

Guidance

BlackBerry 10.3 - Work and Personal - Regulated

Published

Contents

1. Usage scenario
2. Summary of platform security
3. How the platform can best satisfy the security recommendations
4. Network architecture
5. Deployment process
6. Provisioning steps
7. Policy recommendations
8. Enterprise considerations

This guidance is applicable to devices running BlackBerry OS 10.3.x in Work and Personal - Regulated (formerly known as EMM-Regulated with Balance) mode and is an update of the previous guidance for BlackBerry OS 10.2. The guidance was developed following testing performed on a Classic device running BlackBerry OS 10.3.1 and managed with BlackBerry Enterprise Service (BES) 12.

Licensing requirements changed between BES 10.2 and BES 12. Using Work and Personal - Regulated mode requires either a Gold SIM license (purchased from your wireless service provider) or a Gold BES license (purchased from BlackBerry or a BlackBerry partner).

1. Usage scenario

BlackBerry devices will be used remotely over 3G, 4G and non-captive Wi-Fi networks to enable a variety of remote working approaches such as:

- accessing OFFICIAL email
- reviewing and commenting on OFFICIAL documents
- accessing the OFFICIAL intranet resources, the Internet and other web resources

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the confidentiality and integrity of the traffic, and to allow the devices and data on them to be protected by enterprise protective monitoring solutions.
- Arbitrary third-party application installation by users is not permitted on the device. An enterprise application catalogue should be used to distribute in-house applications and trusted third-party applications to run in the work space.
- A combination of procedural and technical controls are put in place to effectively risk manage the end user's use of the personal space. This may include restrictions on which applications users are permitted to install from BlackBerry World into the personal space.

2. Summary of platform security

This platform has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See [How the platform can best satisfy the security recommendations](#) for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	<p>There are two types of VPN:</p> <ul style="list-style-type: none">- BlackBerry VPN- IPsec VPN <p>Neither of the VPNs have been independently assured to Foundation Grade. Traffic from the personal space is not protected by the enterprise VPN.</p> <p>There is currently no assurance scheme to assess the strength and robustness of the proprietary BlackBerry VPN.</p>
2. Assured data-at-rest protection	<p>The device's data encryption has not been independently assured to Foundation Grade.</p>
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	

7. Malicious code detection and prevention

8. Security policy enforcement

9. External interface protection

10. Device update policy


11. Event collection for enterprise analysis

[!] Although system logs can be retrieved remotely from a device, most of the information is encrypted and only intended for decryption by the vendor. Collecting forensic log information from a device is very difficult. Some application-level logs can be collected remotely.

12. Incident response

2.1 Significant risks

The following key risks should be read and understood before the platform is deployed.

- The VPNs have not been independently assured to Foundation Grade, and do not support some of the [mandatory requirements expected from assured VPNs](#) . There is currently no assurance scheme for the proprietary BlackBerry VPN, though it is based on technology which was previously assessed under the CESG Assisted Product Service (CAPS). Without assurance in the VPN there is a risk that data transiting from the device could be compromised.
- The device's Advanced Data At Rest Protection (ADARP) has not been independently assured to Foundation Grade. Without assurance there is a risk that data stored on the device could be compromised.
- BlackBerry 10.3 does not use any dedicated hardware to protect its password hashes. If an attacker can get physical access to the device, they can extract password hashes and perform an offline brute-force attack to recover the personal or work space password.

3. How the platform can best satisfy the security recommendations

This section details what is required to meet the security recommendations for this

platform.

3.1 Assured data-in-transit protection

Use either the native BlackBerry VPN client or the IPsec VPN client as neither has been independently assured. If a Foundation Grade assured VPN client for this platform becomes available, then this assured client should be used instead.

3.2 Assured data-at-rest protection

Use the device's Advanced Data At Rest Protection (ADARP). When the device is locked, work applications that are 'ADARP aware' are able to write data into an encrypted file system, but not decrypt it. Work applications that are not 'ADARP aware' also have their data encrypted, but are suspended when the device is locked.

Work space data is protected when the device is locked or powered off. The decryption keys are not available until the user's work space password has been entered to unlock the work space.

3.3 Authentication

Use a password to authenticate the user to the device and a different, strong 9-character password to authenticate the user to the work space. On first use after boot, the work space password unlocks a key which encrypts certificates and other credentials, giving access to enterprise services.

3.4 Secure boot

This requirement is met by the platform without additional configuration.

3.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration.

3.6 Application whitelisting

An enterprise application catalogue can be established to permit users access to an approved list of applications in the corporate space. If the personal space is enabled, the enterprise cannot whitelist applications users can install in the personal space. This could

be procedurally managed via user security procedures.

3.7 Malicious code detection and prevention

Use an enterprise application catalogue which should only contain approved in-house applications which have been checked for malicious code. For the personal space, the device supports two application stores; namely BlackBerry World and the Amazon App Store. Applications from both are checked for malware by the BlackBerry Guardian system. Disable side-loading of applications by disabling Developer Mode via policy.

3.8 Security policy enforcement

Settings applied through BES cannot be changed by the user.


3.9 External interface protection

Wi-Fi, NFC, Bluetooth and the use of USB interfaces can all be disabled if not required. If BlackBerry Blend is enabled, it should be configured through BES IT policy to not allow access to work data, work files or the work browser.

3.10 Device update policy

The enterprise can update applications remotely using the BES, and can check which device software versions are in use.

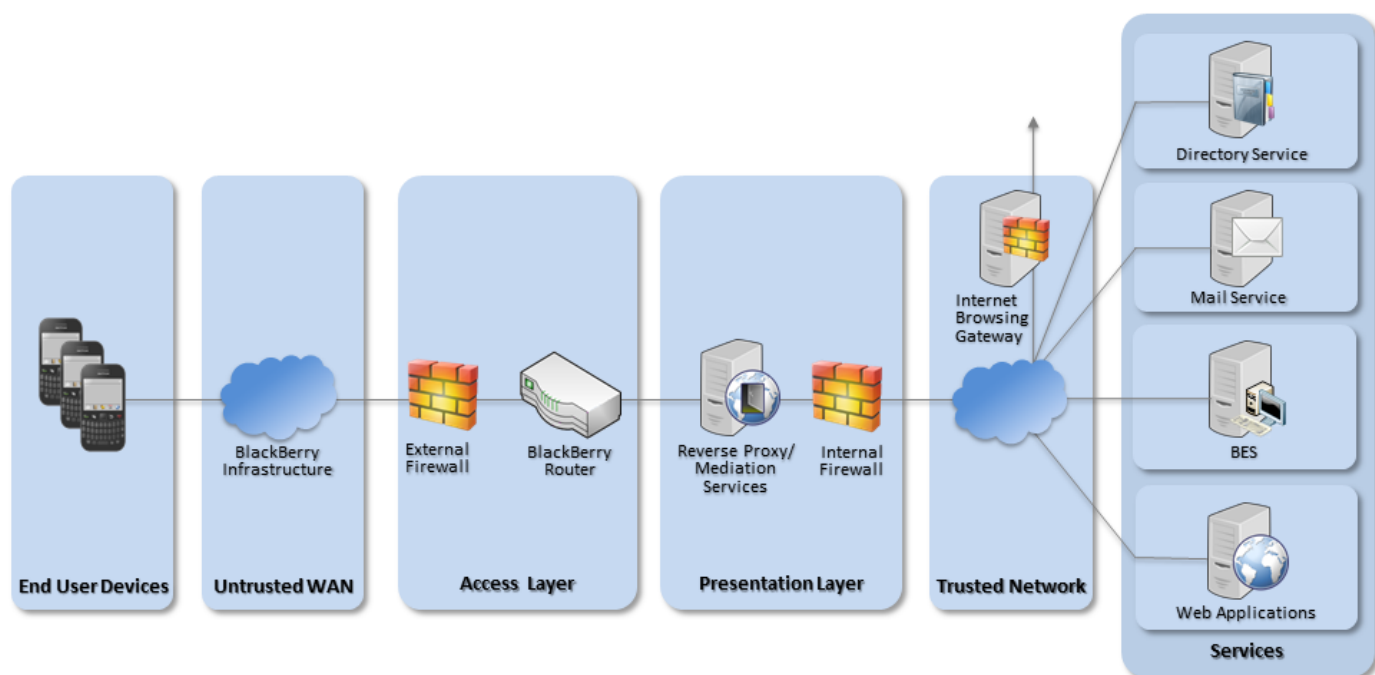
3.11 Event collection for enterprise analysis

BlackBerry 10 devices can be configured to forward the call log and the logs for the BBM, PIN messages, SMS/MMS and video chat applications to the enterprise. Provided the user has enabled Remote Log Collection, the BES can also trigger the device to collect operating system logs, which must be sent to BlackBerry for analysis. More information on logging is given at <http://www.blackberry.com/btsc/KB26038> .

3.12 Incident response

BlackBerry 10 devices can be locked, wiped, and configured remotely by their BES.

4. Network architecture



Recommended network architecture for BlackBerry 10 deployments

BES 12 is managed through a web-based interface and no longer requires a dedicated management workstation.

5. Deployment process

To prepare the enterprise infrastructure:

1. Procure and set up a BES Server which is compatible with BlackBerry 10.3 devices.
2. Obtain SIM cards with Gold SIM Licenses from the carrier or a Gold BlackBerry Server license.
3. Deploy and configure the requisite network components as described previously.
4. Create configuration profiles for the end user devices in line with the guidance given in this document.
5. Any Certificate Authority certificates that are not registered externally will need to be added to a CA certificate profile on the BES. Client certificates can be provisioned either by using a SCEP profile, or by adding certificates to an individual user account or user group.

6. Provisioning steps

To provision each device to the enterprise infrastructure:

1. Assign the IT policy and activation profile to the user or user group using the BES management interface.
2. Use the BES to send an activation email with password to the user's desktop email account, or supply the activation information directly.
3. Supply the device to the user. When the user follows the activation steps, the work space will be created on the device and both the new workspace and existing personal space will be encrypted.

Alternatively, the Wired Activation Tool for BES 12.1 can be used to activate devices locally over USB.

7. Policy recommendations

7.1 BES IT Policy

The following IT Policy settings should be applied to BlackBerry 10 devices by creating configurations on the BES. Other settings are either not applicable to this mode, or should be chosen according to organisational policy and requirements.

Password Section

Password required for work space	Selected
Minimum password length	9
Minimum password complexity	At least 1 letter, 1 number, and 1 special character
Security timeout	10 (minutes)
Maximum password attempts	5
Maximum password history	8
Maximum password age	90
Require full device password	Selected
Define work space and device password behaviour	Different

Device functionality section

Allow voice control	Allow only phone and device status
Allow BlackBerry Assistant when locked	Not selected
Allow voice dictation	Not selected
Allow user-created Wi-Fi profiles	As per organisational policy
Allow media sharing	Not selected
Allow Miracast	Not selected
Allow transfer of work data using NFC	Not selected
Allow Bluetooth file transfer using OBEX	Not selected
Allow Bluetooth page scan	Not selected
Allow transfer of work contacts Using Bluetooth PBAP or HFP	Not selected
Allow transfer of work messages using Bluetooth MAP	Not selected
Allow transfer of work files using Bluetooth OPP or a Wi-Fi Direct connection	Not selected
Allow Mobile Hotspot mode and tethering	Not selected
Allow user-created VPN profiles	Not selected
Allow USB OTG mass storage	Not selected
Apps section	
Allow wireless service provider apps	Not selected
Allow installing apps from other sources	Not selected
Allow Find More Contact Details	Not selected
Allow non-email accounts	Not selected
Allow other email messaging services	Not selected
Allow unified view for work and personal accounts and messages	Not selected
Allow opening links in work email messages in the personal browser	Not selected
Allow forwarding or adding recipients to private messages	Not selected
Display warning message for external email addresses	Selected
External email domain allowed List	Appropriate list of domains

Allow Hotspot Browser	Not selected
Allow joyn	Not selected
Allow BBM Video over work networks	Not selected
Allow sharing work data during BBM Video screen sharing	Not selected
Security and privacy section	
Force personal space data encryption	Selected
Force media card encryption	Selected
Allow lock screen preview of work content	Not selected
Allow app security timer reset	Not selected
Allow personal apps to use work networks	Not selected
Allow personal apps access to work contacts	None
Allow work apps to access shared files or content in the personal space	Not selected
Restrict development mode	Selected
Allow BlackBerry Bridge to access the work space	Not selected
Allow computer to access device	Not selected
Submit logs to BlackBerry	Not selected
Allow CCL data collection	Not selected
Force advanced data at rest protection	Selected

8. Enterprise considerations

8.1 Organisation notices

Organisations can create their own notices to be displayed during device activation and when the device restarts, which can be used to display security policy information to the user. For a notice to be displayed on device restart, the 'Display organization notice after device restart' IT policy must be selected.

8.2 Automatic wipe

Organisations might wish to use the 'Wipe the device without network connectivity' IT policy to delete all data from devices that fail to contact the work network for a defined period of time.

8.3 Proprietary VPN

The BlackBerry VPN is a proprietary set of technologies which operate differently to the remote access functions of other platforms. As such, organisations wishing to deploy BlackBerry 10 in conjunction with other remote access solutions may need to consider how to integrate the two disparate solutions into the same network architecture.

8.4 BlackBerry Balance

Whilst applications in the work space can be whitelisted by the organisation, applications in the personal space cannot. Consequently, users should pay due care and attention to what applications they download and install to the personal workspace, as applications may be able access personal data stored there.

Users must not store sensitive work data in the personal space on the device, as this space is not protected to the same level as the work space. Should a user's device be lost, the administrator can choose to remotely wipe the entire device or just the work space. Whilst wiping the whole device may be preferential from a security perspective, there may be other policy or legal considerations to take into account before erasing the entire device.

Legal information

This guidance is issued by CESA, the UK's National Technical Authority on Information Assurance. One of the roles of CESA is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESA. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESA cannot, then, accept any liability

whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. This guidance is UK Crown Copyright. All Rights Reserved.