ManageEngine

IT Management, Simplified

Real-time IT management solution for the new speed of business

ManageEngine

- Enterprise IT management software division of Zoho Corporation

- Founded in 1996 as AdventNet

- Privately held, Rock solid Supplier and Partner

- Headquartered in Pleasanton, California

- Millions of customers across industries

ManageEngine - the Enterprise IT Management division of ZOHO Corporation

(Est. 2005)

Work.Online

Applications for Business, Collaboration, and Productivity

(Est. 1996)

Privately held, profitable since inception

(Est. 2002)

ManageEngine

Enterprise IT Management Solutions

(Est. 1996)

WebNMS
A Division of ZOHO Corporation

Enterprise Internet of Things and Unified Network Management Solutions

ManageEngine **Solutions**
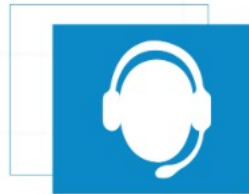
Active Directory Management

Active Directory
Exchange Server
Self-service Portal
Recovery and Backup

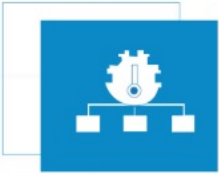## Endpoint Management

Desktop Management
Mobile Device Management
OS Deployment
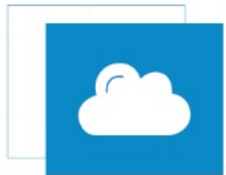Patch Management
Browser Management
Vulnerability Management

IT Service Management

Help Desk
Asset Lifecycle
CMDB and ITIL
Customer Support

IT Operations Management

Network Performance
Application Performance
End user Experience
Network Change and Configuration
Converged Infrastructure
Storage Infrastructure
Bandwidth and Traffic
SQL Server Monitoring

On Demand

Application Performance
Helpdesk Software
Active Directory Recovery and Backup
Mobile Device Management
Patch Management
Log Management

IT Security

Log Management
Firewall Analysis
Vulnerability Analysis
Privileged Password
Network Anomaly Detection

3 Million Users

9 of every **10** Fortune **100 companies** are ManageEngine customers

Standard Chartered

GE

BARCLAYS

L'ORÉAL

SAINT-GOBAIN

JPMorgan Chase & Co.

AT&T

Why Mobile Device Manager Plus MSP ?

Multi-tenant platform for MSPs

Isolated instances for each customer
White label the software with your organization logo

Support for all environments

Modern and legacy management across BYOD, COPE, CYOD, COSU etc

Simple, affordable and easy to use

Simplified user interface and an easy set-up that does not require costly consultants or a long time to get started

Automated device management

From onboarding of devices to distributing apps and applying corporate security policies

Comprehensive security for your mobile endpoints

Secure sensitive business data at rest, in use and in transit

Meet privacy and compliance standards
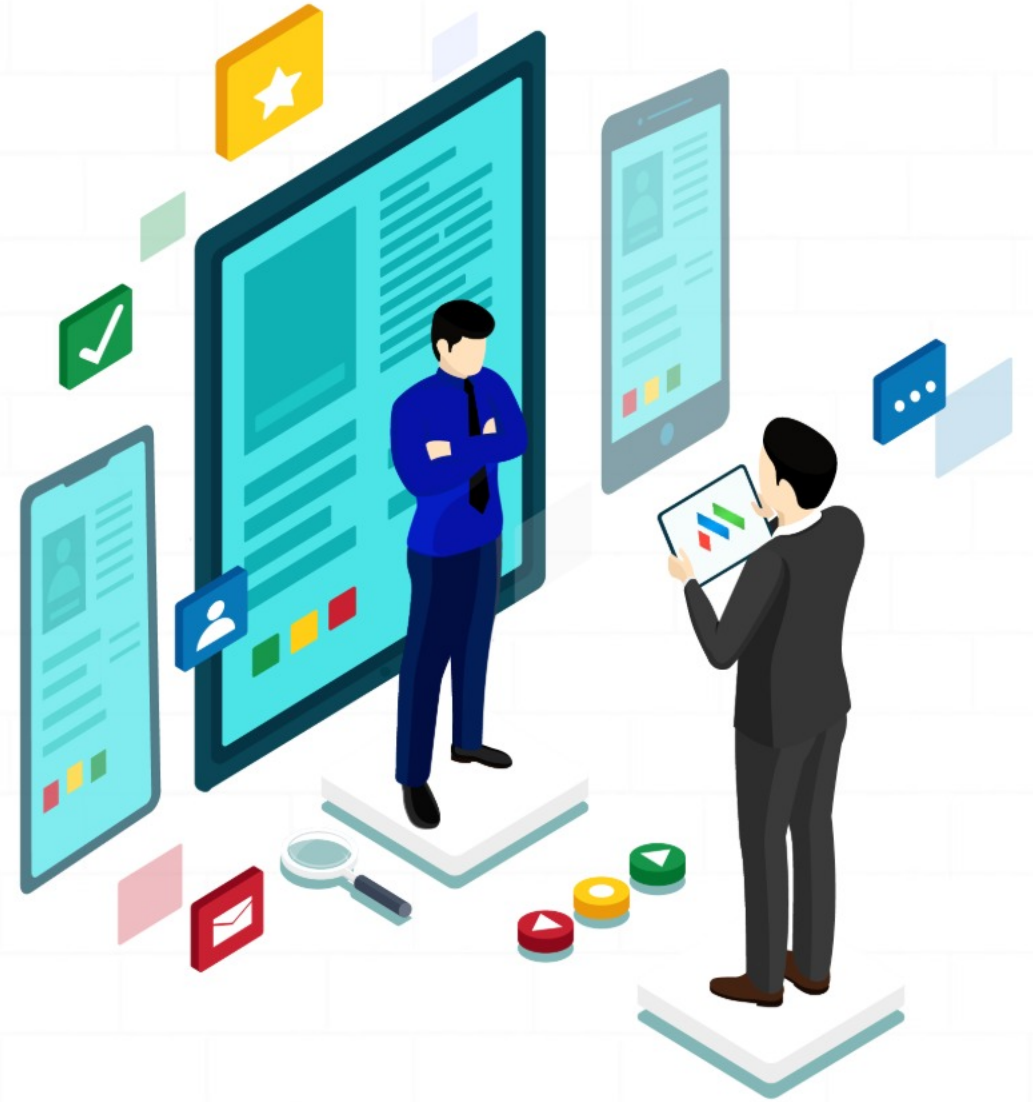From CJIS, PCI DSS and ISO to HIPAA and GDPR, ensure regulatory compliance with ease

One-stop shop for all your IT management needs

Seamless integration with solutions that have been built from the ground up

Supported OS

iOS

versions 4.0 and above

iPadOS

Version 13.0 and above

iPhone, iPad, iPod Touch

macOS

versions 10.7 and above

Laptops

tvOS

versions 7.0 and above

TVs

Chrome OS

versions 57.0 and above

Chromebooks

Windows

versions 8 and above

Smartphones, tablets & laptops (ver.10), Surface Hubs
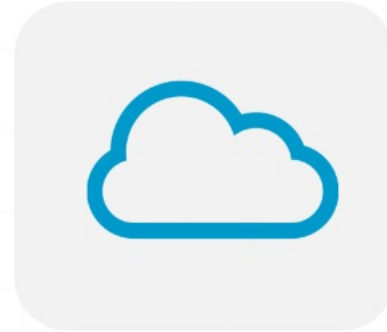
Android

versions 4.0 and above

Smartphones and tablets

Deployment Options

On-premises

Cloud

Feature Highlights

Email management

Content management

Application management

Containerization

Profile management

OS update management

Asset management

Mobile Device Management

Remote control

Device onboarding

Location History

Audit and reports

Geofencing

Security management

Device Onboarding

❖ **Automated Device Enrollment**

- Apple:
  - ➤ Apple Business Manager (ABM)
  - ➤ Apple Configurator
- Android Admin Enrollment
  - ➤ Zero-touch Enrollment
  - ➤ Samsung Knox Mobile Enrollment
  - ➤ EMM Token Enrollment
  - ➤ NFC Enrollment
- Windows ICD and Azure (Autopilot) Enrollment
- Chrome OS Enrollment

❖ **Enrollment by invite**

- Manual enrollment through QR code scanning
- Bulk Enrollment via CSV
- SMS Enrollment
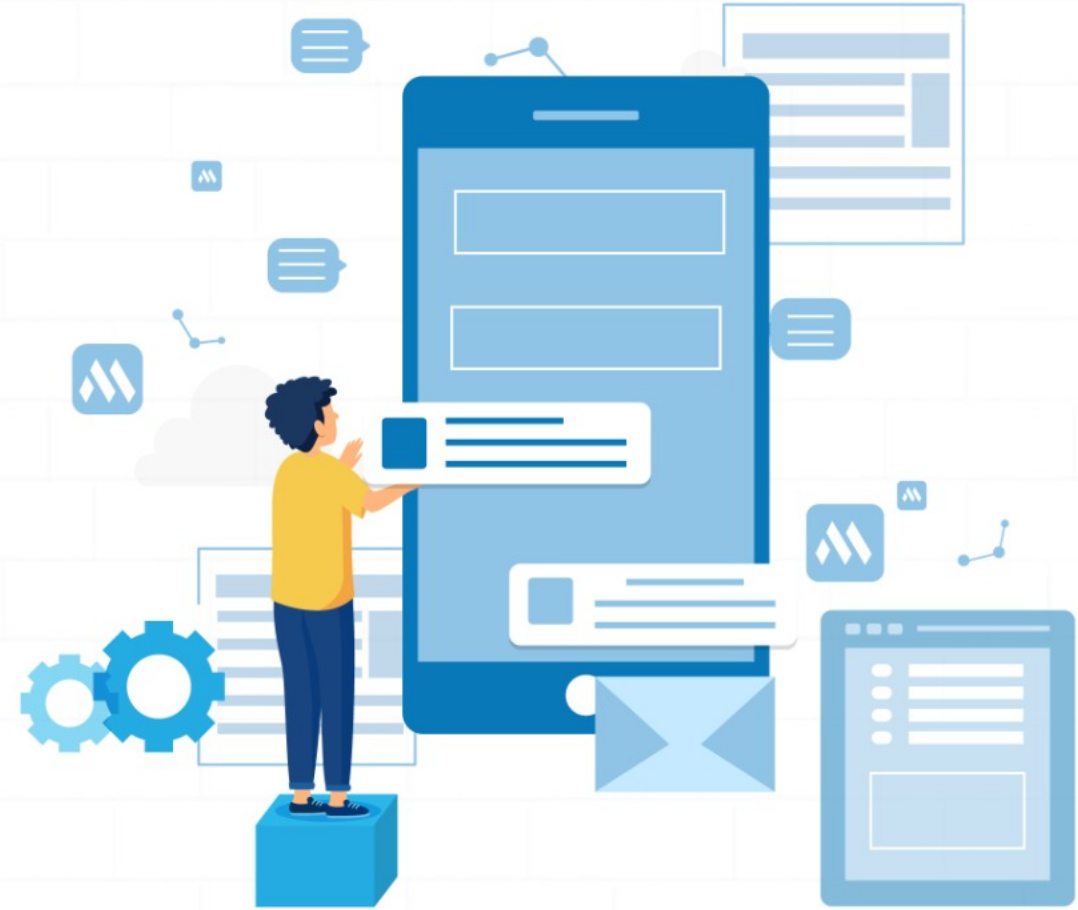
Asset Management

❖ Troubleshoot devices by remotely taking control of them from your desk without requiring additional apps/services

❖ Instantly know the location of corporate devices

❖ View the history of all locations traversed by the devices

❖ View the location of all your devices at the same time on a single map

❖ Automatically get complete details of the device such as network information, certificates etc.

❖ Schedule scans to automate periodic update of device information

Profile Management

❖ **Security Hardening of devices**

➢ Enforce a strong passcode on devices to adhere to enterprise's security standards

➢ Relieve users from password fatigue using Enterprise Single Sign-on

➢ Prevent unauthorized data access by ensuring organizations can use only trusted Wi-Fi networks

➢ Have your essential contacts and important calendar events synced to employee's devices

➢ Disable basic device features/settings such as Bluetooth, camera, calls, SMS, external storage, factory reset etc.

Profile Management

❖ **Security Hardening of devices**

➢ Ensure secure access of corporate data from anywhere and anytime using VPN and per-app VPN

➢ Prevent access to malicious and unapproved websites through URL filtering

➢ Facilitate certificate-based authentication by pushing user-specific security certificates using SCEP

➢ Secure network communications by ensuring it is routed through the enterprise proxy

➢ Apply enterprise specific configurations to devices using Custom Configurations

App Management

❖ **Create and maintain enterprise app catalog containing only enterprise-approved apps**

  • Bulk purchase of Store apps (Apple Business Manager, Managed Google Play, Windows Business Store and Chrome Web Store)

  • Custom business apps/enterprise apps

  • Manage app licenses and revoke/reuse apps across devices

❖ **Install/Uninstall apps without any user intervention**

❖ **Blacklist non-productive apps and prevent its usage/installation on devices**
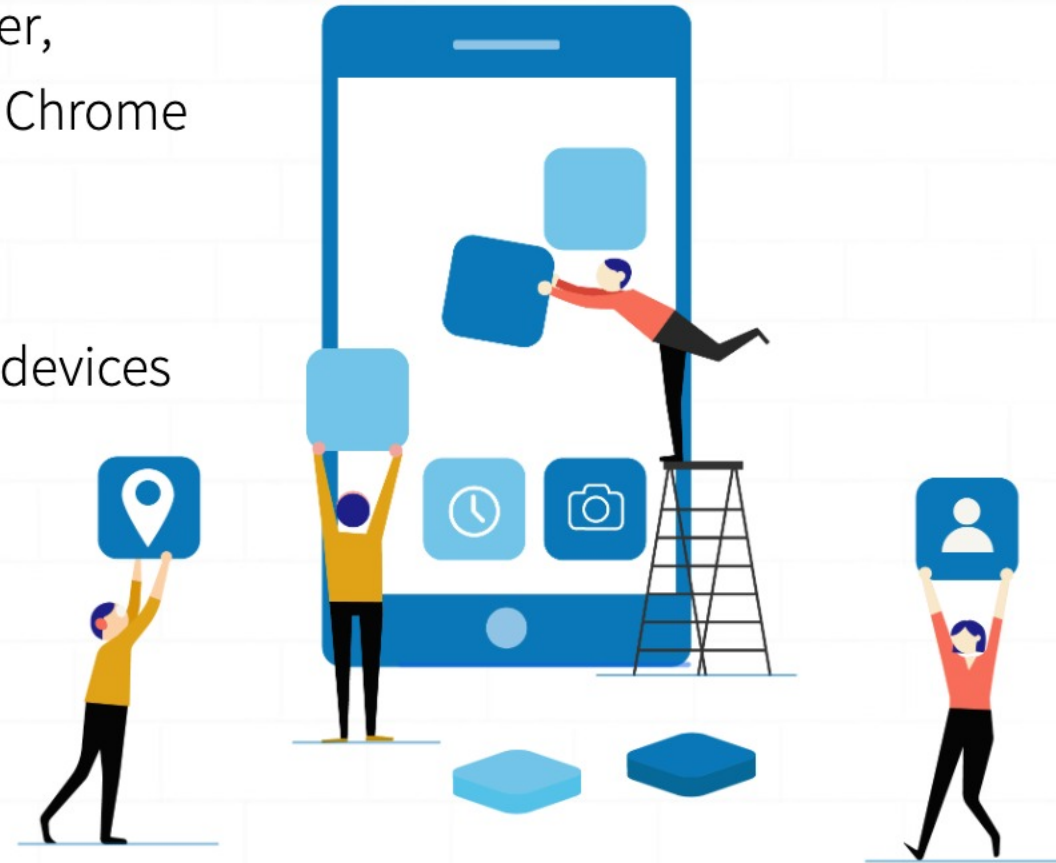
App Management

❖ Lock down devices to a specific app or a set of approved apps, while pre-configuring settings and preventing users from modifying them

❖ Restrict users from uninstalling corporate apps, ensuring there is no drop in productivity

❖ Restrict users from updating specific apps while ensuring critical app updates are deployed immediately without any user intervention and minimal admin action

❖ Pre-define app configurations and permissions, ensuring the apps are ready to use on installation

❖ Deploy enterprise apps to your production environment after testing them on a test bed

E-mail Management

❖ Pre-configure your work email on devices with the requisite settings using Exchange ActiveSync

❖ Prevent the transfer of emails from corporate accounts to user's personal accounts

❖ Securely download and view confidential corporate attachments on the ManageEngine MDM app

Content Management

- ❖ Create a repository containing critical business documents and media files

- ❖ Securely share files in multiple formats to devices without depending on any third-party services

- ❖ Sandbox your corporate documents to securely view distributed content from the ManageEngine MDM app

- ❖ Prevent the backup of corporate data on third-party cloud services and restrict sharing it to other devices

- ❖ Automate content update on mobile devices

- ❖ Centralized removal of content from managed devices.
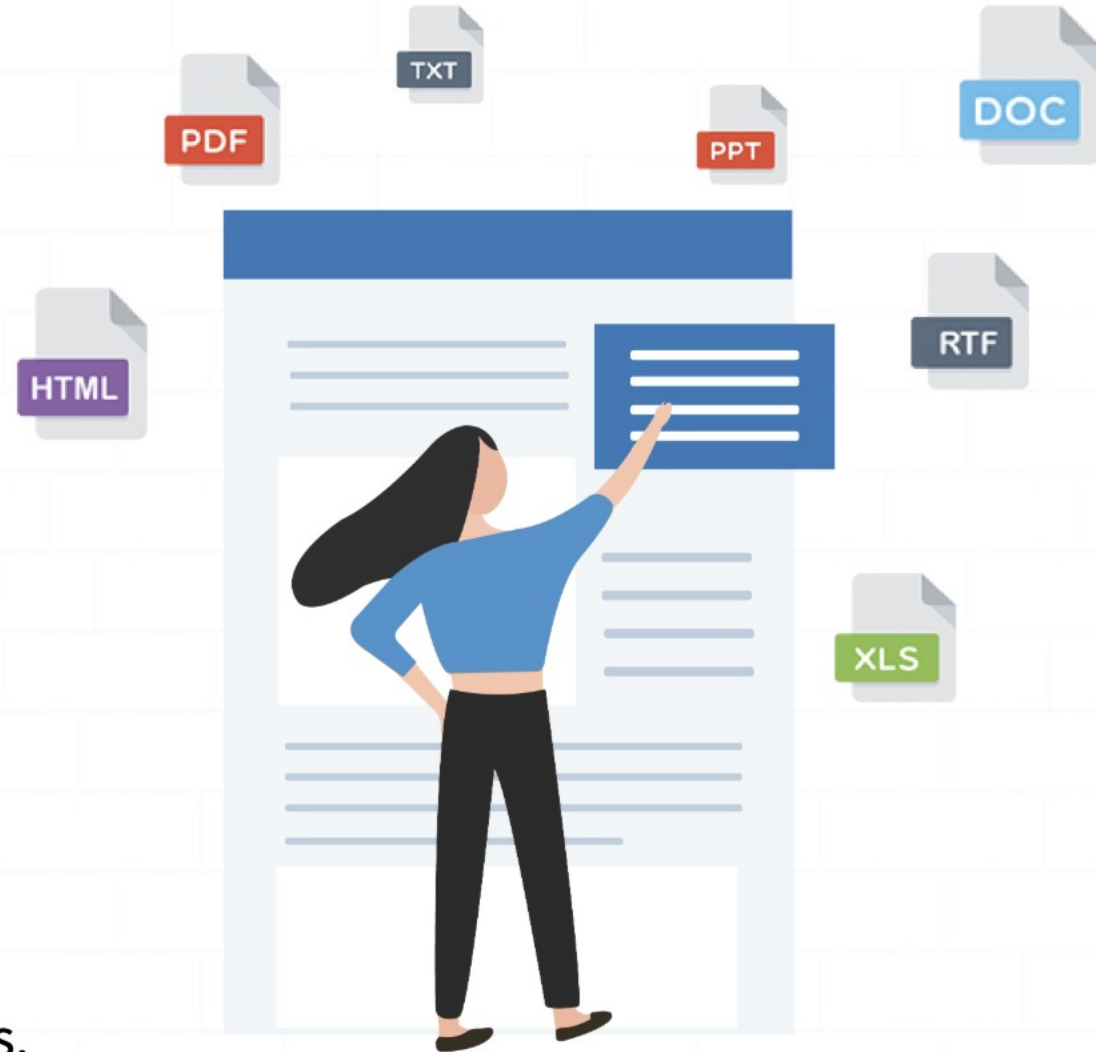
Security Management

❖ Enforce and automate OS updates to prevent ad-hoc updates and bandwidth choking

❖ Apply security restrictions on devices when they leave a designated area with geofencing

❖ Lock down lost or stolen devices using Lost Mode

❖ Secure data on devices and external storage with enforced encryption

❖ Overcome the hassles of Factory Reset Protection with EFRP

❖ Apply security policies to Office 365 apps even when installed on unmanaged devices

Security Management

❖ Remotely lock devices to prevent unauthorized access

❖ Wipe the corporate data or the complete device when lost or stolen

❖ Clear or reset device passcode with a single click

❖ Locate misplaced devices by remotely ringing an alarm

❖ Detect and remove jailbroken/rooted device from your organization's network

Bring Your Own Device (BYOD)

❖ Containerization of corporate data

❖ User's personal data will be untouched

❖ Separate profile strategy to secure corporate data on employee owned devices

❖ Restrict corporate data sharing between

    ➤ corporate and personal apps

    ➤ managed and unmanaged devices

    ➤ device and third-party cloud services

❖ Effective management of multiple device types

Laptop Management

- ❖ Enroll Windows 10 laptops and Macs over-the-air

- ❖ Distribute Store and in-house apps to Windows laptops

- ❖ Lock down Windows laptops to specific app(s)

- ❖ Remotely locate Windows laptops and Macs

- ❖ Secure data on Macs with FileVault encryption and Firmware passwords

- ❖ Remotely restart and wipe Windows laptops

Reports

- ❖ 10+ pre-defined reports

    - ➤ Apps by devices

    - ➤ Devices with/without specific app

    - ➤ Devices by model

    - ➤ Devices by passcode types

    - ➤ Device by enrollment time

    - ➤ Inactive devices

- ❖ Schedule reports

- ❖ Custom query reports

Integrations

Mobile Device Manager Plus MSP integrates with ServiceDesk Plus MSP to provide enhanced actionable insights to IT admins

Know more

https://www.manageengine.com/mdm-msp

Try it for free!

https://www.manageengine.com/mdm-msp-free-trial