

Mobile Device Management Software: Supporting Vuzix Smart Glasses Deployments

Driving Factors in Mobile Device Management

Mobile Device Management (MDM) software is used for the administration, by head-office technology administrators, of mobile devices used by employees, i.e. smartphones, mobile phones, tablets and/or laptops, POS devices, and portable scanners. MDM deals with corporate data segregation, securing email transmissions and telephone conversations, securing the transmission and storage of corporate documents, and enforcing corporate IT policies. While doing this, MDM works to protect the assets that are the physical devices and the corporate information on those devices. It must also enable everyone in the company to communicate with each other, and with suppliers and customers, in an efficient and approved manner. Because of its evergrowing complexity, MDM is now its own segment in the IT industry, valued at $3 billion and with a predicted annual growth rate of 25%.

Managing Volume

Mobile Device Management became its own sub-industry out of necessity—systems had to be found to manage the vast number of devices that employees of corporations use. Added to those corporate devices, in many cases, are employees' own devices, and those of contractors (also known as BYO, or bring-your-own, devices). To use one example, Bechtel Corp. is the largest construction company in the United States. It has 60,000 employees working at 13 international offices. Assume that each one of those employees has a corporate smartphone, and each one has a corporate tablet or desk-top computer, or both. Every call, every email, every document download has to be conducted according to the company's pre-determined information management, security, and ap management protocols. In this example, if an executive in the United States emails a purchase order to a project manager in China, the corporate protocol could be that the employee downloads that purchase order and saves it to his computer. If head office does not want the employee to be able to forward it to anyone, it can embed share blocking into the document. That may sound simple, but enabling that restriction could involve 150,000 devices.

Security

Corporations of all sizes are vulnerable to hacking—hackers may be after money, they may be after trade secrets, or they want to disrupt a competitor's operations. No corporation or government is immune and the struggle to maintain end-to-end security is never-ending. This means that

tech managers have to ensure that all devices are managed in the same fashion, and carry the same approved software, and that security systems on those devices are updated at the same time and in the same way.

Systems Efficiency

Similarly, each piece of software that a company uses has to be regularly updated. That may include accounting software, customer relationship management software, project management software and databases of all kinds. All of this has to be updated for each employee, across all devices, in the same way, and ideally at the same time. Employees' devices have to be tailored for different uses and, in many cases, the way they use their devices has to be monitored or restricted. If head office does not want its smartphones used to access Facebook, that activity can be blocked. Some retail managers must be able to adjust POS systems; others may need mobile scanners. Plus, many companies hire multiple contractors and service providers. Contractors usually use their own devices but, for the length of their contracts, they need to have access to their clients' databases, networks and software, so their devices have to be accommodated and controlled through the corporate system.

Asset Value

The size of a corporation often dictates how many mobile devices it has to have and some companies can spend a small fortune on hardware and software. If we look at a company like Citibank, which has 200,000 employees in 116 countries, that investment involves the purchase, maintenance and upgrades of between 400,000 and 600,000 pieces of hardware. The annual cost of that can easily run into the hundreds of millions of dollars. So Mobile Device Management not only has to make sure that communications functions (systems, software programs and apps) run smoothly and securely, but also that each piece of hardware is properly maintained and tracked. In other words, the logistics of Mobile Device Management can be daunting. There are dozens of MDM apps on the market now, but the goal is to streamline MDM for all deployed devices to make the whole process more efficient.



Mobile Device for Vuzix M-Series Smart Glasses

As companies utilize Vuzix Smart Glasses they quickly recognize the efficiency and return on those investments and begin plans for larger scale deployments. If the goal is to make and streamline technology management of smart glasses more efficient, Mobile Device Management software can be an excellent tool. By controlling and protecting the corporation's data and configuration settings of all mobile devices, including Smart Glasses in a network, MDM can reduce support costs and business risks.

Functionality and Security Optimization:

The intent of MDM software is to optimize the functionality and security of mobile devices and their communications networks while minimizing costs and downtime:

- Ensuring that diverse user equipment is configured to a consistent standard and supported set of applications, functions, and/or corporate policies.
- Updating equipment, applications, functions, and policies in a scalable manner.
- Ensuring that applications are used in a consistent and supportable manner.
- Ensuring that equipment performs consistently.
- Monitoring and tracking equipment, i.e. location, status, ownership, activity.
- Trouble-shooting, diagnosing and addressing issues remotely.



Over-the-Air Distribution of Applications, Data and Configuration

While all Vuzix Smart Glasses come with over-the-air software update capabilities, this tool is limited to device-by-device update processes that have to be managed by the user of each device. But with MDM functionality that also includes over-the-air distribution of applications, data and configuration settings for all types and quantities of Smart Glasses, this becomes a breeze. This tool can automatically detect all relevant devices in the network, and send them settings and updates for immediate and continued usability, simultaneously with simple command instructions. The process is fully automated, keeps a history of user devices, and sends settings only to subscriber devices which were not previously set. Device management software platforms ensure that end-users benefit from plug and play data services for whatever devices they are using. And for mobile security, most MDM products are built with the concept of Containerization. An MDM Container is a secured section of the device using modern cryptographic techniques so that corporate data such as email, documents, and enterprise applications are encryptedvand processed inside the container, ensuring that corporatevdata is separated from users' personal data on the device. In the end, the overall role of MDM is to increase device supportability, security, and corporate functionality while maintaining user flexibility.



VUZIX M4000™
SMART GLASSES

State-of-the-Art Technical Versatility: Best-in-Class MDM Software Compatibility

Numerous companies provide dozens of apps designed to assist with MDM, and Vuzix Smart Glasses are compatible with many of them. The top five MDM apps currently supported on Vuzix glasses include VMWare Airwatch, SOTI MobiControl, Microsoft Intune, 42Gears SureMDM, and Mobile Iron. This list does not include every MDM platform, but Vuzix can integrate, test and certify its glasses to work with virtually any Android MDM software. Therefore Vuzix Smart Glasses can easily integrated into any established MDM system. Vuzix Smart Glasses can be delivered directly to any office in the world. Head office can program and configure them remotely, or they can be pre-loaded, with MDM software installed by Vuzix as requested by the customer. The recipients merely scan a code after powering up their devices, and the Vuzix Smart Glasses are online, synced and secure.

Vuzix Smart Glasses Enable:

- Hands-free access to information in the form of a HUD (step-by-step instructions, diagrams, videos);
- Real-time, see-what-I-see communication (for remote collaboration and teleconferencing support and more);
- Hands-free, point-of-view corporate documentation (audio and visual);
- AR overlays for vision picking, instructions, and remote support and communication (audio and visual);
- Computer Vision for object and character recognition (for scanning codes, text, numbers, step verification, task completion).

These capabilities are essential for Mobile Data Management, allowing hands-free teleconferencing and more.

Vuzix Smart Glasses Solutions

VUZIX M400™



- First Smart Glasses 8 Core 2.52Ghz Qualcomm© XR1 Platform
- See-through Waveguide optics
- 2-12 hours of operation based on external battery choice
- Auto-focus camera with up to 12.8 megapixels and 4K 30fps video
- Various mounting options available for comfort
- Integrated speaker with up to 97db output
- USB, Wi-Fi, and Bluetooth connectivity
- IP67 certification against water and dust

VUZIX M4000™



- First Smart Glasses 8 Core 2.52Ghz Qualcomm© XR1 Platform
- OLED display
- 2-12 hours of operation based on external battery choice
- Auto-focus camera with up to 12.8 megapixels and 4K 30fps video
- Various comfortable mounting options
- Integrated speaker with up to 97db output
- USB, Wi-Fi, and Bluetooth connectivity
- IP67 certification against water and dust

vuzix.com/pages/mobile-device-management

VUZIX®

BE THE NEXT TO GET ON BOARD WITH VUZIX

www.vuzix.com sales@vuzix.com