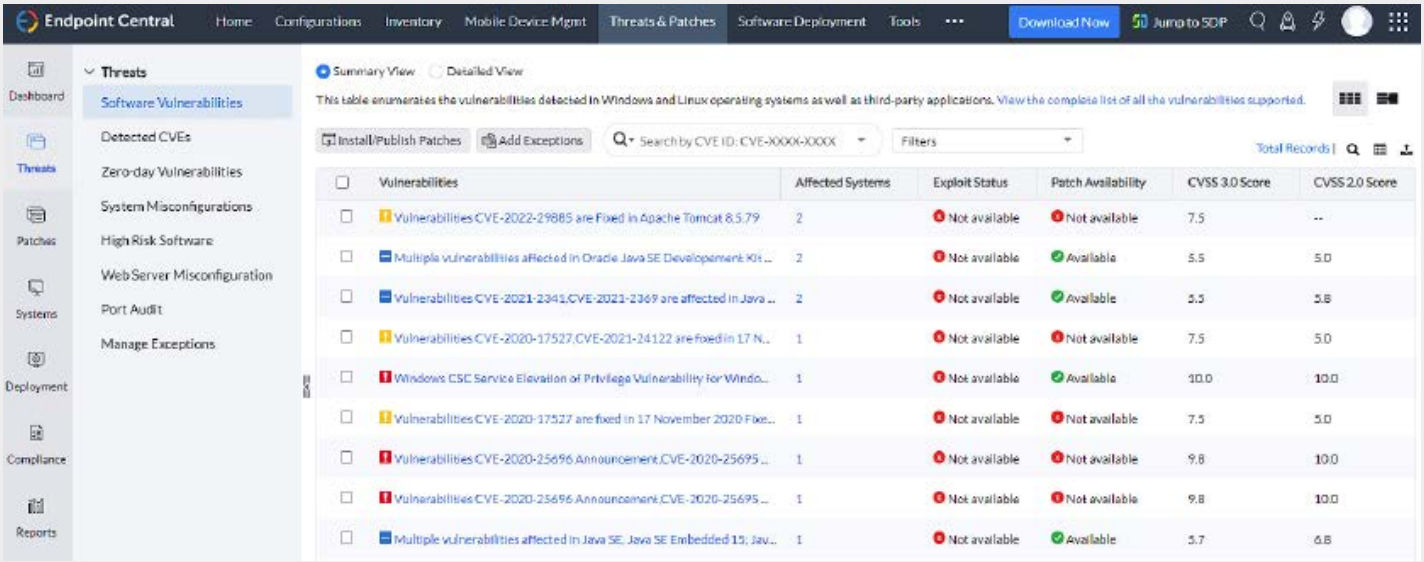
Patch Manager Plus is a intuitive tool that ensures comprehensive monitoring and management of third-party applications. This solution defends against vulnerabilities by providing a central update process for more than 850 third-party applications, including Adobe and Java, utilising prebuilt, tested, and ready-to-deploy packages.



Identifying and installing missing patches in Endpoint Central → Threats & Patches.

5.2.2 Scan for vulnerabilities.

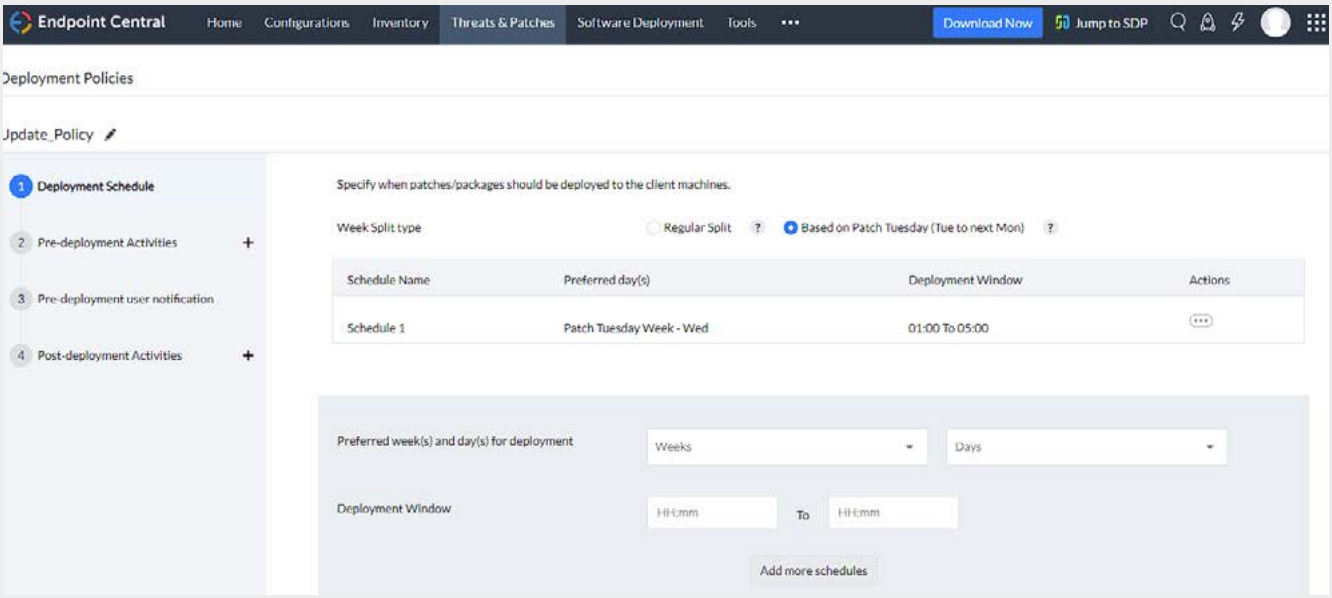
A vulnerability scanner is used to identify missing patches or updates for security vulnerabilities in internet-facing services which are assessed as extreme risks. The same applies to office productivity suites, web browsers, email clients, PDF software, and security products.



Software vulnerabilities scanned in Endpoint Central → Threats & Patches.

5.2.3 Mitigate security vulnerabilities by patching or updating systems.

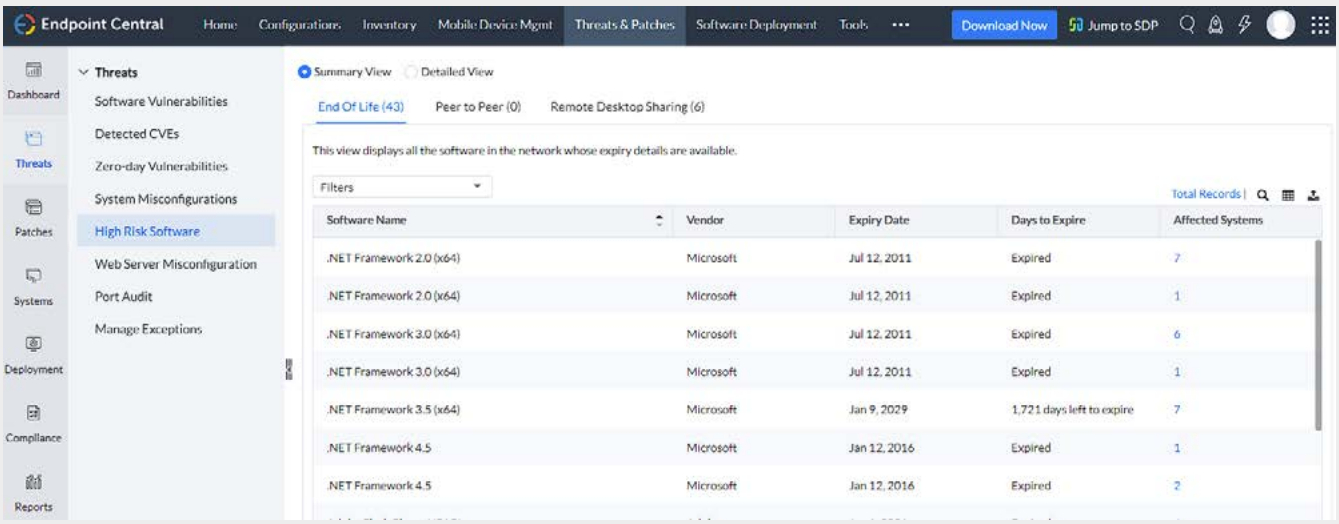
Security vulnerabilities in internet-facing services which are assessed as extreme risks are patched, updated, or mitigated within two weeks of release, or within 48 hours if an exploit exists. This also applies to office productivity suites, web browsers, email clients, PDF software, and security products, which are applied within one month of release.



Configuring a patch deployment policy in Endpoint Central → Threats & Patches.

5.2.4 Remove applications that are no longer supported by vendors.

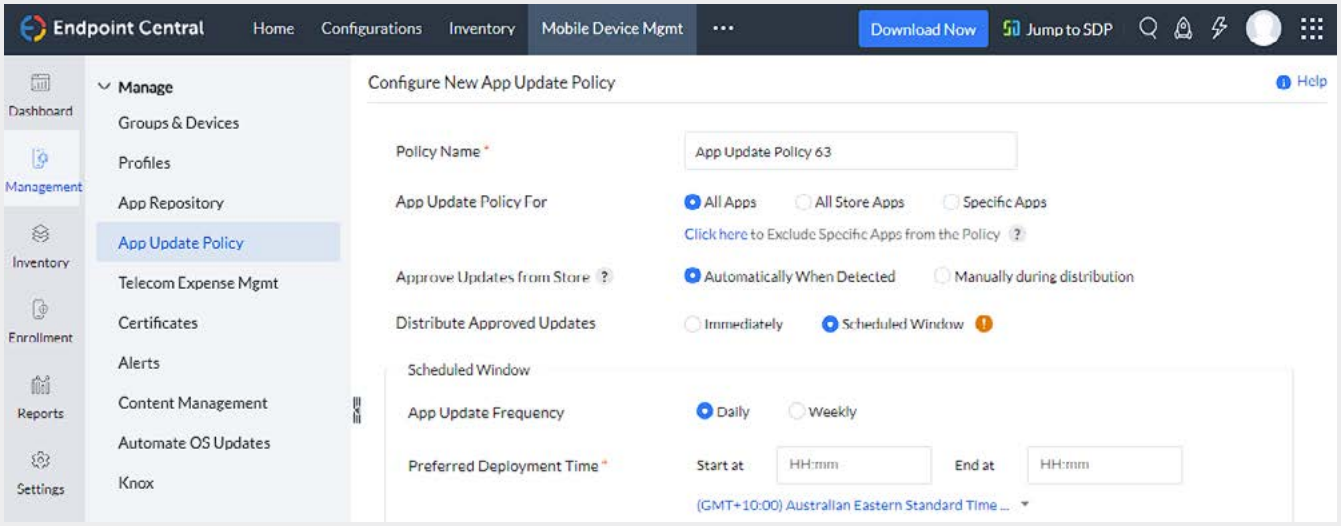
End-of-life applications are rampant in enterprises due to lack of visibility and poor management. The consequences of running an end-of-life application outweighs its benefits. End-of-life OSs and applications will not receive security updates from vendors to patch critical vulnerabilities, which makes them extremely vulnerable to exploits. Moreover, legacy OSs can't run latest applications and they'll be stuck with legacy applications, which will soon reach end of life, too, thus widening the attack surface. Also, businesses in regulated industries may also face significant fines for running out-of-date systems.



Scan for high-risk software in Endpoint Central → Threats & Patches.

5.2.5 Automate mobile app updates using the Mobile Device Management module.

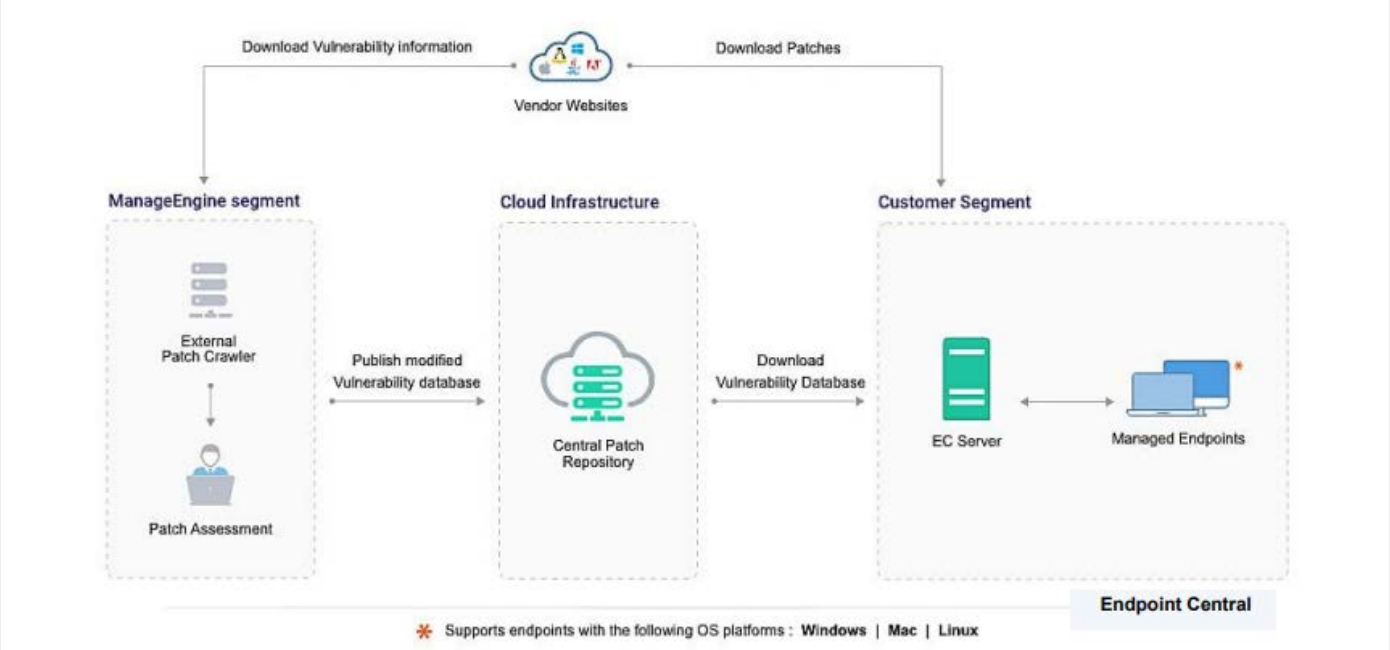
Automating app updates ensures the apps remain current with all the required updates installed. Mobile Device Manager Plus allows IT admins to automate app updates, ensuring the devices are always running the latest app version.



Creating an automated app update policy in Endpoint Central → Mobile Device Mgmt.

5.2.6 Manage workstations and servers on a LAN or WAN.

Endpoint Central periodically scans the systems in your network to assess patch needs. Using comprehensive databases and resources, as well as those from Microsoft, Adobe, Red Hat, and so on, the scanning mechanism checks for the existence and state of the patches by performing file version checks, registry checks, and checksums. The vulnerability database is regularly updated with the latest information on patches from the Central Patch Repository. The scanning logic automatically determines which updates are needed on each client system, taking into account the operating system, application, and update dependencies.



Patch management architecture.

5.2.7 Gather evidence of previous vulnerability scans with date/time stamp and scope of event logs.

Log360 supports logging and analytics of leading vulnerability scanners—Nessus, Qualys, Nexpose, NMAP, and OpenVAS as a part of evidence production. The solution can provide details such as last scanned time and more.

Achieved Maturity Levels: 3, 2, and 1

(Endpoint Central with Security Addons, Log360)

5.3: Restrict Microsoft Office macros

How can ManageEngine help implement this protection strategy?

Using the script configurations in Endpoint Central, you can configure Microsoft Office settings for user and computer groups in your environment. Additionally, using the Browser Security module in Endpoint Central, you can prevent prohibited or malicious software from being downloaded into your network.

Steps to achieve this strategy:

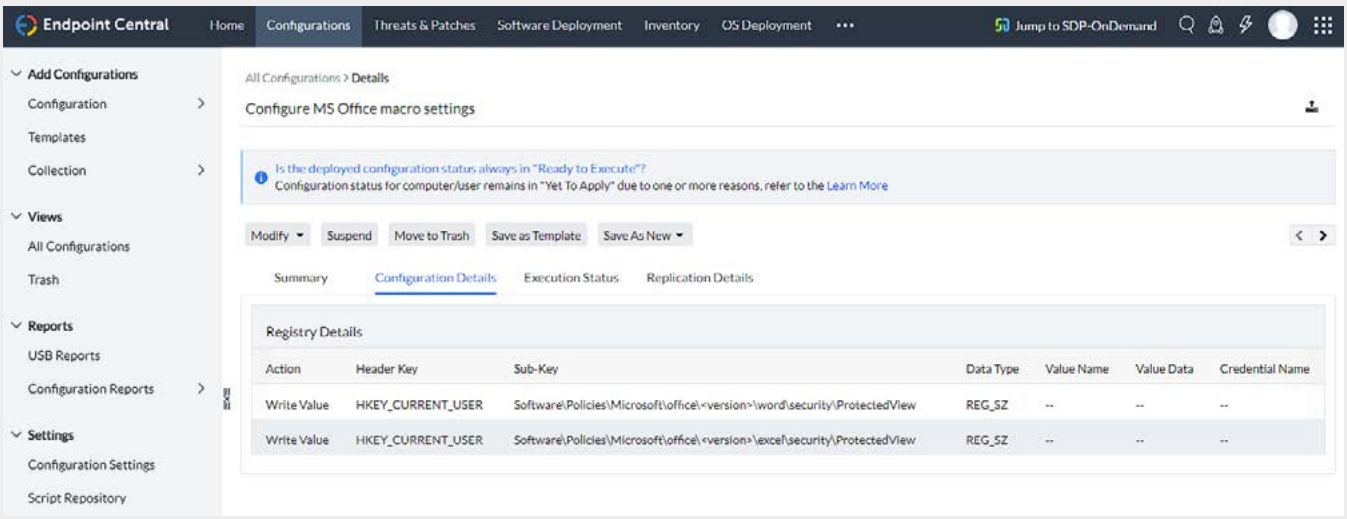
5.3.1 Manage Microsoft Office settings out of the box by disabling macros for users and blocking them in files from the internet.

5.3.2 Microsoft Office macro security settings cannot be changed by users.

5.3.3 Allow users to execute macros only in documents from trusted locations with limited write access.

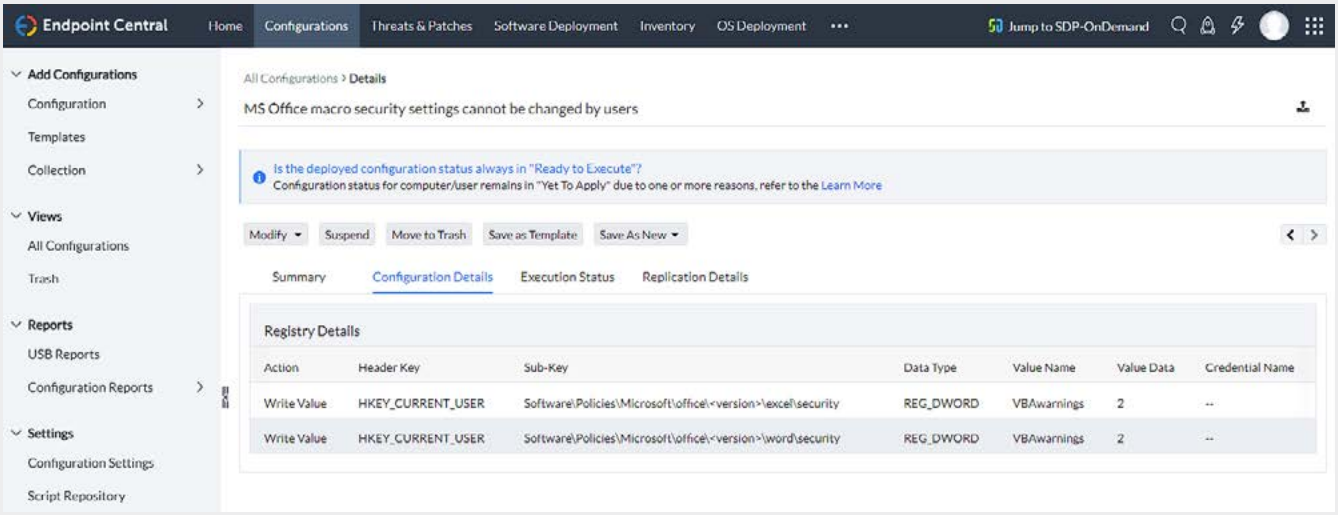
5.3.1 Manage Microsoft Office settings out of the box by disabling macros for users and blocking them in files from the internet.

Microsoft Office macros are allowed to execute,but only after prompting users for approval; documents originating from the internet are blocked.



Configuring Microsoft Office macro settings in Endpoint Central → Configurations.

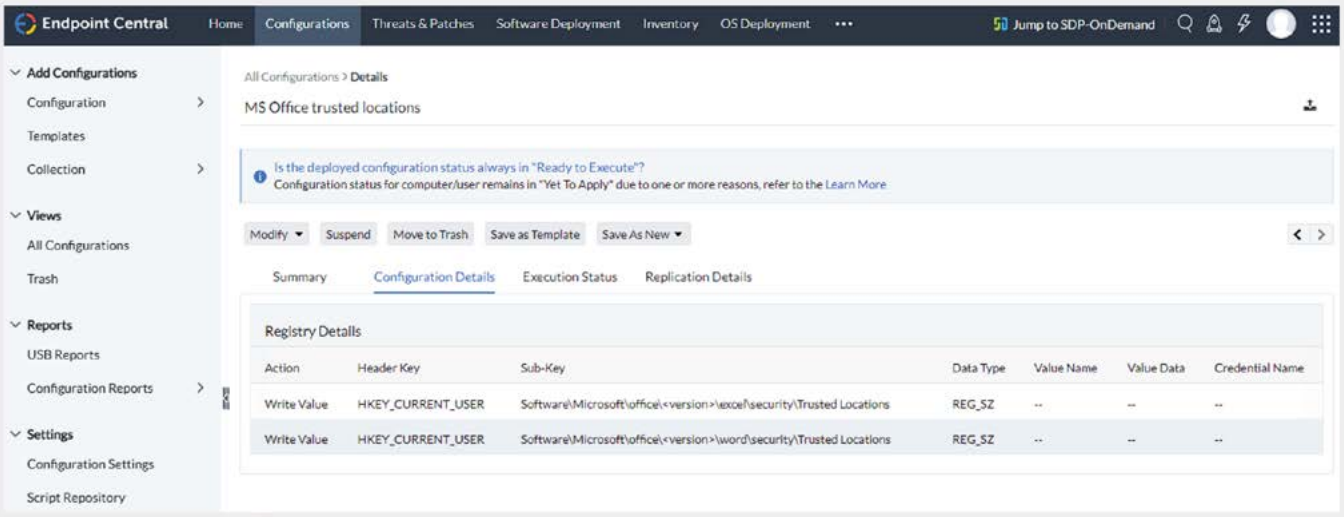
5.3.2 Microsoft Office macro security settings cannot be changed by users.



Restrict users from changing macro security settings in Endpoint Central → Configurations.

5.3.3 Allow users to execute macros only in documents from trusted locations with limited write access.

Microsoft Office macros are only allowed to execute in documents from trusted locations where write access is limited to personnel whose role is to vet and approve macros.



Configuring macros to be executed in Endpoint Central → Configurations.

Achieved Maturity Levels: 3, 2, and 1

(Endpoint Central with Security Addons)

5.4: User application hardening

How can ManageEngine help implement this protection strategy?

Use Endpoint Central, once you have a full list of your organisation's applications, begin by changing any default usernames and passwords. This might seem like a trivial step, but it's important. If an application uses a service such Flash, Java, or web advertisements that are not essential, disable or uninstall these components.

At this level, the mandate also requires you to log PowerShell activities to detect security incidents. Use Log360 to monitor PowerShell commands and detect suspicious executions or unauthorised events spawning using PowerShell.

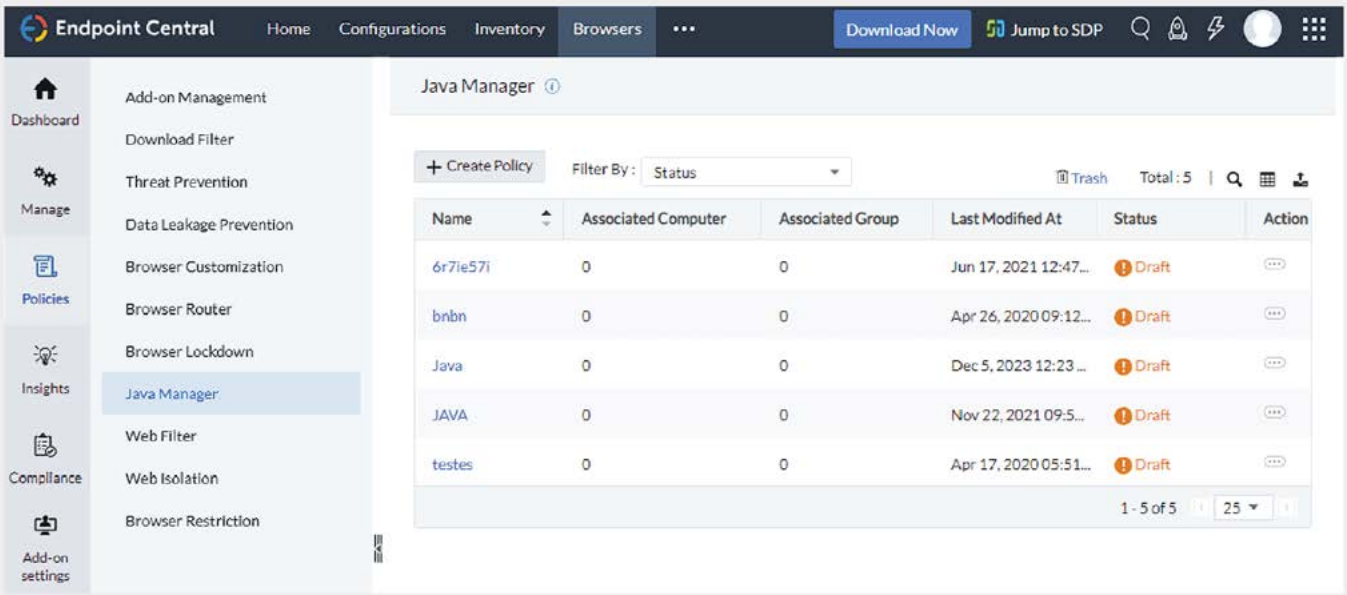
Steps to achieve this strategy:

5.4.1 Control browser plug-ins, extensions, and allowed sites. Stop processing Java and web advertisements from the internet in web browsers.

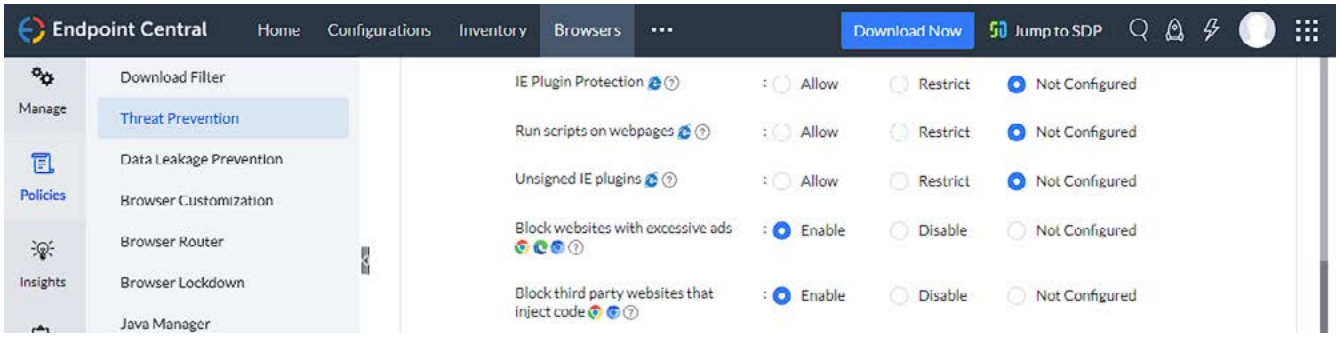
5.4.2 Restrict browsers by providing or restricting access to web applications.

5.4.3 Collect and examine PowerShell event logs centrally, at regular intervals.

5.4.1 Control browser plug-ins, extensions, and allowed sites. Stop processing Java and web advertisements from the internet in web browsers.

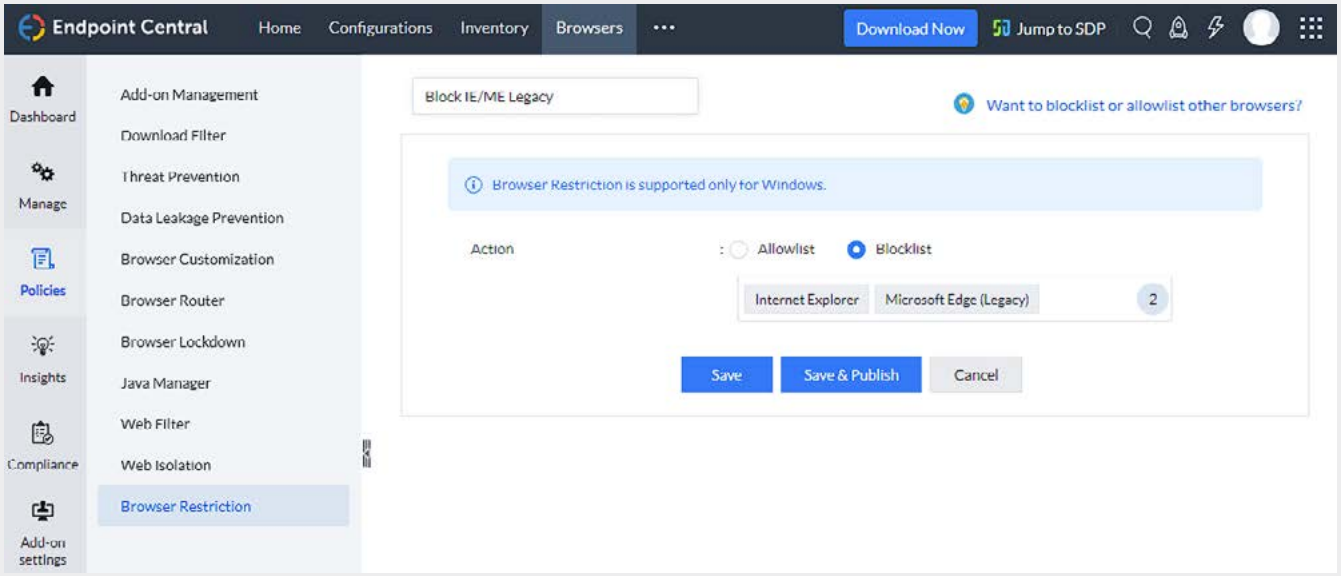


Blocking Java in web sites in Endpoint Central → Browsers.



Blocking advertisements in Endpoint Central → Browsers.

5.4.2 Restrict browsers by providing or restricting access to web applications.



Configuring browser restriction in Endpoint Central → Browsers.

Note: Use the solution to block a browser, irrespective of its version.

5.4.3 Collect and examine PowerShell event logs centrally, at regular intervals.

Log360 monitors events happening through PowerShell and can detect suspicious command executions, unauthorised script executions, and unauthorised or malicious service initiations through PowerShell with its predefined correlation rules. The solution provides you with deeper insights on who did what, from where, and what the impact of the security event is in the form of an intuitive incident report; it can even trigger an alert for malicious activities.

Achieved Maturity Levels: 2 and 1

(Endpoint Central with Security Addons, Log360)

5.5: Restrict administrative privileges

How can ManageEngine help implement this protection strategy?

Using ManageEngine, you can begin by making a thorough list of all of the administrator accounts in your organisation. Include all local, domain, and enterprise admin groups as well as all accounts with elevated privileges. Once you have a list of all administrative privileges, check for the validity of these privileges and how many of them are still required.

At this maturity level, the regulations mandate centralised logging relating to the use of, and changes to, privileged accounts. It states that lack of sufficient logging can impact the ability of an organisation to identify or determine the extent of cybersecurity incidents and the ways to mitigate them. Using ManageEngine, you can centrally log and audit user activities, especially with respect to privileged users, and analyse them for potential threats like account compromises, lateral movement, data exfiltration, and more.

Steps to achieve this strategy:

5.5.1 Validate requests for privileged access.

5.5.2 Implement logon restrictions to privileged operating environments.

5.5.3 Conduct administrative activities through jump servers.

5.5.4 Create a strong password policy.

5.5.5 Log changes to privileged accounts and groups.

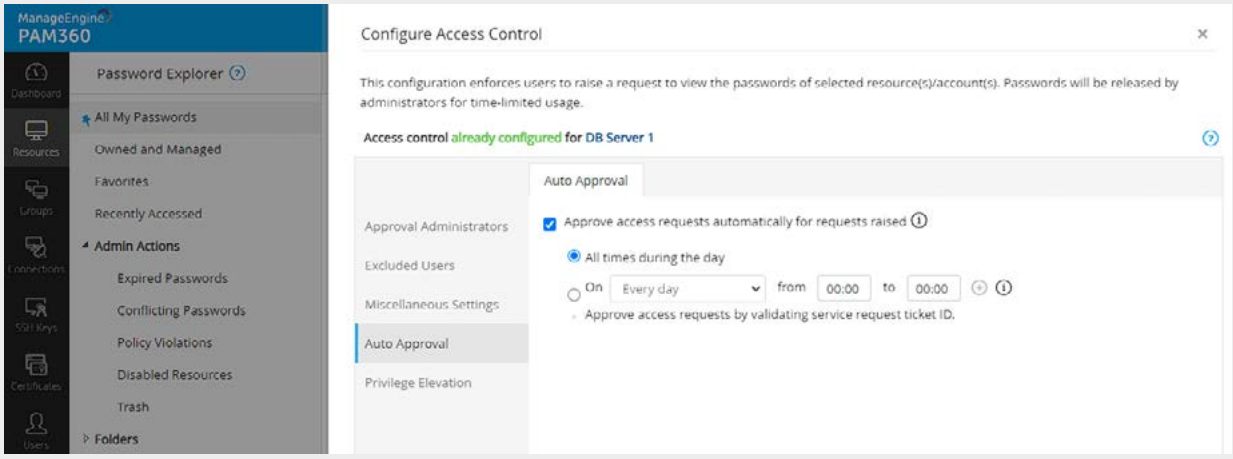
5.5.6 Enable just-in-time privilege elevation.

5.5.7 Delegate role-based access to AD, Exchange, and Microsoft 365.

5.5.8 Centrally log privileged access events.

5.5.1 Validate requests for privileged access.

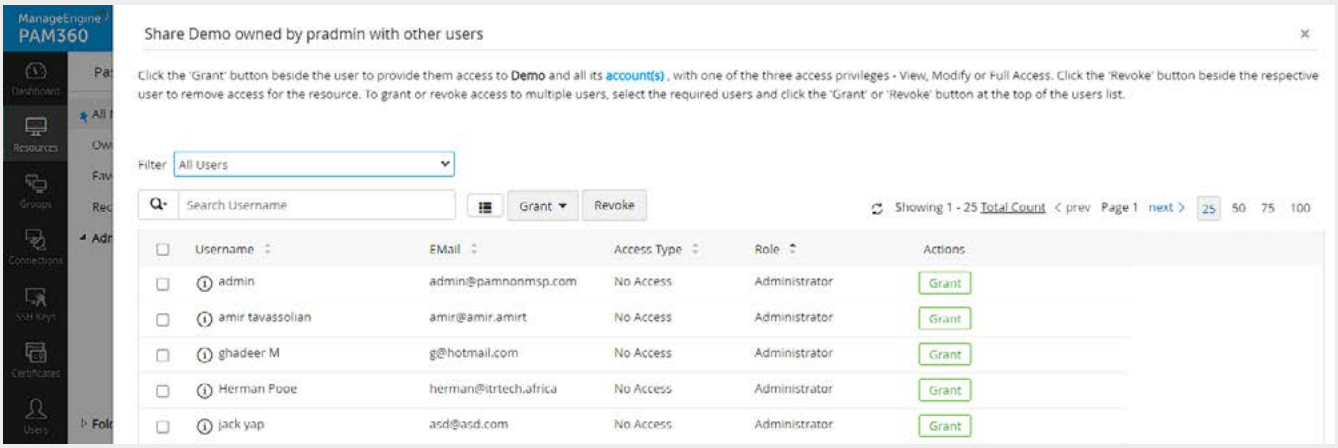
Privileged access to systems, applications, and information is validated when first requested. The validation can be done manually via requests or automatically.



Validating requests by configuring access control in PAM360 → Resources.

5.5.2 Implement logon restrictions to privileged operating environments.

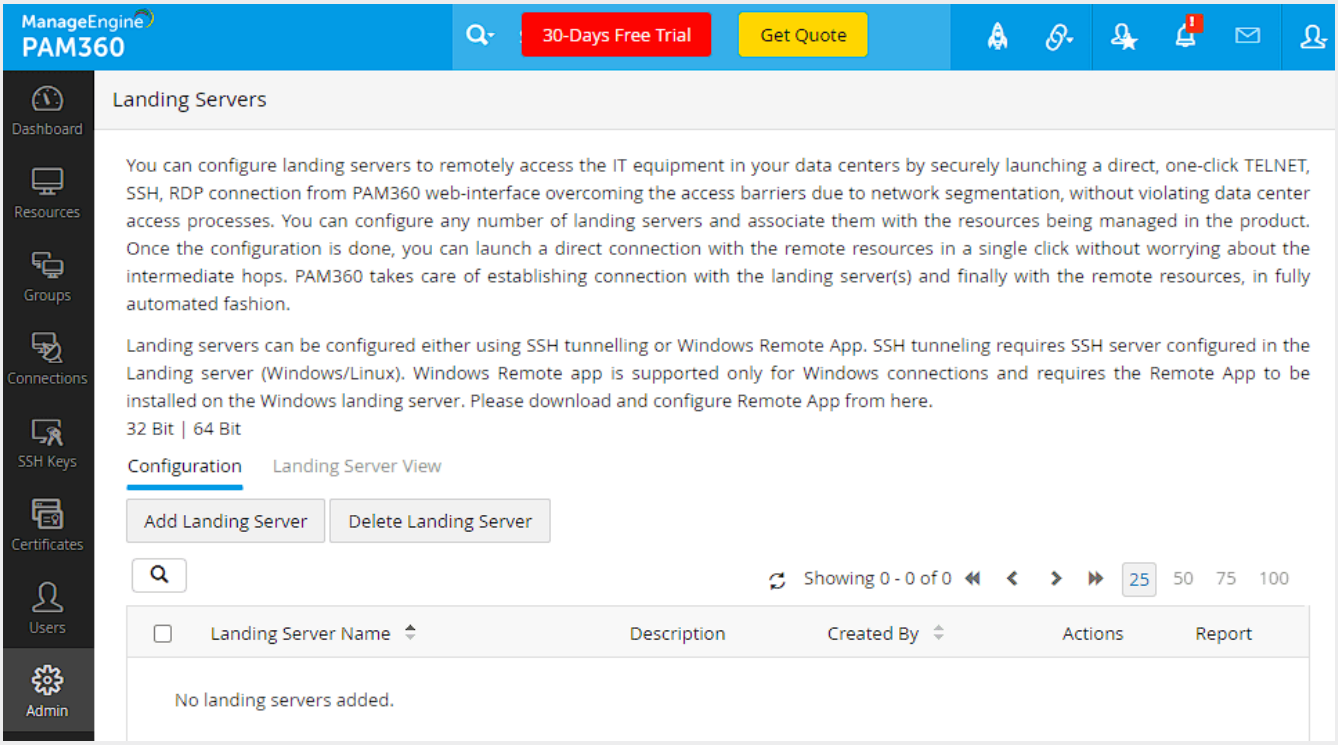
Our solution, PAM360, allows you to share your resources and resource groups in bulk with other users and user groups. When you share a selection of resources, all the passwords of all of the resources will also be shared. You can enforce least privilege by granting access permissions to users and user groups at varying levels based on their roles. Administrative users can be provided with Full Access permissions, while the maximum access permission for standard users is Modify Passwords. Use this to share privileged operating environments only with privileged users.



Sharing resources with users and user groups in PAM360 → Resources.

5.5.3 Conduct administrative activities through jump servers.

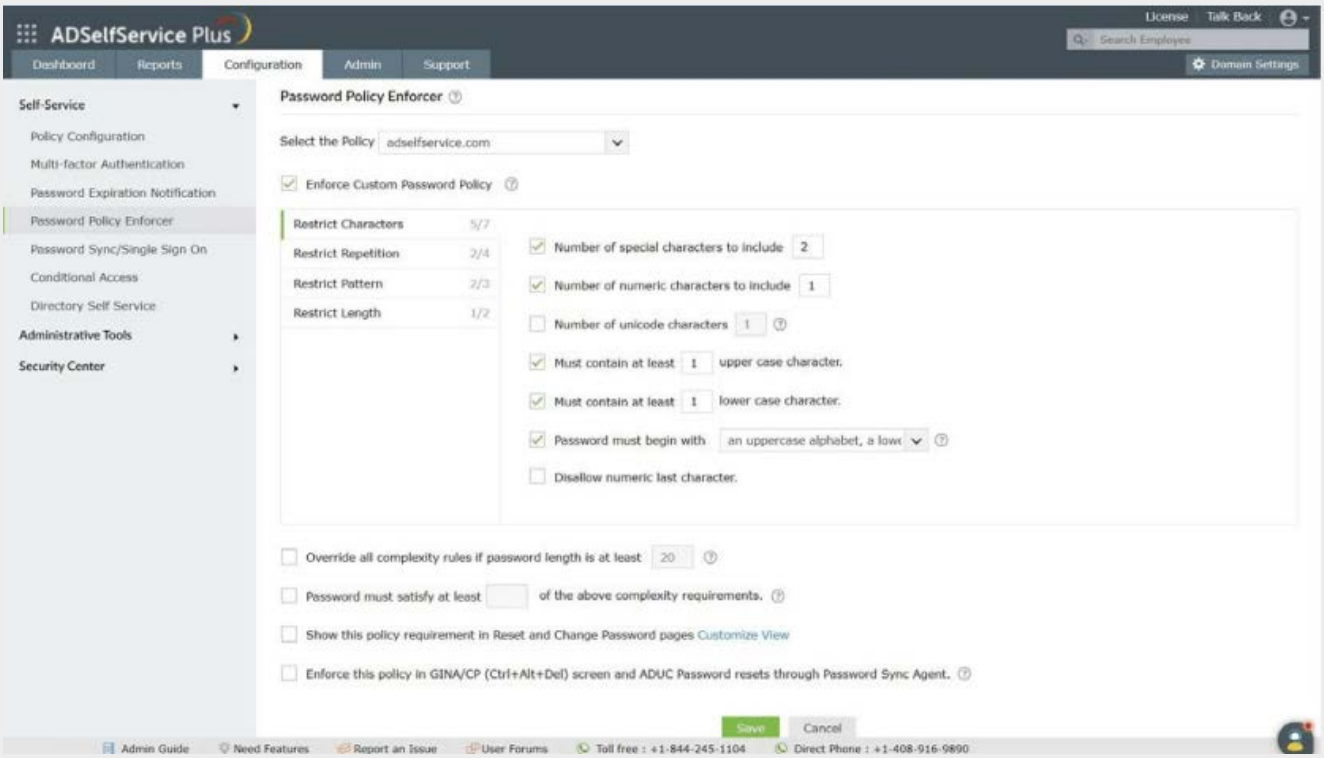
Using our solution, PAM360, simplify remote access management using landing servers. Use PAM360 to effectively launch direct connections (Telnet, SSH, and RDP) to access IT equipment in secure data centres and isolated networks, overcoming access barriers created by network segmentation while adhering to data centre access protocols and performing administrative activities.



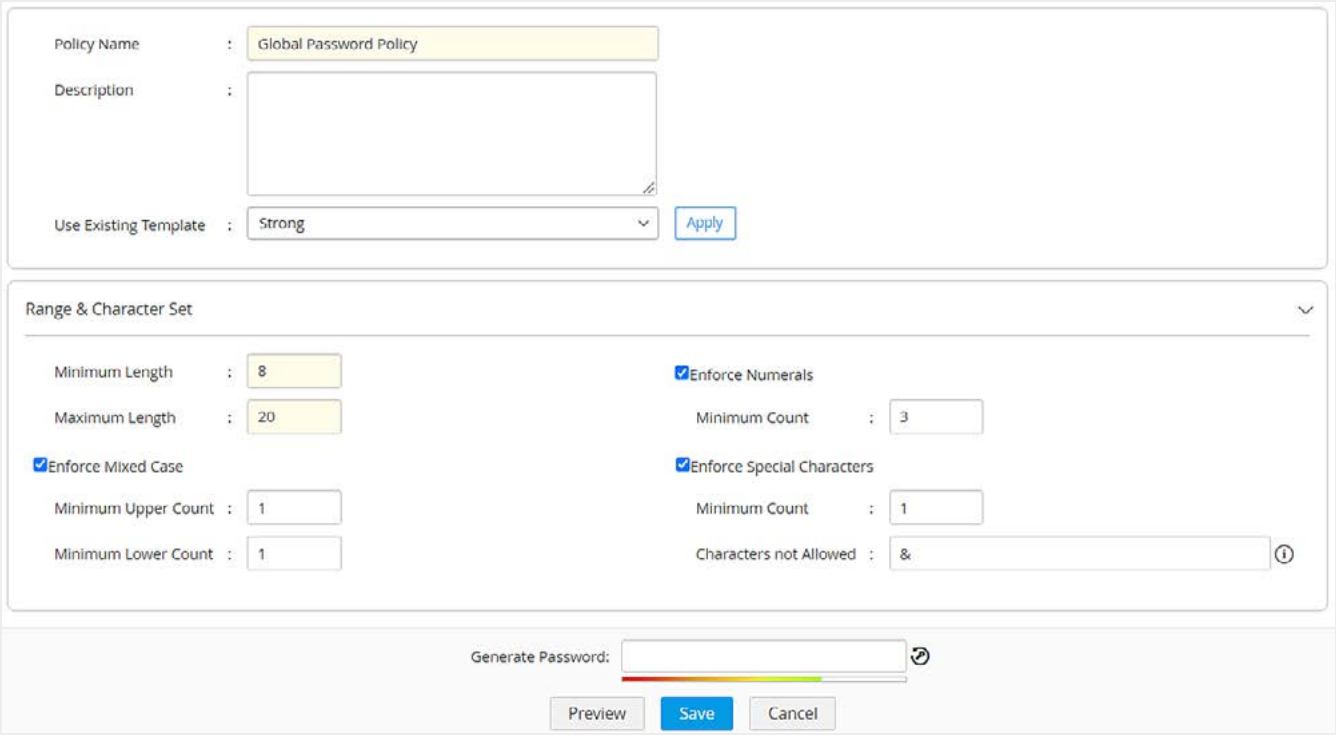
Configuring landing servers in PAM360 → Admin.

5.5.4 Create a strong password policy.

Administrators must use advanced password policy controls to ensure users create strong passwords that are not easily susceptible to sophisticated credential attacks. These controls include banning the use of breached passwords, ensuring sufficient complexity requirements, and encouraging users to use passphrases. ADSelfService Plus' Password Policy Enforcer overcomes the drawbacks of the built-in password policies in enterprise systems like Active Directory and allows you to enforce a custom, advanced password policies to ensure that your organisational resources are protected from potential cyberattacks. Credentials for local administrator accounts and service accounts are unique, critical, and managed. Password policies in PAM360 help you define the structure and complexity of passwords to be used. You can either use the predefined policies or create new policies to suit the needs of your organisation.



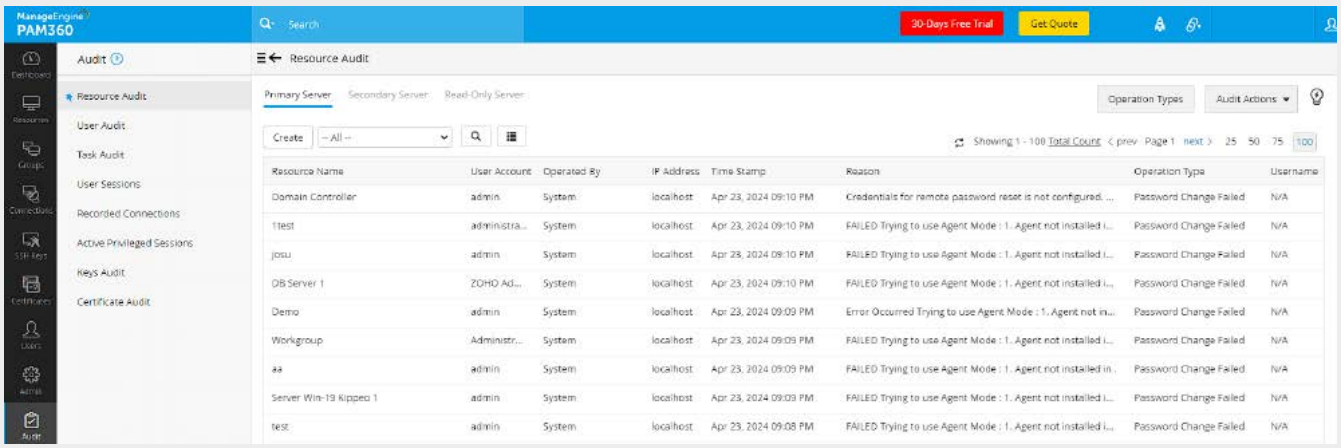
Advanced password policy controls in ADSelfService Plus → Configuration.



Configuring password policies in ADSelfService Plus → Configuration.

5.5.5 Log changes to privileged accounts and groups.

PAM360 comes with an efficient auditing mechanism, which records all activities performed in the product. The audit trails capture information on who performed what operation and when. Apart from monitoring the changes done via PAM360, Log360 centrally logs any privileged accounts and groups management events. With Log360, track critical events such as user addition to groups, changes to GPOs made by privileged users, permission changes, and more.

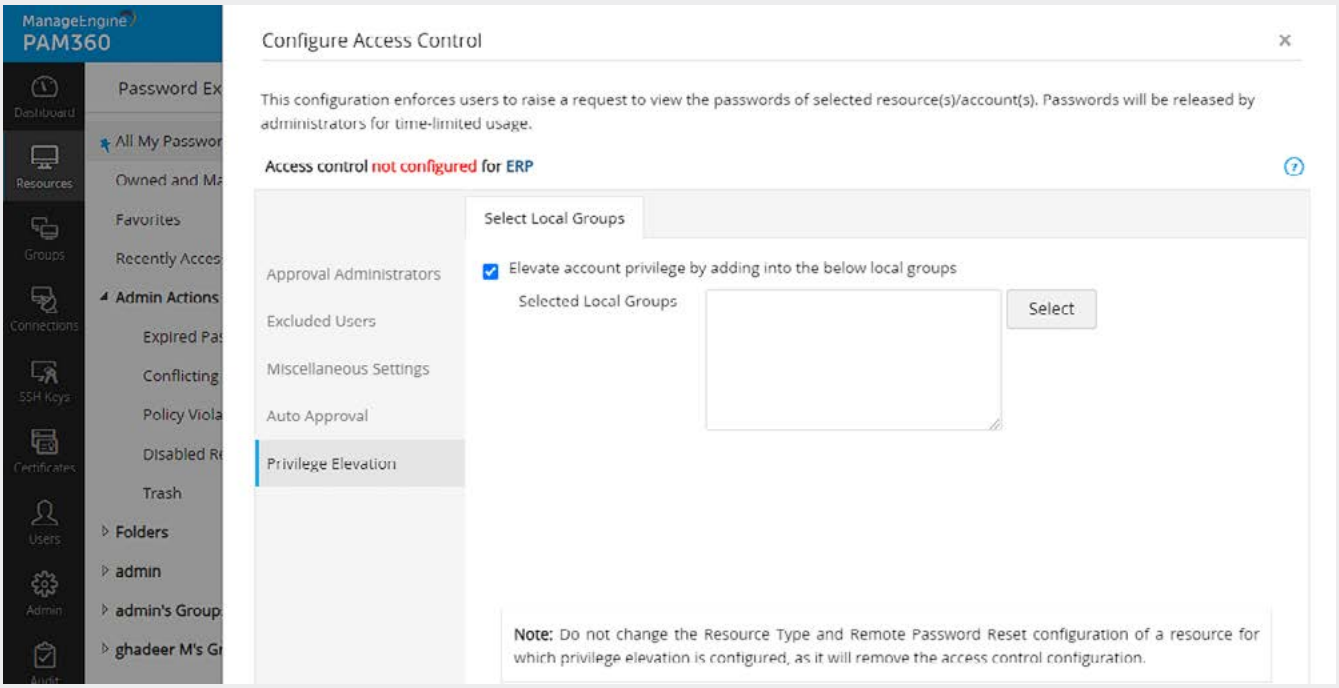


Setting up audit actions in PAM360 → Audits.

5.5.6 Enable just-in-time privilege elevation.

Just-in-time (JIT) privilege elevation is designed to limit the amount of time privileged access is enabled on a critical system. This allows administrators, users, applications, and scripts to access sensitive information only when required and only for the amount of time needed to complete the task. Once the request period ends, access to sensitive systems is revoked, and their associated credentials are rotated instantly after every session.

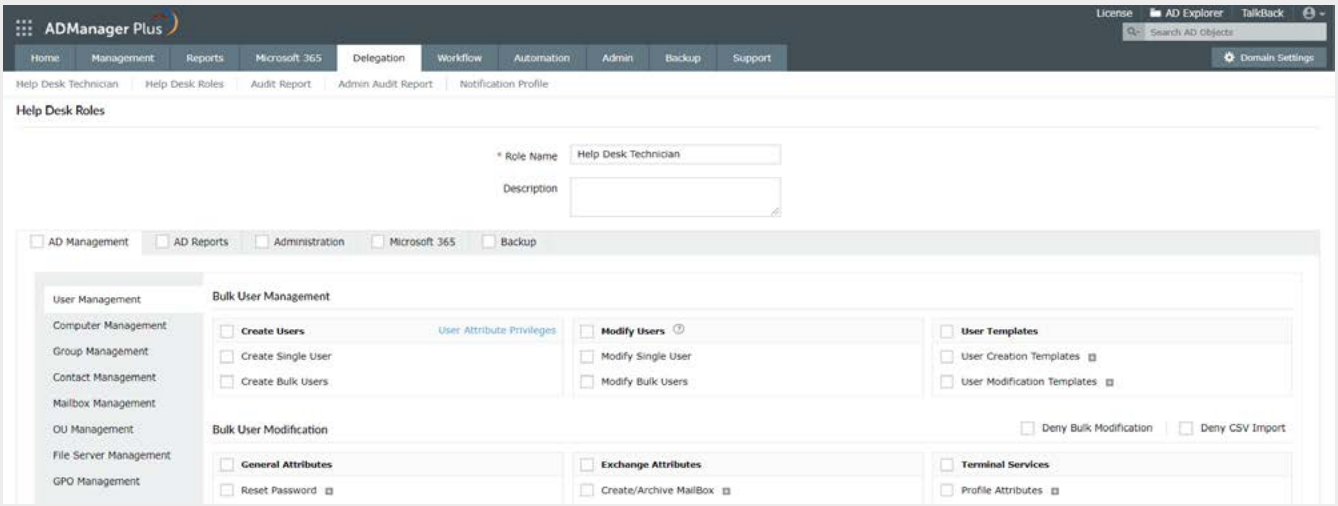
In addition to time-based JIT access to critical systems, PAM360 offers a self-service privilege elevation option for Windows and *Nix environments using which authorised administrative users can allow-list and run sensitive applications and commands with elevated privileges.



Configuring just-in-time privilege elevation in PAM360 → Resources.

5.5.7 Delegate role-based access to AD, Exchange, and Microsoft 365.

For better management of AD, Exchange, and Microsoft 365 administration, AD360 provides out-of-the-box delegations. Delegate day-to-day tasks to non-administrative users with the help of built-in help desk roles or create a customised role. Restrict the activities of delegated technicians to a specific site, tenant, domain, OU, or group. Get detailed audit reports to track all the changes made to a help desk role or technician, along with the changes enacted by the delegated technicians.



Configuring roles for AD administration.

5.5.8 Centrally log privileged access events.

Log360 helps you centrally aggregate privileged users' access events and analyse them to detect any suspicious activity. Further, the solution's ML-based behaviour analytics helps you detect anomalous logons by privileged users based on time and behaviour patterns. Detect unusual access of a resource by a privileged user, logons from unusual locations at unusual times, multiple logon failures, and logons from different locations within a short span of time using Log360's predefined correlation and alert rules.

These rules help you detect security incidents based on privileged access events.

Achieved Maturity Levels: 3, 2, and 1
(PAM360, AD360, Log360)

5.6: Patch operating systems

How can ManageEngine help implement this protection strategy?

With Endpoint Central's Patch Management module, make patch management an integral part of your security maintenance program by implementing central control over your patch management schedule and distribution. Operating systems like Windows, macOS, and Linux can be patched with support for a wide range of drivers. Patches can be deployed to servers, workstations, and mobile devices (using the Mobile Device Management module).

Steps to achieve this strategy:

5.6.1 Patch, update, or mitigate security vulnerabilities based on severity in operating systems such as Windows, macOS, and Linux.

5.6.2 Identify and manage firmware vulnerabilities.

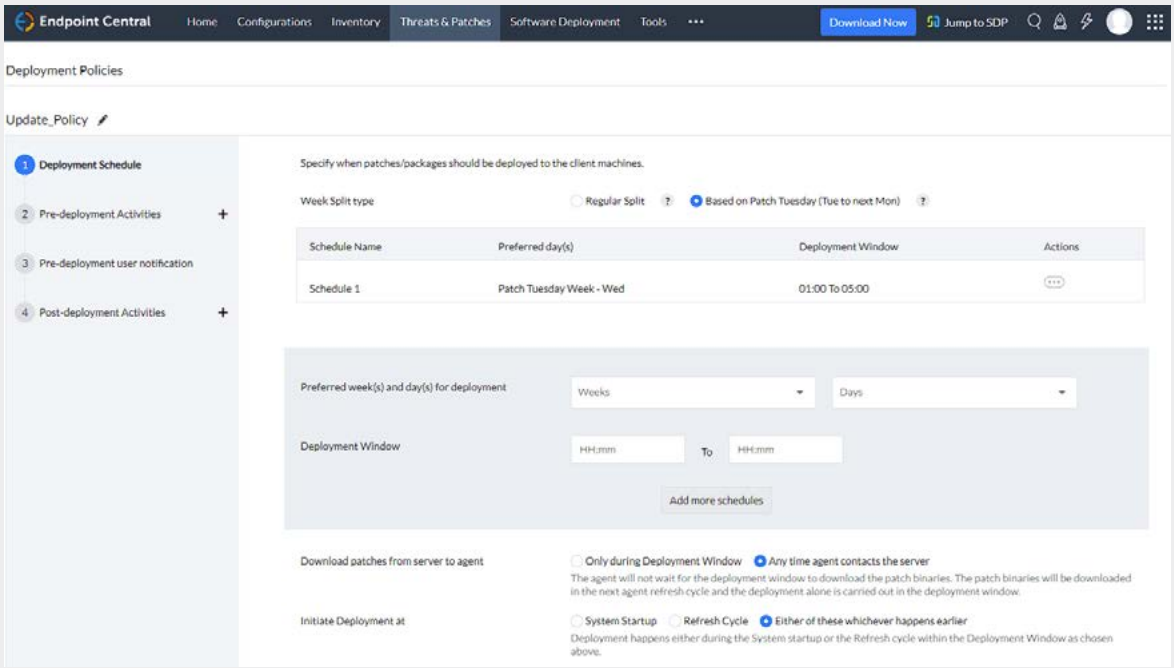
5.6.3 Scan for vulnerabilities.

5.6.4 Automate OS updates on mobile devices using the Mobile Device Management module.

5.6.5 Update Windows legacy EOL systems to avoid a disruption in service.

5.6.1 Patch, update, or mitigate security vulnerabilities based on severity in operating systems such as Windows, macOS, and Linux.

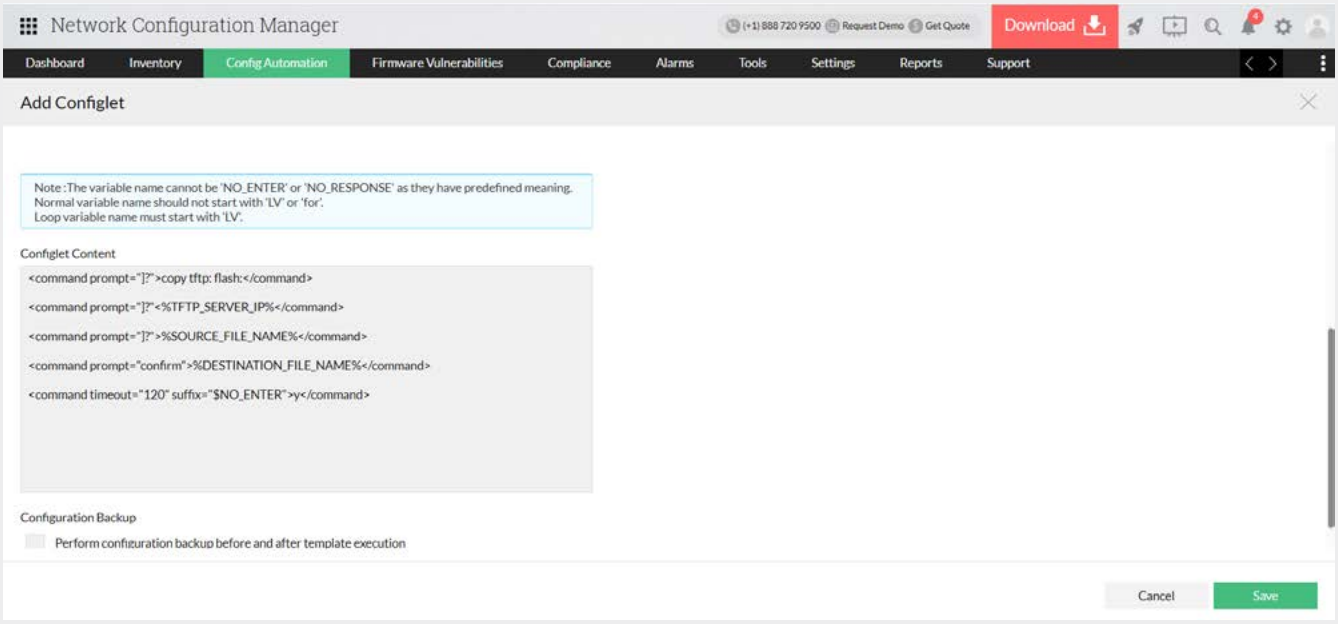
Security vulnerabilities in operating systems of internet-facing services which are assessed as extreme risks are patched, updated, or mitigated within two weeks of release, or within 48 hours if an exploit exists. The same is applied for workstations and servers within one month of release.



Configuring the patch deployment policy in Endpoint Central → Threats & Patches.

5.6.2 Identify and manage firmware vulnerabilities.

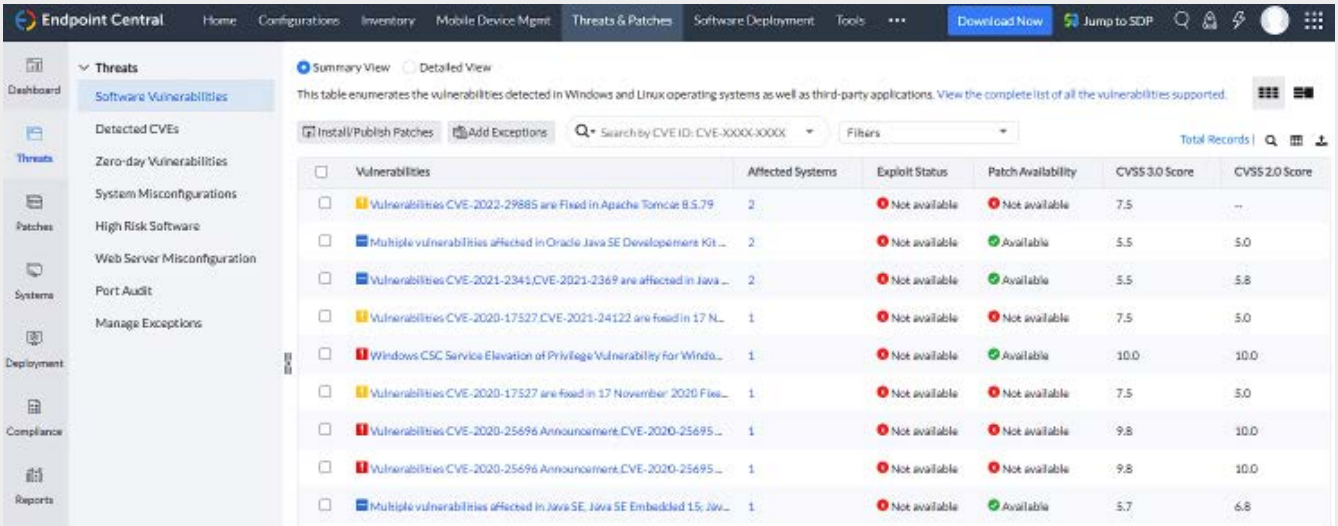
Security vulnerabilities in operating systems of network devices are identified and managed.



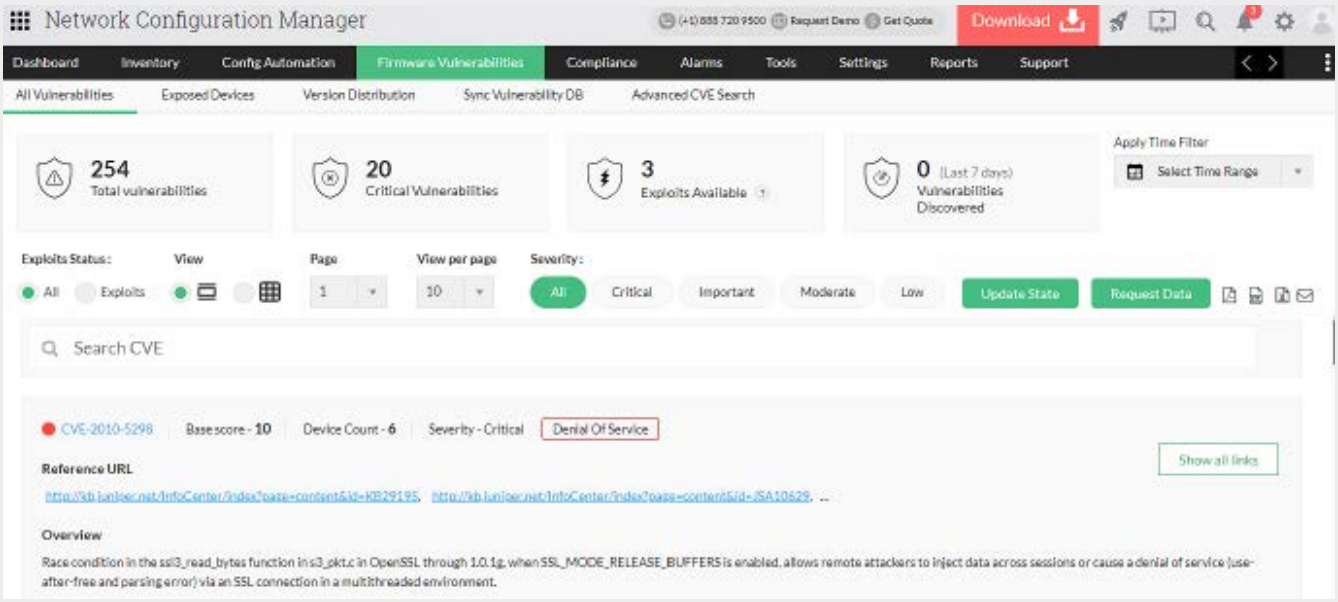
Firmware upgrade using Configlets and scripts in Network Configuration Manager → Config Automation.

5.6.3 Scan for vulnerabilities.

A vulnerability scanner is used to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services and in the operating systems of workstations, servers, and network devices.



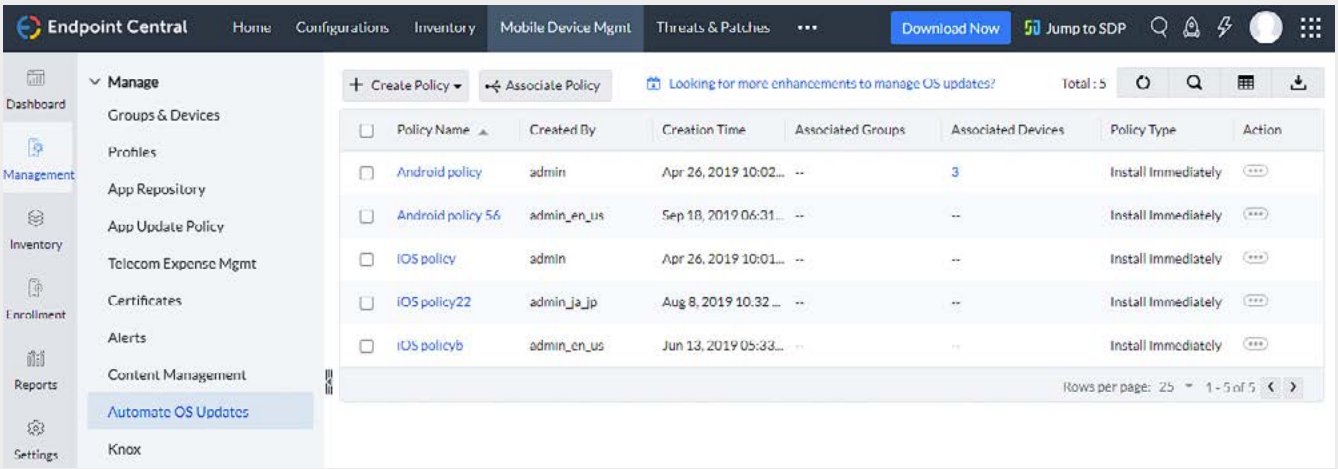
Software vulnerabilities scanned in Endpoint Central → Threats & Patches.



Identifying network devices' firmware vulnerabilities in Network Configuration Manager → Firmware Vulnerabilities.

5.6.4 Automate OS updates on mobile devices using the Mobile Device Management module.

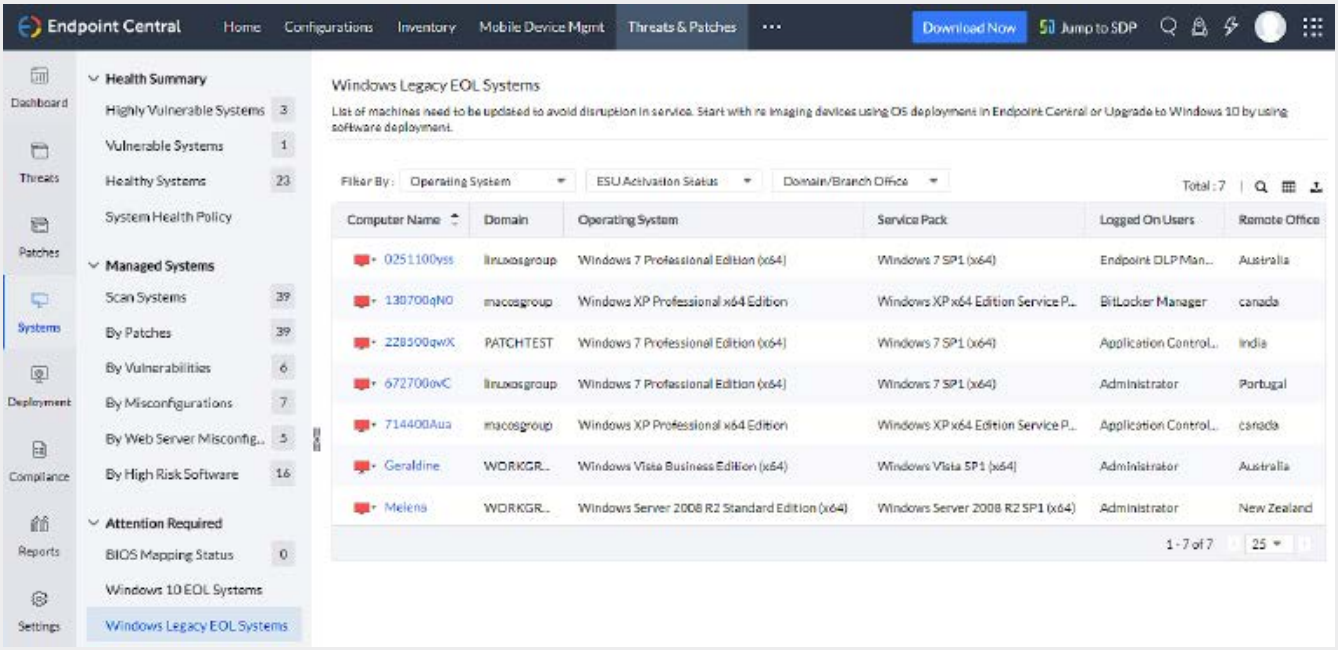
Automating OS updates in mobile devices mitigates many disadvantages that result from running an outdated OS version. This remedy provides additional technical support for devices running lower versions of the OS, addresses the unavailability of vital device and security features which are specific to particular OS versions, and helps ensure that the latest enterprise apps run smoothly.



Automate OS updates for mobile device management in Endpoint Central → Mobile Device Mgmt.

5.6.5 Update Windows legacy EOL systems to avoid a disruption in service.

List all the machines that need to be updated to avoid a disruption in service, and either reimage the devices using OS Deployment in Endpoint Central or upgrade to Windows 10 through the Software Deployment module.



Identifying legacy EOL systems in Endpoint Central → Threats & Patches.

Achieved Maturity Levels: 3, 2, and 1

(Endpoint Central with Security Addons, Network Configuration Manager)

5.7: Multi-factor authentication

How can ManageEngine help implement this protection strategy?

MFA helps reduce the attack surface and protects your organisation by requiring a higher level of identity assurance. In your network, it can be enabled for all users and all systems, and for both cloud and on-premises applications and endpoints.

At this maturity level, the regulation mandates central logging and analysis for multi-factor authentication events to assess the impact of cybersecurity incident, determine how it occurred and understand the remediation steps to be taken.

Steps to achieve this strategy:

5.7.1 Use one or more authentication techniques to verify users' identities during the password reset and account unlock process.

5.7.2 Use MFA to authenticate privileged users of systems.

5.7.3 Introduce MFA to manage endpoints

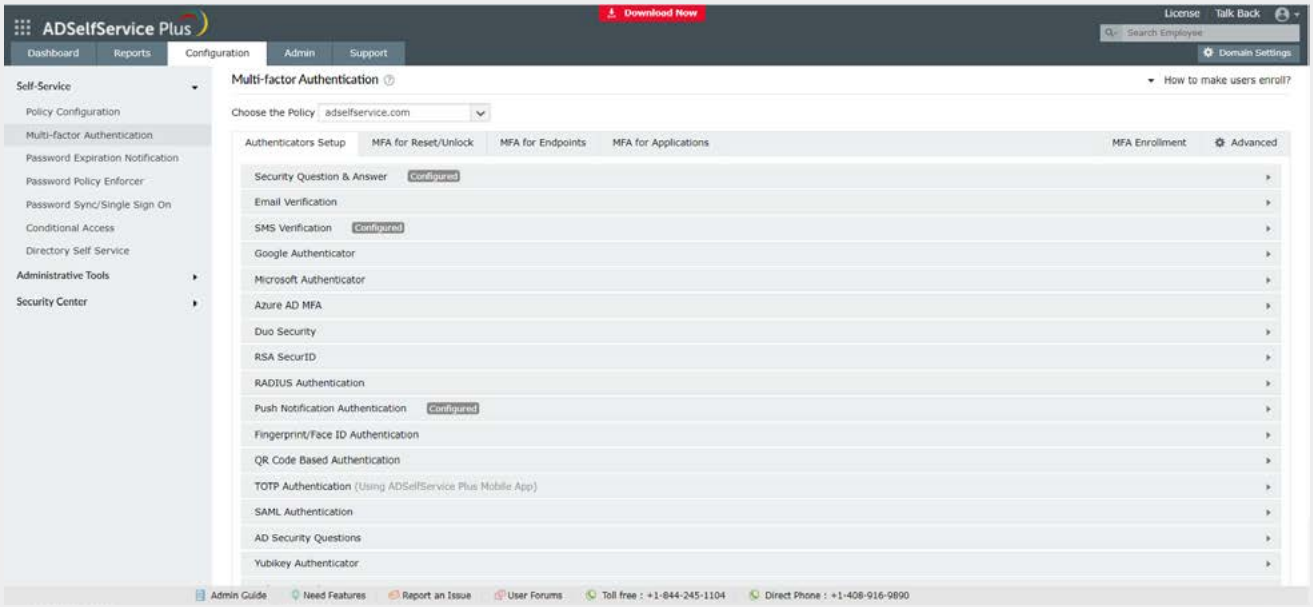
5.7.4 Log successful logins for auditing.

5.7.5 Enable centralised logging of successful and unsuccessful MFA events.

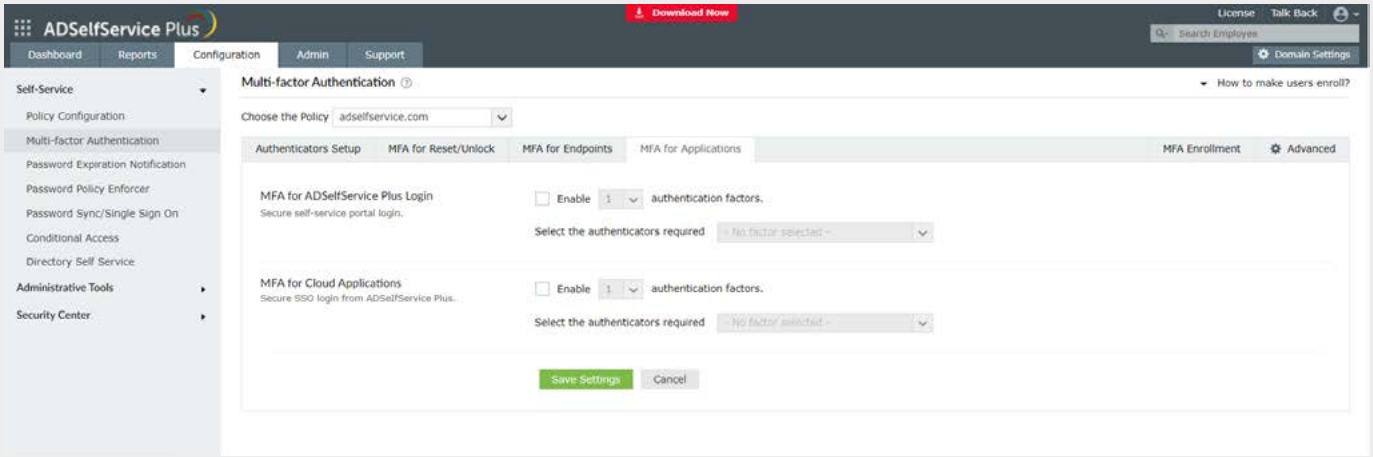
5.7.6 Analyse event logs from internet-facing servers to detect cybersecurity events.

5.7.7 Analyse the detected cybersecurity events in timely manner to identify security attacks and incidents

5.7.1 Use one or more authentication techniques to verify users' identities during the password reset and account unlock process.



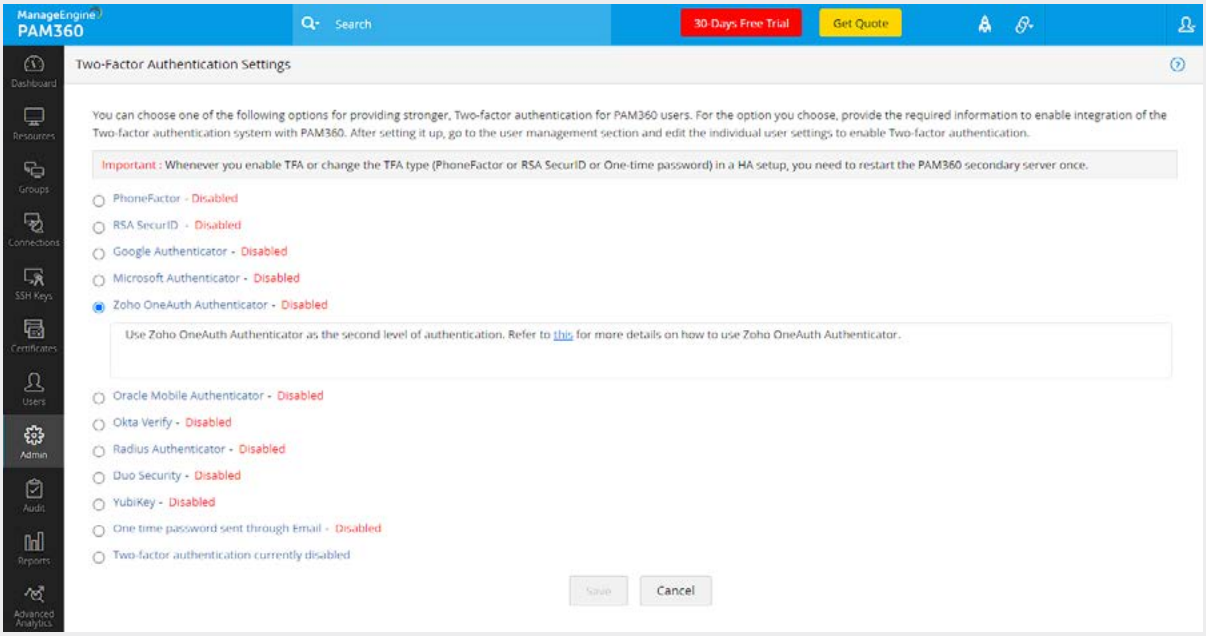
Configuring MFA for users in ADSelfService Plus → Configuration.



Configuring MFA for applications in ADSelfService Plus → Configuration.

5.7.2 Use MFA to authenticate privileged users of systems.

PAM360 stores sensitive administrative passwords of enterprise resources in an encrypted form in the database. To introduce an extra level of security, it provides two-factor authentication. Users will have to authenticate through two successive stages to access the PAM360 web interface.



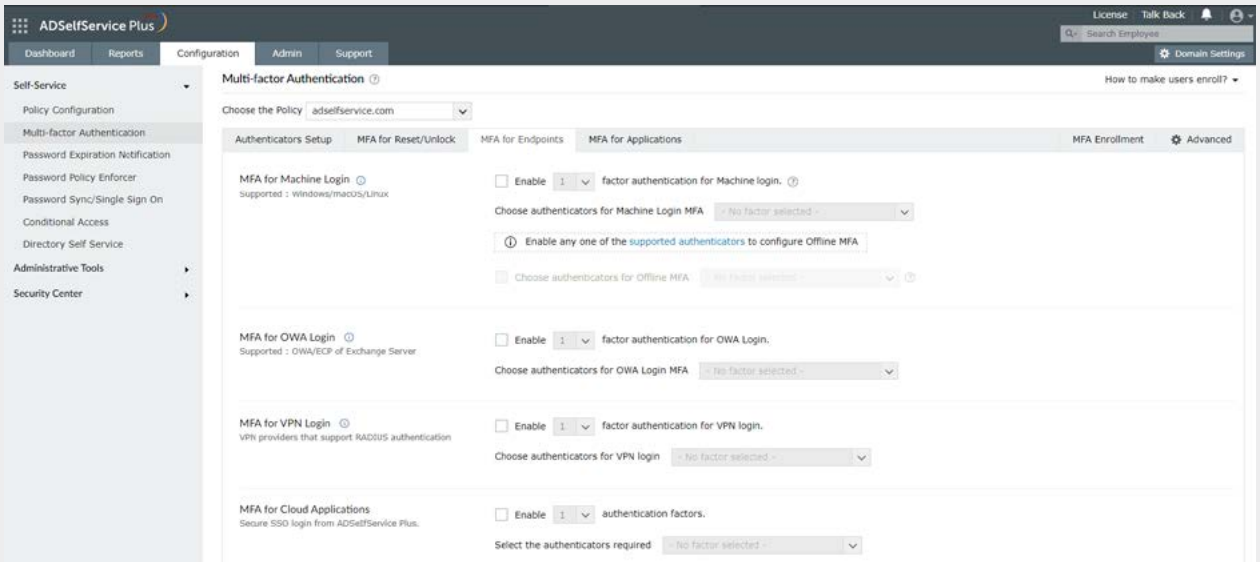
Enabling the configuration by setting two-factor authentication for privileged users in PAM360 → Admin.

5.7.3 Introduce MFA to manage endpoints

ADSelfService Plus offers Endpoint MFA to help organisations secure multiple points of access to organisation's sensitive resources. ADSelfService Plus' Endpoint MFA secures access to:

» Windows, macOS, and Linux machines.
» Top VPN providers like Fortinet, Cisco AnyConnect, Pulse, and more.
» Endpoints supporting RADIUS authentication such as Citrix Gateway, VMWare Horizon, and Microsoft Remote Desktop Gateway (RDP).
» Outlook Web access (OWA) logins.

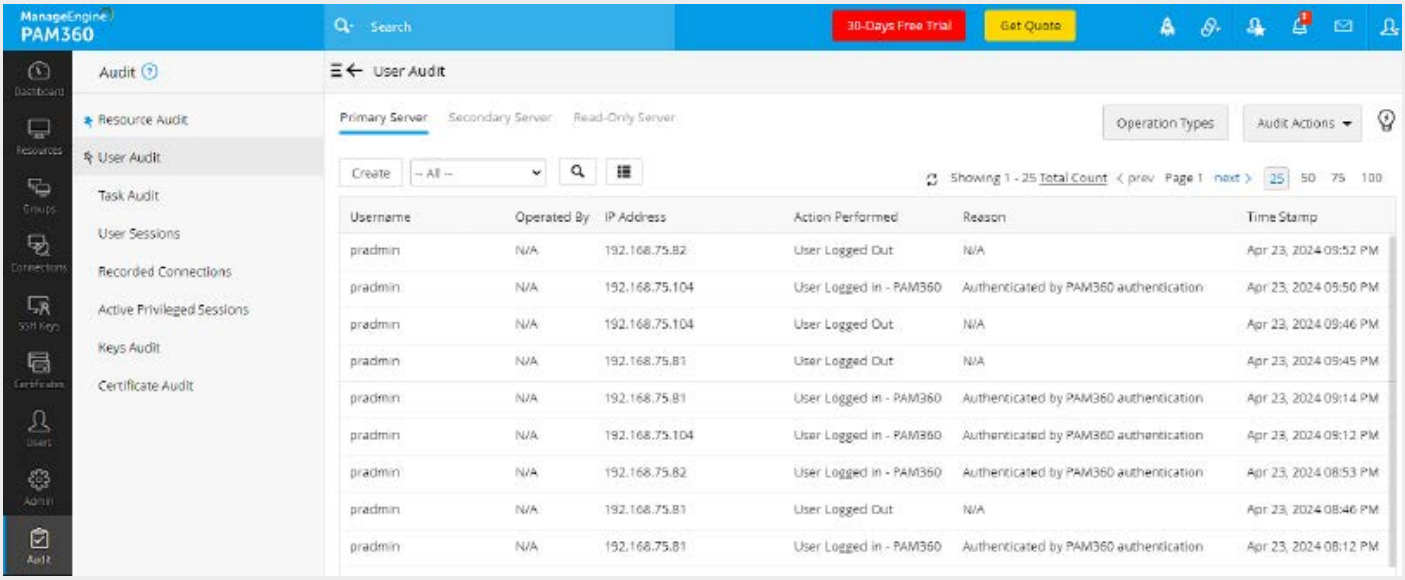
Moreover, ADSelfService Plus offers offline MFA for Windows machines which ensures the security of offline remote workers during machine logons.



Configuring MFA for endpoints in ADSelfService Plus → Configuration.

5.7.4 Log successful logins for auditing.

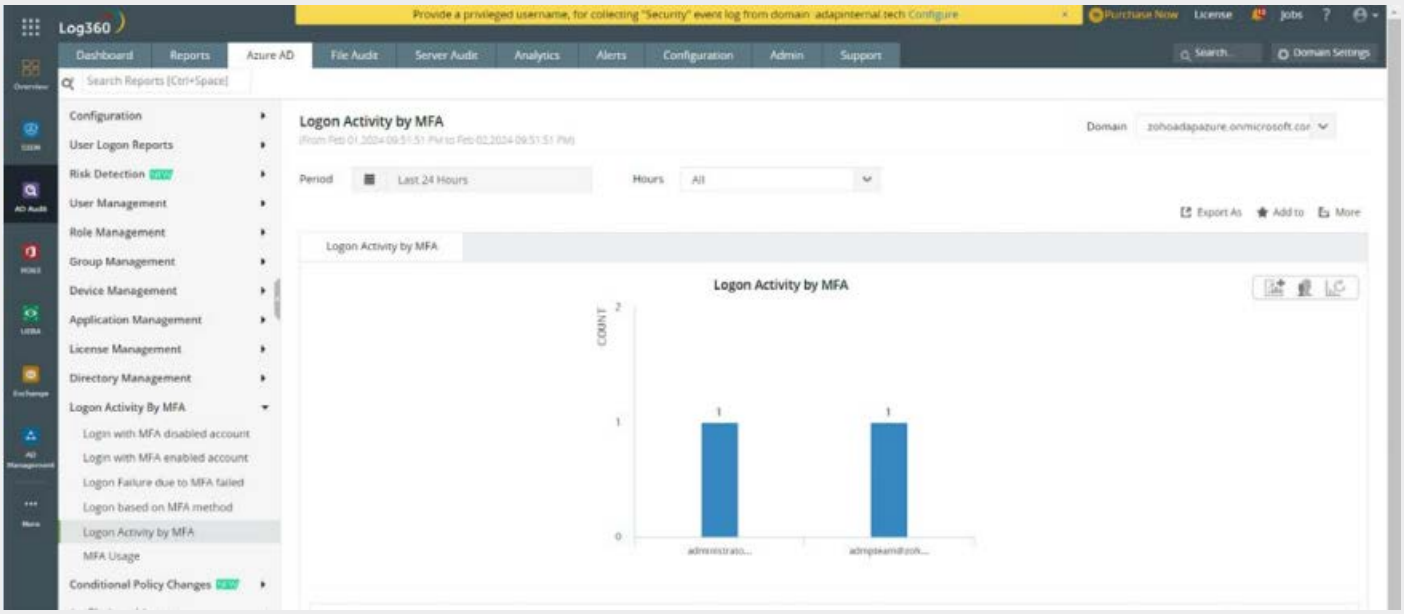
As PAM360 deals with sensitive passwords, it is important to have a complete record of who accessed what resource and when, along with details about every action performed by the users within the application. All operations performed by users are audited with the timestamp and the IP address from where they accessed the application.



User actions are logged for auditing in PAM360 → Audit.

5.7.5. Enable centralised logging of successful and unsuccessful MFA events.

Log360 centrally logs successful and failed MFA events. It provides details such as the IP address from where the logon happened, type of logon, and the reason for MFA failure.



Viewing MFA logon activity in Log360 → AD Audit.

5.7.6 Analyse event logs from internet-facing servers to detect cybersecurity events.

Log360 supports logging and analytics of internet-facing servers and web applications such as IIS and Apache servers, and DHCP applications. The solution's log analytics capability helps enterprises detect red flags, such as bad requests; extended response times; and attacks like SQL injection, cross-site scripting, distributed denial-of-service (DDoS), and more on these servers.

The solution comes with a built-in incident management system with automated workflow execution to immediately neutralise threats. Once reported as incidents, the cases can be assigned, tracked, and closed with the built-in case management system.

5.7.7 Analyse the detected cybersecurity events in timely manner to identify security attacks and incidents.

With Log360, enterprises can periodically review and analyse the security events through its ML-based Incident Workbench, which offers deeper insights into users, entities, and processes connected to security events, contextual data enrichment from AD, supported threat intelligence platforms, its UEBA component, and its option to group and mark the security events as incidents.

The Incident Workbench's process hunting tree provides visibility into the process lineage and thereby detects suspicious process executions or malware attacks. The Incident Workbench also offers users the ability to isolate infected hosts, assess the impact of security incidents, and neutralise them from within its console.

Achieved Maturity Levels: 3, 2, and 1
(PAM360, AD360, Log360)

5.8: Regular backups

How can ManageEngine help implement this protection strategy?

Perform daily backups by determining what you need to back up, the priority of backed-up content, and how you will perform these backups. Depending upon your organisation's requirements, determine whether you will need to perform full backups every day or a full backup once a week with incremental daily backups. Furthermore, you will also need to implement a regular restoration testing and disaster recovery plan.

Steps to achieve this strategy:

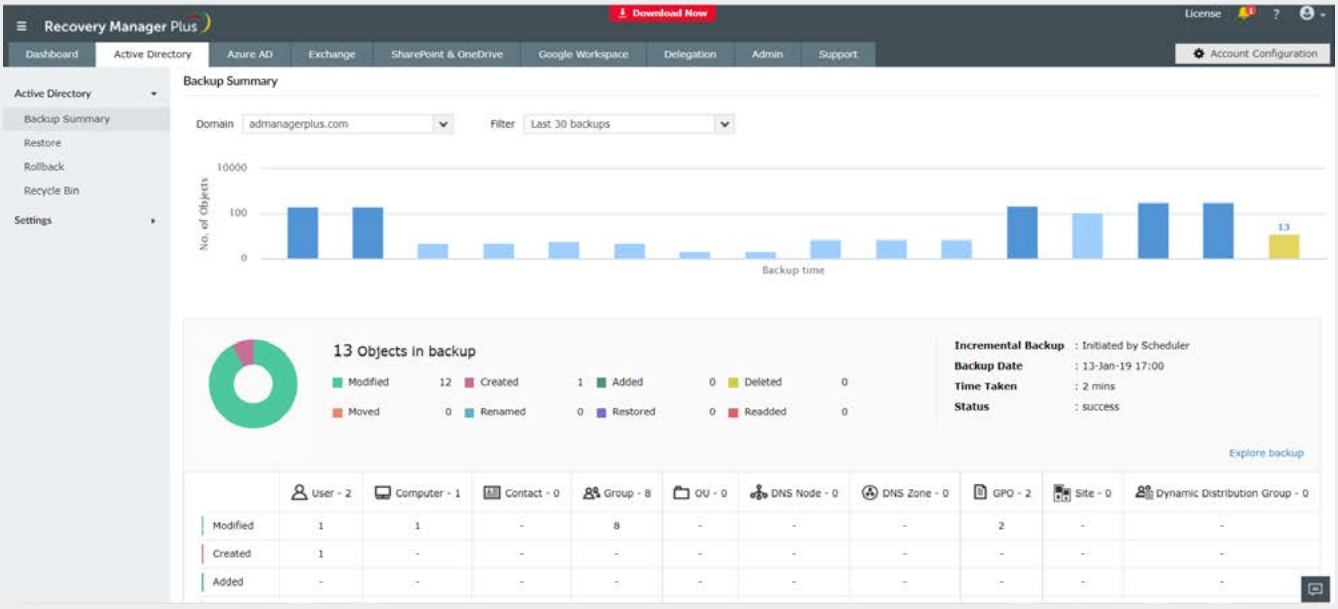
5.8.1 Perform comprehensive, scheduled incremental object- and item-level backups in AD, SharePoint Online, on-premises Exchange, and Exchange Online.

5.8.2 Back up the entire database of application configurations, system settings, and password share permissions through scheduled tasks or live data backup.

5.8.3 Automate configuration backups for firewalls, routers, switches, and more.

5.8.1 Perform comprehensive, scheduled incremental object- and item-level backups in AD, SharePoint Online, on-premises Exchange, and Exchange Online.

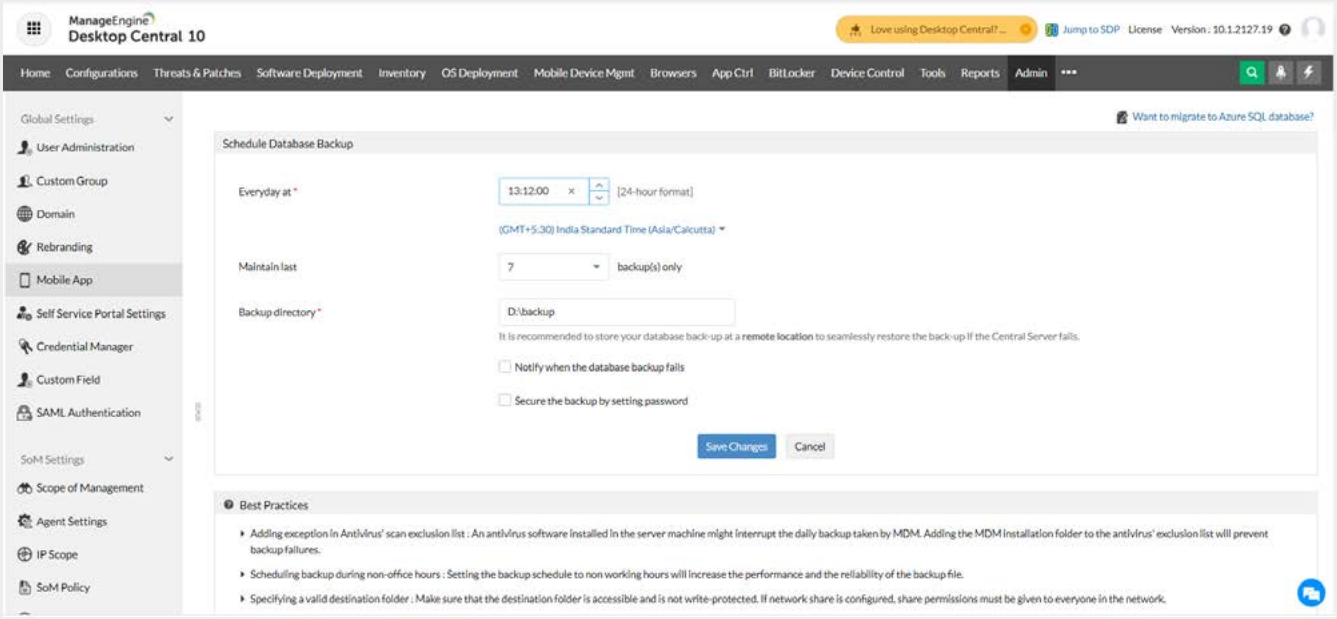
Back up your AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments from a single console, and restore any object, site, or mailbox whenever you need it using RecoveryManager Plus.



Back up AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments in Recovery Manager Plus.

5.8.2 Back up the entire database of application configurations, system settings, and password share permissions through scheduled tasks or live data backup.

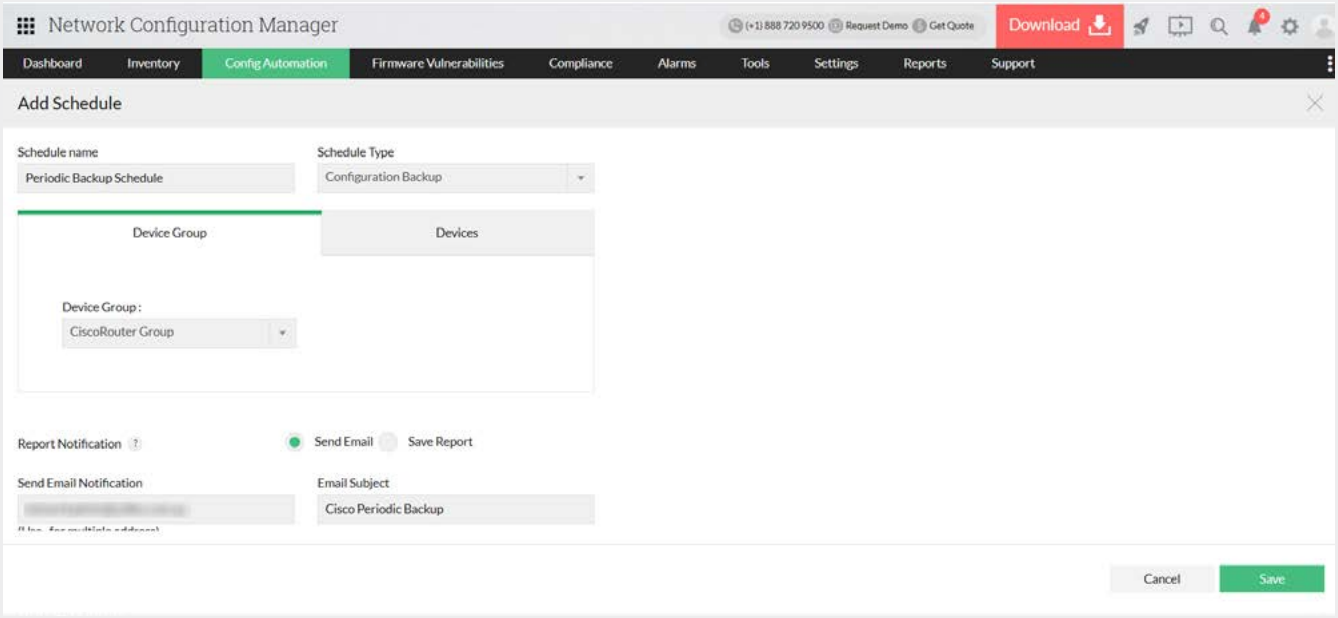
Endpoint Central uses a database to store information like configuration details, the status of deployed configurations, and details about reports, like user logon reports and AD reports. Creating a backup of this database and certain important files, like configuration files, is necessary to prevent loss of data.



Configuring a scheduled database backup in Endpoint Central → Admin.

5.8.3 Automate configuration backups for firewalls, routers, switches, and more.

In Network Configuration Manager, Configuration Backup is a process for saving your existing network configuration files and creating a repository of all incremental versions. Faulty configuration changes can cause network disasters like a data breach or even a network outage. In such times, network admins can upload a stable configuration version from the repository and restore the network promptly. Configuration backups are also important while auditing to identify where a particular fault originated from and for compliance audits.



Scheduling the Network Device Configuration backup in Network Configuration Manager → Config Automation.

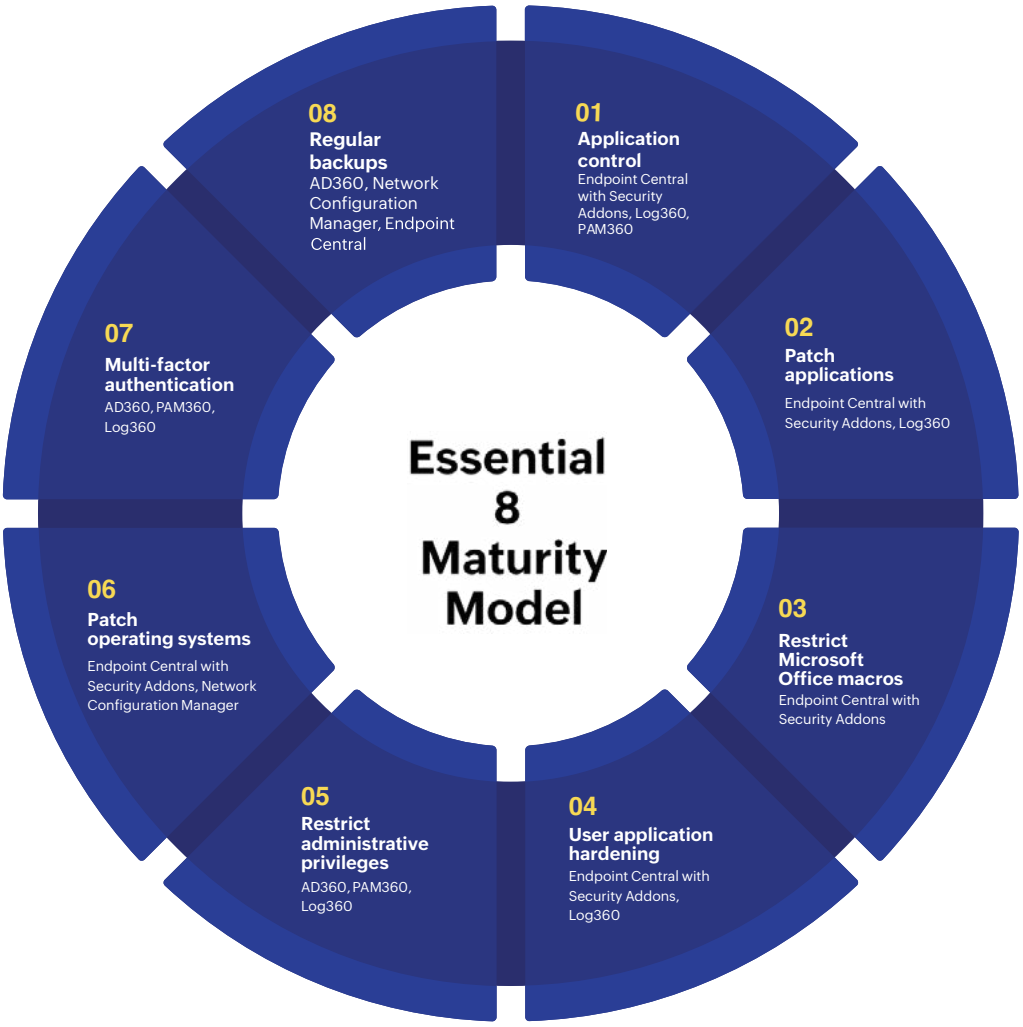
Achieved Maturity Level: 1

(Network Configuration Manager, AD360, Endpoint Central)

Product mapping

MANAGEENGINE SOLUTIONS	ESSENTIAL 8 MITIGATION STRATEGIES							
	Application Control	Patching Applications	Restrict Microsoft Office macros	User Application Hardening	Restrict Administrative Privileges	Patching Operating Systems	Multifactor Authentication	Regular Backups
Endpoint Central with Security Addons	✓	✓	✓	✓		✓		✓
Log360	✓	✓		✓	✓		✓	
AD360					✓		✓	✓
PAM360	✓				✓		✓	
Network Configuration Manager						✓		✓
Strategies Vs. Solutions								

Strategies vs. Solutions mapping.



We have a team of cybersecurity experts who have hands-on experience working with customers in Australia. With all the processes mapped out in the Essential Eight, we provide a suite of solutions that can help organisations implement the Essential Eight Maturity Model seamlessly.

To learn more, write to us at **tech-au@manageengine.com.**

Take control of your IT.

Monitor, manage, and secure your digital enterprise with ManageEngine.

Manage digital identities and access

Manage, govern, and secure digital identities across your organization with identity orchestration, privileged access security, CIEM, MFA, SSO, role-based access controls, and more.

manageengine.com/iam

Deliver smart service experiences

Enhance your service delivery workflows through industry-recommended ITSM best practices, powerful orchestration, and native AI capabilities.

manageengine.com/usm

Control and secure every endpoint

Manage, secure, and control all your endpoints across diverse functions like end-user computing, cybersecurity, governance, risk and compliance, I/O, and more.

manageengine.com/uems

Optimize network and IT opera

Achieve visibility across your network and application stack with AI-driven observabilit Proactively resolve issues, optimise performance, and enhance IT securit

manageengine.com/itom

Enhance IT security and compliance

Detect, investigate, and respond to security threats with UEBA, threat intelligence, and log monitoring. Be compliant with standards and mitigate risks with audit-ready reports.

manageengine.com/siem

Unified insights into all of IT

Visualise every facet of IT effortlessly. decision intelligence, preemptively identify and tackle risks, and gain practical contextual strategies for operational bottlenecks

manageengine.com/ita

Enhance IT with low-code apps

Extend the capabilities of your IT process by combining low-code and GenAI. Rapidly address IT challenges and innovate with minimal coding, making your organization more agile.

manageengine.com/lowcode

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

ManageEngine

For more information:

www.manageengine.com

aus-sales@manageengine.com

ManageEngine