MobileIron

Data Sheet

Multi-user for Shared iOS Devices

Challenge

Sharing mobile devices across multiple users with personalized settings and data

Solution

MobileIron multi-user capability

Benefits

- Deploy shared devices at scale
- Support fast switching between users
- Provide continuous security during and between use
- Push user-specific settings for apps, email, connectivity, and other policies, while retaining shared settings
- Minimize helpdesk requests
- Support iPad, iPhone, and iPod touch

Recent Recognition

Gartner: MobileIron positioned in the Leaders Quadrant of the Magic Quadrant for Mobile Device Management Software (May 2012)

Info-Tech: MobileIron listed as a Champion in the Mobile Device Management Suites Vendor Landscape (Aug 2012)

IDC: MobileIron #1 in market share and growth among pure-play mobile enterprise management ISVs (Sept 2012)

Contact

MobileIron
415 East Middlefield Road
Mountain View, CA 94043 USA
Tel. +1.650.919.8100
Fax +1.650.919.8006
info@mobileiron.com

The largest companies in the world trust MobileIron® as their foundation for Mobile IT. Available as a highly-scalable on-premise or cloud solution, MobileIron was purpose-built to secure and manage mobile apps, documents, and devices. MobileIron was the first to deliver key innovations such as multi-OS mobile device management (MDM), mobile application management (MAM), and BYOD privacy.

MobileIron's multi-user capability is a recent innovation that allows organizations across industries to deploy iOS devices for use by multiple individuals:

- **Education**: iPads are becoming the new standard of computing in the classroom. New curricula rely on each student having tablet access to learn, review, and test. Fast switching between students is essential because one device can be used by many students during the course of just one day.
- **Healthcare**: Mobile is improving patient care and operational efficiency. In hospitals and clinics, multiple medical professionals will use the same device. Because of the sensitivity of healthcare data, the device must always remain under management with enforced security policies even between users.
- **Retail**: Mobile apps are changing point-of-sales and logistics processes for retailers. These apps generally run on corporate-owned devices shared by multiple end users. Because turnover across the employee base can be quite high, multi-user capabilities must be easy to use and require minimal training.
- **Hospitality**: Mobile is taking paper out of the property management process. Connectivity settings are usually shared across shift-based users, but apps and email settings are user-specific. Both need to be managed seamlessly.

Speed, security, and personalization are the core requirements for a scalable multi-user mobile deployment. Traditional approaches that un-enroll and re-enroll the entire device, instead of just the user, are slow, not secure, and complex to troubleshoot. The MobileIron approach is fast, secure, and simple for the user and is part of the MobileIron Advanced Management and Connected Cloud solutions.

Speed

MobileIron provides fast and simple switching between users:

- User clicks on the customizable multi-user sign-in icon on the iOS device.
- User enters standard authentication credentials, generally AD-based.
- MobileIron pushes user-specific settings to the device.
- Email, VPN, Wi-Fi, and other policies are applied in the background.
- Certificates are installed to make email, VPN, and Wi-Fi access easy for the user.
- User is prompted to install approved apps with a single click.

The shared device is now completely personalized, secured, and ready to use.

When finished with work, the user signs out:

- All user-specific apps, email, settings, and data-at-rest are removed.
- Shared settings and apps are retained for the next user.

The only actions the end user takes are sign-in, opt-in for apps, and sign-out when done. No technical knowledge is required. Helpdesk calls are minimized. The user experience is fast, easy, and highly repeatable, which is important in environments with large user populations and high turnover.

Security

MobileIron protects data across the multi-user workflow:

- Device always remains under management, even between users, so it can be locked, wiped, located, and connected at all times if necessary.
- Secure sign-in is tied to the user's corporate authentication credentials.
- Certificates can be used to establish identity for email, Wi-Fi, and VPN.
- Auto-lock ensures other users cannot access the device when idle.
- Device passcodes can be shared or user-specific, based on IT policy.
- All user-specific business data is removed upon sign-out.

Personalization

MobileIron personalizes email, apps, connectivity, and policy settings for each user:

- Shared settings, e.g., Wi-Fi and shared apps, are retained across users.
- User-specific settings, e.g., email and non-shared apps, are only upon sign-in.

About MobileIron

The leader in Mobile IT, MobileIron has been chosen by thousands of organizations that are transforming their businesses through enterprise mobility. Available as an on-premise or a cloud solution, MobileIron was purpose-built to secure and manage mobile apps, documents, and devices for global companies. MobileIron was the first to deliver key innovations such as multi-OS mobile device management (MDM), mobile application management (MAM), and BYOD privacy controls.

MobileIron enables fast, secure, and personalized multi-user workflows for shared devices across large organizations.

Customer Perspective

Apps: "MobileIron has been a very strategic platform for us to support and manage our mobile devices and apps."
Life Technologies (Life Sciences)

BYOD: "MobileIron provides exactly the framework we needed to let our people use the device of their choice."
Thames River Capital (Financial Services)

Innovation: "MobileIron is helping us become a technology innovator."
Norton Rose (Legal)

Multi-OS: "We needed a truly multi-OS solution. MobileIron was without doubt the most comprehensive."
Colt Car Co. / Mitsubishi (Automotive)

Scale: "[MobileIron] did a great job not only helping us getting the product scaled, but also fixing any kind of issues."
Lexington School District (Education)

Security: "In our sector, the right mobile security solution is not a nice to have, it's mandatory."
National Health Service (Healthcare)

Support: "In this day and age of bad customer service, my experience with MobileIron has been consistently great."
City of North Vancouver (Government)

User experience: "MobileIron's strength is its ease of use for iPad owners."
KLA-Tencor (Technology)

Gartner, Inc., Magic Quadrant for Mobile Device Management Software, Phillip Redman, John Girard, Monica Basso, May 17, 2012. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Info-Tech Research Group, Inc., Vendor Landscape: Mobile Device Management Suites, August 2012. Info-Tech Research Group Vendor Landscape reports recognize outstanding vendors in the technology marketplace. Assessing vendors by the strength of their offering and their strategy for the enterprise, Info-Tech Research Group Vendor Landscapes pay tribute to the contribution of exceptional vendors in a particular category.