ManageEngine
Mobile Device Manager Plus

Datasheet

Today's challenge

Enterprises today are seeing an influx of employees using mobile devices to carry out corporate tasks and access corporate resources. Many see this as an opportunity to improve employee productivity, and have begun advocating practices like corporate-owned personally enabled (COPE) and bring your own device (BYOD). However, placing sensitive corporate data in the pockets of your employees poses various threats to your enterprise's privacy and security.

To address this issue, you should adopt a holistic, integrated mobile device management (MDM) solution that can help your IT staff manage every aspect of mobile device use, ranging from enrolling new devices to wiping corporate information when an employee leaves your organization.

How Mobile Device Manager Plus fits into your IT framework

With Mobile Device Manager Plus, you can empower your workforce with mobility and manage devices from enrollment to retirement. Here's what makes Mobile Device Manager Plus a trusted solution for your company:

Highlights

Supported operating systems

iOS 4.0 and above

Android 4.0 and above

Windows Phone 8.0 and above

Chrome OS, macOS, and Windows 10 Desktops/Laptops

Samsung Knox

iPadOS

Compliance

CJIS HIPAA PCI DSS COMPLIANT ISO

Recognition

Gartner FORRESTER IDC Analyze the Future

Over **11 years** of experience in empowering enterprises with mobility.

4500+ Customers

Currently managing more than **1.3 M+** mobile devices.

Support for **20** languages.

Used across **190** countries.

Free management for up to **25** devices.

Mobile application management

- Create your own enterprise-authorized app catalog.
- Comprehensively manage both enterprise and Store (free/paid) apps as well as app licenses.
- Integrate with Apple Business Manager (ABM), Managed Google Play, Chrome Web Store, and Windows Business Store.
- Upload and test multiple versions of enterprise apps before deploying them to the production environment.
- Install/Uninstall apps silently on devices without user intervention.
- Ensure devices are used only for specific purposes by forcing devices to run a single app or set of apps using Kiosk Mode.
- Restrict devices to run on a single app for a specific duration
- Customize the layout of apps and web shortcuts on devices in Kiosk Mode for a consistent user experience.
- Pre-configure app settings and configurations during installation itself using Managed App Configurations.
- Containerize apps and data on devices to prevent potential unauthorized corporate data access.
- Blocklist apps that are non-compliant with your enterprise security and ensure users install apps only from trusted sources.

Robust MDM support

- Monitor devices for up-to-date device information.
- Diagnose device, user, or application issues from a centralized platform.
- Overcome the hassles of factory reset protection.
- Update configuration settings in real time.

High-end device security management

- Force passcodes to be set in accordance with your organization's security standards.
- Enforce restrictions on device functionality such as enabling or disabling the camera, iCloud, Passbook, iTunes, and much more.
- Track the geographical location of managed devices on demand and maintain a history of locations traversed by corporate devices.
- Ensure corporate data stays within the organization's premises or any predefined virtual geographical range by defining a geofence.
- Detect rooted and jailbroken devices, and instantly remove them from the corporate network.
- Prevent data loss or theft by either completely wiping devices or wiping only corporate data.
- Remotely lock devices to prevent misuse of misplaced or stolen devices.
- Secure corporate data present on your Mac machines by encrypting them on-the-fly and by preventing start up from any internal or external storage device.
- Generate and distribute user-specific certificates, by integrating CA servers with MDM.

Secure distribution of content

- Create a content repository for storing documents and media.
- Securely distribute documents in different formats.
- Ensure users securely access content distributed from MDM, by configuring security policies.
- Control content sharing to unmanaged devices and third party cloud services

Product availability

On-premises | SaaS(Cloud) | MSP

Smarter mobile device enrollment

- Enroll devices over-the-air(OTA) through either E-mail or SMS.
- Automate bulk enrollment for Apple, Android and Windows devices using Apple Business Manager (ABM), Windows AutoPilot (Azure), Zero Touch enrollment and Samsung Knox enrollment.
- Authenticate enrollment with a one-time passcode (OTP) or a user's Active Directory (AD) credentials.
- Allow users to enroll their own devices using a self-service portal.
- Enroll and manage multiple devices for the same user.

Complete and secure e-mail management

- Set up e-mail security policies to devices OTA.
- Containerize e-mail apps to prevent unauthorized access to e-mails.
- Restrict users from making changes to a corporate e-mail account or the applied configuration.
- Securely view and save e-mail attachments directly on the ME MDM app.
- Provide conditional access to Exchange on-premises and Office 365.

Supported browsers

Mobile Device Manager Plus requires one of the following browsers to be installed:

- Internet Explorer 7 and above.
- Google Chrome 20 or above.
- Mozilla Firefox 4 or above.
- Apple Safari 5 or above.

Hardware Requirements

Mobile Device Manager Plus on-premises runs on Microsoft Windows.

Instantly update OSs on mobile devices

- Silently deploy OS updates to managed mobile devices.
- Restrict users from upgrading their mobile OS.
- Notify users when mobile OS updates are available.
- Choose immediate, delayed, or windowed deployment of mobile OSs.

Manage mobile assets efficiently

- Track mobile device details including certificates, installed apps, and memory usage to stay up-to-date.
- Get granular reports on hardware and software inventory.
- Get custom reports for any specific needs in your enterprise.
- Monitor the battery levels of devices and receive alerts when the battery level falls below a specified level
- Remotely troubleshoot devices in real-time
- Notify users of emergencies and scheduled maintenance by sending Announcements to devices
- Use iPads as Shared devices by allowing multiple users to access a single device, while ensuring user privacy.

Integrations

- Helpdesk solutions: ServiceNow, ServiceDesk Plus, Jira Servicedesk, and Zendesk.
- Business process automation apps: Zoho Creator and Zoho CRM
- Analytics software: Analytics Plus
- Public APIs available for third-party integrations

Number of managed devices	Processor	RAM	Hard disk space
Up to 250	Intel Core i3 (2 core/4 thread) 2.0 GHz 3MB cache or equivalent	4GB	5GB
251 to 500	Intel Core i3 (2 core/4 thread) 2.4 GHz 3MB cache or equivalent	4GB	10GB
501 to 1000	Intel Core i3 (2 core/4 thread) 2.9 GHz 3MB cache or equivalent	4GB	20GB
1001 to 3000	Intel Core i5 (4 core/4 thread) 2.3 GHz 6MB cache or equivalent	8GB	30GB
3001 to 5000	Intel Core i7 (6 core/12 thread) 3.2 GHz 12MB cache or equivalent	8GB	40GB
5001 to 10000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz 20MB cache or equivalent	16GB	60GB

If you're managing more than 1,000 devices, we recommend installing Mobile Device Manager Plus on a Windows Server machine.

Pricing

Free

- Complete management of up to **25 devices**.

Standard

- Basic mobile device management.
- Pricing starts at **495 USD** for **50 devices/year**.

Professional

- All the necessary features to manage your enterprise mobile fleet.
- Pricing starts at **895 USD** for **50 devices/year**.

© 2025 Zoho Corp. All rights reserved.

ManageEngine
IT Management, Simplified