FancyFon

Mobile Device Management Solutions

FAMOC Security Management

As organizations strive to cope with the tremendous surge in mobile device and application usage, virtualization or employees bringing their own smartphones and tablets to work (BYOD), there is a growing requirement to improve mobile security. Mobile handsets are becoming increasingly powerful, and contain more and more critical corporate and personal data that needs to be protected against loss, theft or misuse. As a result, security management has become a high priority for the IT departments managing mobile devices fleets.

FancyFon fully understands the importance of mobile device security, and is at the forefront in developing state of the art security solutions. FAMOC security management ensures an unparalleled level of security support across multiple platforms, managed centrally, over the air, empowering IT administrators to easily address all the new challenges of enterprise mobility management.

FAMOC security management implements corporate security policy allowing differentiated access rules for groups and shared data including pre-defined user profiles. Moreover, the solution allows for end-to-end certificate lifecycle management, also via integration with existing corporate Certificate Authorities.
If a mobile device is lost or stolen, FAMOC can remove all applications and sensitive data, over the air, to prevent any security breaches. If, on the other hand, an employee leaves the organization or breeches security, the administrator can select and wipe only the sensitive corporate data from the device.
Also, if the system detects an unauthorized SIM card, the device can be locked and wiped. The system ensures secure communication between server and mobile devices, protects stored data and enables seamless corporate policy deployment.

FAMOC security management quick feature guide

Connectivity configuration	▪ **WiFi settings** - ensures that only the pre-selected and pre-configured WiFi connection is used when logging on to the Internet or when using email **Browser and APN restrictions** - sets parameters around approved and forbidden Internet connections, forces corporate APN usage ▪ **VPN configuration** - provides over-the-air VPN connection configuration to company mail servers for predefined groups of users ▪ **Anti-virus application management** - enables the installation, configuration and administration of antivirus applications on mobile devices ▪ **Bluetooth monitor** - blocks Bluetooth connectivity, preventing unauthorized data transfer

- **Certificate management** - a unique system that uses individual certificates for each device, with a remote invalidation option. When transferring data between your phone and FAMOC server, the certificate request comes from the device, the key never leaves the device, so it is not possible to impersonate the device by copying the certificate

Data protection & backup

- **Data encryption** - encrypts all drives on the devices, including removable media, preventing data to be removed from the device
- **Data security management** – improves email security, prevents messages being moved, blocks the use of 3rd party email account, automatically rejects untrusted certificates, manages application installer, enforces password for iTunes, controls iCloud
- **Password policies** - remotely enforces password protection, defining complexity and the regularity of changes
- **Auto-lock** - ensures the user is automatically logged out, or the phone is locked, after a specified period of inactivity
- **Data backup/restore** - enables automated and encrypted backup sessions to be performed, with cross-platform data restore, eliminating the risk of losing critical data on the handset
- **Data wipe** - automatic full or selective wipe settings for the mobile device and memory card if the device is lost or stolen, or if a wrong password is entered, or if the SIM card is changed (even with no Internet connectivity)

Data access control

- **Containerization & BYOD** – provides a clear distinction between corporate and privately owned devices with separate policies based on the ownership of the device
- **Access rules for specific groups or departments** - predefines user profiles, loads sets of shared data for different work groups
- **Exchange Proxy** – real-time EAS traffic control between mobile device and Exchange server with automatic access denial for devices that are:
    - Lost / stolen
    - Not reporting to the server for a predefined period of time
    - Not in compliance with the policy (e.g. contain a blacklisted application)
- **Application password protection** - empowers administrator to block access to an application with a lock code or administrator password, offers challenge response authentication for application access (on-mobile token)
- **Secure access to corporate file server via SecureSource** – enables iPad users to securely access documents that are stored on the corporate server. With SecureSource, documents are only available in the mobile device's temporary memory during the session, and all documents are automatically wiped from memory when connection is terminated. No traces of documents are available on the device, therefore if the device is lost or stolen there is no risk of data leakage. In addition, the entire communication and file access trail is logged for audit purposes.

User restrictions

- **Installation restrictions** - ensures that employees aren't installing inappropriate or unsafe applications, or uninstalling business critical applications or data
- **Application blacklist** - manages lists of forbidden applications for download, preventing the mobile phone coming under attack from malware, spyware or viruses
- **Device functionality restrictions** – sets restrictions around the use of mobile device applications, such as use of the web browser, or the phone's camera

Real-time monitoring and alerts

- **Instant alerting in case of security threats:**
    - SIM card change
    - Devices nor connected to server
    - Stolen/lost devices
    - Breaks in regular backup
    - Jailbreak
- **Instant reaction when security is breached:**
    - Remotely lock device
    - Automatically wipe on X password attempts or SIM change
    - Identify device location