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:

Over **10 years** of experience in empowering enterprises with mobility.

Trusted by over **10,000** IT professionals across the globe.

Currently managing more than **500,000** mobile devices.

Support for **16** languages.

Used across **185** countries.

Free management for up to 25 devices.

Highlights

Supported operating systems

iOS 4.0 and above

Android 2.2 and above

Windows Phone 8.0 and above

Chrome OS, Mac OS, and Windows 10 Desktops/Laptops

Samsung KNOX

Compliance

CJIS HIPAA PCI DSS COMPLIANT ISO

Recognition

FORRESTER IDC Analyze the Future EMA

Mobile application management

- Create your own enterprise-authorized app catalog.
- Comprehensively manage both enterprise and Store(free/paid) apps.
- Integrate with Apple Volume Purchase Program(VPP), Google Play for Work(PfW) and Windows Business Store.
- Ensure devices are used only for specific purposes by forcing devices to run a single app or set of apps using Kiosk mode.
- Install apps silently on devices without user intervention.
- 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.
- Blacklist apps that are non-compliant with your enterprise security and regulation standards.

Robust MDM support

- Monitor devices for up-to-date device information.
- Diagnose device, user, or application issues from a centralized platform.
- Reset forgotten passcodes.
- Update configuration settings in real time.

High-end device security management

- Force passcodes to be set in accordance with your organization's security standards. Configure granular details such as the passcode length, uppercase characters etc.,
- Enforce restrictions on device functionality such as enabling or disabling the camera, iCloud, Passbook, iTunes, and much more.
- Protect corporate data by preventing unauthorized devices from accessing the corporate network.
- Track the geographic location of your managed devices on demand.
- Remotely lock devices to prevent misuse of misplaced or stolen devices.
- Detect rooted and jail broken devices, and instantly remove them from the corporate network.
- Prevent data loss or theft by either completely wiping devices or wiping only corporate data.
- Collect and wipe devices when an employee leaves your company.

Secure distribution of content

- Create a content repository for storing documents.
- Securely distribute documents in different formats.
- Control document sharing between unmanaged devices.

Product availability

On-premises | SaaS(Cloud)

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.

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.
- Regulate devices with access to a corporate e-mail account.
- 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.

Assertive asset tracking with configurable reports

- 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.
- Create out-of-the-box reports on apps by devices and devices by model.

Smarter mobile device enrollment

- Enroll devices over-the-air(OTA) through either E-mail or SMS.
- Enroll any number of mobile devices in a single instance using a CSV file.
- Automate bulk enrollment for iOS and Android devices.
- Ease enrollment through Apple Device Enrollment Program(DEP) for iOS devices, Windows AutoPilot(Azure) for Windows devices, Zero Touch enrollment for Android devices 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.

Hardware Requirements

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

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

ManageEngine
IT Management, Simplified