

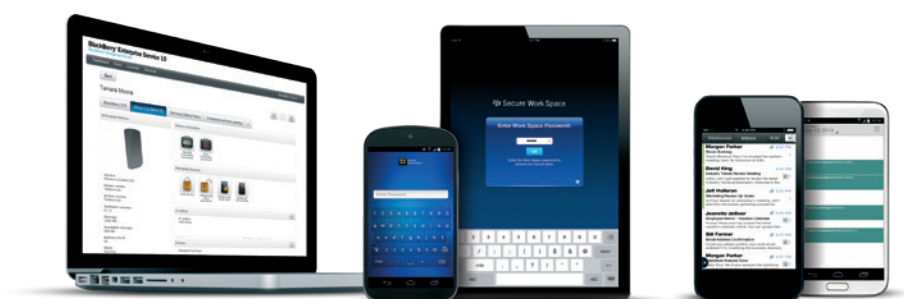
# SECURE WORK SPACE FOR IOS AND ANDROID

Gold level<sup>1</sup> EMM for iOS & Android  
Containerization, app-wrapping and  
secure connectivity

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, all managed through the BlackBerry Enterprise Service 10 administration console.

## BlackBerry makes it simple

Managed applications are secured and separated from personal apps and data, providing integrated email, calendar and contacts app, an enterprise-level secure browser, a software token for generating one-time passwords, and secure attachment viewing and editing with Documents To Go™.



## What's included with BES10 and Secure Work Space for iOS and Android

Containerization, application-wrapping and secure connectivity option for iOS and Android devices

Secured apps for email, calendar and contacts, enterprise-level secure browsing, generating TokenCodes 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 true BYOD mode, where management is confined to the Secure Work Space container only

Full device MDM control can be activated if required and managed through the BES10 console

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

# GOLD LEVEL EMM FOR IOS & ANDROID BES10 WITH SECURE WORK SPACE

The convenience, strength and efficiency of the trusted BlackBerry security model now extends to iOS and Android smartphones and tablets.

BlackBerry delivers comprehensive multi-OS device management for iOS, Android and BlackBerry devices through BES10. Secure Work Space easily and cost effectively extends these capabilities by adding containerization, application-wrapping and secure connectivity for iOS and Android devices.

## Functionality

- Secured apps for email, calendar and contacts (PIM), web browsing and document viewing and editing (Documents to Go) come as standard
- Data in secured apps is encrypted and separated from personal data and apps. Users cannot copy or paste corporate data into personal apps
- Ability to deploy and manage additional securely wrapped apps within the Secure Work Space
- Optional two-factor authentication delivered through a mobile software token offers enhanced security for use within the Secure Work Space and can also be used outside the mobile application for traditional authentication tasks, such as one-time password to access online systems such as VPN, WiFi, or secure web portals
- iOS and Android devices can be deployed in true BYOD mode, where management is confined to the Secure Work Space container only
- Full device MDM control can be activated if required and managed through the BES10 console

## Deployment of secured enterprise applications

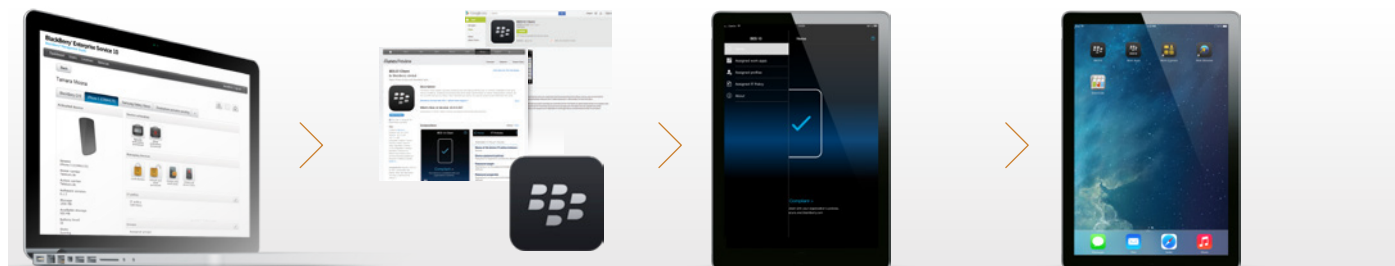
- Additional apps can be securely wrapped and deployed to the Secure Work Space
- No custom development is necessary to enable applications for secure deployment
- All deployed applications are subject to the same security controls and application data is encrypted
- Deployed applications are able to directly access data behind-the-firewall via BlackBerry Secure Connectivity
- Pre-wrapped applications for SWS are available from the Apple App Store and Google Play, including ISEC7 Mobility for SAP, harmon.ie and Box<sup>3</sup>

## BlackBerry Secure Connectivity

- FIPS 140-2 certified
- Provides built in AES-256-bit encryption for iOS and Android devices
- Provides access to behind-the-firewall application servers for apps deployed to the Secure Work Space
- No separate VPN infrastructure required
- All supported through a proven connectivity model
- Allows secure browsing of web pages on the corporate intranet on iOS and Android devices

## Administrator experience

The Secure Work Space container and its contents can be easily configured and managed through the BES10 management console. With a comprehensive selection of controls and settings, the Secure Work Space can be configured to an individual user or group of users.



Administrator creates a user account within BES10 and specifies an activation password. An activation email is then sent to the user

User downloads the BES10 Client from the relevant app store.

User opens BES10 Client and enters the activation details, the activation process begins.

Once activation is complete, the user is prompted to create a Secure Work Space password and install some, or all of the applications specified by the administrator.

## Work Security ID for BES10

Work Security ID for BES10 generates a one-time password from a soft token found within the Secure Work Space, enhancing mobile security, while also simplifying life for users. No need to carry a separate hardware authenticator to securely access RSA Tokencodes!

The Work Security ID client is integrated with the RSA SecurID SDK to deliver two-factor authentication from the Mobile Device. This mobile software token is used within Secure Work Space, allowing end-users to copy and paste the token code from the Work Security ID app to

other apps within the SWS with just one tap. The token code can also be used outside the mobile application for traditional authentication tasks, such as one-time password to access online systems such as VPN, WiFi, or secure web portals.

Administrators of the RSA Authentication Manager can rapidly and securely deploy software tokens to Secure Work Space users' devices.

The BES10 Secure Work Space gives users the ability to securely access work email, contacts,

calendar, browser and RSA Tokencodes through applications contained within a Secure Work Space. Additional applications that run within the Secure Work Space can be found at <http://bizblog.blackberry.com/2014/04/secure-work-space-apps-for-ios-and-android/>

Important note:

Secure Work Space for BlackBerry Enterprise Service 10 with Work Security ID requires BlackBerry Enterprise Service 10 software and the RSA Authentication Manager to be installed within your organization. Additional security and functionality including application wrapping and secure connectivity can be achieved through the Secure Work Space option. For more information visit [www.BES10.com](http://www.BES10.com)

## Key components of Secure Work Space for iOS

### Email, calendar, contacts, notes and tasks

Work Connect in the Secure Work Space offers iOS users convenient access to corporate email, Calendar, Contacts, Notes and Tasks through a single application while ensuring data is secured.

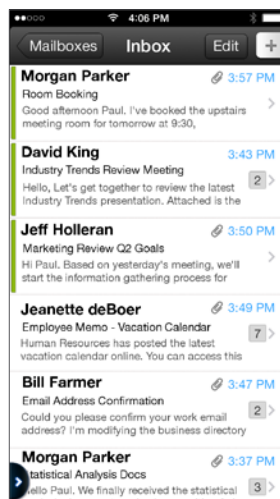
Work Connect supports ActiveSync and connects to enterprise mail servers via BlackBerry Secure Connectivity, removing the need to expose ActiveSync to the Internet.

### Work Browser

The Work Browser within Secure Work Space for iOS devices is HTML5 compatible. Enabled by BlackBerry Secure Connectivity, users can safely browse internal pages (intranet) and web pages from within the Secure Work Space.

### Documents to Go

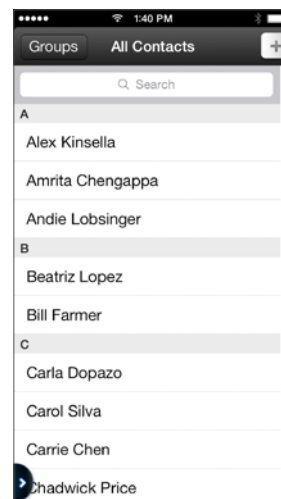
Documents to Go is included with Secure Work Space to enable iOS users to create, edit and view work documents. Documents to Go supports files downloaded via the Work Browser, files received as an attachment through Work Connect or via other applications in the Secure Work Space.



Email view  
iPhone



Calendar (monthly view)  
iPhone



Contacts  
iPhone

## Key components of Secure Work Space for Android

### Customized home screen

Android users can conveniently access Secure Work Space via a separate home screen. Users can customize their Secure Work Space home screen via work application shortcuts and widgets.

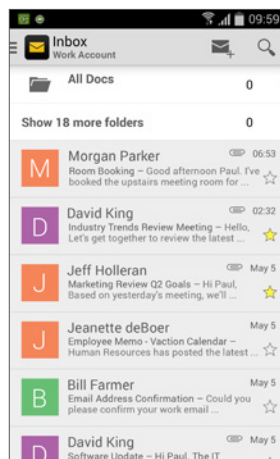
### Email, calendar and contacts

Android users can access email, contacts and calendar information through applications within Secure Work Space. These applications provide a user experience closely aligned to the native application experience on the device, whilst fully securing and protecting corporate data.

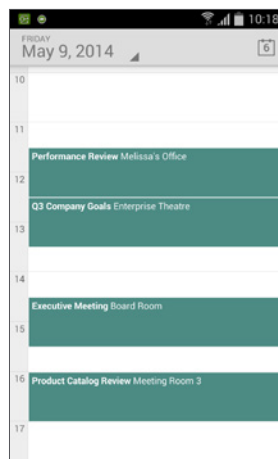
PIM applications are synchronized using ActiveSync and utilize BlackBerry Secure Connectivity, removing the need for enterprises to expose ActiveSync to the Internet.

### Work Browser

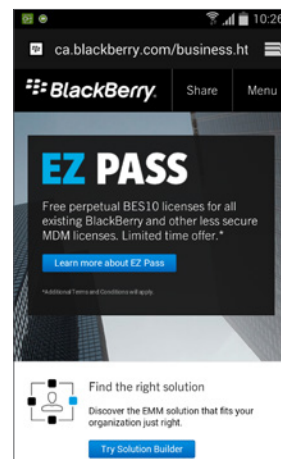
The Work Browser within Secure Work Space for Android devices means users can safely browse internal pages (intranet) and web pages from within the Secure Work Space. Enabled via BlackBerry Secure Connectivity, the browsing experience is aligned with the device's native browsing experience.



Email view  
Android smartphone



Calendar (list view)  
Android smartphone



Secure browser  
Android smartphone

### Documents To Go

Included with Secure Work Space, Documents to Go allows Android users to create, edit and view documents. Documents to Go supports files downloaded via the Work Browser, files received as an attachment through a PIM source or via other applications in the Secure Work Space.



# Controls and settings for Secure Work Space

The controls and settings listed below are features that Secure Work Space delivers in addition to the standard device management capabilities of BES10. For more information please see the Silver level<sup>2</sup> EMM datasheet available at [BES10.com](https://www.bes10.com)

## Lock Work Space

Lock the Work Space on a device so that the user must type the existing Work Space password to unlock the device.

## Disable/enable Work Space

Temporarily prevent access to the Work Space apps on the device.

## Delete only work data

Delete any profiles that are assigned to the device and remove the device from BES10.

If the device has a BES10 Work Space, the Work Space information is deleted and the Work Space is removed from the device.

## Allow sequence and single character passwords

Allow a user to set a password that uses only one character, such as 1111, or a sequence of characters, such as abcd.

## Require letters

Specify the minimum number of letters required in the Work Space password.

## Require lowercase letters

Specify the minimum number of lowercase letters required in the Work Space password.

## Require numbers

Specify the minimum number of numerals required in the Work Space password.

## Require special characters

Specify the minimum number of special characters required in the Work Space password.

## Require uppercase letters

Specify the minimum number of uppercase letters required in the Work Space password.

## Minimum length for the Work Space password

Specify the minimum number of characters required in the Work Space password.

## Maximum length for the Work Space password

Specify the maximum number of characters required in the Work Space password.

## Lock Work Space after inactivity

Specify the period of inactivity after which the Work Space locks. You can specify any number of days, hours, minutes, or seconds.

## Lock Work Space when device locks:

Specify whether the Work Space locks when a device locks after a period of inactivity.

## Lock device after inactivity in Work Space:

Specify the period of inactivity in the Work Space that can elapse before a device locks.

## Track incorrect password attempts

Specify the number of times that a user can try an incorrect password before the action specified in the Action after maximum incorrect password attempts setting occurs.

## Action after maximum incorrect password attempts

Specify what happens when the user enters an incorrect password more than the number of times specified in the Track incorrect password attempts setting.

## Enable plugins in secure work browser Work Space (Android only)

Prevent plug-ins from being added to the browser app in the Work Space on Android devices. Use: Control whether plug-ins are allowed to run in the Work Space browser.

## Delete Work Connect data after period of inactivity

Specify the number of days of Work Space inactivity, after which the user's work data, including PIM data, is deleted.

## Allow apps in the Personal Space to access data in the Work Space (Android only)

Allow personal apps to access data within the Work Space.

## Notification level (Android only)

Specify the level of notifications that a user sees for apps in the Work Space when the Work Space is locked.

## Allow S/MIME

Choose whether or not to enable S/MIME in the Work Connect app on the device.

## Work Connect contacts (iOS only)

Specify whether work contacts are exported from the Work Connect app in the Work Space to the personal address book on the device, e.g. for displaying caller ID. (iOS only)





## 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](http://blackberry.com/btss)

# EZ PASS

FREE perpetual BES10 licenses for all existing BlackBerry and other active MDM licenses, plus receive world class BlackBerry Advantage Level Technical Support FREE of charge!\*

Learn more at [blackberry.com/eypass](http://blackberry.com/eypass)

\*Additional Terms and Conditions will apply

For more information on Secure Work Space and BlackBerry Enterprise Service 10 please visit [BES10.com](http://BES10.com)

<sup>1</sup> Silver level EMM provides the management and control feature set for BlackBerry 10, iOS and Android devices previously known as BES10 EMM Corporate.

<sup>2</sup> 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.

<sup>3</sup> Availability of applications may vary across mobile platforms.

Screen images simulated.

