BLACKBERRY ENTERPRISE SERVICE 10

Full device management for iOS, Android and BlackBerry

iOS7 and Android 4.3 Now supported

BlackBerry Enterprise Service 10 is a unified multi-OS device, application and content management platform with integrated security and connectivity enabling you to effectively manage complex fleets of mobile devices.

BES10 makes it simple to manage corporate and BYOD iOS, Android™ and BlackBerry users from a single management console.

BlackBerry® simplifies Enterprise Mobility Management by bringing together:

Mobile device management
BES10 provides comprehensive management and security controls for corporate and BYOD iOS, Android and BlackBerry devices

Gold standard mobile security
The trusted BlackBerry® security model now extends to iOS and Android devices to deliver the best protection for work content on device and in transit

Enterprise application management
The easiest way to get apps out to employees. Deploy, manage and secure apps to iOS, Android and BlackBerry users from one unified BES10 console

What's included with BES10

- User-friendly intuitive management console for comprehensive multi-OS device, security and application management
- Ability to separate work and personal content for data leak prevention without any impact on user experience and privacy
- Flexible levels of security to meet evolving business and end user needs
- Advanced application management functionality to deploy and manage applications with ease
- Monitoring and reporting of devices and applications to meet compliance requirements
- Support included as standard to help you deliver more valuable mobile IT

BlackBerry®

BES10 Enterprise Mobility Management, implemented as either:

Full EMM controls and setting to meet the needs of organizations of all sizes

BlackBerry delivers comprehensive device management, security and application management for corporate-owned and BYOD iOS, Android and BlackBerry devices.

Delivered through a single end-to-end platform in BES10, it provides proven security and controls over and above standard ActiveSync capabilities, to organizations of all sizes with mixed mobile environments.

BES10 enables the seamless separation of work and personal content to satisfy both user and corporate needs without compromising on either.

Comprehensive application deployment, management and security provides the ability to push and install mandatory apps & publish recommended apps to users through a corporate app storefront to the Work Space on all managed devices, without impacting their ability to access and use personal apps and content in their Personal Space.

Regulated level EMM controls and settings to meet the needs of secure, government and regulated environments

Ultimate security. Regulated level Enterprise Mobility Management control options are available for iOS, Android and BlackBerry devices to enable compliance for government, regulated and other high-security environments.

Where granular device, content and app control policies are in place for either BYOD or corporate-owned device users, BES10 delivers the ultimate device management solution for high-security mobility.

Specific controls and settings for Regulated EMM can be found in a separate data sheet.

Satisfy the full range of security needs; from full device management to the high levels of security required by government and regulated industries

	EMM service level requirement				
	Managed for some	Managed for all	Segmented	Locked down and managed mix	100% locked down
Regulated level device management			■	■	■
Full device management	■	■	■	■	
Type of enterprise	**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 & regulated industries**

Secure Work Space

Secure Work Space for iOS and Android is a containerization, application-wrapping and secure connectivity option that delivers a higher level of control and security to iOS and Android™ devices, all managed through the BES10 administration console.

Managed applications are secured and separated from personal apps and data, providing an integrated email, calendar and contacts app, an enterprise-level secure browser and secure attachment viewing and editing with Documents To Go.

User authentication is required to access secure apps and work data cannot be shared outside the Secure Work Space.

The trusted BlackBerry security model provides built-in secure connectivity for all enterprise apps deployed to the Secure Work Space – no VPN needed.

BlackBerry Balance

BlackBerry® Balance™ technology gives your employees the freedom and privacy they want for their personal use while delivering the security and management you need for business use. It's the best of both worlds, seamlessly built into every BlackBerry® 10 smartphone and managed through BES10.

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 letting users get the most out of their smartphone for their personal use.

Full BlackBerry device management controls and settings

General

Roaming
Specify whether a BlackBerry device can use data services over the wireless network when the device is roaming.

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.

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.

Password

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.

Apply Work Space password to full device
Specify a single password to be used for both the device and Work Space. The Work Space can still be locked independently of the device.

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.

Development mode Access to Work Space
Specify whether development mode can be used to allow software development tools to connect to the work space on a BlackBerry device using a USB or Wi-Fi connection and install apps directly in the work space.

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.

Smart Card Password Caching
Specify whether a BlackBerry device can cache the smart card password. (Smart Card Reader)

Smart Password Entry
Specify whether the smart card password can be cached.

Lock on Smart Card Removal
Specify whether the BlackBerry device locks when the user removes the smart card from a supported smart card reader or disconnects a supported smart card reader from the BlackBerry device.

Maximum Bluetooth Range
Specify the maximum power range, as a value between 30% (the shortest range) and 100% (the longest range), that the BlackBerry Smart Card Reader uses to send Bluetooth packets.

Minimum PIN Entry Mode
Specify the minimum PIN entry mode required when pairing the BlackBerry Smart Card Reader with a BlackBerry device or computer.

Security Timer Reset
Specify whether apps can reset the security timer on a BlackBerry device to prevent the device from locking after the period of user inactivity that you specify in the Security Timeout rule or the user specifies in the Password Lock settings on the device elapses.

Personal Space Data Encryption
Specify whether data encryption is turned on for the Personal Space 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 the 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 Applications Access to Personal Data
Specify whether work applications on a BlackBerry device can access personal data if a BlackBerry device user permits it.

Work Domains
Specify a list of domain names that a BlackBerry device identifies as work resources. Specific to the Print To Go application only.

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.

Assign Two-Factor Authentication for Work
Specify whether a BlackBerry device user can use two-factor authentication only for Work Space authentication.

Lock Screen Previews of Work Content
Specify whether a BlackBerry device displays lock screen previews of work content when the work space is unlocked in the background.*

IRM-Protected Email Messages
Specify if a BlackBerry device user can read IRM-protected messages.*

Owner Information
Specify the owner information or a disclaimer message on top of the lock screen of a locked device.*

*Requires a BlackBerry 10 device with 10.2.1 device code

Forward or Add Recipients to Private Messages
Specify whether a BlackBerry device user can forward, or add new recipients when replying to, email messages marked as Private.*

External Email Address Warning Message
Specify whether a BlackBerry device displays a warning message when a user attempts to send a work email message to external recipients.*

External Email Domain Allowed List
Specify a list of external email domains that BlackBerry device users can send work email messages to without the device displaying a warning.*

External Email Domain Restricted List
Specify a list of email domains that BlackBerry device users are not allowed to send work email messages to.*

Software

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

Unified View for Work and Personal Accounts and Messages
Specify whether the Messages application on the BlackBerry device displays work and personal accounts and messages together in a single view.

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 Data using NFC
Specify whether a BlackBerry device can send work data to another NFC-enabled device using NFC.

Transfer Work Messages using Bluetooth MAP
Specify whether a BlackBerry device can send messages from the Work Space (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.

Smart Calling Data Analysis
Specify whether a BlackBerry device can send certain contact and device data to BlackBerry for analysis to help the device recommend the best method to call a specified contact at that time based on device and call quality data received from both the user's device and the contact's device.

Logging

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

CCL Data Collection
Specify whether a BlackBerry device allows Context Collection Library (CCL) data collection across all apps.

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.

Full iOS and Android™ device management controls and settings

iOS

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
Disable wireless certificate updates

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
Disable AirDrop
Disable changes to wireless data usage for apps

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

Lock Screen
Hide Today view in lock screen
Hide Notification Center in lock screen
Hide Control Center in lock screen

Security
Disable changes to accounts on the device
Disable Touch ID to unlock device
Limit ad tracking
Limit personal data to personal apps and accounts
Limit work data to work apps and accounts

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 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
Specify 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
Disable changes to Find My Friends settings

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
Hide user-generated content in voice assistant apps

Android

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
Specify minimum length for the device password that is allowed

Encryption
Apply encryption rules
Encrypt internal device storage

TouchDown support
BES10 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 BES10 TouchDown client on a users phone for use of ActiveSync™ profiles assigned in BES10.

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 Techincal Support Services Included as standard when you deploy BES10

Support is a key component of your Enterprise Mobility Management strategy. Implementing BES10 is easier than ever, but having a strategic support partner is still essential to assist you in delivering your mobility objectives. BlackBerry Technical Support Services offers a unique blend of technical expertise, rapid issue resolution and proactive, relationship-based support to help you realise the full potential of your BES10 multi-platform management infrastructure.

BlackBerry Care Support is included as standard when you deploy BES10, providing electronic access to BlackBerry experts for 2 Named Contacts, with a next business day response, as well as access to training, productivity and diagnostic tools. Optional services and higher levels of support are available to tailor a solution that delivers the exact level of technical expertise, assistance, response and guaranteed resolution time that your business requires.

For more information visit blackberry.com/btss

For more information on BlackBerry Enterprise Service 10 please visit: www.BES10.com

BlackBerry