Guidance

BlackBerry 10.2 - EMM-Corporate

Published 10 June 2014

Contents

This guidance is applicable to devices running BlackBerry OS 10.2.1 in EMM-Corporate (or Work and Personal - Corporate) mode. The guidance was developed following testing performed on a Z30 device running BlackBerry OS 10.2.1.

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 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 from the corporate perimeter 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
- An enterprise application catalogue should be used to distribute in-house applications and trusted third-party applications to run in the corporate perimeter

- Procedural 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	Traffic from the personal perimeter on the device is not protected by the enterprise VPN.* There are two types of VPN: - BlackBerry VPN - IPsec VPN Neither of the VPNs have been independently assured to Foundation Grade. There is currently no assurance scheme to assess the strength and robustness of the proprietary BlackBerry VPN.
2. Assured data-at-rest protection	The device's data encryption has not been independently assured to Foundation Grade. Encryption keys protecting sensitive data in the corporate perimeter remain in device memory when the device is locked. The enterprise cannot control password and encryption settings for data in the personal perimeter.*
3. Authentication	
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	BlackBerry World app installation cannot be configured or monitored within the personal perimeter and Android apps from any source can be installed.*
7. Malicious code detection and prevention	
8. Security policy enforcement	Security policies primarily only apply to the corporate perimeter and the boundary between the two perimeters. Security policies do not allow enterprise control of personal applications, interface usage, mail or browsing within the personal perimeter.
9. External interface protection	Radio interfaces such as Wi-Fi and Bluetooth cannot be controlled by policy, as these are required for the personal perimeter.*

10. Device update policy	The enterprise cannot force the user to update their device software, or software within the personal perimeter.*
11. Event collection for enterprise analysis	[!] There is no facility for collecting logs remotely from a device. Collecting forensic log information from a device is very difficult.
12. Incident response	

If BlackBerry Balance is disabled by using EMM-Regulated mode, the risks marked with an asterisk associated with requirements 1, 6, 8, 9 and 10 are effectively mitigated.

2.1 Significant Risks

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

- The VPN has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured VPNs. Without assurance in the 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
- 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 needing to know the password
- 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
- The personal perimeter of the device cannot be managed by the enterprise, meaning that the attack surface cannot be minimised by disabling external interfaces such as Bluetooth and NFC
- Traffic from the personal perimeter will also bypass the enterprise VPN, negating any protections granted by corporate monitoring and filtering solutions. To avoid this for non-Wi-Fi communications, a private Access Point Name (APN) could be procured from a chosen cellular carrier and assigned to accounts using BlackBerry Balance
- Arbitrary native BlackBerry applications can be installed from BlackBerry World. Whilst there are processes in place which attempt to identify and remove malicious code from BlackBerry World, it could be defeated by a skilled attacker. The operating system is required to protect enterprise data from personal applications. A vulnerability giving elevation of privilege to root, or a flaw in the code handling the perimeters could compromise this separation
- Arbitrary Android applications can be installed from any source, with no mechanisms in place to identify potentially hostile applications. Although Android applications run in a sandboxed environment, it is possible that implementation flaws in the Android runtime might give an Android application the same access to the device as a native BlackBerry application within the personal perimeter

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 corporate perimeter on 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. The enterprise cannot whitelist applications users can install in the personal perimeter. This could be procedurally controlled via user security procedures.

3.7 Malicious code detection and prevention

The enterprise application catalogue should only contain approved in-house applications which have been checked for malicious code. Disable developer mode via policy to prevent side-loading of applications in the corporate perimeter.

3.8 Security policy enforcement

Settings applied through BES cannot be changed by the user. On BlackBerry Balance devices, these settings only apply to the corporate perimeter.

3.9 External interface protection

With BlackBerry Balance enabled, no technical controls exist to prevent users from enabling Wi-Fi, NFC and Bluetooth, or using USB.

3.10 Device update policy

On devices with BlackBerry Balance, the enterprise cannot control when applications in the personal perimeter are updated. The enterprise can update applications in the corporate perimeter remotely using the BES, and can check which device software versions are in use.

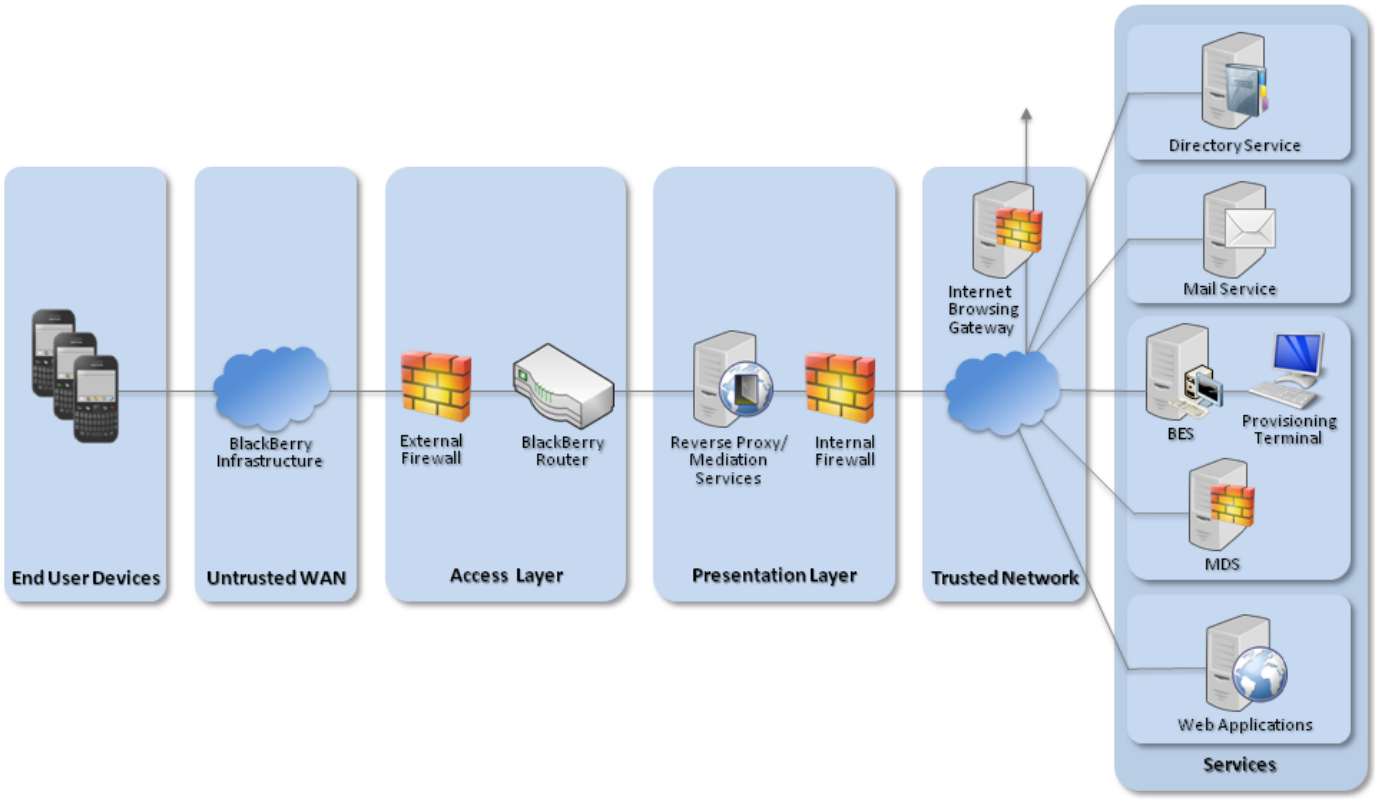
3.11 Event collection for enterprise analysis

BlackBerry 10 does not support remote or local historic event collection for enterprise analysis of security incidents. 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.

As the personal perimeter cannot be controlled by policy, network routing will bypass the corporate VPN. This means that the personal side of the device will not be subject to any corporate enterprise monitoring or auditing measures.

5. Deployment Process

To prepare the enterprise infrastructure:

1. Procure and provision a dedicated APN to backhaul traffic into the enterprise, and obtain SIM cards provisioned exclusively to this APN
2. Procure and set up a BlackBerry Enterprise Server (BES) 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.

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
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
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

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.

8.2 BlackBerry Balance

Whilst applications in the corporate workspace can be whitelisted by the organisation, applications in the personal workspace 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 perimeter on the device as that perimeter is not protected to the same level as the corporate perimeter. Should a users' device be lost, the administrator can choose to remotely wipe the entire device or just the corporate perimeter. 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