Just another day at the office

Fujitsu's Managed Mobile for iPhones, iPads and iPod Touch

Advanced security, reliability and scalability for iOS devices in your mobile enterprise infrastructure. With over 100 million iOS devices in use, the odds are that someone is connected to your corporate network with an unauthorized iPhone, iPad or iPod Touch right now. Left unsecured, the iPhone OS can present security risks to both corporate and customer data. Fujitsu Managed Mobile helps you secure enterprise iOS devices immediately. The software allows IT departments to identify who is using an iOS device and accessing the network. Security policy and compliance reporting capabilities ensure that unauthorized, non-updated, or non-compliant iOS devices can be isolated and blocked from the corporate network. Fujitsu makes centralized security management a reality for iOS devices.

Quickly identify authorized and unauthorized devices

Fujitsu Managed Mobile automatically discovers all devices that are currently connecting into the network. This visibility allows the IT team to remedy potential security problems without delay. Fujitsu's historical asset reports allows you to spot trends in iOS device hardware, iOS upgrades and other mobile app compliance problems so your teams can collaborate to achieve risk-free mobile enterprise management.

Protect enterprise data without compromising user experience

Fujitsu Managed Mobile leverages sandbox capabilities on the iPhone to segregate critical enterprise data from personal data & applications. For example, when an employee leaves the organization, IT can decide to wipe the entire device clean of data, or can decide to selectively wipe only the corporate data from the device. The selective wipe capability means that you can protect your corporate assets, while still giving the end user control over devices and applications.
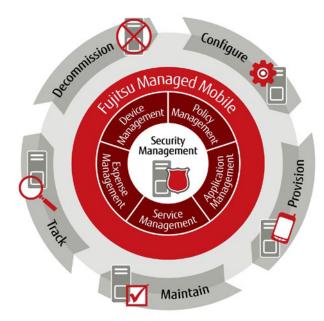
Works well with what you have

Fujitsu leverages and extends the security capabilities that exist within your enterprise. All data transmission to the iOS device is encrypted through SSL and is not required to pass through a third party NOC. Security policies are enforced either through use of Apple's MDM device side APIs or via ActiveSync policies. Most importantly, Fujitsu preserves the user experience by allowing use of the native email, calendar, and contact iOS device applications.

Remote iOS device lock and wipe

When an iOS device is lost, Fujitsu gives you the ability to respond proactively to avert potential corporate data security breaches. IT helpdesk representatives can immediately lockdown and remotely wipe an iPhone clean of corporate data to prevent unauthorized use.

shaping tomorrow with you

FUJITSU

Fujitsu automates and eases the management of iOS devices,
including iOS 4, at every stage in the mobile lifecycle.

Mobile Device Lifecycle Stage	Feature	Benefit
Configure	Applications & Device Settings ■ Email configurations ■ Wifi settings (WPA, personal, WEP, WPA2) ■ VPN settings (LT2P, PPTP, IPSEC, Cisco, Juniper SSL) ■ Proxy server settings ■ Enable/Disable application installs ■ Disable camera ■ Prevent unauthorized app purchases ■ Disallow multiplayer gaming ■ Enforce encrypted backups ■ Disable YouTube, Safari, iTunes	Enforces Sarbanes Oxley and HIPAA requirements to iPhones, iPads, and iPod Touches. Protects enterprise from loss of confidential data.
Secure	Security Configurations ■ Attach certificates for two factor authentication ■ Enforce passcodes (simple, complex) ■ Auto-lock device after inactivity ■ Auto-wipe after a specified number of failed attempts ■ Maintain passcode history ■ Configure Access Point Node (APN)	Enforces security compliance and protects your company from non-compliance penalties. 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. Ability to encrypt profiles sent to device. Profile-lock: Ensures that profiles remain on device.	Quickly activate thousands of users. Maintain consistency across all deployed devices for corporate compliance.
Maintain	Proactively detect user or infrastructure problems (e.g., mail outage, LDAP problems, carrier outages). Return real time device statistics ■ OS version number ■ Carrier ■ Phone Number ■ Available storage ■ Applications installed ■ Encryption levels ■ Profiles installed	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	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.	Protect corporate data on device should device be lost or stolen.