

BES12 is a highly secure and flexible way to manage Android.

BES12: EMM FOR ANDROID

Enhance your enterprise's productivity without sacrificing security

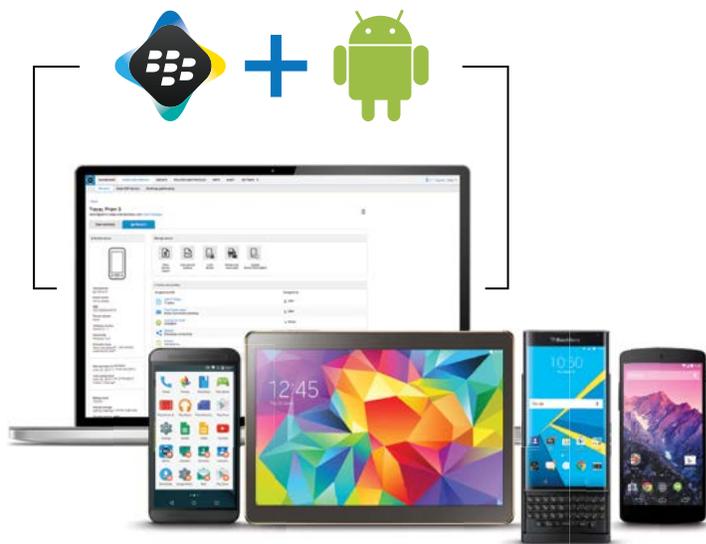
BES®12 is a complete, highly secure Enterprise Mobility Management (EMM) solution that is designed to protect your business data and increase the productivity of your workforce by fully enabling their mobility.

Securely manage Android™ devices across different ownership models (personally owned or corporate liable devices). Manage your mobile workers' access to apps, data and content. Do it all from a single, easy-to-use console that offers a complete set of IT policies and profiles to suit your needs and preferences.

Android for Work

Google provides enhanced security aimed at protecting business and private data with Android. Android™ for Work allows for simplified management across BYOD and corporate-owned devices and serves as an open platform for innovation on Android.

Android for Work separates business content from personal information, bringing more simplicity and convenience to end users. The Work Profile enables platform enhancements for security, management, and application support, while EMM integration completes the solution by providing a single console to manage devices, set policies, and distribute approved applications.¹



BES12 + Android for Work

BES12 helps transform workplace mobility by enabling organizations to further secure work and personal data on Android devices, while enabling integration with Google Play™ for Work.

Simplified IT management gives full control of work-related policies, profiles and data while providing a consistent end-user experience on Android devices.¹ With the familiarity of the Android experience, the user's learning curve substantially reduced and requires fewer IT resources for initial activation and ongoing support. BES12 integration enables you to manage devices, apps and data, by person or by group, through one consolidated, easy-to-use console.

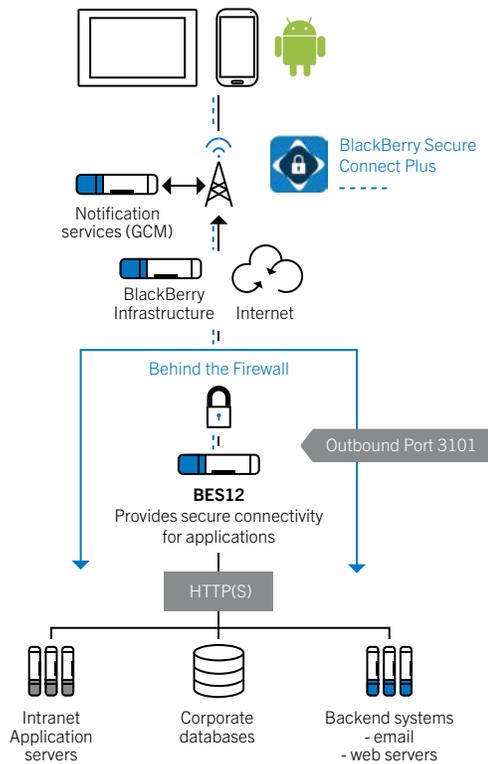
A secure mobile experience with a dedicated work profile and hardware-based encryption and sharing restrictions. Android ensures work data is kept separate and safe from malware, and keeps personal data private. BES12 support for Android for Work includes the ability to secure work data end-to-end through BlackBerry® Secure Connect Plus.³

All the apps you need, with access to any third-party Android app on Google Play for Work. Your app catalog can be seamlessly integrated with IT systems and distributed to end users.

BES12 + ANDROID FOR WORK

Simplify management. Enhance security

- › Separate work and personal data on a single device
- › Corporate security and privacy remains uncompromised
- › Intuitive setup and configuration of users and groups
- › Granular controls with settings for ‘work and personal’ and ‘work space only’
- › Distribute approved apps - enterprise hosted, from Google Play
- › Easy-to-manage deployment from a unified console
- › Streamline behind-the-firewall access and eliminate mobile VPNs



BES12 support for Android for Work²

IT Policies and Commands	Workspace
<ul style="list-style-type: none"> › Require storage encryption › Disable camera › Screen capture › Keyguard customizations › Camera on secure keyguard screens › Fingerprint sensor on secure keyguard screens › Only redacted notifications on secure keyguard screens › Trust agents on secure keyguard screens › Installation of non-Google Play apps › Access debugging features 	<p><i>Work and Personal – User Privacy</i></p> <ul style="list-style-type: none"> › Specify caller ID information for incoming calls › Install apps using the app installer › Specify enable/disable app verification › Add new users and user profiles › Copying data to the clipboard and paste in a related profile › Add or remove accounts <p><i>Work Space only</i></p> <ul style="list-style-type: none"> › Configure Bluetooth settings › Configure mobile network settings › Configure tethering and mobile hotspots › Reset device to factor defaults › Mount external physical media › Delete users from the device › Send/receive SMS messages › Transfer files to/from the device via USB › Specify automatic date/time settings
Passwords	
<ul style="list-style-type: none"> › Minimum password requirements › Failed attempts › Inactivity time lock › Minimum length › Expiration timeouts › Minimum letters (uppercase, lowercase) › Minimum symbols › History restrictions 	

BlackBerry Secure Connect Plus³

BlackBerry Secure Connect Plus provides BES12 customers with a secure, network interface from Android devices to the enterprise servers. The service offers high throughput with an additional layer of encryption for data-in-transit. It can be automatically deployed to user’s devices via Google Play for Work.

- › Eliminates the need for managing mobile VPNs
- › Allows all types of IP traffic (including TCP and UDP)
- › Enhances the user experience when streaming data and video
- › Increases operational efficiencies

For more details visit blackberry.com/googleandroid

¹BES12 support for Android™ for Work is included for Android™ 5.1 devices and above. ²Requires a BES12 Silver license (Perpetual or Subscription). Refer to BES12 support documentation for details on BES12 v12.3 policies. ³Requires BES12 Gold license (Perpetual or Subscription).