

Guidance

BlackBerry 10.2 - EMM-Regulated with Balance

Published 10 June 2014

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 10.2 in EMM-Regulated with Balance (or Work and Personal - Regulated) mode. The guidance was developed following testing performed on a Z30 device running BlackBerry OS 10.2.1.

Licensing requirements changed with BlackBerry Enterprise Server (BES) 10.2 and were further simplified in BES 10.2.1. Using an EMM-Regulated mode requires either a Regulated-level EMM data plan or an EMM-Regulated for BlackBerry license. EMM-Regulated with Balance mode was introduced with BES 10.2. It has the same work/personal split as the existing EMM-Corporate mode but gives the enterprise far more control of the whole device.

When deciding which mode is appropriate for a BlackBerry 10.2 deployment, departments should consider not only the security implications, but also cost and usability associated to the three modes. Where the department deems the residual risks of using EMM-Corporate to be acceptable they should feel free to do so.

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
- BlackBerry Balance is disabled where possible to minimise the risk of the device being attacked or data leaking from the personal perimeter of the device
- 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
- A blend of procedural and technical controls are put in place to effectively risk manage end-user's use of the personal perimeter. This may include restrictions on which applications users are permitted to install from BlackBerry World into the personal perimeter

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.</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> <p>Encryption keys protecting sensitive data remain in device memory when the device is locked.</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 [!] There is no facility for collecting logs remotely from a device, and collecting forensic log information from a device is very difficult.

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 chosen VPN there is a risk that data transiting from the device could be compromised
- The device's native data encryption has not been independently assured to Foundation Grade, and does not support some of the [mandatory requirements expected from assured full disk encryption products](#). Without assurance there is a risk that data stored on the device could be compromised
- BlackBerry 10.2 does not use any dedicated hardware to protect its keys. 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 encryption password
- Encryption keys protecting sensitive data in the corporate perimeter remain in device memory when the device is locked. This means that if the device is attacked while powered on and locked, keys and data on the device may be compromised without the attacker knowing the 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 the native BlackBerry VPN client instead of the IPsec VPN client as neither has been independently assured, but BlackBerry recommend the native client for usability reasons. 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 native data encryption. The corporate perimeter is protected when powered off, but is not protected when the device is locked.

The key is protected in hardware and not available until the user's password has been entered for the first time after boot.

3.3 Authentication

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

Users should be encouraged to secure the personal perimeter with a suitable PIN/password.

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 perimeter. If the personal perimeter is enabled, the enterprise cannot whitelist applications users can install. 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. 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.

3.10 Device update policy

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

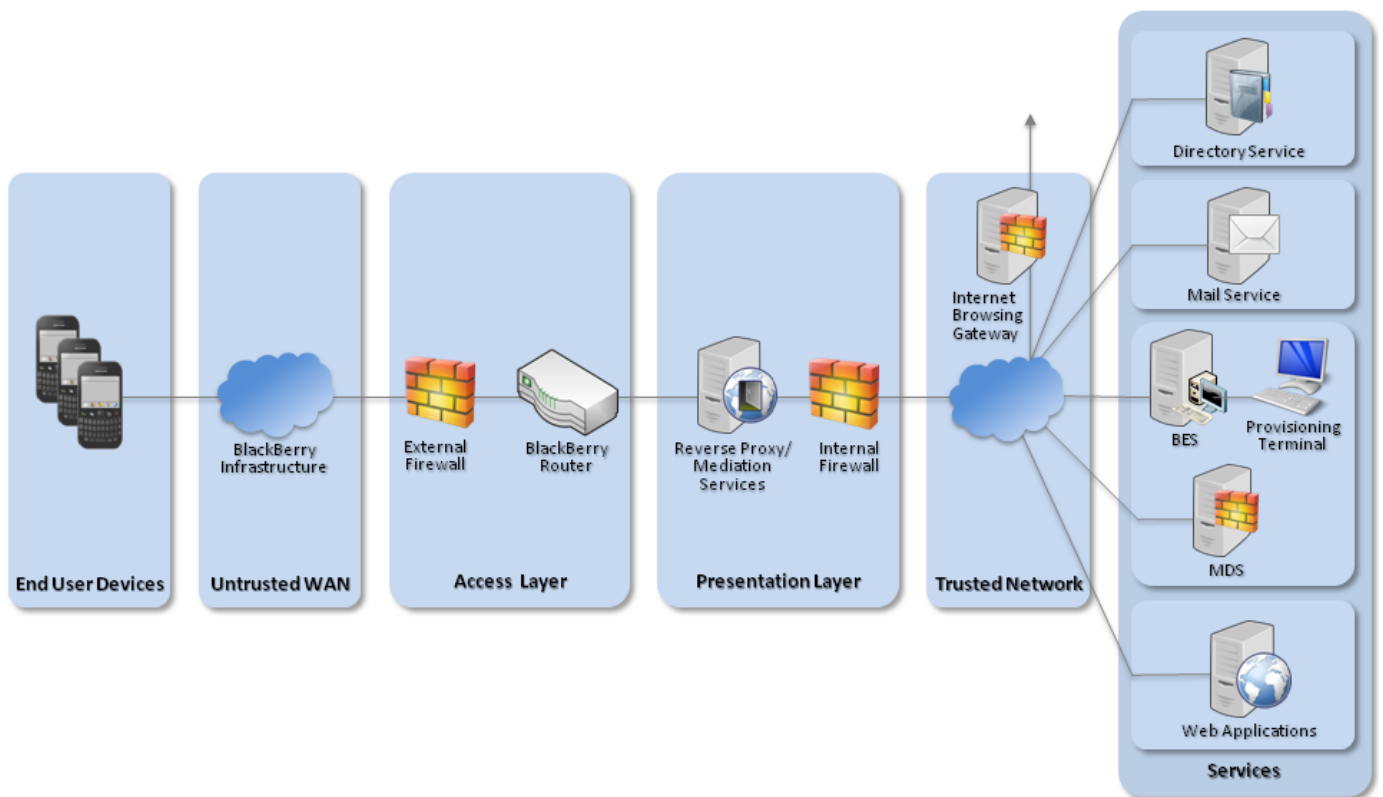
3.11 Event collection for enterprise analysis

BlackBerry 10 does not support remote or local historic event collection for enterprise analysis of security incidents, though the devices can be configured to forward sent messages (for example, SMS) to the enterprise for logging. 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

The provisioning terminal should only be used for managing the BES and BlackBerry devices, and should not be used for accessing the Internet or any other corporate applications.

5. Deployment Process

To prepare the enterprise infrastructure:

1. Obtain SIM cards on an EMM-regulated tariff from the carrier
2. Procure and set up a BES Server which is compatible with BlackBerry 10.2 and later devices
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. Enterprise and User certificates will need to be installed into the shared folder on the BES under the `certs` folder. This includes any Certificate Authority certificates that are not registered externally.

6. Provisioning Steps

To provision each device to the enterprise infrastructure:

1. Put the appropriate SIM cards purchased earlier into the device and connect it to the provisioning terminal via USB
2. Assign the device to a user and upload the IT policies and any software configuration to the device
3. On the device, confirm that the work data on the device will be reset and that the new workspace will be encrypted. Then enter a new password for the device. The personal side will be disabled and the whole device will be encrypted

7. Policy Recommendations

The following IT Policy settings should be applied to BlackBerry 10 devices by creating configurations on the BES. Other settings (e.g. server address) should be chosen according to the relevant network configuration.

General Section

Mobile Hotspot Mode and Tethering	Disallow
-----------------------------------	----------

Hardware Section

Transfer Work Contacts Using Bluetooth PBAP or HFP	Disallow
--	----------

Transfer Work Data Using NFC	Disallow
------------------------------	----------

Transfer Work Files Using Bluetooth OPP	Disallow
---	----------

Transfer Work Messages Using Bluetooth MAP	Disallow
--	----------

Bluetooth File Transfer Using OBEX	Disallow
------------------------------------	----------

Bluetooth MAP	Disallow
---------------	----------

Logging Section

CCL Data Collection	Disallow
---------------------	----------

Log Submission	No
----------------	----

Password Section

Maximum Password Age	90
Maximum Password Attempts	5
Maximum Password History	8
Minimum Password Complexity	At least 1 letter, 1 number, and 1 special character
Minimum Password Length	9
Security Timeout	10
Apply Work Space Password to Full Device	No
Password Required for Work Space	Yes
Security Section	
Application Security Timer Reset	Disallow
BlackBerry Bridge	Disallow
Lock Screen Preview of Work Content	Disallow
Media Card Encryption	Yes
Network Access Control for Work Apps	No
Backup and Restore Work Space	Disallow
Personal Apps Access to Work Contacts	None
Personal Space Data Encryption	Yes
Restrict Development Mode	Yes
Share Work Data During BBM Video Screen Sharing	Disallow
Work App Access to Shared Files in Personal Space	Disallow
Work Network Usage for Personal Apps	Disallow
Backup and Restore Device	Disallow
Computer Access to Device	Disallow
Software Section	
External Email Address Warning Message	Yes
External Email Domain Allowed List	Appropriate list of domains
Find More Contact Details	Disallow

Forward or Add Recipients to Private Messages	Disallow
BBM Video Access to Work Network	Disallow
Open Links in Work Email Messages in the Personal Browser	Disallow
Unified View for Work and Personal Accounts and Messages	Disallow
Hotspot Browser	Disallow
joyn	Disallow
Media Sharing	Disallow
Miracast	Disallow
Non-email Accounts	Disallow
Other Email Messaging Services	Disallow
User-Created VPN Profiles	Disallow
Wireless Service Provider Apps	Disallow
Install Apps From Other Sources	Disallow

8. Enterprise Considerations

8.1 Proprietary VPN

The BlackBerry VPN is a proprietary set of technologies which operate differently to the remote access functions of other platforms in this guidance set. 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. The BlackBerry Enterprise Server can be used to facilitate this through its Universal Device Service component.

Legal Information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG 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 CESG. 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. CESG 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.