



## **Blackberry Security Cheat Sheet**

These recommendations apply to an individual user of a Blackberry device and include configurations that can be performed using the user interface.

Corporate users may be subject to alternate or additional security provisions offered by the Blackberry Enterprise Server or Microsoft Exchange ActiveSync.

Mandatory settings should be performed by all users of Blackberry devices, while optional settings are intended for high security environments and may impact the usability of the device.

Please be aware that the exact process for activating security features will vary from device to device and between versions of the operating system. The instructions below relate to BlackBerry Bold 9900/9930 smart phones with Blackberry v7.0 operating system. It is recommended that users follow the instructions contained in the operating manual for their device where possible.

### **Mandatory Settings**

Update firmware to the latest version:

**Options > Device > Software Updates**

Require a passcode:

**Options > Security > Password > Enter password**

Set a security time-out:

**Options > Security > Password > Change Lock After to 5 minutes or less**

Copyright Ian Parker 2011. All rights reserved.

Add a message that appears when device is locked:

**Options > Display > Message on Lock Screen > Enter contact information**

Set maximum number of password attempts:

**Options > Security > Password > Change Number of Password Attempts to 10**

Enable file encryption:

**Options > Security > Encryption > Device Memory section > Encrypt**

**Options > Security > Encryption > Media Card section > Encrypt > Device Password & Device Key > Include Media Files**

**Options > Security > Encryption > Change Strength to Strongest**

Erase all data before return, repair or recycle:

**Options > Security > Security Wipe**

Enable remote wipe functionality:

**Download BlackBerry Protect from BlackBerry App World store**

**Create a BlackBerry ID**

**Log in to Web site to locate, lock or wipe phone**

Encrypt device backups using whole disk encryption solution on workstations where backups will be stored. Examples include TrueCrypt, BitLocker, and WinMagic SecureDoc.

## **Optional Settings**

Turn off Bluetooth when not needed:

**Manage Connections > uncheck Bluetooth**

Prevent device from connecting to a saved Wi-Fi network:

**Manage Connections > Set Up Wi-Fi > Saved Wi-Fi Networks > Highlight a saved Wi-Fi network > Disable**

Block incoming messages from unknown sources:

**Options > Security > Firewall > Enabled > Check all message types > Check except messages from contacts**

Set Restrictive Permissions for Third Party Applications:

**Options > Device > Application Management > Edit default or application specific permissions > Expand Connections, Interactions, or User Data > Change permissions**

*Ian Parker is the president of Sentinel Ridge Consulting Group, a firm specializing in the security of corporate computer networks. You can reach him at [sentinelridgeconsulting.com](http://sentinelridgeconsulting.com).*