Just another day at the office

Fujitsu's Managed Mobile for Android Smartphones and Tablets

Advanced security, reliability and scalability for Google Android smartphones and tablets in your mobile enterprise infrastructure. Now IT departments can ensure that users have consistent, reliable and secure access to enterprise data and applications while avoiding costly delays, downtime and compliance violations. Fujitsu helps you provision Android smartphones and tablets; proactively monitor and troubleshoot Android user and infrastructure problems; and manage Android policies and configurations. Fujitsu also supports Apple iOS, BlackBerry, Windows Mobile, Windows Phone and HP Palm OS devices.

Greater insights for end-to-end control

With Fujitsu, you know when devices connect to your corporate network, whether these devices are employee or company-owned and if they are missing security policies or have the incorrect policies applied. Fujitsu keeps you informed of critical system details to help you manage every step of the mobile device lifecycle, from Exchange ActiveSync provisioning to the decommissioning of devices.

Fast, sure-fire protection

With Fujitsu's device management capabilities, you can proactively monitor the Android smartphones and tablets in your mobile enterprise. When problems occur, Fujitsu performs automated diagnostic tests to quickly identify the root cause of Android device issues for faster troubleshooting.

Immediate locks and wipes

When smartphones or tablets are lost, Fujitsu gives you the ability to avert potential corporate data security breaches. IT help desk representatives can immediately remotely wipe clean an Android device to prevent access to unauthorized corporate data.

shaping tomorrow with you
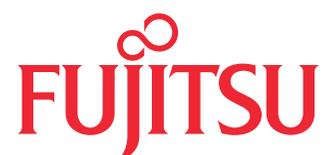
FUJITSU
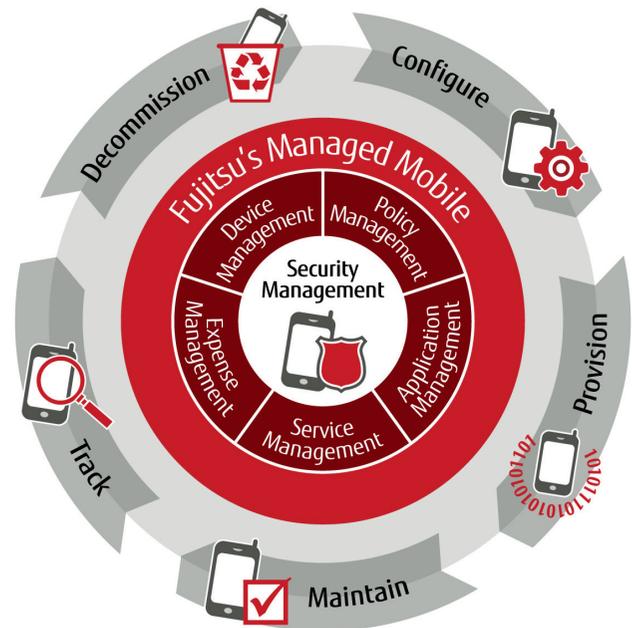
Fujitsu automates and eases the management of Google Android smartphones at every stage in the mobile lifecycle.

Mobile Device Lifecycle Stage	Feature	Benefit
Configure	**Applications & Device Settings** ■ Wifi settings (WPA, personal, WEP, WPA2) ■ Enable/Disable application installs	Enforces Sarbanes Oxley and HIPAA requirements to Android smartphones and tablets. Protects enterprise from loss of confidential data.
Secure	**Device Security** ■ Enforce passcodes (simple, complex) ■ Auto-lock device after inactivity ■ Auto-wipe after a specified number of failed attempts ■ Configure APN ■ Restrict ports used by mobile apps on device ■ Data loss protection–identify all files installed on device ■ Track lost or stolen devices **Application & Infrastructure Security** ■ Encrypt data between mobile apps & enterprise infrastructure ■ Audit & log all mobile app traffic ■ Remotely kill rogue app processes ■ Remotely remove malicious apps	Enables organizations to document compliance with HIPAA, SOX and other global standards. Mitigates risks and averts potential security breaches.
Provision	Roles based provisioning integrated with LDAP. Profile-lock: Ensures that profiles remain on device. **Enterprise App Store** ■ Provision applications ■ Provision application updates	Quickly activate thousands of users. Maintain consistency across all deployed devices for corporate compliance. Quickly deploy enterprise applications.
Maintain	Proactively detect user or infrastructure problems (e.g., mail outage, LDAP problems, carrier outages). **Return real time device statistics** ■ Processes running ■ Carrier ■ Device memory & CPU ■ Available storage ■ Signal strength ■ SD card details ■ Battery level ■ Applications installed ■ OS version number	Reduce support calls from end users.
Track	**Assets** ■ Employee owned & corporate provided devices ■ Hardware versions ■ SIM IDs ■ IMEI/Serial # **Expenses** ■ Detect roaming users ■ Detect inactive users ■ Track expense plans of employees ■ Require roaming users to connect applications through Wifi only	Reduce overall wireless bill. Facilitate device refreshes/ updates.
Decommission	Full wipe of device- returns device back to factory default. Select wipe of device–only removes corporate data and leaves personal data on device. Lock device.	Protect corporate data on device should device be lost or stolen.