RxD Summary of Firmware Changes

This document summarizes the following firmware releases:

Hardware Requirements

This firmware requires one of the following Zebra Mobile Printers (where "X" means the value is not important):

- RW 420 (R4D-XXXXXXXX-XX)
- RW 220 (R2D-XXXXXXXX-XX)

Note • This firmware does not run on the older RW RxA models (RxA-XXXXXXXX-XX) or the RW4-PS (R4P-XXXXXXXX-XX).

Caution • Loading a RxD release on a RxA model is not supported, will make the printer inoperable, and could make it unable to revert back to a previous version. Check the label on the back of the printer to determine the model number.

11z62

Release Date: 03 April 2013

Enhancements

- Implemented `bluetooth.connected_security_mode` SGD.

Note • This command sets the minimum Bluetooth Security mode required by the printer. The security mode that will be used during communication Is controlled by the terminal. During the pairing process, the printer and terminal will negotiate to the highest security level supported by both units. To confirm the security mode during operation, use the

```
! U1 getvar  "bluetooth.connected.security_mode"
```

command.

Issues Corrected

- Mirror processing time has been improved.
- Pairing in Bluetooth Security Mode 3 is now functioning correctly.
- Line mode support for .FNT fonts has been improved.

11z58

Release Date: 10 October 2011

Enhancements

- WLAN: Added SHA2 support for PEAP authentication
- Mirror: Added support for encrypted command files, see below for description

Issues Corrected

- Print.tone SGD parameter does not handle values above 127
- Unable to save multiple files to flash using Bluetooth
- WLAN: “G” radio incompatible with Symbol 4131 access point
- WLAN: PEAP auth unsuccessful due to unsupported certificate fields
- WLAN: EAP-FAST failing on ACS 5.1
- WLAN: Inability to connect or roam using WEP on the ‘G’ radio
- WLAN; User was allowed to turn the unsupported 802.1 d feature on, which resulted in wireless communication interruptions
- Avalanche auto-run does not update correctly with multiple packages enabled
- Avalanche custom properties not working correctly
- ZPL: MicroPDF printing text behind barcode
- ZPL: Page width not working correctly with `^JUS` command

Additional information regarding the WEP issue

The problem is only present with the new “G” radio configuration (RxD-xxGxxxxx-xx). Older radios, (RxD-xxKxxxxx-xx), are not affected.

Encrypted Command Files

Benefit

Secure configuration files.

Summary

Configuring the printer to operate on a secure wireless network requires commands containing sensitive information, such as encryption keys, passwords, pass phrases, etc., to be sent to the printer. For customers using the mirror function to upgrade their printers, this new feature allows those files to be stored in encrypted form.

The feature requires several steps, as follows:

1. Use a printer (any Zebra mobile printer that supports this feature) to encrypt the sensitive command file. First send the following command to install the encryption key:

   ```
   ! U1 setvar "device.crypt.key" "key data"
   ```

Note • Key data is a 64 bit ASCII value representing a 32 byte binary key. For example, the string “11223344” represents 0x11, 0x22, 0x33, 0x44. The key is saved in printer NVRAM. If the length of ‘key data’ is not 64 bytes, the operation will fail.

2. Save the file on the printer’s flash file system using Label Vista:

   Printer Menu > Send File > Browse and select file > Check the Store to flash file system box > Send

3. Encrypt the file by sending the following command to the printer:

   ```
   ! U1 setvar "device.crypt.file" "input filename, output filename"
   ```

Note • ‘output filename’ is optional. If no ‘output filename’ is provided, the encrypted file created will be named ‘input filename.nre’

Example • This example will encrypt a file named ‘settings.txt’ and write the encrypted data to a file named ‘settings.nre’.

```
! U1 setvar "device.crypt.file" "settings.txt"
```

4. Retrieve the encrypted file from the printer using Label Vista:

   Printer Menu > Read Files > Select encrypted file from directory listing > Clone file

5. Install the decryption key on the printers to be updated using mirror with the encrypted command file, by sending the following command to each printer:

   ```
   ! U1 setvar "device.crypt.key" "key data"
   ```

6. Load the encrypted command file to the “commands” directory on the mirror server

7. The next time the printer performs a mirror operation it will download the encrypted command file, decrypt it, and execute the commands provided in the file.

Note •

- Files in the mirror server commands directory are not stored in the printer's flash memory.
- The encrypted command file can be updated as often as needed, as long as the same key is used.
- It may be desirable to create a custom configuration with the decryption key pre-installed at the factory. If this is of interest contact Zebra Sales and request information on Zebra professional services via telephone at +1-866-230-9495.

11z52

Release Date: 18 October 2010

Enhancements

- 802.1 : Add support for "G" radio, p/n RxD-xxGxxxxx-xx.
- 802.1 : Add EAP session resumption (see below for description).
- 802.1 : Removed VPN firmware.

Issues Corrected

- ZPL: Saving to ZPL flash erases RAM and deleting flash hangs or reboots printer.
- ZPL: Firmware does not disable bar sensor in continuous mode (`^MNN`).
- CPCL: PACE command not functioning properly for labels.
- EAP Session Resumption

  After a printer and the network have previously negotiated an EAP session, and due to roaming or falling out of range and returning into range, begin a new EAP negotiation, they can agree to resume the previous session. This significantly reduces the time required to establish the new session from tens of seconds to seconds. In order for this to work, EAP Session Resumption must be enabled in the network infrastructure equipment by the network administrator. EAP Session Resumption is automatically supported in the printer when using any EAP-based protocols such as PEAP, LEAP, EAP-TLS, EAP-TTLS, or EAP-FAST. No printer configuration changes are required.

Note • Releases 11x20 and 11z37 are not compatible with the new "G" radio, p/n RxD-xxGxxxxx-xx, released in October 2010.

11z37

Release Date: 25 June 2010

Enhancements

None

Issues Corrected

- CPCL: Sending a BEEP command followed by pressing the FEED key resets the printer.
- CPCL: Pressing FEED after power up prints first PRESENT-AT label at max speed.
- ZPL graphic only prints 15 times then stops.
- ZPL label with embedded ~SD command causes printer to hang.
- ZPL ~JS or ~SD commands cause printer to hang.
- 802.1 : Authentication failed with PEAP on IAS2008 server.
- 802.1 : Not responding to TCP packets when sent too quickly.
- 802.1 : Radio locks up during long duration testing.
- 802.1 : Improper TCP handshake.
- 802.1 : Not responding to duplicate TCP SYN packets.
- 802.1 : Printer locks up in power save mode.
- Improved Bluetooth operation.

11x20

Release Date: 27 February 2009

Enhancements

Original release on R2D and R4D.

Issues Corrected

None.

Additional Notes

Compressed Application: Starting with the RxD models, the firmware is stored on the printer in com- pressed format. This is done to reduce the amount of storage needed in flash memory. It also has the benefit of reducing the file transfer time. The firmware is stored in compressed form in flash, and then decompressed at power up and run out of RAM memory. This decompression takes roughly 5-8 seconds after power is turned on. A progress bar is displayed on the LCD during this process.

Failsafe Download: Starting with the RxD models, a new feature has been added that protects the printer from transmission failures during firmware download. The printer retains the current ver- sion in flash while downloading the new version. If the download succeeds the printer will reboot and flip over to the new version. If the download fails the printer will revert to the old version of firmware and continue to operate properly, allowing a second download attempt.