Experience the most secure mobility management solution with BES12 and Gold Enterprise Mobility Management (EMM) subscriptions.

HIGH-SECURITY MOBILITY MANAGEMENT FROM BLACKBERRY

Get ultimate security with Gold EMM for BlackBerry, iOS and Android devices.

Regulated-level security at its best

BlackBerry® 10 devices managed by BES12 with Gold EMM provides comprehensive management and security controls to enable compliance for government, financial services, regulated and other high-security environments.

Extending the trusted BlackBerry security model

BES12 with Gold EMM delivers a higher level of control and security to iOS and Android™ devices, with Secure Work Space providing containerization, application-wrapping and secure connectivity.

BES12 is the command and control center for the secured enterprise

Comprehensive EMM
Whether you manage a single, hardened, connected endpoint or to allow BYOD (iOS, Android, BlackBerry, Windows Phone® or Samsung KNOX), BES12 gives you control over the availability and usage of devices, apps, activities and mission-critical data.

End-to-end security
BlackBerry security is trusted by thousands of enterprises around the world. Using encryption, containerization, app-wrapping and BlackBerry’s secure global infrastructure, BES12 locks down mission-critical data both on-device and in-transit.

Enterprise mobility ecosystem
BES12 is the ‘central nervous system’ of a powerful ecosystem that brings together mobile devices, apps, cloud services and carrier services.

For BlackBerry 10 Policies see pg. 3
For Secure Work Space Policies see pg. 6
## BlackBerry 10 Devices

BlackBerry 10 EMM capabilities designed for government, financial services, regulated option to manage device in highly secured 'work space only mode', including other high-security environments.

- Enforcement of work space-only use and granular controls with ability to audit device communications, including BBM/PIN/SMS/MMS/Phone
- Option to enable a managed Personal Space through BlackBerry® Balance™ while ensuring all work content is fully protected within the work space
- Built-in secure connectivity with user-friendly and intuitive management console to manage your devices, users, groups, apps and services, including reporting and dashboard capabilities
- The best technical support on the market, with service options to meet your exact needs

## Secure Work Space

- Containerization, application-wrapping and secure connectivity option for iOS and Android devices
- Secured apps for email, calendar and contacts, enterprise level secure browsing and document viewing and editing with Documents to Go™
- Built-in secure connectivity for all enterprise apps deployed to the Secure Work Space – no VPN needed
- Option to deploy iOS and Android devices in BYOD mode with user privacy, where management is confined to the Secure Work Space container only
- Option to deploy iOS and Android with Secure Work Space and full device MDM controls
- User-friendly and intuitive management console including reporting and dashboard capabilities
- The best technical support on the market, with service options to meet your exact needs

### BlackBerry Balance for BlackBerry 10 devices

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 BES12 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.

### Secure Work Space for iOS and Android

Secure Work Space is a containerization, application-wrapping and secure connectivity option that delivers a higher level of control and security to iOS and Android devices managed through BES12.

- Managed applications are secured and separated from personal apps and data, providing integrated email, calendar and contacts app, an enterprise-level secure browser, and secure attachment viewing and editing with Documents to Go.
Controls and settings for regulated-level BlackBerry 10 device management:

**General**

**Allow 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.

**Allow wireless service provider billing**
Specify whether a BlackBerry device user can purchase applications from the BlackBerry World storefront and the BlackBerry World for Work storefront using the purchasing plan for your organization’s wireless service provider.

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

**Password**

**Require full-device password**
Specify whether a BlackBerry Balance or regulated BlackBerry Balance device requires a password for the full device. If you want to protect only the work space, do not select this rule.

**Minimum password length**
Specify the minimum length of the work space password.

**Security timeout**
Specify the period of BlackBerry device user inactivity that must elapse before the work space locks.

**Maximum password age**
Specify the maximum number of days that the work space password can be used. After the specified number of days elapse, the password expires and a BlackBerry device user must set a new password.

**Minimum password complexity**
Specify the minimum complexity of the work space password.

**Maximum password attempts**
Specify the number of times that a BlackBerry device user can attempt an incorrect password before a 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 work space password.

**Password required for work space**
Specify whether a BlackBerry Balance or regulated BlackBerry Balance device requires a password for the work space. A work space only device always requires a password and this rule must be selected to specify the password requirements.

**Security**

**Wipe the work space without network connectivity**
Specify the time (in hours or days) 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 apps directly on the device using a USB or Wi-Fi connection.

**Allow 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.

**Allow voice control**
Specify whether a BlackBerry device user can use the voice control commands with the Voice Control or BlackBerry® Assistant apps on a device.

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

**Allow BlackBerry Bridge to access the work space**
Specify whether a BlackBerry 10 device user can use a BlackBerry® PlayBook™ tablet to access work data on a device using the BlackBerry Bridge app.

**Smart card password caching**
Specify whether a BlackBerry device can cache the smart card password.

**Smart password entry**
Specify whether a BlackBerry device can use smart password entry with two-factor authentication.

**Lock on smart card removal**
Specify whether a BlackBerry device or the work space on a device locks when a user removes the smart card from a supported smart card reader or disconnects a supported smart card reader from the device.
Maximum Bluetooth range
Specify the maximum power range that a BlackBerry Smart Card Reader uses to send Bluetooth packets to a BlackBerry device or a computer. The permitted range is between 30% and 100%.

Minimum PIN entry mode
Specify the PIN entry mode that is required when a BlackBerry Smart Card Reader connects to a BlackBerry device or a computer. The user must use the specified PIN format when typing the smart card password during the Bluetooth connection process.

Allow app 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.

Force network access control for work apps
Specify whether work applications on a BlackBerry device must connect to your organization’s network through BES12.

Allow personal apps to use work networks
Specify whether personal apps on a BlackBerry device can use a work VPN or work Wi-Fi network to connect to the Internet.

Allow lock screen preview of work content
Specify whether a BlackBerry device displays a preview of work content when the device is locked.

Allow IRM-protected email messages
Specify whether a BlackBerry device user can download IRM-protected messages.

Display owner information on lock screen
Specify the owner information that a BlackBerry device displays when the device is locked.

Force advanced data at rest protection
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
Allow SMS/MMS
Specify whether a BlackBerry device can send SMS text messages and MMS messages.

Allow BBM
Specify whether BBM® is available on a BlackBerry device.

Allow media sharing
Specify whether a BlackBerry device can share music, pictures, and videos over a Wi-Fi connection with DLNA Certified devices.

Allow BlackBerry Maps
Specify whether BlackBerry® Maps is available on a BlackBerry device.

SMS/MMS signature
Specify the signature (for example, a web address or a short disclaimer) that is appended to outgoing SMS text messages and MMS messages that a BlackBerry device user sends from a device.

Allow BlackBerry Protect
Specify whether a BlackBerry device can use BlackBerry® Protect.

Allow Miracast
Specify whether a BlackBerry device can send streaming video over a Wi-Fi Direct connection to other Wi-Fi certified Miracast devices.

Allow user-created VPN profiles
Specify whether a BlackBerry device user can create VPN profiles on a device.

Allow PIN messages
Specify whether a BlackBerry device can send and receive PIN messages.

Allow unified view for work and personal accounts and messages
Specify whether the BlackBerry® Hub displays work and personal accounts and messages together in a single view.

Allow non-email accounts
Specify whether a BlackBerry device user can add third-party accounts for services, such as Facebook, Twitter, LinkedIn and Evernote, to the device.

Forward or add recipients to private messages
Specify whether a BlackBerry device user can forward or add new recipients when replying to email messages with “(PRIVATE EMAIL)” in the subject line.
Display warning message for external email addresses
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.

Logging
Submit logs to BlackBerry
Specify whether a BlackBerry device can generate and send log files to the BlackBerry Technical Solution Center.

Synchronize phone logs
Specify whether a BlackBerry device synchronizes the call log for the Phone app with BES12.

Synchronize video chat logs
Specify whether a BlackBerry device synchronizes logs for the BBM Video feature with BES12.

Synchronize SMS/MMS logs
Specify whether a BlackBerry device synchronizes logs for SMS text messages and MMS messages with BES12.

Synchronize BBM logs
Specify whether a BlackBerry device synchronizes logs for BBM with BES12.

Synchronize PIN to PIN logs
Specify whether a BlackBerry device synchronizes logs for PIN messages with BES12.

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

Hardware
Allow Bluetooth
Specify whether a BlackBerry device can use Bluetooth technology.

Allow Bluetooth pairing
Specify whether a BlackBerry device can connect to another Bluetooth enabled device.

Allow Bluetooth Handfree Profile (HFP)
Specify whether a BlackBerry device can use the Bluetooth HFP.

Allow Bluetooth Serial Port Profile (SPP)
Specify whether a BlackBerry device can use the Bluetooth SPP.

Allow Bluetooth discoverable mode
Specify whether a BlackBerry device can use Bluetooth discoverable mode.

Allow Bluetooth contacts transfer Using PBAP
Specify whether a BlackBerry device can exchange Contacts data with other Bluetooth enabled devices using the Bluetooth PBAP.

Allow Bluetooth file transfer using OBEX
Specify whether a BlackBerry device can exchange files with other supported Bluetooth Object Exchange (OBEX) devices.

Allow Bluetooth PAN profile
Specify whether a BlackBerry device can use the Bluetooth Personal Area Networking (PAN) profile.

Allow Bluetooth A2DP
Specify whether a BlackBerry device can use the Bluetooth Advanced Audio Distribution Profile (A2DP) to perform audio streaming via Bluetooth.

Allow Bluetooth AVRCP
Specify whether a BlackBerry device can use the Bluetooth Audio/Video Remote Control Profile (AVRCP) to facilitate remote control of audio and video via Bluetooth.

Enforce Bluetooth SSP numeric comparison
Specify whether a BlackBerry device must use the numeric comparison mode if the device uses Bluetooth SSP to connect to another Bluetooth enabled device.

Allow Bluetooth MAP
Specify whether a BlackBerry device can use the Bluetooth MAP to allow a Bluetooth enabled device to access email messages.

Allow Wi-Fi
Specify whether a BlackBerry device can use Wi-Fi connections.

Allow camera
Specify whether a BlackBerry device can use the camera.

Allow location services
Specify whether a BlackBerry device can provide its geographic location to applications that are running on the device.

Allow NFC
Specify whether a BlackBerry device can use NFC.

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

Allow HDMI
Specify whether a BlackBerry device can use the HDMI port.

Minimum Bluetooth encryption key length
Specify the minimum encryption key length that a BlackBerry device uses to encrypt Bluetooth connections.
GOLD EMM SUBSCRIPTIONS

CONTROLS AND SETTINGS FOR SECURE WORK SPACE (IOS AND ANDROID)

The controls and settings listed below are features that Secure Work Space delivers in addition to the standard device management capabilities of BES12.

Password

Allow sequential and repeated character passwords
Specify whether the work space password can contain sequential or repeated characters, such as abcd or 1111.

Require letters
Specify whether the work space password must contain letters.

Minimum number of letters
Specify the minimum number of letters that the work space password must contain.

Require lowercase letters
Specify whether the work space password must contain lowercase letters.

Minimum number of lowercase letters
Specify the minimum number of lowercase letters that the work space password must contain.

Require numbers
Specify whether the work space password must contain numbers.

Minimum number of numerals
Specify the minimum number of numerals that the work space password must contain.

Require special characters
Specify whether the work space password must contain special characters.

Minimum number of special characters
Specify the minimum number of special characters that the work space password must contain.

Require uppercase letters
Specify whether the work space password must contain uppercase letters.

Minimum number of uppercase letters
Specify the minimum number of uppercase letters that the work space password must contain.

Limit password length
Specify whether the work space password has a minimum and maximum length.

Maximum password length
Specify the maximum number of characters that the work space password must contain. The minimum password length cannot be greater than the maximum password length.

Maximum password age
Specify the maximum number of days that the work space password can be used. After the specified number of days elapse, the password expires and a user must set a new password.

If set to 0, the password does not expire.

Limit reuse of previous passwords
Specify whether a device prevents a user from reusing work space passwords.

Number of previous passwords checked
Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a work space password.

Security

Lock work space when device locks
Specify whether the work space locks when a device locks after a period of inactivity.

If this rule is selected, when a user is in the work space, the work space locks after the period of inactivity specified in the “Lock device after inactivity in work space” rule. When the user is in the personal space, or if the “Lock device after inactivity in work space” rule is not selected, the work space locks after the period of inactivity specified in the auto-lock setting on the device.
Lock device after inactivity in work space
Specify whether the device should lock after a period of inactivity in the work space. When a user is in the work space, the device locks after the period of inactivity specified. Otherwise, the device locks after the period of inactivity specified in the auto-lock setting on the device.

If you configure the “Lock device after inactivity in work space” rule, the following behavior occurs after the specified inactivity period:

› On Android devices with a password, the device locks when a work space app is open. The work space isn’t locked.

› On Android devices without a password, the device turns off the screen when a work space app is open. The work space isn’t locked.

The inactivity period that you specify is the maximum time for inactivity. A user can set a shorter inactivity period on the device. If the user sets a shorter inactivity period, the screen locks when that inactivity period is met.

Inactivity period before locking
Specify the period of inactivity in the work space that must elapse before a device locks.

Lock work space after inactivity
Specify the period of inactivity in the personal space that must elapse before the work space locks.

Limit number of failed password attempts
Specify whether a device should limit the number of times that a user can enter an incorrect work space password before the action specified in the “Action after maximum number of attempts” rule occurs.

Maximum number of attempts
Specify the number of times that a user can enter an incorrect work space password.

Action after maximum number of attempts
Specify the action that occurs after the maximum number of failed password attempts has been reached.

If set to “Disable work space,” the work space is disabled and can only be restored by an administrator. If set to “Deactivate device,” all data in the work space is deleted and the device is deactivated.

If set to “Disable work space and after N days, deactivate device,” you must also specify a number of days. The work space is disabled immediately and can only be restored by an administrator.

If the work space is not restored before the specified number of days elapse, all data in the work space is deleted and the device is deactivated.

Number of days
If you selected “Disable work space and after N days, deactivate device,” specify the number of days before deactivating a device.

Deactivate device after period of inactivity
Specify whether all data in the work space is deleted and the device is deactivated after a number of days of inactivity in the work space.

Inactivity period before deactivation
Specify the number of days of inactivity in the work space that must elapse before all data in the work space is deleted and the device is deactivated.

Allow all apps to access files in the work space
Specify whether all apps on an Android device can access files in the work space. If this rule is not selected, files in the work space are encrypted and only secured apps can access files in the work space.

If this rule is selected and then you later update the IT policy and do not select this rule, apps in the personal space still have access to existing files in the work space but do not have access to files added to the work space after the rule is updated on the device.

Notification level
Specifies the level of notifications that a user sees for apps in the work space when the work space is locked.

Software

Allow S/MIME
Specify the maximum number of characters that the work space password must contain.

Enable autofill
Specify whether the work browser remembers information that users enter in web forms.

Enable JavaScript
Specify whether the work browser allows websites to run JavaScript.

Block pop-ups
Specify whether pop-up blocking is enabled in the work browser.
BlackBerry Technical Support Services

You can rely on the industry-leading Advantage Support that is included with all BES12 Annual Subscriptions to help evolve your EMM strategy and maintain your complex and demanding environment.

With relationship-based Premium Support and Optional Services, you can provide even greater user satisfaction, drive business continuity, and achieve cost efficiencies.

For more information visit blackberry.com/btss

Upgrading to BES12 has never been easier

Getting up and running with BES12 and managing BlackBerry 10 devices at the ultra-secure Gold level is easy.

Step 1:
Download BES12 server software for FREE from blackberry.com/bes12. That’s right, our server software is completely free.

Step 2:
Purchase new Gold level BlackBerry licenses from your preferred software reseller. Or, where available, buy the appropriate Gold level data plan from your mobile operator. Where your operator offers a Gold level data plan, you don’t need a BES12 license to manage BlackBerry 10 devices.

Step 3:
Activate, manage and secure BlackBerry 10, iOS, Android and Windows Phone devices from your BES12 server. Congratulations! You now have the ultimate level of mobile security and management.

For more information on buying Gold or Silver EMM subscriptions, and associated pricing, please visit blackberry.com/bes12