BlackBerry Enterprise Service 10 is a powerful device, application and content management platform with integrated security and connectivity enabling you to easily manage and secure complex fleets of mobile devices.

**BlackBerry® simplifies Enterprise Mobility Management by bringing together:**

**Mobile device management**
BES10 Silver level EMM provides comprehensive management and security controls for Corporate-Owned, Personal Enabled (COPE) and Bring Your Own Device (BYOD) environments.

**Ultimate mobile security**
The BlackBerry platform is purpose built for security to deliver the best protection for work content, on device and in transit.

**Enterprise application management**
The easiest way to get apps to your employees. Deploy, manage and secure apps to users from one unified administration console.

---

**What’s included with BES10 and the Silver level EMM option**

- 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
- The best technical support on the market, with service options to meet your exact needs
**BES10 ENTERPRISE MOBILITY MANAGEMENT, IMPLEMENTED AS EITHER:**

**Silver level EMM²** – EMM controls and settings to meet the needs of organizations of all sizes

BlackBerry delivers comprehensive device management, security and application management for Corporate-owned and BYOD devices.

Delivered through a single end-to-end platform, BES10 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 on BlackBerry 10 devices through the unique BlackBerry Balance containerization technology, to satisfy both user and corporate needs without compromise. Comprehensive application deployment, management and security provides the ability to push and install mandatory apps and publish recommended apps to users through a corporate app storefront to the Work Space on all managed BlackBerry 10 devices, without impacting their ability to access and use personal apps and content in their Personal Space.

BES10 also provides comprehensive device management, application management and security for iOS and Android devices.

**Gold level EMM³** – Controls and settings to meet the needs of security-conscious organizations up to the strictest regulated environments

Ultimate security. BlackBerry 10 devices, BES10 and the Gold level EMM option together deliver the ultimate device management solution to enable compliance for government, financial services, regulated and other high-security environments.

Where highly granular device, content and app controls are required, Gold level EMM delivers the optimum solution for high-security mobility. Detailed specifications for managing BlackBerry 10 devices with Gold level EMM controls can be found in the separate Gold level datasheet.

Gold level EMM also includes Secure Work Space for iOS and Android, a containerization, application wrapping and secure connectivity option that delivers a higher level of control and security for iOS and Android devices. Detailed specifications for Secure Work Space can be found in the separate datasheet.

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

<table>
<thead>
<tr>
<th>Type of enterprise</th>
<th>EMM service level requirement</th>
<th>Managed for some</th>
<th>Managed for all</th>
<th>Segmented</th>
<th>Locked down and managed mix</th>
<th>100% locked down</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gold – Regulated-level device management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Silver – Device management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of enterprise</th>
<th>EMM service level requirement</th>
<th>Small &amp; Medium Business that do not require locked-down devices.</th>
<th>Large &amp; Medium Enterprises that do not require locked-down devices.</th>
<th>Large Enterprises with different levels of device management.</th>
<th>Large Enterprises that are security sensitive.</th>
<th>Government &amp; regulated industries</th>
</tr>
</thead>
</table>

**BlackBerry Balance**

A Personal Space can be optionally enabled on the device through BlackBerry Balance, which 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 for the ultimate end-to-end solution.

Personal and work apps and information are kept separate, and the user can switch from their Personal Space to their Work Space seamlessly 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.
Silver level EMM²
BlackBerry 10 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 unlocks 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 access.

- **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.
### Silver level EMM

iOS and Android™ device management controls and settings:

<table>
<thead>
<tr>
<th><strong>iOS</strong></th>
<th><strong>Android</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Browser</strong></td>
<td><strong>Camera and video</strong></td>
</tr>
<tr>
<td>Hide the default web browser</td>
<td>Hide the default camera application</td>
</tr>
<tr>
<td>Disable autofill in the default browser</td>
<td><strong>Password</strong></td>
</tr>
<tr>
<td>Disable cookies</td>
<td>Define password properties</td>
</tr>
<tr>
<td>Disable fraud warnings in the default browser</td>
<td>Require letters</td>
</tr>
<tr>
<td>Disable JavaScript in the default browser</td>
<td>Require numbers</td>
</tr>
<tr>
<td>Disable popups in the default browser</td>
<td>Require special characters</td>
</tr>
<tr>
<td><strong>Camera and video</strong></td>
<td><strong>Device password</strong></td>
</tr>
<tr>
<td>Disable output</td>
<td>Enable auto-lock</td>
</tr>
<tr>
<td>Disable screen capture</td>
<td>Limit password age</td>
</tr>
<tr>
<td>Hide the default camera application</td>
<td>Limit password history</td>
</tr>
<tr>
<td>Hide the default video-conferencing application</td>
<td><strong>Encryption</strong></td>
</tr>
<tr>
<td><strong>Certificates</strong></td>
<td>Apply encryption rules</td>
</tr>
<tr>
<td>Disable untrusted certificates</td>
<td>Encrypt internal device storage</td>
</tr>
<tr>
<td>Disable untrusted certificates after prompt</td>
<td><strong>Profiles and certificates</strong></td>
</tr>
<tr>
<td>Disable wireless certificate updates</td>
<td>Disable interactive installation of profiles and certificates</td>
</tr>
<tr>
<td><strong>Cloud service</strong></td>
<td><strong>Social</strong></td>
</tr>
<tr>
<td>Disable cloud services</td>
<td>Disable social applications</td>
</tr>
<tr>
<td>Disable cloud backup service</td>
<td>Disable social gaming</td>
</tr>
<tr>
<td>Disable cloud document services</td>
<td>Disable adding friends in default social-gaming application</td>
</tr>
<tr>
<td>Disable cloud picture services</td>
<td>Hide multi-player gaming functionality</td>
</tr>
<tr>
<td>Disable cloud picture sharing services</td>
<td>Hide the default social-gaming application</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td><strong>Storage and backup</strong></td>
</tr>
<tr>
<td>Disable network connectivity</td>
<td>Disable device backup</td>
</tr>
<tr>
<td>Disable wireless connectivity</td>
<td>Require that the device backup data is encrypted</td>
</tr>
<tr>
<td>Disable roaming</td>
<td><strong>Voice assistant</strong></td>
</tr>
<tr>
<td>Disable data service when roaming</td>
<td>Disable the default voice assistant application</td>
</tr>
<tr>
<td>Disable background data service when roaming</td>
<td>Disable voice assistant application when device is locked</td>
</tr>
<tr>
<td>Disable voice service when roaming</td>
<td>Hide user-generated content in voice assistant apps</td>
</tr>
<tr>
<td>Disable AirDrop</td>
<td><strong>Encryption</strong></td>
</tr>
<tr>
<td>Disable changes to wireless data usage for apps</td>
<td><strong>Encryption</strong></td>
</tr>
<tr>
<td><strong>Content</strong></td>
<td><strong>Profiles and certificates</strong></td>
</tr>
<tr>
<td>Disable content</td>
<td>Disable interactive installation of profiles and certificates</td>
</tr>
<tr>
<td>Hide explicit content</td>
<td><strong>Social</strong></td>
</tr>
<tr>
<td><strong>Maximum allowed rating for applications</strong></td>
<td>Disable social applications</td>
</tr>
<tr>
<td><strong>Maximum allowed rating for movies</strong></td>
<td>Disable social gaming</td>
</tr>
<tr>
<td><strong>Maximum allowed rating for TV shows</strong></td>
<td>Disable adding friends in default social-gaming application</td>
</tr>
<tr>
<td><strong>Region that defines the rating restrictions</strong></td>
<td>Hide multi-player gaming functionality</td>
</tr>
<tr>
<td><strong>Diagnostics and usage</strong></td>
<td>Hide the default social-gaming application</td>
</tr>
<tr>
<td>Disable submission of device diagnostic logs to device vendor</td>
<td>Hide the default social-video application</td>
</tr>
<tr>
<td><strong>Messaging</strong></td>
<td><strong>Storage and backup</strong></td>
</tr>
<tr>
<td>Hide the default messaging application</td>
<td>Disable device backup</td>
</tr>
<tr>
<td><strong>Lock Screen</strong></td>
<td><strong>Voice assistant</strong></td>
</tr>
<tr>
<td>Hide Today view in lock screen</td>
<td>Disable voice assistant application when device is locked</td>
</tr>
<tr>
<td>Hide Notification Center in lock screen</td>
<td>Hide user-generated content in voice assistant apps</td>
</tr>
<tr>
<td>Hide Control Center in lock screen</td>
<td><strong>Encryption</strong></td>
</tr>
</tbody>
</table>

**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 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.

For more information visit blackberry.com/btss

Switching to BES10 has never been easier
Getting up and running with BES10 and managing BlackBerry, iOS and Android devices is fast, easy and FREE*

Step 1:
Download BES10 server software for FREE from BES10.com.
That’s right, our server software is completely free.

Step 2:
Go to blackberry.com/EZPass before January 31 2015
We will give you perpetual Silver level EMM licenses for all of your existing on-premise BES licenses plus all your other active MDM licenses on a 1 for 1 basis.
Even if you’re using BES Express which is already a free product, and even if you’re using one of our competitor’s MDM platforms.
As an added bonus, you get world class BlackBerry Advantage Level Technical Support FREE of charge until January 31 2015.

Step 3:
Activate, manage and secure BlackBerry 10, iOS and Android devices (BYOD and corporate owned) from your BES10 server.
Congratulations! You now have multi-platform EMM.

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

1 November 2013
2 Silver level EMM provides the management and control feature set for iOS, Android and BlackBerry 10 devices previously known as BES10 EMM Corporate.
3 Gold level EMM provides the management and control feature set for BlackBerry 10 devices previously known under the name EMM Regulated, and also covers the containerization option for iOS and Android management known as Secure Work Space for iOS and Android.
4 Additional Terms and Conditions apply, see blackberry.com/EZPass

© 2014 BlackBerry. All rights reserved. BlackBerry® and related trademarks, names and logos are the property of BlackBerry Limited and are registered and/or used in the U.S. and countries around the world. All other trademarks are the property of their respective owners. iOS is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS is used under license by Apple Inc. Apple Inc does not sponsor, authorize or endorse this brochure. Android is a trademark of Google Inc. which does not sponsor, authorize or endorse this brochure.