

Embracing Employee-Acquired Smartphones without Compromising Security



Best practices for managing personal-liable devices
with BlackBerry Enterprise Server Express.

Table of Contents

Introduction	1
BlackBerry Enterprise Server Express	2
Best Practices for Activating Devices on BlackBerry Enterprise Server Express	2
Easily Manage personal-Liable Devices with Built-In IT Policy Controls	3
Minimizing Support Time	4
Conclusion	4
Appendix A: Getting started email template	5
Appendix B: Intranet page example	6
Appendix C: IT Policy Quick Reference Guide for an Personal-Liable Strategy	7 - 9

Introduction

Individually acquired smartphones - those devices that employees purchase outright or get reimbursed for by the organization - are on the rise. A number of factors are influencing the fast growth of these “personal-liable” devices, including: corporate cost-cutting measures which have slowed the purchase of company-issued devices; employees purchasing devices in response to employer expectations that workers be increasingly mobile; and employees increasingly desiring smartphones with data plans for personal use with the intention that the device will serve “double duty” for their business email and network access.

The trend toward personal-liable smartphones is not going away. IDC expects personal-liable devices to outnumber corporate-liable devices by 2013.⁽¹⁾

With the influx of these personal-liable devices, IT departments are faced with a rapidly accelerating growth of mobility in the enterprise - growth that is often occurring outside of their central plan for scaled expansion. And while this growth can offset the burden of procurement to the user population, managing growth requires the right technology and policy approach. IT needs a solution for heterogeneous device support that does not compromise security or cost controls.

“Personal-Liable” Defined...

A term used to describe converged mobile devices (commonly referred to as smartphones) that are purchased outright by the personal user, or purchased and expensed back, but not reimbursed formally as part of a company-established reimbursement policy.⁽¹⁾ Often used interchangeably with “individual-liable.”

BlackBerry Enterprise Server Express

According to Yankee Group, most employees prefer employee-acquired versus employer-issued smartphones to access corporate applications.⁽²⁾ IT departments, of course, prefer the centralized control that employer-issued smartphones afford.

BlackBerry® Enterprise Server Express is designed to provide this common ground, where the needs of both IT and users can be met. That is, IT can allow individual employees to use the personal devices they paid for themselves.

BlackBerry Enterprise Server Express offers a cost-effective solution for businesses of any size that want to manage BlackBerry® smartphones that employees purchase and pay for, but use for work purposes. It provides advanced BlackBerry smartphone business features with no software licensing fees or additional per user license fees, and works with most personal BlackBerry data plans or BlackBerry enterprise data plans.

Visit blackberry.com/go/express to learn more about BlackBerry Enterprise Server Express.

Top IT Security Risk: Lack of Auto Destruct Data-Wiping Plans

Computerworld lists, “No auto-destruct/data-wiping plans” as a top security risk threatening IT departments amidst the growth of personal-liable devices:

While other platforms can perform remote wipes, the BlackBerry server also provides confirmation that the wipe was accomplished, which would give a company a stronger position if a case involving a smartphone data breach ended up in court... “If you can’t prove you did the wipe, it doesn’t sound good,” says Philippe Winthrop, analyst at consultancy Strategy Analytics Inc.⁽³⁾

Best Practices for Activating Devices on BlackBerry Enterprise Server Express

IT can transfer set-up tasks to their users by creating a simple self-service process for users to configure their personal-liable smartphones.

There are two options for doing so, the first of which can provide a lighter workload for IT administrators:

- 1) The first option is to use BlackBerry® Web Desktop Manager - a web-based application that allows users to configure and manage BlackBerry smartphones via USB connection at their own computer (or from any computer with Microsoft® Internet Explorer and an internet connection). Learn more about BlackBerry Web Desktop Manager at blackberry.com/go/webdesktopmanager
- 2) Alternatively, users can download BlackBerry® Desktop Manager and proceed with the configuration using software installed on their workstation.

In addition to these two self-service models, IT can choose to activate devices on behalf of the employee. If the BlackBerry smartphone is provisioned on a BlackBerry enterprise data plan, IT can wirelessly activate the device from the BlackBerry® Administration Service console. Another option is for IT to activate the devices using the BlackBerry Administration Service and a USB cable. This requires that the BlackBerry smartphone is brought to an IT person.

Whichever approach is used, employees will need to email IT to request access to corporate data on their BlackBerry smartphones. To help increase adoption, IT can provide easy-to-follow instructions on an intranet page or by email.

Appendices A and B include examples.

Easily Manage Personal-Liable Devices with Built-In IT Policy Controls

Supporting personal-liable devices in your organization means striking a balance between enterprise and employee needs. This can be done by leveraging the built-in IT Policy controls of BlackBerry Enterprise Server Express. Certain policies can also help keep costs predictable in the event that the organization is paying for the monthly service plan fees.

Application Policies

Application use on smartphones has been increasing steadily with worldwide downloads from application stores growing over eight times from 2009 to 2013 reaching 21.6 billion a year. ⁽⁴⁾

Placing minimal limitations on how employees use their own device (for example, not restricting applications) can promote wider acceptance of company policy around personal-liable devices.

BlackBerry Application Security

J Gold Associates states, “BlackBerry includes an inherent mechanism for verifying the signature of each installed application to assure the application has not been tampered with.”

“Further, since third party applications run in a Java Virtual Machine, hacking into the base operating system of the device is extremely difficult if not impossible. This makes it very difficult for malware and rogue applications to affect the core operations of the device.” ⁽⁵⁾

Security Policies

With personal-liable devices and security there is a balance between protecting corporate data and minimizing user frustration. Password protection on the device can be relatively unobtrusive to the user and can help to ensure that data is not readily available in the event that the device is lost or stolen.

Cost Policies

If the company is paying for the monthly service plan fees, then IT may want to use IT policy control to help make monthly costs more predictable. Limiting attachment sizes or the use of tethered modem (unless this is used for work purposes) can help reduce the number of megabytes used per month. Especially for users that are roaming, having some limitations on the amount of data used can help keep costs under control.

Appendix C includes further recommendations around IT policy control for a personal-liable strategy.

Minimizing Support Time

IT can help to reduce their workload by promoting self-service tools for employees with personal-liable BlackBerry smartphones and by training help desk staff.

- getting started instructions
- dos and don'ts for corporate security
- who to contact with support issues
- support FAQs
- steps for employees to follow to secure the BlackBerry smartphone if it is lost or stolen

Appendix B includes examples.

Conclusion

With an increasing number of individually acquired smartphones, IT departments need to be defining their strategy for dealing with these devices. BlackBerry Enterprise Server Express can be used as a cost effective solution to help IT manage the challenges of security, cost and IT control while balancing the needs of employees.

Smartphones on the CIO Agenda

“...smartphones are now finally on the CIO agenda and, in fact, one of the most difficult topics: there are a variety of different platforms; employees are bringing their own phones to work; applications can compromise security; and the monthly costs are unpredictable.

What they told me again and again is that IT is losing control of smartphones and yet retaining all the accountability.”⁽⁶⁾

Sources:

- (1) IDC: “Market Analysis. Worldwide Business Use Converge Mobile Device 2009-2013 Forecast and Analysis” Doc # 218524; June 2009
- (2) Yankee Group Anywhere Enterprise—Large: “2009 U.S. Transforming Infrastructure Applications Survey, Wave 1-4”
- (3) Computerworld: “News: Smartphones need smart security practices”; 20 January 2010
- (4) Gartner: “Dataquest Insight: Applications Stores; The Revenue Opportunity Beyond the Hype”; 16 December 2009
- (5) J. Gold Associates White Paper: “Choosing an Enterprise-Class Wireless Operating System: A Comparison of BlackBerry, iPhone and Windows Mobile”; February 2009
- (6) CIO Magazine: “Five Trends Influencing the CIO Smartphone Agenda”; 2 February 2010

Appendix A

Getting started email template



Bring Your BlackBerry Smartphone to Work

Get Synced With Work and Home!

We're now connecting BlackBerry® smartphones that you purchase and pay for yourself to our company IT systems. By connecting your BlackBerry smartphone, you will have access to:

- Advanced business email features – including setting out-of-office notifications, email flagging, folder management and more, all from your BlackBerry smartphone
- Wireless sync with your Microsoft® Outlook® calendar – send out, respond to or forward meeting invitations, lookup availability of colleagues before scheduling a meeting
- Document and file access – find local and remote files using the “Files” application. You can open, view, edit, save or email files directly from your BlackBerry smartphone. Popular supported file formats include JPEG, Adobe® PDF, Microsoft® Word, Microsoft® Excel and Microsoft® PowerPoint®.

To request having your personal BlackBerry smartphone connected to our company's IT systems, please email the IT desk at [\[email address here\]](#).

For more information and resources, visit: [\[url for intranet page\]](#)

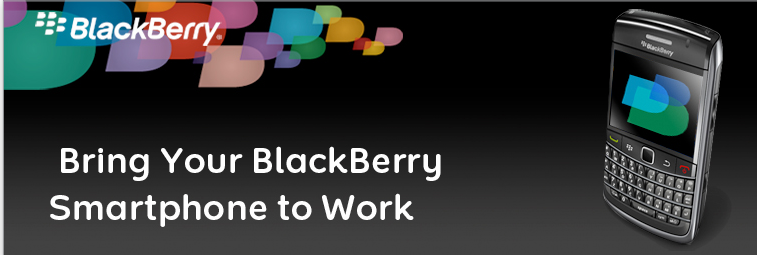
Note: Certain features may require a minimum version of BlackBerry® Desktop Software and/or BlackBerry® Device Software.

Company logo goes here

An HTML version of this template is available at <http://na.blackberry.com/eng/support/software/quickstart/express.jsp>

Appendix B

Intranet page example



Bring Your BlackBerry Smartphone to Work

Get Synced with Work and Home!
We're now connecting BlackBerry® smartphones that you purchase and pay for yourself to our company IT systems. You'll have access to exciting new features like wireless syncing with your Microsoft® Outlook® calendar and document access. [Click here](#) to learn more about business software for BlackBerry smartphones.

Getting Started
How to connect your BlackBerry smartphone to our IT systems:

- Contact the IT Help Desk**
email: address@here.com or call: XXX-XXXX
- Download BlackBerry® Desktop Software**
and proceed with activating your device using a USB cord.

or

Access BlackBerry® Web Desktop Manager
from your computer and activate your device using a USB cord.

Self-service Tools
Get the most out of connecting your BlackBerry smartphone to work:

- [FAQs for commonly asked support questions](#)
(post additional information or provide link to another area in your intranet)
- [Check your phone usage](#)
(post additional information or provide link to another area in your intranet)
- [Corporate security – do's and don'ts](#)
(post additional information or provide link to another area in your intranet)

For further assistance, please email the [IT Help Desk](#) or call us at XXXXX

Help Desk Support
Training and resources to support employees connecting their BlackBerry smartphones to work

Online Training
[BlackBerry Enterprise Server Express Installation](#)
[BlackBerry Enterprise Server Express Activation](#)
[BlackBerry Enterprise Server Express Administration Tutorials](#)

Resources
[Support Documentation](#)
Installation, administration and policy reference guides, release notes
[BlackBerry Expert Support Center](#)
[Knowledge Base Articles](#)

Company logo goes here

An HTML version of this template is available at <http://na.blackberry.com/eng/support/software/quickstart/express.jsp>

Appendix C

IT Policy Quick Reference Guide for an personal-Liable Strategy

IT Policies	Default Setting	Notes for an personal-liable strategy
Common policy group		
Disable MMS	False	Set this IT policy rule to TRUE to hide MMS functionality on the BlackBerry smartphone. <u>Personal Liabile Note:</u> MMS files can have executables attached, which increases malware exposure. Other considerations are how prevalent the use of MMS is with your users and how much data is consumed by MMS attachments.
Disable Voice Note Recording	No	Set to YES to turn off the voice note recording feature and prevent applications on the BlackBerry smartphone from accessing it
Device Only Items		
Allow SMS	True	Set this rule to TRUE to allow text messaging. <u>Personal Liabile Note:</u> SMS is a popular method of communication outside of work.
Maximum Password Age	Null	Can be set to 65,535 days
Maximum Security Timeout	Null	Can be set between 10 and 480 minutes
Minimum Password Length	Null	Can be set between 4 and 14 characters
Password Pattern Checks	No Restriction	This rule can be changed to require that a BlackBerry smartphone password contains a combination of upper-case alphabetic, lower-case alphabetic, numeric, and special characters.
Password Required	False	Set this rule to TRUE to require the user to enter a password to unlock the BlackBerry smartphone
User Can Change Timeout	True	Specify whether the BlackBerry smartphone user can change the security timeout to any value less than the value you can set using the Maximum Security Timeout rule.
User Can Disable Password	True	Set this rule to FALSE to prevent users from disabling the BlackBerry smartphone password
Allow Peer-to-Peer Messages	Yes	Set to NO to hide PIN messaging functionality on the BlackBerry smartphone. Note: To block incoming PIN messages, set the Firewall Block Incoming Messages IT policy rule in the Security policy group.
Enable Long-Term Timeout	Yes	Set to YES to force the BlackBerry smartphone to lock automatically after 60 minutes. Note: You can use the Periodic Challenge Time rule to shorten the timeout interval.
Bluetooth® policy group		
Disable Bluetooth	False	Set to FALSE to support Bluetooth technology on the BlackBerry smartphone. <u>Personal Liabile Note:</u> Bluetooth smartphone accessories such as ear pieces are commonly used for hands-free calling.
Camera policy group		
Disable Photo Camera	False	Set to FALSE to allow the ability to take pictures with the camera on the BlackBerry smartphone. <u>Personal Liabile Note:</u> Camera functionality is often used for personal use. Set this rule to FALSE to turn on the video camera feature.
Disable Video Camera	False	<u>Personal Liabile Note:</u> Video camera functionality is often used for personal use.
Email Messaging policy group		
Confirm External Image Download	False	Set to FALSE to specify that the BlackBerry smartphone does not displays a confirmation dialog box to a user when the user clicks Get Images in an HTML-formatted email message
Disable Manual Download of External Images	False	Set to FALSE to specify that the BlackBerry smartphone user can manually request URL-reference content (images) that are embedded in email messages.
Disable Rich Content Email	False	Set to FALSE to specify that email messages sent to the BlackBerry smartphone in Rich Content (HTML) format. <u>Personal Liabile Note:</u> HTML and rich text viewing is practical for viewing e-newsletters as well as emails that contain formatting such as bold or underline.
Maximum Native Attachment MFH Attachment Size	3145728 Bytes	<u>Personal Liabile Note:</u> Can be lowered to help control monthly service plan costs.
Maximum Native Attachment MFH Total Attachment Size	5242880 Bytes	<u>Personal Liabile Note:</u> Can be lowered to help control monthly service plan costs.
Maximum Native Attachment MTH Attachment Size	10240 Kilobytes	<u>Personal Liabile Note:</u> Can be lowered to help control monthly service plan costs.

IT Policies	Default Setting	Notes for an personal-liable strategy
Password policy group		
Forbidden Passwords	Null	This rule specifies the passwords that a BlackBerry® smartphone user cannot use. You must separate multiple passwords with a comma (,).
Maximum Password History	0	Can be set to a maximum of 15 passwords
Periodic Challenge Time		If you set the Enable Long-Term Timeout IT policy rule to YES, the security timeout is 60 minutes after which the BlackBerry smartphone locks and prompts the user to type the password, regardless of whether the BlackBerry smartphone has been idle or in use during that interval. Type a periodic challenge time to shorten or extend the interval to a value between 1 to 1440 minutes (24 hours). Note: To disable the security timeout, set the Enable Long-Term Timeout IT policy rule to NO and do not set a Periodic Challenge Time. Rule dependency: The BlackBerry smartphone uses this rule only if a password is set.
Set Password Timeout	2-30 Minutes*	Can be set between 0 and 60 minutes.
Set Maximum Password Attempts	10	Can be set between 3 and 10 attempts
Suppress Password Echo	Yes	Set to YES to specify whether, after a given number of incorrect password attempts, the characters that a BlackBerry® smartphone user types in the Password dialog box appear on the screen.
Periodic Challenge Time		If you set the Enable Long-Term Timeout IT policy rule to YES, the security timeout is 60 minutes after which the BlackBerry smartphone locks and prompts the user to type the password, regardless of whether the BlackBerry smartphone has been idle or in use during that interval. Type a periodic challenge time to shorten or extend the interval to a value between 1 to 1440 minutes (24 hours). Note: To disable the security timeout, set the Enable Long-Term Timeout IT policy rule to NO and do not set a Periodic Challenge Time. Rule dependency: The BlackBerry smartphone uses this rule only if a password is set.
Security policy group		
Content Protection Strength	Null	Can be configured to strong to use a 160-bit ECC public key, stronger to use a 283-bit ECC public key, or strongest to use a 571-bit ECC public key. As protection strength increases performance becomes slightly slower.
Disable External Memory	False	Set to FALSE to allow the expandable memory (microSD) feature to work on supported BlackBerry smartphones.
Disable IP Modem	False	Set to TRUE to turn off the Internet Protocol (IP) modem feature on application BlackBerry devices. <u>Personal Liable Note:</u> Using the BlackBerry smartphone as a tethered modem can add cost to the monthly service plan.
Disallow Third Party Application Downloads	False	Set to FALSE to specify that applications that are not digitally signed by the Research In Motion® signing authority system are permitted on the BlackBerry® smartphone if the user tries to download the applications or the BlackBerry Enterprise Server or another party sends the applications to the device.
Encryption On On-Board Device Memory Media Files	Allowed	Change this rule to Required or Disallowed to prevent a user from changing this setting on the BlackBerry smartphone.
External File System Encryption Level	Not Required	Use this rule to require that a BlackBerry smartphone encrypt a media card, either including or excluding media card files. This rule cannot be used to encrypt files that a BlackBerry smartphone user transfers to the media card manually (for example, from a USB mass storage device).
Force Lock When Holstered	No	Use to specify whether a BlackBerry® smartphone locks when a BlackBerry smartphone user inserts it in the holster.
Required Password Pattern	Null	Use to specify the permitted structure of a BlackBerry® device password. Passwords can contain Latin-1 character only.
Allow Third Party Apps to Use Serial Port	Yes	Specify whether third-party applications on the BlackBerry smartphone can use the serial port, IrDA®, or USB ports.
Allow External Connections	Yes	Specify whether applications can initiate external connections (for example, to WAP, SMS, or other public gateways) on the BlackBerry smartphone.
Allow Split-Pipe Connections	No	Specify whether applications can open both internal and external connections simultaneously. Note: If you set this rule to YES, applications can surreptitiously collect data from inside the firewall and send it outside the firewall without any auditing, introducing a possible security issue.
Disable 3DES Transport Crypto	No	Prevent the BlackBerry device from using the Triple DES algorithm to encrypt and decrypt packets that the BlackBerry smartphone and the BlackBerry Enterprise Server that sends the IT policy send between them. Set to YES to require the BlackBerry smartphone and the BlackBerry Enterprise Server to use the AES algorithm to encrypt and decrypt the communication between them.
Disable GPS	No	Specify whether the GPS functionality on the BlackBerry smartphone is turned on.
Disable USB Mass Storage	No	Prevent the USB Mass Storage feature or the Media Transfer Protocol feature from working on supported BlackBerry smartphone. If you set to YES, the BlackBerry smartphone cannot use an external file system connected to the USB port. This means that the ability to transfer files to an external file system using the Media Manager with BlackBerry Desktop Manager Version 4.2.2 and 4.3 is turned off.
Allow Resetting of Idle Timer	No	Specify whether the BlackBerry smartphone will allow third party applications to reset the device's idle timer, bypassing the security timeout.
Reset to Factory Defaults on Wipe	No	Set to YES to require the BlackBerry smartphone to permanently delete its stored IT policy and delete all third party applications, in addition to performing the BlackBerry smartphone wipe process. For BlackBerry smartphone version 5.0.0 and above, the IT policy is enforced on the remote wipe and will also be enforced on a local wipe i.e. when the user exceeds the maximum password attempts or performs a security wipe.

IT Policies	Default Setting	Notes for an personal-liable strategy
PIN Synchronization policy group		
Disable SMS Messages Wireless Sync	Yes	If you change this rule to No, the BlackBerry Enterprise Server Express logs all SMS text messages in unencrypted format to the log file that you specify. Make sure that the log file is in a location that restricts internal and external user access.
Wired Software Updates policy group		
Allow Web-Based Software Loading	No	Use to specify whether a user can update the BlackBerry Device Software using the web-based software loading feature.
Cryptographic Services Backup	Yes	Use to specify whether the BlackBerry® smartphone can back up cryptographic services data when a user updates the BlackBerry Device Software.
BlackBerry App World policy group		
Enable Wireless Service Provider Billing	No	Set to YES to permit a user to purchase applications from BlackBerry App World using the wireless service provider's purchasing plan. Set to NO to prevent
Global policy group		
Allow Phone	Yes	Set to NO to prevent users from making and receiving any phone calls except emergency calls from their BlackBerry smartphones. NOTE: The phone icon is still visible to users on their BlackBerry smartphone.
Allow Browser	Yes	Set to NO to hide the BlackBerry Browser icon on the BlackBerry smartphone.

Visit blackberry.com/go/swdocs for additional installation and administrative information on BlackBerry Enterprise Server Express.



This material, including all material incorporated by reference herein or made available by hyperlink, is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors or omissions in this material and shall not be liable for any type of damages related to this material or its use, or performance, or non-performance of any software, hardware, service, or any references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites.

© 2010 Research In Motion Limited. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ 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. MKT-31475-001