



ManageEngine Mobile Device Manager Plus

Manage and secure devices, apps and data
from a unified console.



Table of Contents

Introduction	3
Company Overview	3
Product Introduction	5
Benefits	7
Associated Services	9
Product Features	10
Data Protection	14
Information Assurance	14
Data Backup, Data Restoration and Disaster Recovery	15
Business continuity statement/plan	15
Using the service	16
Ordering and Invoicing	16
Pricing Overview	16
Availability of Trial Service	17
On-Boarding, Off-Boarding, Service Migration, Scope, etc.	17
Training	17
Implementation Plan	18
Service Management	18
Service Constraints	18
Service Levels	19
Provision of the service	19
Customer Responsibilities	19
Technical Requirements and Client-Side Requirements	20
After-sales Account Management	20
Termination Process	21
Social Value	21
Our experience	27
Testimonials	27



Introduction

Company Overview

History: Formerly known as AdventNet Inc., Zoho Corporation started its operations in 1996 delivering web-based network management tools for telecom service providers. In 2002, the company diversified into IT management solutions for small, medium, and large enterprises. In 2005 with cloud taking off the company forayed into business SaaS with the introduction of Zoho Writer. By 2009, as the product portfolio became vast and diverse, the company was rechristened Zoho Corporation, which now serves as the umbrella firm for four distinct divisions: ManageEngine, Zoho.com, Qntrl, and TrainerCentral.

About our Company: ManageEngine is the enterprise IT management division of Zoho Corporation. We offer comprehensive on-premises and cloud-native IT and security operations management solutions for global organisations and managed service providers. With a powerful, flexible, and AI-powered digital enterprise management platform, we help businesses get their work done from anywhere and everywhere better, safer, and faster.

Established and emerging enterprises organisations-rely on ManageEngine's real-time IT management tools to ensure the optimal performance of their IT infrastructure, including networks, servers, applications, endpoints and more. ManageEngine has 18 data centres, 20 offices and 200+ channel partners worldwide to help organisations tightly align their business to IT.

ManageEngine's solutions include tools for Identity and Access Management, Enterprise Service Management, Endpoint Management and Security, IT Operations Management, Security Information and Event Management, Advanced IT Analytics, and Low-code app development.

Our Global Market: ManageEngine's solutions are industry-agnostic, designed to support organisations of all sizes across diverse sectors. In the UK, our customer base spans a wide range of industries, with strong adoption across BFSI, Healthcare, Government and Public Sector, Manufacturing, Education, IT & Technology, and

Hospitality, among others. This broad presence reflects the flexibility and scalability of our portfolio in addressing varied IT management and security needs.

Our Values & Goals

Simplicity without compromise

We aim to simplify IT management without sacrificing functionality. Our solutions are designed to be intuitive, easy to deploy, and straightforward to manage eliminating unnecessary complexity and reliance on third-party services.

Customer-led innovation

Customer needs drive our product strategy. Backed by a strong in-house R&D team, we continuously develop solutions that address real-world IT challenges, guided by direct feedback and hands-on usage.

Transparency and long-term value

We follow a transparent pricing model with no hidden costs. Our solutions are built to scale with organisations of all sizes, ensuring sustained value as business requirements evolve.

Empowering business-aligned IT

We focus on enabling strong alignment between IT and business objectives through continuous innovation, contextual integrations, and forward-looking solutions that support long-term growth.

Product Introduction

What it does

Mobile Device Manager Plus is a comprehensive mobile device management solution offered by ManageEngine. With this service, you can manage and secure various devices, applications, and data from a unified console. Our solution is designed to empower your enterprise workforce with the power of mobility, enhancing employee productivity without compromising on corporate security. You can manage smartphones, tablets, laptops, desktops, TVs, and rugged devices running on different operating systems such as Android, iOS, iPadOS, tvOS, macOS, Windows, and ChromeOS. With ManageEngine Mobile Device Manager Plus, you can streamline device management, enforce security policies, distribute applications, and remotely troubleshoot devices, all from a single platform.

Today, almost every organisation uses mobile devices for their day-to-day tasks. However, this widespread use of mobile devices poses a formidable challenge for these organisations. Government agencies, in particular, often grapple with the complexities of securing and coordinating a diverse array of mobile devices, leading to potential vulnerabilities in data security and operational inefficiencies. To ensure that these devices and the data on them remain safe, organisations rely on mobile device management or MDM. ManageEngine Mobile Device Manager Plus is a web-based enterprise mobility management solution that helps you manage and secure mobile devices across Apple OSs, Android, Windows, and ChromeOS from a central console. Available both in the cloud and on-premises, it automates the complete device management life cycle from enrolling devices and configuring them to be work-ready to managing device apps and content. With added features like workspace containerisation, location tracking, remote troubleshooting, lost device management, device lockdown, and automated report generation, it enables IT teams to boost productivity and enhance the device user experience through secure, compliant mobile endpoints.

Who might benefit

Executive & Leadership Stakeholders

- CIO – Chief Information Officer: Responsible for overall IT strategy, technology investments, and ensuring secure, efficient operations.
- CISO – Chief Information Security Officer: Prioritizes threat mitigation, incident response, and maintaining a strong cyber-resilience posture.

IT Operations & Endpoint Management Teams

- IT Manager / IT Operations Manager: Drives endpoint standardisation, device lifecycle management, and workflow automation.
- Endpoint Management Lead / UEM Lead: Deeply involved in device enrollment, OS updates, compliance, imaging, and policy enforcement.
- Desktop Engineers / EUC Engineers: Manage end-user devices, application provisioning, and device configuration at scale.
- Workplace / Digital Experience (DEX) Teams: Focus on improving user productivity, device performance, and employee digital experiences. Executive & Leadership Stakeholders

Security Operations & Cybersecurity Teams

- Cybersecurity Engineers: Oversee threat prevention, hardening, attack surface reduction, and endpoint defense policies.

Compliance, Governance & Risk Teams

- IT Compliance Officers / GRC Teams: Require consistent policy enforcement, audit logs, asset visibility, and configuration compliance.
- Data Protection Officers (DPOs): Concerned with safeguarding personal data and ensuring the organisation complies with privacy rules.

Support & Helpdesk Teams

- Helpdesk Managers & Technicians (L1–L3): Benefit from remote control, device diagnostics, automated scripts, and rapid issue resolution.

Benefits

1. Remote device management for smartphones, tablets, laptops, desktops, and TVs

Modern mobile fleets are rarely in one location. Devices roam between offices, homes, field sites, and networks, creating massive gaps in oversight. Unified MDM control closes these gaps by giving IT real-time visibility and enforcement across every mobile endpoint, regardless of where it is. This reduces unmanaged devices, strengthens security posture, and ensures mobile fleets remain compliant even in highly distributed environments.

2. Zero-touch onboarding for rapid mobile device deployment

Manually staging mobile devices is slow, inconsistent, and unscalable for growing mobile workforces. Zero-touch enrolment transforms provisioning by allowing devices to auto-configure the moment users turn them on. This accelerates rollout during mass deployments (new stores, field teams, remote onboarding) and ensures every device enters the MDM ecosystem securely from day one.

3. Preconfigured MDM policies for out-of-box readiness

Mobile users expect to be productive instantly, but IT delays often stem from configuring policies, restrictions, Wi-Fi, VPN, certificates, and apps. Out-of-box MDM configuration ensures every device starts fully secured and work-ready. This standardises the mobile experience across departments and dramatically reduces onboarding friction and IT backlog.

4. Automated configuration, app, and content distribution through MDM

Mobile ecosystems change constantly. Apps update, policies evolve, networks shift, and teams move between roles. Relying on users to self-configure leads to drift and non-compliance. MDM-driven automation ensures every mobile device continuously receives the right apps, settings, and content without user action, maintaining policy consistency and dramatically lowering operational noise.

5. Block malicious mobile apps and risky web content

On mobile platforms, threats often originate from unvetted app installs, sideloaded APKs, or unsafe browsing on public networks. MDM enforcement blocks harmful mobile

apps, phishing sites and malicious URLs, reducing the organisation's exposure to mobile-based attacks. This proactive control dramatically lowers incident frequency and keeps mobile devices compliant with corporate security baselines.

6. Over-the-air mobile app and firmware update delivery

Mobile endpoints can't be brought into IT offices for updates, meaning unpatched phones and tablets accumulate vulnerabilities fast. OTA updates ensure every mobile device receives critical upgrades instantly with no cables, no depot visits and no downtime. This leads to smoother app performance, higher device stability, and safer mobile operations.

7. Automated OS and app patching for mobile devices

Unpatched mobile OS and apps are prime targets for exploits, especially in Android and iOS ecosystems where vulnerabilities spread rapidly. Automated MDM patching ensures devices receive tested, approved updates on schedule, reducing security risk and maintaining compliance with regulatory frameworks that require timely mobile patching.

8. Remote troubleshooting for mobile endpoints

Field teams, frontline workers, and remote staff often experience mobile issues that IT cannot physically access in time. MDM-powered remote troubleshooting allows IT to view screens, capture logs, and fix problems instantly. This reduces device downtime, increases productivity for remote workers and eliminates costly in-person support.

9. Conditional access tied to mobile device compliance

Unmanaged or non-compliant mobile devices often become entry points for attackers seeking email, apps, or internal systems. MDM-enforced conditional access ensures only trusted, encrypted, policy-compliant mobile devices can access corporate apps and data. This protects cloud workloads, email and business apps from unauthorised mobile access and strengthens zero-trust posture.

10. Mobile containerisation & DLP for corporate data

BYOD introduces risk because personal devices mix corporate files with personal apps and storage. Mobile containerisation isolates corporate data in a secure workspace with strict DLP rules, preventing copy/paste, screenshots, sharing, or backups to consumer apps. This ensures sensitive data stays protected on every mobile device without

invading user privacy or restricting personal use.

Associated Services

ManageEngine Mobile Device Manager Plus offers a range of associated services that can be bought or are available alongside the main service. These include:

- **Device onboarding:** ManageEngine Mobile Device Manager Plus provides APIs that allow for integration with other systems and applications, enabling seamless data exchange and automation.
- **Professional Services:** ManageEngine offers professional services to assist with the implementation, customisation, and optimisation of ManageEngine Mobile Device Manager Plus. Our team of experts can provide guidance and support to ensure a smooth deployment and maximise the value of the service.
- **Maintenance and Support:** We provide ongoing maintenance and support services to ensure the smooth operation of the ManageEngine Mobile Device Manager Plus. This includes regular updates, bug fixes, and technical assistance to address any issues or concerns.
- **Video Tutorials:** ManageEngine Mobile Device Manager Plus also maintains a repository of video tutorials and conducts live webinars with our product experts throughout the year for every module and function at <https://www.manageengine.com/mobile-device-management/training.html>
- **Workshops and User Conferences:** ManageEngine Mobile Device Manager Plus conducts workshops where users are given a deep-dive on the product based on business challenges and use-cases along with an opportunity to avail a product associate certification.
- **Product customisations and feature requests:** ManageEngine Mobile Device Manager Plus is open to facilitate any customer use-case or feature after careful internal vetting.
- **Online Documentation:** ManageEngine Mobile Device Manager Plus provides in-depth help documentation that is hosted online at <https://www.manageengine.com/mobile-device-management/help/>, which provides step by step guidance for administrators, technicians, and end-users.

These associated services enhance the functionality and value of ManageEngine Mobile Device Manager Plus, providing a comprehensive solution for mobile device management.

Product Features



Figure 1 Feature highlights

1. Mobile device management for enterprises

Enterprise mobile device management provides a centralised system through which IT teams can enrol, configure, secure, and monitor every smartphone, tablet, or laptop used in the organisation. Instead of treating devices as scattered, individual endpoints, MDM consolidates everything into a single, consistently governed fleet. This approach allows IT administrators to push policies, enforce restrictions, deploy apps, and maintain security from anywhere, creating a unified operational structure. It is particularly valuable for distributed or hybrid workforces where devices rarely come back to the office. The result is stronger oversight, reduced administrative effort, and a fully managed mobile ecosystem that remains compliant and secure regardless of scale.

2. Mobile security baselining through granular configuration profiles

Security baselining establishes the minimum security standards that every mobile device must adhere to before it is considered safe for corporate use. Through configuration profiles, IT teams can dictate the exact password rules, encryption settings, connectivity

configurations, and usage restrictions that must be applied. These profiles ensure that each enrolled device enters the ecosystem with built-in protections such as enforced passcodes, secure Wi-Fi settings, pre-installed certificates, and disabled risky features. This level of granular control helps organisations maintain consistent compliance across all devices, especially in regulated environments, and greatly reduces the attack surface that typically arises when users configure devices on their own.

3. Silent app installation and automated app update management

Silent installation ensures that corporate apps are delivered directly to devices without requiring the user to initiate, approve, or interact with the installation process. This eliminates delays and ensures that every employee receives the correct set of tools the moment they need them. Automated update management extends this by ensuring that apps stay current and secure without manual intervention. Devices always run the approved versions that IT has vetted, which prevents issues caused by outdated software. This approach benefits large mobile workforces that rely heavily on business-critical apps, as it keeps everyone aligned, reduces compatibility problems, and significantly lightens the burden on users and support teams.

4. Single- and multi-app mode and shared device configurations

Single-app and multi-app modes convert devices into controlled, purpose-built tools by restricting what users can access. For example, a tablet can be locked into a single POS app for frontline retail, or into a curated set of apps suited for a delivery agent or warehouse associate. Shared device configurations further enable scenarios where multiple users share the same device but receive personalised workspaces with their own apps and settings. These capabilities transform general-purpose devices into reliable, tightly controlled work instruments that minimise misuse, reduce distractions, and ensure consistent user experiences in environments such as retail, healthcare, education, logistics, and field service.

5. Mobile asset and inventory management for easier auditing

MDM automatically captures detailed information about each device, such as hardware specifications, installed apps, OS versions, security status, and ownership. This creates a real-time inventory that replaces manual asset tracking and gives auditors a precise, always-updated picture of the organisation's mobile deployment. IT teams can instantly identify outdated devices, spot potential compliance gaps, track device lifecycle stages, and review app usage trends. This level of visibility is essential for organisations that need

accurate audit trails, predictable refresh cycles, and a clear, consolidated understanding of how mobile assets are being used across the business.

6. BYOD and COPE device management with containerization capabilities

Managing personal and hybrid-use devices requires a balance between corporate security and user privacy. Containerisation solves this by creating a dedicated, encrypted workspace on the device where all corporate apps and data reside. IT can fully control this workspace-enforcing policies, restricting data movement, and performing selective wipes-while leaving the user's personal content untouched. This setup works seamlessly for both BYOD and COPE scenarios, allowing organisations to embrace flexible device models without compromising data protection. It gives employees freedom to use personal devices while reassuring them that their private photos, messages, and apps remain beyond the reach of corporate management.

7. Secure remote troubleshooting to resolve technical issues

Remote troubleshooting tools allow IT teams to view the device screen, replicate issues, capture logs, and resolve problems as if they were physically present with the device. This capability dramatically reduces downtime for mobile employees who depend on their devices in the field. Support teams can diagnose issues faster, avoid unnecessary device returns, and provide real-time guidance to users who may be struggling with configuration or performance problems. Whether a delivery driver is facing an app crash or a retail staff member's device is stuck in kiosk mode, remote troubleshooting ensures that issues are resolved promptly and efficiently.

8. Device location tracking and geofencing to secure data

Location tracking enables IT teams to see where corporate devices are at any given moment, which is crucial for field operations, logistics, and security-conscious workplaces. Geofencing builds on this by allowing IT to define virtual boundaries and trigger automatic actions when devices move in or out of those areas. For example, a device leaving a secure facility can automatically lock itself, or a notification can alert IT to investigate potential loss or misuse. These capabilities enhance both operational visibility and data protection, particularly for companies that rely on mobile devices outside traditional office environments.

9. Secure access to sensitive data with conditional access

Conditional access ensures that only devices meeting defined security requirements can access corporate resources such as email, cloud apps, or internal systems. This means that unmanaged, rooted, jailbroken, or non-compliant devices are blocked before they can interact with sensitive data. By enforcing this gatekeeping model, the organisation reduces the risk of data breaches caused by untrusted devices. It supports a zero-trust security philosophy where access is granted based on device health and trustworthiness rather than location or network perimeter.

10. Automated OS update and patch management services for improved security

Keeping mobile OS versions and security patches up to date is critical, yet difficult when devices are dispersed. Automated OS update management allows IT to schedule and enforce updates while also delaying them when testing is required. This ensures that devices remain protected against emerging threats without disrupting user workflows. Automatic patching closes vulnerabilities quickly, supports compliance obligations, and prevents the buildup of outdated devices that could expose the organisation to unnecessary risk. It creates a stable, predictable mobile operating environment where security and usability remain in balance.

Data Protection

Information Assurance

ManageEngine adheres to industry-leading security standards and has implemented robust security measures to protect sensitive information. ManageEngine follows best practices and complies with relevant policies and standards. ManageEngine has a strong commitment to information security and employs processes and facilities to safely manage data. The service prioritises data protection, confidentiality, and integrity, ensuring that organisations can trust their identity management processes. By implementing ManageEngine solution, organisations can have confidence in the security of their identity-related information and mitigate the risk of unauthorised access or data breaches.

As part of the development team's training, they are briefed about the various networking protocols that are used in the product and are encouraged to use only secure communication protocols such as HTTPS and TLS in their code.

- To ensure access to critical information by the development team, measures such as strong passwords, controlled access to test machines, and network segmentation are implemented.
- All the data collected through online forms has a field to obtain consent for collecting and processing data from the prospect.
- Marketing team members are strictly asked to check if a prospect has given consent to receive marketing communications before sending marketing emails.
- Support and pre-sales engineers who communicate directly with customers are trained to maintain privacy of customer information.
- Dedicated guidelines on handling customer data has been given to the members of the team in light of regulations such as GDPR.
- The customer data is stored in databases that can be accessed only by authorised employees.

Data Backup, Data Restoration and Disaster Recovery

ManageEngine runs incremental backups everyday and weekly full backups of our databases using Zoho Admin Console (ZAC) for ManageEngine's Data Centres (DC). Backup data in the DC is stored in the same location and encrypted using AES-256 bit algorithm. We store them in tar.gz format. All backed up data are retained for a period of three months. If a customer requests for data recovery within the retention period, we will restore their data and provide secure access to it. The timeline for data restoration depends on the size of the data and the complexity involved.

To ensure the safety of the backed-up data, we use a redundant array of independent disks (RAID) in the backup servers. All backups are scheduled and tracked regularly. In case of a failure, a re-run is initiated and is fixed immediately. The integrity and validation checks of the full backups are done automatically by the ZAC tool.

From your end, we strongly recommend scheduling regular backups of your data by exporting them from the respective Zoho services and storing it locally in your infrastructure.

Business continuity statement/plan

Application data is stored on resilient storage that is replicated across data centres. Data in the primary DC is replicated in the secondary in near real time. In case of failure of the primary DC, the secondary DC takes over and the operations are carried on smoothly with minimal or no loss of time. Both the centres are equipped with multiple ISPs. We have power back-up, temperature control systems, and fire-prevention systems as physical measures to ensure business continuity. These measures help us achieve resilience.

In addition to the redundancy of data, we have a business continuity plan for our major operations, such as support and infrastructure management.

Privacy by Design

Every change and new feature is governed by a change management policy to ensure all application changes are authorised before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our code analyser tools, vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, cross site scripting and application layer DOS attacks.

Our privacy commitment: Zoho has never sold your information to someone else for advertising, or made money by showing you other people's ads, and we never will. This has been our approach for almost 25 years, and we remain committed to it. This policy tells you what information we collect from you, what we do with it, who can access it, and what you can do about it.

More information on our privacy policy can be found at <https://www.manageengine.com/privacy.html>

Using the service

Ordering and Invoicing

Paid subscription can be availed from ManageEngine by contacting our team to discuss your requirements in detail. They will guide you through the ordering process and provide any necessary assistance in completing the Order Form (Call-off contract). We accept payment via Visa, MasterCard, American Express, and PayPal. We also accept payment via bank transfer or cheque transfer for yearly subscriptions. We strive to make the ordering and invoicing process as smooth as possible, ensuring that you have a clear understanding of the fees and payment terms.

Pricing Overview

Pricing is based on endpoint count and number of technicians. Refer Pricing document for more details.

Availability of Trial Service

We offer an all-inclusive, free, 30-day trial for all users. Once the trial period has lapsed, the product with all of its features will be free for up to 25 devices. Users can sign up from [here](#).

On-Boarding, Off-Boarding, Service Migration, Scope, etc.

During the on-boarding process, we provide comprehensive documentation that guides users through the setup and configuration of ManageEngine Mobile Device Manager Plus. This documentation includes step-by-step instructions and troubleshooting tips.

When users decide to stop using our service, we have an off-boarding process in place to ensure a smooth transition out of ManageEngine Mobile Device Manager Plus. We understand that circumstances may change, and we aim to make the off-boarding process as hassle-free as possible. Our dedicated point of contact will work closely with the user to understand their reasons for discontinuing the service and provide any necessary assistance.

We also provide a migration tool that helps users migrate from other services to ManageEngine Mobile Device Manager Plus.

Training

We offer training sessions to familiarise users with the features and functionalities of our service. These training sessions can be conducted remotely or on-site, depending on the user's preference and requirements.

Onsite Training: Whether it's training for a few employees, a team, or your entire organisation, we offer convenient and affordable training at a location of your choice. This option is cost-effective when you have multiple individuals in need of training. You pay one flat training fee along with logistics expenses to receive two to five days of onsite, hands-on instruction.

Online Training: If you prefer to learn at your own pace, we provide a paid online option offering comprehensive training from experts- all from the convenience of your office

or home. All you need is an internet connection, and the training will be delivered over the web. Reduce your travel expenses with online training.

Implementation Plan

Options for Implementation

- Requirement discussion
- Allocating time and required resources
- Assessment of the organisation's existing identity management, directories, applications, etc.
- Formulating an implementation plan with timelines and prerequisites
- The signup process to perform the initial configuration and integrations.
- Conducting tests based on various use cases.
- Extending the implementation to other groups in the production environment.
- Post-implementation monitoring.

Service Management

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. Likewise, we track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence in the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

Service Constraints

ManageEngine Mobile Device Manager Plus does not have any specific service constraints. The service is designed to provide high performance, availability, and support. There are no limitations on customisation, allowing users to tailor the service to their specific needs. Maintenance windows are scheduled in a way that minimises disruption to users, and any deprecation of functionality/features is communicated well in advance to ensure a smooth transition.

Service Levels

ManageEngine Mobile Device Manager Plus offers robust service levels to ensure optimal performance, availability, and support for our customers. Our goal is to provide a reliable and responsive service that meets the specific needs of our customers while ensuring compliance with industry standards and best practices.

The following workflow is adopted in handling customer requests:

- Questions received from customers through live chat and web-forms will be created as tickets in Zoho Desk.
- The tickets will be assigned manually by agents or admin users.
- Customers will be provided with a valid first response via email/phone call within the defined SLA.
- The ticket is processed further based on the customer's response.
- Based on the ticket category, the ticket is assisted at various levels.
- Upon providing a resolution and receiving the customer's confirmation for the same, the ticket will be closed.

Provision of the service

Customer Responsibilities

- Choose a unique, strong password and protect your login information. Use multi-factor authentication.
- Use the latest browser versions, mobile OS, and updated mobile applications to ensure they are patched against vulnerabilities and to use latest security features. Exercise reasonable precautions while sharing data from our cloud environment.
- Classify your information into personal or sensitive and label them accordingly.
- Monitor devices linked to your account, active web sessions, and third-party access to spot anomalies in activities on your account and manage roles and privileges to your account.
- Be aware of phishing and malware threats by looking out for unfamiliar emails,

websites, and links that may exploit your sensitive information by impersonating Zoho or other services you trust.

Technical Requirements and Client-Side Requirements

Being a cloud solution, ManageEngine Mobile Device Manager Plus has no specific technical requirements or client-side requirements that users should be aware of.

ManageEngine Mobile Device Manager Plus is compatible with major browsers such as Google Chrome, Microsoft Edge, and Mozilla Firefox. It can be accessed from desktops, laptops, or mobile phones.

After-sales Account Management

We offer customer support via email and chat to address queries, troubleshoot issues, and provide guidance.

- We keep customers informed about the latest product updates, enhancements, changes/planned downtime, and new features.
- We manage license renewals and communicate with customers regarding upcoming renewals.
- We provide information about licensing options, upgrades, and any relevant promotions or discounts.
- We gather customer feedback to understand their satisfaction with ManageEngine products, using surveys and feedback mechanisms to identify areas for improvement and address customer concerns.
- We provide customers with information about complementary products that could enhance their IT management capabilities.
- We maintain regular communication with customers through newsletters, announcements, and product updates, ensuring that customers are informed about relevant events, workshops, webinars, and training sessions.
- We conduct periodic account reviews to assess customers' usage of ManageEngine products, discussing any challenges or opportunities for improvement and providing recommendations accordingly via health checks.
- We also implement customer success programs to proactively engage with

customers, ensuring they achieve their goals with ManageEngine solutions and providing best practices, use cases, and success stories to inspire effective utilisation of the products.

Termination Process

You have the right to terminate your user account for convenience or if Zoho Corporation Limited breaches its obligations under our Terms and in such event, you will be refunded the subscription fee for the unused portion of the subscription period. Termination of user account will include denial of access to all Services, deletion of information in your user account such as your e-mail address and password and deletion of all data in your user account in accordance with our deletion cycle.

Social Value

Fighting Climate Change

ManageEngine and its parent company Zoho Corp have committed to working towards achieving Net-zero by 2050. Some initiatives for this:

- **Green data centres:** We've partnered with Equinix to host our UK data centres in London and Manchester. Equinix is also committed to sustainability and is compliant with the Climate Neutral Data Centre Pact, ISO 14001, LEED, etc.
 - **Energy initiatives at Zoho UK's workspace at Bletchley** - The energy supply for the UK office is derived from renewable sources, accounting for 21% of total power consumption. LED retrofits have been implemented to enhance energy efficiency throughout the building.
 - **Renewable energy:** We've built a 5 megawatt on-grid solar energy farm at Abinimangalam near Trichy, India. This farm offsets the electricity consumption of our Chennai headquarters and data centre. Designed with a focus on energy efficiency, data centres that support Zoho UK are powered by renewable energy.
 - Further, these data centres are progressing towards integrating with a solar grid to reduce environmental impacts.
 - **Green Energy Procurement** - All purchased energy for the data centres is sourced from green energy providers. This enables us to minimise the carbon footprint associated with our operations.
-

- Emissions - The United Kingdom has committed to achieving carbon neutrality by 2050. Supporting this pledge, we have taken steps to monitor greenhouse gas (GHG) emissions from our operations and implement measures to mitigate them. We account for Scope 2 and Scope 3 emissions and exclude Scope 1 emissions as our work does not involve fuel combustion within operational boundaries.

Globally, emissions need to be cut down by 45% by 2030, in order to achieve net-zero by 2050. 60% of fossil fuels (coal, oil, and gas reserves) need to be replaced by efficient energy sources to achieve net-zero.

- E-mobility: We've switched completely to electric vehicles for movement within the campus.
- Energy efficient operations: We use IoT to measure and optimise energy consumption across our offices. We've also implemented LED lighting, energy-efficient equipment, and IoT based energy management to reduce our energy consumption and greenhouse gas emissions.
- Recycling and waste reduction: All the waste generated on campus is segregated at source. Food waste is processed in our own biogas plant, which generates the electricity used to run the plant. All other waste is sent to the recycling vendors for recycling it.
- Minimising water usage: We use an in-house sewage treatment plant to treat wastewater for reuse for flushing, gardening and cooling tanks. We've also implemented IoT sensors to detect water leakage, rain-detecting sprinklers systems, and smart water management, to monitor and reduce our water usage and wastage.
- Sustainable procurement: We encourage sourcing materials from suppliers who have environment friendly practices. We also recycle obsolete gadgets by sending them to an e-waste recycling unit.
- Reduced paper use: We've reduced paper use at work. Most our documents are now digitally maintained, reducing our print-related environment impact.
- Reducing business travel: We've reduced our business travel. Many Events and meetings are conducted online using our in-house meeting tools.

COVID-19 Recovery

- During the COVID-19 pandemic, ManageEngine and its parent company Zoho Corp. worked to minimise the impact of COVID on our customers, other business, and our local community.
- Supporting remote work: At the start of the pandemic, ManageEngine and its parent company Zoho Corp. created and distributed a Secure Remote Access Toolkit to help organisations quickly adapt to and work securely during the pandemic. This toolkit was made free for the first 100 days.
- Discounts and waivers: To assist organisations impacted by the pandemic, ManageEngine and its parent company Zoho Corp offered free licenses of flagship products and offered discounts and waivers on licenses on a case-by-case basis.
- Food to the underprivileged: While most of our employees worked from home, we kept the kitchen at our Chennai headquarters running with a skeletal staff to provide food to underprivileged people in the local area, many of whom were impacted due to a loss of employment during the lockdown.
- Infrastructure support: We converted one of our office buildings into a temporary COVID-19 ward to accommodate citizens who were required to quarantine.
- We ran Covid vaccination camps for our employees. their dependents and the support staff who worked in Zoho.
- ManageEngine Site24x7 introduced the Small Business Emergency Subscription Assistance Program (ESAP) during Covid-19. ESAP gives our small business customers a chance to use Site24x7 and other Zoho products free for three months.

Tackling Economic Inequality

ManageEngine and its parent company Zoho Corp. has always aimed to tackle economic inequality and give back to the community. This is reflected in the following:

- Transnational localism: Coined by our CEO, transnational localism is the philosophy that underpins our staffing and office location plans. Instead of focusing on crowded urban centres, we've been opening spoke offices in smaller towns and villages. The goal is to improve local infrastructure, boost the economy of these smaller towns and villages, and provide more employment opportunity.
- Local hiring: As part of our philosophy of transnational localism, we believe in hiring locally for each spoke office. This helps promote local talent and bring high-paying

jobs back to the villages and towns where we are based.

- **Zoho Schools of Learning:** Started in 2004, Zoho Schools of Learning (formerly Zoho University) provides training and employment for high school students and those holding or pursuing diplomas. Those inducted into Zoho Schools are trained by industry experts in the fields of their choice - technology, business, or design. The students are also trained in social skills. The course is completely free, and students are paid a monthly stipend throughout its duration. Graduates from this program are automatically inducted into Zoho Corp.

Equal Opportunity

- As part of our efforts to tackle inequality, ManageEngine and its parent company Zoho Corp. have made efforts to provide equal opportunities and tackle workforce inequality.
- **Helping women restart their careers:** Zoho Schools of Learning has begun a program called Marupadi. Aimed at helping women restart their tech careers after a break, Marupadi is a 3-month program comprising a mix of lectures, experiential learning and internships. At the end of the program, the candidates who've successfully completed training get to sit for exclusive face-to-face interviews for jobs at Zoho Corp.
- **Diversity and inclusion in hiring:** All roles at ManageEngine and its parent company Zoho Corp. are open to all people irrespective of gender, sex, race, ability, or religion. We hire solely based on skill and have a diverse team.
- We eschew discrimination on any grounds, including age, colour, disability, ethnicity, family or marital status, gender identity or expression, language, national origin, physical and mental ability, political affiliation, race, religion, sexual orientation, socio-economic status, and other unique characteristics that define our associates. Instead, we espouse fairness, striving to ensure that a merit-based approach allows wage parity among associates with comparable experiences and responsibilities, irrespective of their gender.
- **Accessible campus:** Our campus has been designed to be accessible to all, including differently abled colleagues. The layout design includes ramps and lifts in every building, allowing ease of mobility and access to all.
- **On-campus crèche and day care:** We support new parents within the organisation by providing them with on-campus crèche, day-care and play school.
- Apart from the usual shuttle facilities, special cab service covering a certain distance

is given for women during their third trimester.

Wellbeing

ManageEngine and its parent company Zoho Corp. in UK adheres to industry standards in remuneration, ensuring that compensation is equitable across genders.

Recognising the diverse needs of our people, we provide essential support such as parental leave, aligning with our efforts to build an organisation that values and cares for every individual.

- Free on-campus medical services: We have trained medical practitioners and a dedicated medical clinic available on all days of the week. Employees can freely avail their services for any medical requirements. The cost of consultation is borne completely by the company. This is for all employees based out of India.
- Hazard Management Framework: The Hazard Identification & Risk Assessment (HIRA) Framework is followed rigorously at the premises. Under this, regular assessments are conducted to identify workplace hazards and evaluate social risks.
- In-house mental health counselling: We provide in-house counselling to our employees for free via our team of trained and qualified therapists.
- Free medical camps: We organise free medical check-ups for our employees on an annual basis.
- Blood donation camps: We organise regular blood donation camps in association with various blood banks.
- We have open house sessions conducted by the CEO periodically where employees can raise any concerns. Team level open house sessions (from operations teams) are done every week.
- Day Care facilities provided for employees' children.
- Continuous Improvement: The compliance monitoring framework involves ongoing reviews and enhancements of occupational health programs, guided by feedback, data analysis, and emerging best practices. We foster a culture of continuous improvement, encouraging employee engagement, and incorporating insights from incidents or near misses.

Employee Engagement

With respect to employee engagement, we prioritise transparent communication and foster a supportive work environment. Our talent acquisition process emphasises diversity and inclusion with the aim of building a talent pool that offers the richness of diverse skills, experiences, and cultural perspectives.

The onboarding for new employees begins with the Security and Privacy Awareness (SPA) quiz. This short assessment ensures that our employees possess a basic understanding of our compliance regulations and ethical practices. Subsequently, they undergo a comprehensive departmental training spread over 3-4 weeks. This immersive program is designed to equip new joiners with the necessary understanding and skills to excel in their role. In addition, they can access learning resources through our Zoho Learn platform. This online portal houses a range of materials, including product tutorials, system guides, and best practices, enabling them to enhance knowledge and expertise.

Employee retention is an area of focus which we address by implementing programs tailored for professional development, mentorship, and work-life balance. In turn, these contribute to a dynamic, inclusive, and fulfilling work culture. Further, we make sure to communicate career growth opportunities, enabling employees to feel valued and motivated. By emphasising continuous progress and adapting to evolving employee needs, we work to build an organisation remains a place where talent flourishes over the long term.

Governance

ManageEngine and its parent company Zoho Corp.'s operations in the UK are underpinned by ethical governance, which require every employee to demonstrate integrity in business conduct, while also ensuring the company's compliance with legal and regulatory requirements. Business integrity is not only the foundation on which Zoho UK's reputation is being built, it also enhances our capacity to forge enduring stakeholder relationships that enable us to create shared value in the long term. The following section outlines our policy framework comprising the Code of Ethics, Modern-Slavery and Anti-Bribery Policies.

Policy Framework Code of Ethics

The Code of Ethics is a set of guidelines for ethical behaviour characterised by integrity, respect, and responsibility. It is applicable to all workforce of ManageEngine and its parent company Zoho Corp. in the UK, including employees, consultants, and interns.

The Code of Ethics emphasises the following for workplace and business conduct:

- **Fairness:** We foster a diverse and inclusive work environment, promoting equal opportunities for all, thereby embracing the values of Equality Act 2010.
- **Respect:** Harassment is eschewed, and a clear reporting mechanism has been put in place to register concerns.
- **Ethical Sourcing:** Zoho UK stands against forced labor, slavery, and human trafficking, and promotes ethical procurement practices.
- **Privacy:** Responsible handling of personal information, acknowledging resource limitations.

Our experience

Lessons learned and best practice recommendations

Testimonials

ManageEngine Mobile Device Manager Plus has a customer base of over 10,000 with a mix of SMBs, enterprises and government organisations across multiple verticals (education, healthcare, finance, IT, manufacturing, defence and more).

You can find the list of our customers [here](#).

Contact Details

Company Name: ManageEngine, a division of Zoho Corporation

Primary Contact: gcloud@manageengine.com

Address: Suite 1.09, Challenge House, Sherwood Dr, Bletchley, Milton Keynes MK3
6DPUK

Toll Free: 0800 028 6590

<https://www.manageengine.com/mobile-device-management/customers.html>



www.manageengine.com