FancyFon

Enhanced management of Samsung Android devices

With Android-powered smartphones and tablets spreading across enterprise mobile eco-systems, it is crucial to ensure simple enrollment, secure access to corporate data and real-time control over devices connecting to business network.

FAMOC is a complete mobility management solution for enterprise deployed android devices, across any device OS, model and manufacturer. The solution provides market's most advance management capabilities, ensuring automate infrastructure inventory, application and content management, bulk device configuration, BYOD support, efficient data protection, policy enforcement, secure email through 3rd party solutions and compliance tracking. FAMOC leverages the generic Android capabilities, as well as Samsung specific Enterprise APIs, to provide a more comprehensive, secure and feature-rich management.

Samsung SAFE device management feature guide

Perform simple, over-the-air, bulk device enrollment

- Seamlessly synchronize FAMOC with internal corporate infrastructure – use directory services, bulk imports, external server synchronization and FAMOC API
- Remotely provision FAMOC client components and automatically collect device data within a few minutes
- Allow end-user self enrollment

Remotely configure devices and set useful enterprise tools limiting end-user effort

- Set VPN, WiFi and connectivity
- Set data and common resources synchronization(email, calendar, business phonebook)
- Configure email clients (both native and 3rd party, such as NitroDesk Touchdown)

Manage applications

- Create a custom app catalogue with publicly available and in-house business apps
- Offer a one-click installation or push apps directly to device without user interaction
- Get insight into applications installed and track software version
- Define application policy (whitelist or blacklist)
- Remotely remove software

Use 24/7 automate compliance monitoring

- Set alerts for specific events such as malware reporting
- Automatically lock access to incompliant devices/disable their access to enterprise services
- Set automated actions for policy incompliance accordingly to your specific business needs e.g. wipe on SIM card change
- Send your users info on how to be compliant
- If necessary wipe the device in case user does not response

Enforce efficient security policy

- Use device level and SD card encryption
- Configure VPN manage network access policies
- Disable native or third party browsers
- Set Exchange ActiveSync policies
- Install and manage unique user certificates
- Require strong password and auto-lock policy
- Protect application access through password
- Deploy a number of device restrictions (roaming policies, system apps, camera, Bluetooth, Google Play Store)
- Perform encrypted backup of contacts, SMS messages and files and cross-platform data restore

Lock down smartphones or tablets into a KIOSK mode

- Restrict users to allowed applications only
- Block users from playing games, browsing or installing unapproved applications
- Lock access to certain device features and settings
- Block users from accessing default home screen
- Show or hide widgets on home screen
- Create custom layout on home screen, brand background wallpaper and display custom icons for allowed apps
- Limit device features to a secure web browser
- Turn consumer tablets into secure interfaces for customers in retail spaces
- Securely lock the device with a password, set inactivity timeout

Remotely access device for troubleshooting

- Access device's touchscreen and keypad over-the-internet –view device emulation
- Browse and manage files, applications or configurations
- Get visibility into ongoing processes

Be prepared for BYOD

The bring-your-own-device movement has significant productivity, convenience and cost benefits, but it is leading to serious challenges for IT administrators. Giving your employees access to corporate resources via their personal

- Android devices can be an extremely risky issue.
- Do your employees use passcodes and auto-lock?
- Can you control apps being downloaded to devices?
- Can you prevent employees accessing SalesForce using an unsecure WiFi?
- Can you protect your employee’s device from being hacked?
- What happens if a CFO leaves his tablet at Starbucks?
- What happens if an employee leaves the organization, having used their personal devices to store corporate data?

This is a whole host of new challenges for the IT department to address. Moreover, a well-crafted BYOD policy is not only about protecting corporate data and meeting proper regulations, but also about ensuring the privacy of personal information. FAMOC offers a complete mobile device management with intelligent BYOD support. With FAMOC you are able to have a clear distinction between corporate and privately owned devices and set separate policies based on device ownership.

Corporate-owned device

- Isolate corporate data through:
  - Apps containerization
  - ActiveSync
  - Connectivity settings
  - VPN configuration
- Secure apps with passwords or tokens
- Be aware of apps accessing corporate data
- Restrict device features
- Act silently in the device (add or remove apps, disable AppStore, prevent required apps uninstallation, silently remote blacklisted apps)
- Lock access for incompliant devices
- Wipe the device clean when security

Employee-owned device

- Protect private data:
  - Mobile banking
  - Social networks
  - Healthcare apps
  - Private gaming
  - Private email, contact, calendar
  - Family photos
- Install and managecorporate apps only
- Set policies that do not restrict application installation but which alertthe administrator in case of a threat to corporate data
- In case of security breach, perform a selective wipe functionality, deleting only the corporate data