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.

**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**

- HIPAA
- PCI DSS
- ISO

**Recognition**

- Forrester
- IDC
- EMA

**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 17**

languages.

**Used across 185**

countries.

**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 the beta version 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.
- 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 ensure users install apps only from trusted sources.

**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 or maintain a history of locations traversed by corporate devices.
- Ensure devices stay 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.

**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.

**Secure distribution of content**

- Create a content repository for storing documents and media.
- Securely distribute documents in different formats.
- Control content sharing to unmanaged devices and third party cloud services.
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.
- 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.

### Number of managed devices

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

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

### Integrations
- Business process automation apps: Zoho Creator and Zoho CRM
- Public APIs available for third-party integrations

### Pricing

<table>
<thead>
<tr>
<th>Plan</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free</td>
<td>Complete management of up to 25 devices</td>
</tr>
<tr>
<td>Standard</td>
<td>Basic mobile device management.</td>
</tr>
<tr>
<td></td>
<td>Pricing starts at $495 USD for 50 devices/year</td>
</tr>
<tr>
<td>Professional</td>
<td>All the necessary features to manage your enterprise mobile fleet.</td>
</tr>
<tr>
<td></td>
<td>Pricing starts at $895 USD for 50 devices/year</td>
</tr>
</tbody>
</table>