BITTIUM SAFEMOVE® EMM

Comprehensive Mobility Management Solution

Bittium SafeMove® EMM is a comprehensive mobility management solution designed for security-critical environments. It combines secure connectivity, device management, and identity protection into one easy-to-use platform. SafeMove EMM provides multi-platform support and flexible deployment, even in private networks, where everything is in your control.

Operate and control all the SafeMove services on your secure premises, or use a trusted operator to host the services. Single step provisioning and self-service portal enable easy enrollment in large-scale organizations.

Together with Tough Mobile smartphones, SafeMove forms the world's most secure mobile communication solution that has been approved up to CONFIDENTIAL (NCSA-FI, TL III) and NATO RESTRICTED level communications.

For more information, please contact:
secure@bittium.com

Multi-platform support

Android™, iOS, Microsoft Windows, Tough Mobile, software routers

Always up-to-date

Firmware and application updates delivered over-the-air

Approved applications only

Android Enterprise or in-house enterprise app library for mobile application management

Unified, security-driven control over entire device fleet

With Mobile Device Management feature

No data leaks

Access to services granted only for devices that have been remotely attested for integrity

For private and closed networks

Secure push messaging to devices without the risk of public clouds

Undeniable audit trail from devices

Audit trail from devices and server components with Log Serverthat have been remotely attested for integrity

Bittium
DEFENCE & SECURITY

Mobile VPN profile management

- IPsec, ML-KEM (Android), IKEv2 MOBIKE
- Integrated firewall and IPsec policy
- Always-on, cannot be bypassed by apps or user
- Require successful remote attestation for VPN access
- Per-app and per-container VPN
- Extensively tested and externally audited code base
- VPN tunnel for USB tethered traffic

Mobile device management (Android)

- Remote policy update (push)
- Remote wipe, lock and password change
- Manage trusted CA certificates
- Factory reset protection
- Android Enterprise support
- SafeMove VPN policy management
- Device history and audit logs
- Wi-Fi management: SSID configuration, security policy and credentials
- Always-on security monitoring
- Seamless enrollment process: mass provisioning by operators, or self-provisioning by end users

Device policy (Android)

- Device lock password policy:
  - Numerical, alphanumeric, complex
  - Password length
- Altogether, it is possible to control a total of 100+ parameters
- Device wipe after failed password entry
- Device lock timeout
- Password expiration time
- Wallpaper and owner info management
- Enable/disable:
  - Software from untrusted sources
  - Android Debugging Bridge (ADB)
  - Developer settings
  - Bluetooth
  - Camera
  - MMS send and receive
  - Location services
  - iZat (Qualcomm AGPS)
  - Android connectivity check
  - 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
- USB whitelist

Mobile application management

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

Bittium SafeMove® Comms account management

- Determine which users have the possibility to use the communication software
- Add, modify, and revoke users
- Assign specific embedded contact directories

Certificate authority (CA)

- Includes production grade CA system
- EST and SCEP protocols for certificate enrollment to devices
- Automatic over-the-air renewal of certificates
- Integration with external CA systemsE-compass

Log server and 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)
- Volume up and down

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(Gorilla® Glass Victus® 2)

Supported server platforms

- SafeMove Server Appliance
- VMware virtual appliance
- Common cloud and virtualization platforms

Supported client platforms

- Android 11 onwards
- Microsoft Windows 11 onwards
- iOS readiness by the end of 2026

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

Bittium
DEFENCE & SECURITY