Bittium SafeMove® for Android™

Secure Mobility Management Software

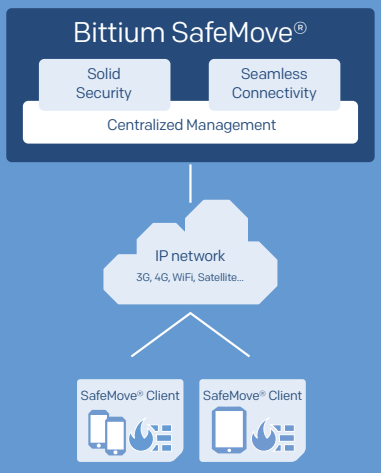
Bittium SafeMove® for Android™ is a secure mobility management software for Android devices. The unique always-on features of the software maintain a working, secure connection to your organization's network resources at all times, and the IPsec VPN ensures that all connections are strongly authenticated and all traffic is encrypted using industry standard encryption and best practice policies. The software also provides a wide range of mobile device management capabilities.

The enrollment of the software on the device fleet has been streamlined with QR codes, and using the software requires as little action from the user as possible. It is the natural choice for mobile workforces for example in corporations, government, public safety, field services and healthcare to enable constant, secure connections to protected network resources.

FOR MORE INFORMATION, PLEASE CONTACT:
safemove.sales@bittium.com

Benefits

- Secured network traffic with Bittium SafeMove® Mobile VPN
- Efficient control over device fleet with Mobile Device Management feature
- Always-on & easy to use
- Streamlined enrollment of device fleet with QR code
- Undeniable audit trail from devices and server components
- Secure delivery in private closed networks as well as in public networks



Bittium SafeMove® for Android™
Technical Specifications

Top-class security: Bittium SafeMove relies on established industry standards and best practices to build a solid security architecture. IPsec provides strong authentication and encryption of all network traffic. The automatic, always-on nature minimizes the risk of user error. Device security policies can be managed centrally and enforced on the device.

Easy provisioning, management and monitoring: Initial configuration and certificate enrollment can be done easily with a QR code. The Bittium SafeMove Manager web UI can be used to manage and monitor the device fleet, and to provision configuration changes over-the-air. Device connectivity data can be optionally collected and delivered to the Bittium SafeMove® Analytics for detailed reporting and analysis.

Mobile VPN Features

- IPsec, IKEv2 MOBIKE
- Integrated firewall and IPsec policy
- Always-on, cannot be bypassed by apps or user
- Per-App VPN
- Extensively tested and externally audited code base

Mobile VPN Crypto

- CNSA/NSA suite B compatible
- SHA2-512
- AES-256, SERPENT
- Elliptic curve cryptography:
  - ECDH groups 19,20, 21 (NIST) and 27,28,29 and 30 for IKEv2 (Brainpool)
  - ECDSA certificates
- RSA keys up to 16k
- Hardware accelarated crypto

Mobile Device Management

Centralized, remote management of mobile devices and Android security features from the server.

- Either as private standalone or Android Enterprise (Google Cloud) solution
- Mass provisioning by operators, or self-provisioning by end users
- Security dashboard
- Locate device on map
- Remote policy update (push)
- Remote wipe, lock, and password change
- Manage trusted CA certificates
- SafeMove VPN policy management
- Device history and audit logs
- Wi-Fi management: SSID configuration, security policy, and credentials

Device Policy

All controls supported by Android are supported by SafeMove, inluding:

- Device lock password policy:
  - Numerical, alphanumeric, complex
  - Password length
- Device wipe after failed password entry
- Device lock timeout
- Password expiration time
- Enable/disable:
  - Software from untrusted sources
  - Android Debugging Bridge (ADB)
  - Developer settings
  - Bluetooth
  - Camera
  - Location services
  - Volume adjustment
  - Application settings control
  - Cell broadcasts
  - Configuration of device credentials
  - Configuration of mobile networks
  - Tethering
  - Configuration of VPN
  - Configuration of WiFi
  - User-initiated factory reset
  - Apps installation and uninstallation
  - Modify accounts
  - Mount external physical media (USB, SD card)
  - User-initiated network settings reset
  - Outgoing NFC beam
  - Outgoing calls
  - SMS
  - Microphone volume adjustment
  - USB file transfer

Mobile Application Management

- Managed private application library from Bittium
- Managed public application library from Google Play
- Configuration of 3rd party apps (Android managed configurations)
- Application install base kept up-to-date with new versions and security fixes

Log Server & Visualization

- Visual log analytics for efficient incident response and even proactive incident avoidance
- Collecting and analyzing log data for keeping administrators up-to-date on what happens on device and infrastructure side
- Integrates with Bittium SafeMove® Analytics (optional)

Secure Push Messaging

Secure and scalable push system that can be easily implemented in apps. Familiar API, similar to common cloud messaging systems.

- Low power requirements
- Low latency
- Low bandwidth
- Can be hosted on customer premises
- TLS security and optionally VPN

Supported Server Platforms

- Virtualized server appliance
- BIttium SafeMove® server appliances
- Red Hat® Enterprise Linux® 8 certified server hardware
- Microsoft Azure, AWS, common cloud and virtualization platforms

Supported Android Versions

SafeMove supports all current Android versions starting from Android 10.

Older Android versions may not be available via Google Play.

Bittium • Ritaharjuntie 1, FI-90590 Oulu, Finland • Tel. +358 40 344 2000 • **www.bittium.com**