Ultimate security. Regulated level Enterprise Mobility Management control options are available for 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, BlackBerry Enterprise Service 10 (BES10) delivers the ultimate device management solution for high-security mobility.

When a BlackBerry 10 device is managed through BES10, organizations have the option to deploy a corporate-only use model whereby device features and capabilities including social media feeds and public application access is turned off.

Alternatively, a Personal Space can be enabled on the device through BlackBerry® Balance™, which allows users to make the most of their device for personal use whilst the enterprise retains full device control and all work related content is fully protected within the Work Space.¹

**Regulated level Enterprise Mobility Management control options are also available for iOS and Android**

| The Secure Work Space option for iOS and Android devices ensures work 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. | For more information please see the Secure Work Space data sheet or visit www.BES10.com |

**What’s included with BES10 and Regulated level device management**

- BlackBerry 10 Mobile Device Management (MDM) capabilities designed for secure, government and regulated environments
- Enforcement of corporate-only use and granular controls to manage use of camera, storage, WiFi, Bluetooth and other device features
- Option to enable a Personal Space through BlackBerry Balance whilst ensuring all work content is fully protected within the Work Space
- User friendly and intuitive management console to manage your devices, users, groups, apps and services including reporting and dashboard capabilities
- Support included as standard to help you deliver more valuable mobile IT

**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>Regulated level device management</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>Full device management</td>
<td>Managed service level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of enterprise</td>
<td>Managed service level</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small &amp; Medium Business</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large &amp; Medium Enterprises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large Enterprises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government &amp; regulated industries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ Regulated level EMM with BlackBerry Balance for BlackBerry 10 devices is available with BES10, version 10.2
Regulated level
BlackBerry Device Management
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 whenever the device is roaming.

Password
Password Required for Device
Specify whether a BlackBerry device requires a password to protect the Work Space 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 inactivity before a BlackBerry device locks.

Maximum Password Age
Specify the maximum number of days that a password can be used before a BlackBerry device user must change a 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 to unlock a BlackBerry device before it locks.

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 before a BlackBerry device can be wiped of its contents without being connected to your organization's network.

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

Development Mode Access to Work Space
Specify whether development mode is enabled 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.

Lock on Smart Card Removal
Specify whether a BlackBerry device user can use voice dialing on a device.

Backup and Restore Work Space Using BlackBerry Desktop Software
Specify whether a BlackBerry device user can backup and restore applications and data that are located in the Work Space of the device using the BlackBerry Desktop Software.

BlackBerry Bridge
Specify 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 Card 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 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 Timeout 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 specified in the Password Lock settings on the device's eula.

Network Access Control for Work Applications
Specify whether work applications on a BlackBerry device must connect to your organization's network through BES10.

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

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

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

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

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

Backup and Restore Work Space
Specify whether the work space on a BlackBerry device must use advanced data at rest protection.

Advanced Data at Rest Protection Timeout
Specify the number of minutes after the work space locks that the BlackBerry device turns on advanced data at rest protection for the work space.

Two-Factor Authentication for Advanced Data at Rest Protection
Specify whether two-factor authentication must be used to protect the encryption keys for advanced data at rest protection.

Software
SMS/MMS
Specify whether a BlackBerry device can send SMS text messages and MMS messages.

BBM
Specify whether BlackBerry Messenger is available on a BlackBerry device.

Media Shared
Specify whether a BlackBerry device can share music, pictures, and videos over a Wi-Fi connection.

BBM Video/BBM Voice
Specify whether a BlackBerry device can use the BBM Video and BBM Voice apps.

YouTube for BlackBerry Devices
Specify whether a BlackBerry device can send certain contact and device data to BlackBerry for analysis to help improve the YouTube experience. BlackBerry recommends 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.

Non-Email Accounts
Specify whether a BlackBerry device user can add third-party accounts for services, such as Facebook, Twitter, LinkedIn and Evernote to your organization's BES10.

E-mail Messages Services
Specify whether a BlackBerry device can use email messaging services to access the e-mail messages service.

Wireless Software Updates
Specify whether a BlackBerry device can download BlackBerry 10 updates through BES10. This rule can be set to All, Allow Security Updates Only or Disallowed.

Hotspot Browser
Specify whether a BlackBerry device user can use the BlackBerry hotspot browser.

Maps
Specify whether a BlackBerry device can use the BlackBerry Maps app to navigate your location.

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

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 Rating List
Specify a list of email domains that BlackBerry device users can send work email messages to.

External Email Domain Rating Limit
Specify a limit on the number of email messages that BlackBerry device users are allowed to send to any email address.

External Email Domain Rating Policy
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.

External Email Domain Rating Policy Report
Specify whether to prevent a BlackBerry device user from sending email messages to external email addresses.
Get BES10 Ready

Getting up and running with BlackBerry 10 and BES10 is fast and straightforward. Importantly, it does not impact your existing BES infrastructure.

Step 1:
Download BES10 for free at BES10.com

Step 2:
Transfer existing BlackBerry Enterprise Server Client Access Licenses (CAL) to BES10 CALs for managing BES10 devices at no additional cost. Go to blackberry.com/blackberry10ready
Purchase new BES10 CALs for additional BlackBerry 10 devices and add Regulated level EMM data plan from your preferred data provider.

Step 3:
Connect new BlackBerry 10 devices to BES10. You can continue to manage existing BlackBerry OS devices connected to BlackBerry Enterprise Server 5.0.3 and above, alongside BES10 devices, through the centralized BES10 management console.

BlackBerry Technical 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/bes10ready

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

© 2013 BlackBerry. All rights reserved. BlackBerry® and related trademarks, names and logos are the property of Research In Motion 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.