BMC Mobile Device Management

Securely manage the mobile device lifecycle from a single console — regardless of device type or mobile operating system

Flexible Delivery

» **On-premise —** BMC Mobile Device Management can be deployed, managed and maintained on-premise using dedicated hardware or virtualized environments. This delivery method provides the most control, flexibility, scalability, and integration with enterprise systems.

» **Software as a Service (SaaS) —** BMC Mobile Device Management is available in both a shared hosted or dedicated hosted environment for enterprises deploying SaaS. BMC Mobile Device Management leverages multiple redundant data centers, best-in-class hardware, high availability and an US-based network operations center to support its SaaS customers.

As advanced mobile devices and applications become critical to an organization's success, IT is challenged with efficiently managing the full lifecycle management of devices across the enterprise. BMC Mobile Device Management provides IT organizations the control they need to securely manage mobile devices throughout their entire lifecycle, simplifying these processes across multiple device types and mobile operating systems in a single console. With discovery, configuration, apps, and policy management, organizations now have the peace of mind that their mobile devices, critical data, and networks are secure from potential threats.

Mobile Device Lifecycle Management

Deploy

» Activate devices using SMS, email, URL, and other flexible options

» Enroll corporate and employee-liable devices individually or in scale

» Authenticate users and devices through basic and directory-services-based authentication

» Instantly configure policies, settings, certificates, and access to enterprise accounts over the air

» Wirelessly provision internal and recommended apps through the enterprise app catalog

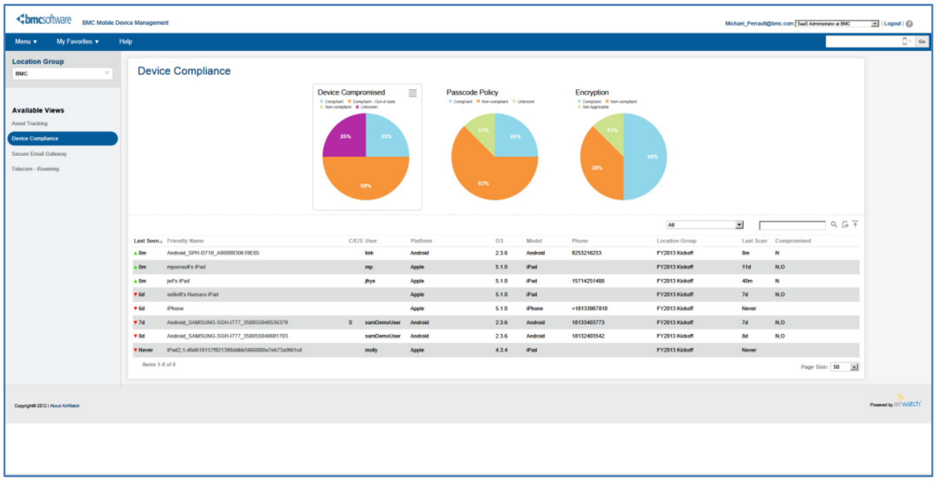
Secure

» Protect personal and corporate data and the entire device through encryption and passcode policies

» Prevent unauthorized device use by locking down device features and enforcing restrictions

» Audit devices for compliance with corporate policies, settings, applications, third parties, and more

» Automate business policies for non-compliant or jail-broken devices



Last Seen	Friendly Name	C/E/S	User	Platform	OS	Model	Phone	Location Group	Last Scan	Compromised
▲ 8m	Android_SPH-D710_A0000030619E85		kirk	Android	2.3.6	Android	9253216253	FY2013 Kickoff	8m	N
▲ 8m	mperrault's iPad		mp	Apple	5.1.0	iPad		FY2013 Kickoff	11d	N,O
▲ 8m	jwf's iPad		jfrye	Apple	5.1.0	iPad	15714251488	FY2013 Kickoff	40m	N
▼ 6d	selliott's Numara iPad			Apple	5.1.0	iPad		FY2013 Kickoff	7d	N,O
▼ 6d	iPhone			Apple	5.1.0	iPhone	+18133907810	FY2013 Kickoff	Never	
▼ 7d	Android_SAMSUNG-SGH-I777_358055040536379	S	samDemoUser	Android	2.3.6	Android	18133403773	FY2013 Kickoff	7d	N,O
▼ 8d	Android_SAMSUNG-SGH-I777_358055040691703		samDemoUser	Android	2.3.6	Android	18132403542	FY2013 Kickoff	8d	N,O
▼ Never	iPad2,1-d6d618157f921398ddbb5666880a7eb73a9fd1cd		molly	Apple	4.3.4	iPad		FY2013 Kickoff	Never	

Items 1-8 of 8

Copyright© 2012 | About AirWatch

Figure 1. Compliance dashboard

Key Differentiators

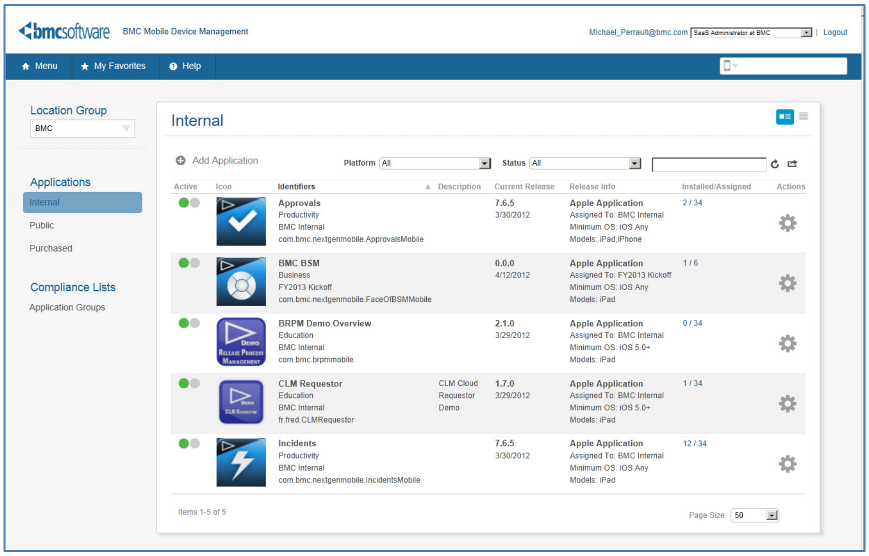
- Cross-platform solution
- Highly scalable
- Secure role-based access
- Secure email gateway
- Multi-lingual console
- SDK developer toolkit
- Mobile telecom management
- Web-based (HTML 5) console
- Multi-tenant architecture
- Enterprise app catalog
- Enterprise integration
- Robust reporting
- Intelligent notifications

Monitor

- Monitor devices, as well as network health status and statistics, for exceptions
- Track user activity, such as app downloads, voice, SMS, and data usage, against pre-defined thresholds or white or black lists
- Monitor system access and console user activity through detailed event logs
- Set up alerts and automated business rules for specific device or network actions, user actions, or system performance
- Generate actionable reports with automated distribution across the IT team

Manage

- Streamline and automate mobile asset and inventory management
- Update and provision new policies, settings, certificates, apps, software, and access to enterprise accounts — Exchange Active Sync, Wi-Fi, VPN, CA, LDAP, and more — over the air
- Push down configuration profiles, apps, software, or remote lock/wipe commands on demand, at a scheduled time or the next time a device or group of devices checks in



Internal

Active	Icon	Identifiers	Description	Current Release	Release Info	Installed/Assigned	Actions
●●		Approvals Productivity BMC Internal com.bmc.nextgenmobile.ApprovalsMobile		7.6.5 3/30/2012	Apple Application Assigned To: BMC Internal Minimum OS: iOS Any Models: iPad,iPhone	2 / 34	⚙
●●		BMC BSM Business FY2013 Kickoff com.bmc.nextgenmobile.FaceOfBSMMobile		0.0.0 4/12/2012	Apple Application Assigned To: FY2013 Kickoff Minimum OS: iOS Any Models: iPad	1 / 6	⚙
●●		BRPM Demo Overview Education BMC Internal com.bmc.brpmmobile		2.1.0 3/29/2012	Apple Application Assigned To: BMC Internal Minimum OS: iOS 5.0+ Models: iPad	0 / 34	⚙
●●		CLM Requestor Education BMC Internal fr.fred.CLMRequestor	CLM Cloud Requestor Demo	1.7.0 3/29/2012	Apple Application Assigned To: BMC Internal Minimum OS: iOS 5.0+ Models: iPad	1 / 34	⚙
●●		Incidents Productivity BMC Internal com.bmc.nextgenmobile.IncidentsMobile		7.6.5 3/30/2012	Apple Application Assigned To: BMC Internal Minimum OS: iOS Any Models: iPad	12 / 34	⚙

Items 1-5 of 5

Figure 2. Sample Administrator Console view

Support

- Perform device diagnostics remotely to identify issues
- Provide remote assistance to mobile users and communicate from the console via SMS messaging
- Take remote control of a device for more efficient troubleshooting
- Provide users with remote management capabilities through a self-service portal
- Manage troubleshooting cases and system incidents using an integrated case management system

Retire

- Remotely wipe corporate data from personal mobile devices to ensure security and integrity of corporate data
- Revoke network and email access for devices owned by employees leaving or no longer with the organization
- Wipe corporate data from mobile devices to be removed from service and, if requested for an employee-owned device, wipe all data to restore device to original factory settings

Figure 3. Securely manage the mobile device lifecycle— regardless of device type or mobile OS

Why BMC Mobile Device Management

- **Cross-platform solution** — BMC Mobile Device Management is the industry's most comprehensive solution for the enterprise. With BMC Mobile Device Management, IT administrators can centrally deploy, secure, monitor, manage, support, and retire corporate and employee-liable mobile devices across all major operating systems.
- **Highly scalable** —BMC Mobile Device Management is designed to support an unlimited number of devices and mobile data. Leveraging enterprise-class servers in state-of-the-art, highly secure data centers, BMC Mobile Device Management scales quickly and efficiently as your mobility initiatives expand.
- **Secure role-based access** — BMC Mobile Device Management secures console access using custom roles integrated with enterprise Directory Services. A user's role can be tied to a specific device group (tier) and defines the capabilities available to that user. BMC Mobile Device Management provides a detailed audit trail of users accessing the system and of events and actions taking place.
- **Secure Email Gateway** — The secure email gateway monitors every device interaction with your corporate email infrastructure to identify any exceptions or threats. Its flexible rules engine allows or blocks devices using white lists and black lists or manually based on exceptions.
- **Multi-lingual console** — BMC Mobile Device Management enables global enterprises to set a preferred language at the location group level and even edit fields within the application with custom values.
- **SDK developer toolkit** — BMC Mobile Device Management offers the industry's most developed SDK library for building secure enterprise apps featuring advanced MDM capabilities.
- **Mobile telecom management** — BMC Mobile Device Management enables companies to reduce wireless expenses through real-time monitoring and alerting of roaming status across iOS devices, regardless of carrier or location.
- **Web-based (HTML 5) console** — The BMC Mobile Device Management console is accessible over the web and optimized for PC or tablet browsers. BMC Mobile Device Management leverages the latest HTML 5 standards to provide an intuitive user interface with customizable branding and dashboards, advanced filters, searches, and fast data processing.
- **Multi-tenant architecture** — The BMC Mobile Device Management solution's multi-tenant architecture allows for one instance of the software to support multiple organizations (tenants) or groups within a large organization. Each tier (tenant) provides an additional layer of security, configuration, customization, and access control.

- **Enterprise app catalog** — BMC Mobile Device Management enables IT administrators to centrally deploy, manage, and secure internal and public apps using a custom app catalog. Only compliant users can view, download, and update enterprise apps, as well as access purchased, recommended, and blacklisted public apps in iTunes.
- **Enterprise integration** — BMC Mobile Device Management provides seamless integration with key enterprise systems, such as SCEP, PKI (CA), Directory Services, email, and VPN, to enable companies to leverage existing data to manage users and devices. BMC Mobile Device Management offers its own APIs for additional integration of data across BI tools and other enterprise systems.
- **Robust reporting** — BMC Mobile Device Management generates actionable, results-oriented reports and provides automated distribution to IT-defined lists. Enterprises can choose from the solution’s extensive library of 100+ reports and customize reports based on specific data elements captured in the system.
- **Intelligent notifications** — BMC Mobile Device Management notifies IT departments when a pre-defined incident occurs via email, text, or dashboard message. To minimize impact on IT operations, BMC Mobile Device Management can be configured with business rules to proactively respond to specific incidents affecting security or compliance.

For More Information

To learn more about BMC MDM, please visit www.komputerkraft.co.nz/kkc-products/bmc-mobile-device-management

Komputer Kraft Consulting
Australian Office
(07) 3103 2231 or 0451 832 544
Email: info@kkc.net.au
Web: www.kkc.net.au

Komputer Kraft Consulting
New Zealand Office
(09) 889 4290
Email: info@kkc.co.nz
Web: www.kkc.co.nz

Komputer Kraft Consulting

powered by airwatch™

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC SOFTWARE.

Business runs better when IT runs at its best. That's why more than 25,000 IT organizations – from the Global 100 to the smallest businesses – in over 120 countries rely on BMC Software to manage their business services and applications across distributed, mainframe, virtual and cloud environments. With the leading Business Service Management platform, Cloud Management, and the industry’s broadest choice of IT management solutions, BMC helps customers cut costs, reduce risk and achieve business objectives. For the four fiscal quarters ended March 31, 2012, BMC revenue was approximately $2.2 billion.

bmcsoftware
BUSINESS RUNS ON I.T.™