BLACKBERRY KEEPS YOUR BUSINESS MOVING

With the growing diversity of mobile devices and platforms in the workplace, a multitude of security requirements and the rise in mobile app use, there are significant challenges ahead. The need? A new approach that embraces Enterprise mobility Management (EMM). Introducing BlackBerry® Enterprise Service 10.

BlackBerry® is re-inventing Enterprise Mobility Management by bringing together:

Device management
BlackBerry enables enterprises to manage complex fleets of mobile devices

Security
BlackBerry is the gold standard for secure end-to-end mobility

Unified communications
BlackBerry enables a truly integrated voice, messaging, PIM, apps and social experience built for business users

Applications
BlackBerry® 10 delivers a comprehensive business and productivity app portfolio, an enterprise-grade app management framework and a low-cost app development environment

What's included with BlackBerry Enterprise Service 10

- A single intuitive management console to manage your devices, users, groups, apps and services
- Full Mobile Device Management (MDM) for BlackBerry 10 smartphones, BlackBerry® PlayBook™, iOS® and Android™ devices
- BlackBerry® Balance™ technology, providing a secure Work Space and Personal Space on BlackBerry 10 devices
- BlackBerry® World™ for Work: a fully integrated corporate app storefront
- Ability to manage instances of BlackBerry® Enterprise Server 5.0.3 and above through the BlackBerry Enterprise Service 10 management console

Satisfy the full range of security needs; from a basic level up to the high levels of security required by government and regulated industries

EMM service level requirement	Type of enterprise					
	Open	Managed for some	Managed for all	Segmented	Locked down and managed mix	100% locked down
Advanced Enterprise Mobility Management				■	■	■
Enterprise Mobility Management		■	■	■	■	
Basic Mobility Management (ActiveSync™)	■	■		■		
	Small to Medium Business with no company policy.	**Small & Medium Business** that do not require locked-down devices.	**Large & Medium Enterprises** that do not require locked-down devices.	**Large Enterprises** with different levels of device management.	**Large Enterprises** that are security sensitive.	**Government and regulated industries**

BlackBerry

BlackBerry Balance
BlackBerry Balance technology gives users the freedom and privacy they want for their personal use while delivering the security and management organizations need. It's the best of both worlds, seamlessly built into every BlackBerry 10 smartphone and managed through BlackBerry Enterprise Service 10.

Personal and work apps and information are kept separate, and the user can switch from their Personal Space to their Work Space with a simple gesture. The Work Space is fully encrypted, managed and secured, enabling organizations to protect critical content and applications, while at the same time letting users get the most out of their smartphone for their personal use.

BlackBerry World for Work
Enabled seamlessly through BlackBerry Balance, businesses can easily manage and curate a corporate app storefront (BlackBerry World for Work) within the Work Space to push and install mandatory apps & publish recommended apps to both corporate and BYOD users.

With BlackBerry Balance enabled, BlackBerry 10 users can still access and download great apps, games, video and music through BlackBerry World and keep it in their Personal Space, safe and separate from their work life.

BlackBerry Enterprise Service 10 – Enterprise Mobility Management, implemented as either:

Basic Mobility Management:
Basic device control via ActiveSync™.
Available at launch
For those users in roles or environments where little device management or security is required, BlackBerry 10 smartphones support ActiveSync™ as standard. Both corporate and personal-owned BlackBerry 10 smartphones can be quickly setup to synchronize email, calendar, tasks and contacts with Microsoft® Exchange and other on-premise and cloud messaging platforms that support the ActiveSync™ protocols.

Enterprise Mobility Management:
Device management, security and application management for BlackBerry (inc. BlackBerry Balance technology), iOS® and Android™ devices.
Available at launch
Device management and security for corporate and personal-owned BlackBerry OS, BlackBerry 10, iOS® and Android™ devices. BlackBerry Enterprise Service 10 gives you proven BlackBerry device management capabilities, along with rich management control through a single, easy to use administration console.

The evolution of BlackBerry Enterprise Server (BES) makes it easy to upgrade your existing BES infrastructure to add robust BlackBerry 10, iOS®, and Android™ smartphones and tablet management.

Advanced Enterprise Mobility Management:
The highest security and control for BlackBerry 10 devices.
Available in Q2 2013
Stay secure. Advanced Enterprise Mobility Management control options are available for BlackBerry 10 smartphones to enable compliance for government and regulated environments. Where a high degree of granular control over device features is required and for enterprises where strict corporate-only use and application restriction policies are in place, BlackBerry 10 smartphones and BlackBerry Enterprise Service 10 combine to provide the ultimate device management solution for high-security mobility.

BlackBerry 10 Enterprise Mobility Management

Password

Password Required for Device
Specify whether a BlackBerry device requires a password that protects both the personal and work spaces on the device.

Minimum Password Length
Specify the minimum length of the password on a BlackBerry device.

Security Timeout
Specify the maximum number of minutes of BlackBerry device user inactivity that can elapse before a BlackBerry device locks.

Maximum password age
Specify the maximum number of days that can elapse before a BlackBerry device password expires and a BlackBerry device user must set a new password.

Minimum Password Complexity
Specify the minimum complexity of the password on the BlackBerry device.

Maximum Password Attempts
Specify the number of times that a BlackBerry device user can attempt an incorrect password before a BlackBerry device deletes the data in the Work Space.

Maximum Password History
Specify the maximum number of previous passwords that a BlackBerry device checks to prevent a BlackBerry device user from reusing a previous password.

Password Required for Work Space
Specify whether a BlackBerry device requires a password for the Work Space.

General

Mobile hotspot mode and tethering
Specify whether to allow Mobile Hotspot mode, tethering using Bluetooth technology, and tethering using a USB cable on a BlackBerry device.

Plans application
Specify whether the Plans app can run on a BlackBerry device. You can use this rule to prevent users from buying wireless service plans that are available from the Plans app.

Wireless Service Provider Billing
Specify whether a BlackBerry device user can purchase applications from the BlackBerry App World storefront using the purchasing plan for your organization's wireless service provider.

Security

Wipe the Work Space without Network Connectivity
Specify the time in hours that must elapse without a BlackBerry device connecting to your organization's network before the device deletes the data in the work space.

Restrict development mode
Specify whether development mode is restricted for BlackBerry device users. Development mode allows software development tools to connect to a device and also allows you or a user to install applications directly on the device using a USB or Wi-Fi connection.

Voice control
Specify whether a BlackBerry device user can use the voice control commands on a BlackBerry device.

Voice dictation in work apps
Specify whether a BlackBerry device user can use voice dictation in work apps.

Voice dictation
Specify whether a BlackBerry device user can use voice dictation on a device.

Backup and restore work space using BlackBerry Desktop Software
Specify whether a BlackBerry device user can back up and restore the applications and data that are located in the Work Space of the device using the BlackBerry Desktop Software.

BlackBerry Bridge
Specifies whether a BlackBerry 10 smartphone can use a BlackBerry PlayBook tablet to access work data on the smartphone using the BlackBerry Bridge app.

Computer access to work space
Specify whether a computer can access work files on a BlackBerry device using a USB connection or the file-sharing option with Wi-Fi after the user enters the Work Space password.

Computer Access to Device
Specify whether a computer can access content on a BlackBerry device using a USB connection or the file-sharing option with Wi-Fi.

Personal Space Data Encryption
Specify whether data encryption is turned on for the personal perimeter of a BlackBerry PlayBook tablet.

Network Access Control for Work Applications
Specify whether work applications on a BlackBerry device must connect to your organization's network through BlackBerry Enterprise Service 10.

Personal Applications Access to Work Contacts
Specify whether personal applications (applications that are located in the Personal Space) can access work contacts on a BlackBerry device.

Share Work Data During BBM Video Screen Sharing
Specify whether a BlackBerry device user can share work data (data that is located in the Work Space) on a device using the BBM Video screen sharing option.

Work Domains
Specify a list of domain names that a BlackBerry device identifies as work resources.

Work Network Usage for Personal Applications
Specify whether applications in the Personal Space on a BlackBerry device can use your organization's Wi-Fi or VPN network to connect to the Internet.

Software

Open Work Email Messages links in the personal browser
Specify whether BlackBerry device users can use the browser in the Personal Space to open links in work email messages.

Transfer work contacts using Bluetooth PBAP or HFP
Specify whether a BlackBerry device can send work contacts to another Bluetooth enabled device using the Bluetooth Phone Book Access Profile (PBAP) or Hands-Free Profile (HFP).

Transfer work files using Bluetooth OPP
Specify whether a BlackBerry device can send work files to another Bluetooth enabled or NFC-enabled device using the Bluetooth Object Push Profile (OPP).

Transfer work messages using Bluetooth map
Specify whether a BlackBerry device can send messages from the work perimeter (for example, email messages and instant messages) to another Bluetooth enabled device using the Bluetooth Message Access Profile (MAP).

BBM Video Access to Work Network
Specify whether the Video Chat app on a BlackBerry device can use your organization's Wi-Fi network, VPN network, or the BlackBerry MDS Connection Service for incoming and outgoing video chats.

Logging

Log submission
Specify whether a BlackBerry device can generate and send log files to the BlackBerry Technical Solution Center.

BlackBerry Enterprise Server (BES) management

Ability to manage instances of BlackBerry Enterprise Server 5.0.3 and above through the BlackBerry Enterprise Service 10 management console.

Please note the features mentioned on this page are specific to BlackBerry 10 devices and BlackBerry Enterprise Service 10.

See overleaf for information on device management for corporate and personal-owned iOS® and Android™ devices.

iOS® Enterprise Mobility Management

Browser	Hide the default web browser Disable autofill in the default browser Disable cookies Disable fraud warnings in the default browser Disable JavaScript in the default browser Disable popups in the default browser
Camera and video	Disable output Disable screen capture Hide the default camera application Hide the default video-conferencing application
Certificates	Disable untrusted certificates Disable untrusted certificates after prompt
Cloud service	Disable cloud services Disable cloud backup service Disable cloud document services Disable cloud picture services Disable cloud picture sharing services
Connectivity	Disable network connectivity Disable wireless connectivity Disable roaming Disable data service when roaming Disable background data service when roaming Disable voice service when roaming
Content	Disable content Hide explicit content Maximum allowed rating for applications Maximum allowed rating for movies Maximum allowed rating for TV shows Region that defines the rating restrictions
Diagnostics and usage	Disable submission of device diagnostic logs to device vendor
Messaging	Hide the default messaging application
Online store	Disable online stores Disable purchases in applications Disable storage of online store password Hide the default application store Hide the default book store Disable erotica purchases from the default book store Hide the default music store
Passbook application	Disable Passbook Disable Passbook notifications when device is locked
Password	Define password properties Avoid repetition and simple patterns Require letters Require numbers Require special characters Delete data and applications from the device after incorrect password attempts Device password Enable auto-lock (Time after a device locks that it can be unlocked without a password) Limit password age Limit password history Restrict password length Minimum length for the device password that is allowed
Phone and messaging	Disable voice dialing
Profiles and certificates	Disable interactive installation of profiles and certificates
Social	Disable social applications Disable social gaming Disable adding friends in default social-gaming application Hide multi-player gaming functionality Hide the default social-gaming application Hide the default social-video application
Storage and backup	Disable device backup Require that the device backup data is encrypted
Voice assistant	Disable the default voice assistant application Disable voice assistant application when device is locked

Android™ Enterprise Mobility Management

Camera and video	Hide the default camera application
Password	Define password properties Require letters Require lowercase letters Require numbers Require special characters Require uppercase letters Delete data and applications from the device after incorrect password attempts Device password Enable auto-lock Limit password age Limit password history Restrict password length Minimum length for the device password that is allowed
Encryption	Apply encryption rules Encrypt internal device storage
TouchDown support	BlackBerry Enterprise Service 10 includes TouchDown™ integration, a solution that provides Microsoft Exchange synchronization on the Android™ platform. The integration allows the sending of email profiles to Android™ devices. The BlackBerry Enterprise Service 10 client detects and then automatically configures the TouchDown client on a users phone for use of ActiveSync™ profiles assigned in BlackBerry Enterprise Service 10.

ActiveSync™ Gatekeeping
BlackBerry Enterprise Service 10 can be configured to control the access to Microsoft® Exchange Server 2010 for managed iOS® and Android™ devices. Devices that are managed and in compliance with the policies defined in BlackBerry Enterprise Service 10 are automatically added to the Exchange Mailbox device approved list. Devices that do not comply are blocked from accessing Microsoft® ActiveSync™.

BlackBerry Technical Support Services
Support is a key component of any Enterprise Mobility Management strategy. You need a strategic support partner to ensure you can deliver on your mobility objectives. BlackBerry Technical Support Services provides direct access to our technical experts and tools that help ensure your BlackBerry solution performs at its best. Three levels of support are available together with optional services, giving a wide range of choices to tailor a support package that delivers the level of technical expertise, assistance, response time and resolution time that your business requires. For more information: **blackberry.com/btss**

Keep your business moving:
BlackBerry.com/business

BlackBerry®