Guidance

BYOD Guidance: BlackBerry Secure Work Space

Published 17 February 2015

Contents

1. About this guidance

1.1 Who is this guidance for?

This guidance is for UK public sector organisations, their agencies and their suppliers who are considering deploying Secure Work Space (SWS) on iOS and/or Android devices. It is written for system administrators and information risk owners responsible for deploying this product on end user devices (EUDs) for remote working at OFFICIAL. Readers are expected to be familiar with the operation and functionality of SWS in addition to the EUD Platform Security Guidance and BYOD Guidance which this guidance builds on.

1.2 What is Secure Work Space?

Secure Work Space (SWS) for iOS and Android is a containerisation, application-wrapping and secure connectivity option that delivers a higher level of control and security to iOS and Android devices, all managed through the BlackBerry Enterprise Service (BES) administration console.

Work space applications are secured and separated from personal applications and data. The work space applications include an integrated email, calendar, and contacts

application, an enterprise-level secure browser, and a secure document viewing and editing application.

The work browser allows users to securely browse the organisation’s intranet and the Internet. If the device is lost or the employee leaves the organisation, you can chose to delete only corporate information or all information from the device.

Work space-enabled devices can run three different types of applications:

Type of application	Description
Personal application	An application that the user, manufacturer or wireless provider installs on the device. The BES treats these applications and the data they store as personal data.
Work application	An application that the enterprise installs and manages on a user's device. The BES treats these applications and the data they store as work data.
Work space application	A work application that the work space secures with additional protections. The BES treats these applications and the data they store as work space data.

There are three different types of work space applications:

Type of application	Description
Default work space application	A work space application that appears on every work space-enabled device.
Internal work space application	An application developed by the enterprise and modified to run in the work space.
External work space application	An application developed by a third party and modified to run in the work space.

The process for modifying applications to run in the work space has not been assessed.

2. Summary of key risks

In addition to the common risks of unmanaged hardware the following significant risks have been identified:

- Without confidence in the underlying platform, applications cannot add extra security. If a device is compromised by malware or jailbroken then the protection offered by the

SWS client and SWS-secured applications can be circumvented and sensitive information would be accessible. For this reason it is important to ensure that appropriate protection is provided to the device as a whole, as well as to applications.
- All network data transferred from the SWS client and SWS-secured applications is routed via the BlackBerry infrastructure. All user data is encrypted in such a way that it is not accessible even with privileged access to the BlackBerry infrastructure. However, some metadata might be available which will permit attackers with privileged network access to identify users.

In addition, if the application wrapping functionality of SWS is used, the following significant risk should be read and understood:

- The process of converting regular applications into work space applications has not been fully assessed, and there are a number of residual risks. There might be some APIs that write data onto the device that are not wrapped, which would leave unencrypted data on the device. Supplying a malformed application to the wrapping process might lead to incorrect or incomplete wrapping, or potentially compromise the wrapping server. The process of wrapping an application then requiring the original developer to re-sign it leaves scope for the wrapped application being modified (intentionally or otherwise).

3. Secure Work Space components

Secure Work Space comprises several components. The server components are installed as part of BlackBerry Enterprise Server 10.2. This section discusses how an organisation can align this with both the EUD Platform Security Guidance and the Walled Garden Architectural Pattern (which eligible organisations can obtain from CESG).

The server components are:

- BlackBerry Management Studio
- Universal Device Service
- BES10 Self-Service

BlackBerry Management Studio handles overall management of devices, users and licenses. The other device management consoles can be found within BlackBerry Management Studio to perform advanced administration tasks. Universal Device Service handles configurations and deployment of Policies, Profiles and Work Space applications for iOS and Android. BES10 Self-Service allows users to manage their own devices and set activation passwords.

The client components are:

- BES10 Client
- Work Connect
- Work Browser
- Documents To Go

Work Connect supports email, calendar, contacts, notes and tasks. Work Browser supports secure web browsing. Documents To Go supports viewing and editing Microsoft Office files. These are the default work space applications and appear on every work space-enabled device.

3.1 Common principles

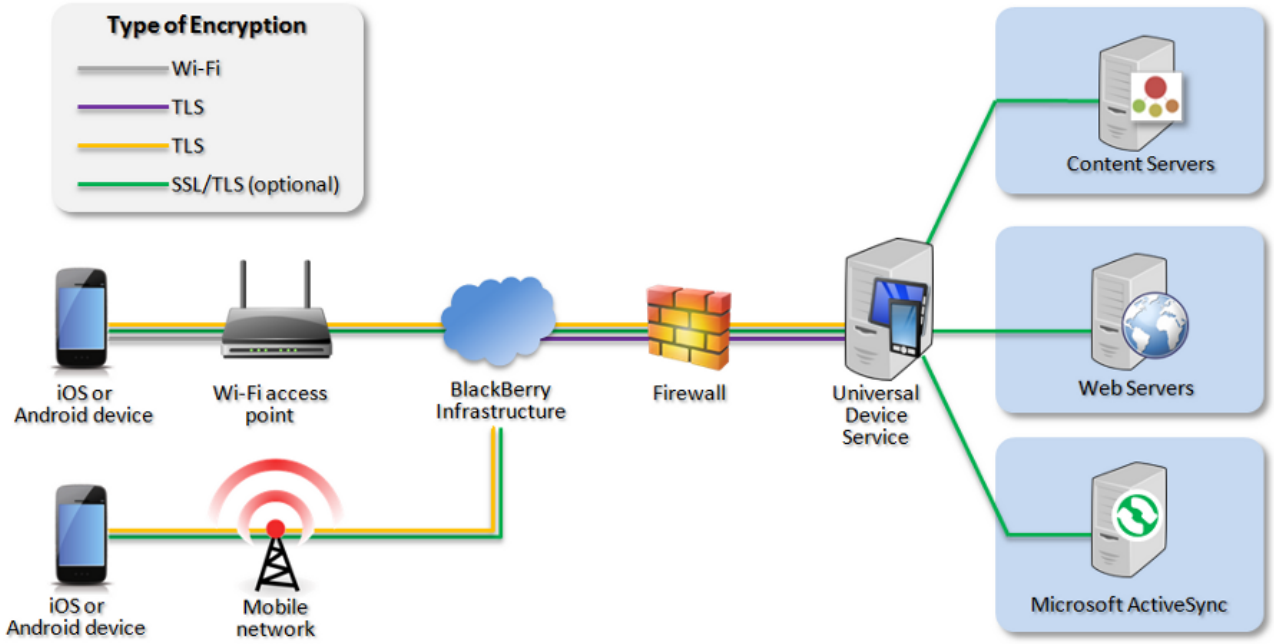
Where possible, organisations should reuse existing infrastructure rather than installing duplicate systems solely for SWS. One of the main features of SWS is that an existing BES 10.2 service can manage iOS and Android devices in addition to BlackBerry handsets. Network traffic between the BlackBerry infrastructure and the BES server should be routed through existing protective monitoring solutions.

The underlying server platforms should be configured in accordance with good practice, such as ensuring timely patching and creating accounts with minimum necessary privileges. Access to critical configuration files should be restricted so that sensitive settings are protected.

Inbound and outbound TCP connections on ports 443 and 3101 are required to manage iOS and Android devices, so these must be permitted by firewalls. These ports are the same as those required to manage BlackBerry devices.

3.2 Recommended network architecture

The walled garden architecture, shown below, aims to limit the impact of a compromise of an EUD and isolate high risk components from high value components where possible. The enterprise servers installed as part of SWS are high value resources that require suitable protection but are also high risk; they perform complex processing tasks that are more likely to contain exploitable vulnerabilities. These competing priorities make securely placing the servers into an existing network challenging, and organisations that wish to deviate from this architecture below should ensure they understand the risks of doing so.



Recommended network architecture for BlackBerry SWS

4. Technical assessment

4.1 Summary of application security

The EUD Security Framework describes 12 areas for security controls for devices, each of which must be considered when deploying a particular solution. The EUD Platform Security Guidance details how several specific platforms meet or fall short of these controls.

Organisations should consider the common risks of using unmanaged devices in addition to specific risks highlighted in this guidance.

The following table highlights how SWS impacts the 12 tenets on an EUD configured in line with this guidance, although these only apply to applications running within the SWS container, rather than the whole device. Further technical details are provided in the following sections.

Principle	Impact

1. Assured data-in-transit protection	The work space enforces end-to-end encryption of data-in-transit that cannot be disabled by an end user but this has not been independently assured to Foundation Grade.
2. Assured data-at-rest protection	The work space enforces encryption of data-at-rest that cannot be disabled by an end user. The encryption libraries are components of the FIPS validated BlackBerry Cryptographic Library for Secure Work Space.
3. Authentication	As well as the native platform's password protection, an additional password is required to access the work space. The rules on acceptable passwords are controlled by a policy on the Universal Device Service.
4. Secure boot	SWS does not provide functionality for this security control. Protection is reliant on the native platform.
5. Platform integrity and application sandboxing	The work space uses sandboxing to separate and restrict the capabilities and permissions of work space apps that run on the device. Each application process in the work space runs in its own sandbox.
6. Application whitelisting	In order to run in the work space, an application must be secured using the Universal Device Service administration console and re-signed. Organisations control which applications can be installed using software configurations.
7. Malicious code detection and prevention	The work space fingerprints applications to ensure only known and trusted applications can run as work space applications.
8. Security policy enforcement	SWS does not provide functionality for this security control. Protection is reliant on the native platform.
9. External interface protection	SWS does not provide functionality for this security control. Protection is reliant on the native platform.
10. Device update policy	SWS does not provide functionality for this security control. Protection is reliant on the native platform.
11. Event collection for enterprise analysis	The Universal Device Service logs various events.
12. Incident response	An administrator can send commands to lock or wipe a device if an incident is detected.

4.2 Data-in-transit protection

The data in transit between a work space-enabled device and a BES is protected using both AES-256 and TLS. A device enabled with work space sends data to the BlackBerry Infrastructure, which then communicates with a BES over its outbound-initiated, bi-directional ports. Data travels back from the BES to the device using the same path.

Traffic for work space applications uses TLS authenticated sessions to encrypt the session between the device and a BES. This traffic uses SSL or TLS encryption to encrypt the data for the session between the device and the various servers.

The encryption does not meet some of the mandatory requirements expected from assured TLS VPNs. Without assurance in the data-in-transit protection, there is a risk that data could be compromised.

Recommendation: Unless confident that sensitive data will never be stored or accessed from outside the SWS client and/or SWS-secured applications, and the risks of not protectively monitoring all device network traffic are acceptable, organisations should use a device-level VPN.

4.3 Data-at-rest protection

By default, work space applications protect their data using AES-256 encryption. The encryption libraries are components of the FIPS validated BlackBerry Cryptographic Library for SWS.

The encrypted container sits on top of the EUD file system, therefore the security of the encrypted data on a device is linked to the strength of the user's password. The work space randomly generates a separate encryption key for each work space application and encrypts the keys with both the device and work space passwords. It is therefore essential to have a strong device password. The work space encrypts all of the data that a work space application writes to files.

To avoid users being required to enter their work space password every time they open an application, a timeout period can be configured by the administrator. User data is not protected during this period. A shorter timeout period decreases the opportunity for an adversary to access sensitive information but is likely to impact the user experience.

Recommendation: The password for the work space should be different from the device password and handled in line with organisational policy. The EUD Platform Security Guidance contains advice on appropriate policy.

Recommendation: When deciding on an appropriate timeout period, departments should balance user experience against security. The maximum timeout should be 10 minutes.

4.4 Malicious code detection and prevention

The work space fingerprints applications to ensure that only those which are known and trusted can run as work space applications. Work space applications are validated before they are sent to a device's work space and every time that the device runs them. However, the work space relies on the underlying device operating system to ensure it has not been modified.

In combination with SWS, the BlackBerry Universal Device Service is designed to detect if a device is jailbroken or rooted. A user with a work space-enabled device cannot access the work space if the device is jailbroken or rooted. However, malware could bypass these checks, so their accuracy should not be relied on.

> Recommendation: Jailbreak detection should be enabled but administrators should be aware of its limitations.

4.5 Application sandboxing

The work space uses sandboxing to separate and restrict the capabilities and permissions of work space applications that run on the device. Each application process in the work space runs in its own sandbox. The work space evaluates the requests that a work space application's processes make for memory or device resources outside of its sandbox.

Applications can share information in a controlled manner using federating. A dynamic federation list on the device identifies which work space applications can federate. Federated applications perform a Diffie-Hellman key exchange, which ultimately gives them access to the same data in the encrypted file system.

4.6 Software patching

BlackBerry SWS can be updated through the device's native application store, though this may require the user to take action - see the EUD guidance for that platform for further details.

5. Device provisioning

By default, devices can be activated over any Wi-Fi network or mobile network through the BlackBerry infrastructure.

Devices can be activated in one of three ways. Departments need to carefully consider the benefits and risks of each type of activation when deciding which is appropriate.

Activation type	Description
MDM controls	Provides basic device management. It does not create a separate work space on the device.
Work and personal - full control	Creates a separate work space on a device, and gives the enterprise full control over the device. This mode is similar to EMM-Regulated with Balance on BlackBerry devices.
Work and personal - user privacy	Creates a separate work space on a device but only gives the enterprise control over the work space. This mode is similar to EMM-Corporate on BlackBerry devices.

The process for activating iOS and Android devices is slightly different. Both are detailed below.

5.1 iOS

1. Obtain and install an APNS certificate.
2. Create a user account on the BES.
3. Download the BES10 Client application from the App Store.
4. Launch it and enter the URL containing the SRP ID. It will be of the form `gb.bbsecure.com/S12345678`
5. Enter the username and password and click Activate My Device.
6. Click Accept to install the certificate.
7. Click OK then Install Now and Done to install the certificate.
8. Create a work space password if prompted.
9. Download the work space applications if requested.

5.2 Android

1. Create a user account on the BES.
2. Download the BES10 Client application from the Play Store.
3. Launch it and enter the URL containing the SRP ID. It will be of the form `gb.bbsecure.com/S12345678`
4. Enter the username and password and click Activate My Device.
5. Click Accept to install the certificate.
6. Create a work space password if prompted.
7. Download the work space applications if requested.

6. Policy recommendations

The following Work Space IT Policy settings should be applied to iOS and Android devices by creating configurations on the BES. Other settings (e.g. server address) should be chosen according to the relevant network configuration, or left as their default values.

Work space password	
Allow sequential and repeated character passwords	Disable
Require letters	1
Require numbers	1
Require special characters	1
Password length	
Restrict password length	Enable
Minimum length for work space password	9
Maximum length for work space password	32
Maximum password history	8
Password lock	
Lock work space after inactivity	Enable
Inactivity period	5 minutes
Time after the work space locks that it can be unlocked without the password	5 minutes
Incorrect password attempts	
Track incorrect password attempts	Enable
Maximum incorrect password attempts	5
Action after maximum incorrect password attempts	Disable work space
Work space restrictions	
Enable plugins in secure browser	Off
Work Connect contacts	Do not export to personal address book

Legal information