BLACKBERRY ENTERPRISE SERVICE 10

Corporate-level device management for BlackBerry, iOS and Android

Corporate-level Enterprise Mobility Management (EMM) delivers comprehensive device management, security and application management for corporate and personal-owned BlackBerry, iOS and Android devices. Delivered through a single end-to-end platform in BlackBerry Enterprise Service 10, it provides proven BlackBerry security and controls designed to meet the needs of organizations of all sizes.

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 and Corporate-level EMM

- Complimentary BlackBerry Support providing 12x5 telephone access to technical experts, responsive online support, access to training, productivity and diagnostic tools
- A single intuitive management console to manage your devices, users, groups, apps and services including reporting and dashboard capabilities
- 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 & above through the BlackBerry Enterprise Service 10 management console

BlackBerry

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

Basic Mobility Management (ActiveSync™ only):

Basic device control via ActiveSync™.

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 set up to synchronize email, calendar, tasks and contacts with Microsoft® Exchange and other on-premise and cloud messaging platforms that support the ActiveSync™ protocols.

Corporate-level Enterprise Mobility Management:

Device management, security and application management for BlackBerry (inc. BlackBerry Balance), iOS and Android™ devices.

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™ smartphone and tablet management.

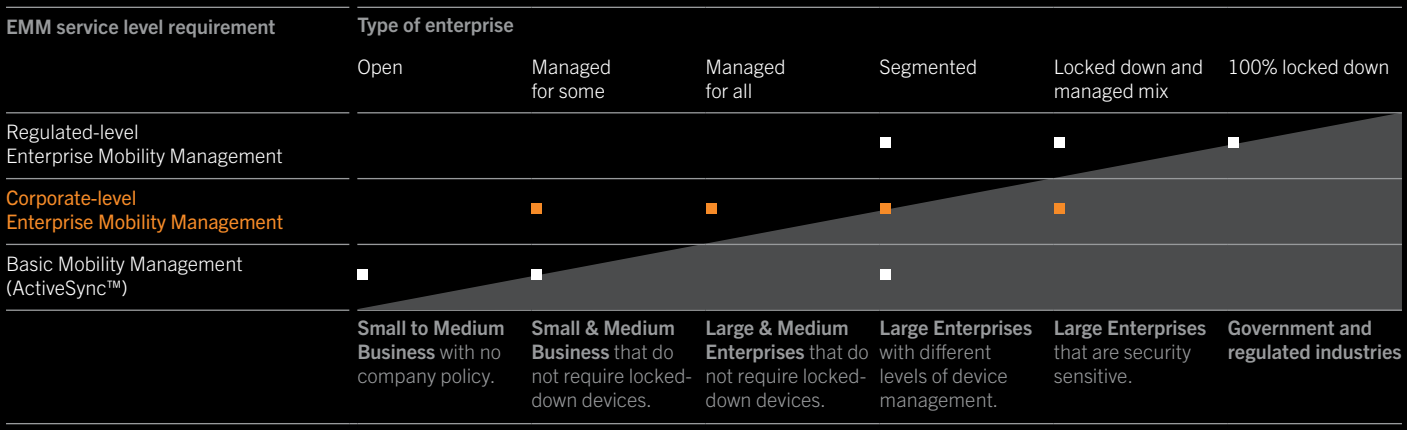
Regulated-level Enterprise Mobility Management:

The highest level of security and control for BlackBerry 10 devices.

Regulated-level Enterprise Mobility Management control options are available for BlackBerry® 10 smartphones to enable compliance for secure, government and regulated environments. Where a high degree of granular control over device features is required and for enterprises where corporate-only use and application management policies are in place. BlackBerry 10 smartphones and BlackBerry Enterprise Service 10 combine to provide the ultimate device management solution for high-security mobility.

For more information on EMM capabilities for secure, government and regulated environments please read the BlackBerry Regulated-level Enterprise Mobility Management Datasheet.

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



Get BlackBerry 10 Ready

Getting up and running with BlackBerry 10 and BlackBerry Enterprise Service 10 is fast and straightforward. Importantly, it does not impact your existing BlackBerry Enterprise Server infrastructure.

Step 1:

Download BlackBerry Enterprise Service 10 for free at **BES10.com**

Step 2:

Transfer existing BlackBerry Enterprise Server Client Access Licenses (CAL) to BES10 CALs for managing BlackBerry 10 devices at no additional cost. Go to **blackberry.com/blackberry10ready**

Purchase new BES10 CALs for additional BlackBerry 10, iOS and Android devices from your preferred partner.

Step 3:

Connect new BlackBerry 10 devices to BlackBerry Enterprise Service 10. You can continue to manage existing BlackBerry OS devices connected to BlackBerry Enterprise Server 5.0.3 and above, alongside BlackBerry 10 devices, through the centralized BlackBerry Enterprise Service 10 management console.

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
Through BlackBerry® Enterprise Service 10, businesses can seamlessly manage and curate a corporate app storefront (BlackBerry World for Work) within the BlackBerry® Balance™ 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 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.

Corporate-level Enterprise Mobility Management BlackBerry 10 Controls and Settings

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.

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.

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

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.

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.

WebGL - BlackBerry PlayBook Only
Specify whether a BlackBerry PlayBook Tablet can use WebGL in the browser.

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.

Computer Access to Work Space
Specify when 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.

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.

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.

Personal Applications Access to Work Contacts
Specify whether personal apps can access specific data for work contacts on a BlackBerry device.

Personal Apps Access to Work Contacts when Work Space is Locked
Specify whether personal apps that can access specific data from work contacts can access that data when the Work Space is locked.

Work Data Uses Only Work Network
Specify whether a BlackBerry device must route work data traffic through a work VPN or work Wi-Fi connection.

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 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.

Cloud Storage Access from Work Space
Specify whether BlackBerry cloud storage applications are available in the Work Space.

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.

Corporate-level Enterprise Mobility Management iOS and Android™ 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

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
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

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

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
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 Support (NEW)
Now 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 ensure you deliver your mobility objectives. BlackBerry Support provides direct access to technical experts and resources to help ensure your BES10 multi-platform management infrastructure performs at its best.

BlackBerry Support is now included as standard for your BES10 deployment, giving you 12x5 telephone access to our experts, responsive online support, access to training, productivity and diagnostic tools. Higher Support levels with priority queuing and account management are available to tailor a solution that delivers the exact level of technical expertise, assistance and response time that your business requires. Additional services are also available to help you drive your mobility strategy. For more information visit **BlackBerry.com/btss**

* Deployment includes installation of BES10 v10.1 server software and purchase of BES10 Client Access Licenses

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

BlackBerry®