BLACKBERRY ENTERPRISE SERVICE 10

Secure Work Space for iOS and Android

iOS7 and Android 4.3 Now supported

Containerization, application-wrapping and secure connectivity option 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, all managed through the BlackBerry Enterprise Service 10 administration console.

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™.

Features

- 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
- 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

BlackBerry Secure Connectivity

- 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 single-outbound port via BES10
- 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. Through a selection of controls and settings (see overleaf) the Secure Work Space can be configured to an individual user or group of users.

Deploying Secure Work Space is simple:

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.

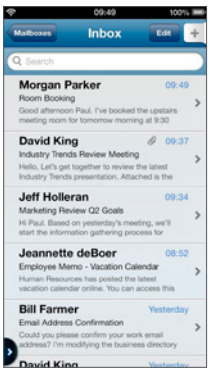
BlackBerry

Key components of Secure Work Space for iOS and Android

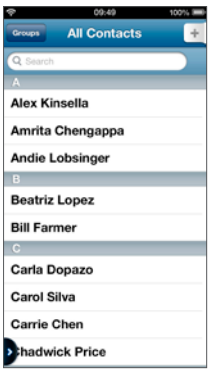
Email, calender, contacts, notes and tasks*

Secure Work Space offers iOS and Android users convenient access to work productivity tools including email, calendar, contacts, notes and tasks through a familiar and secured application.

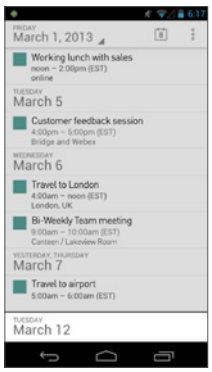
ActiveSync is supported and connection to enterprise mail servers is achieved through BlackBerry Secure Connectivity, removing the need to expose ActiveSync to the Internet.



Email view iPhone



Contacts iPhone



Calendar (list view) Android smartphone

*Notes and tasks are currently only available in Secure Work Space for IOS.

Work Browser

The Work Browser within Secure Work Space for iOS and Android 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. The browsing experience is aligned with the device's native browser.

Documents to Go

Documents to Go is included with Secure Work Space to enable iOS and Android 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 email or via other applications in the Secure Work Space.

Controls and Settings for Secure Work Space

The below controls and settings are in addition to the full device management capabilities of BES10. For more information please read the BES10 full device management datasheet available from 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.

Time after the Work Space locks that it can be unlocked without the password

Specify the period of time after the Work Space locks that the user can unlock it without a password. You can specify any number of days, hours, minutes, or seconds.

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.

Disable 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.

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)

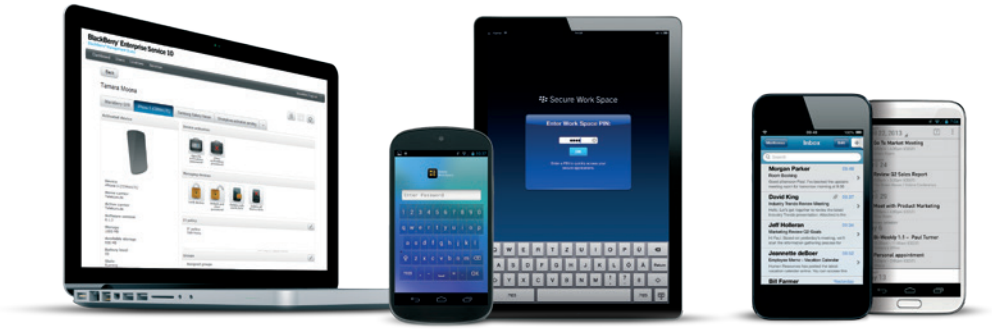
Allow personal apps to access data within the Work Space.

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.



For more information on Secure Work Space for iOS and Android and BlackBerry Enterprise Service 10 please visit www.bes10.com

BlackBerry