![ZEBRA TECHNOLOGIES]

P4T Summary of Firmware Changes

This document summarizes the following firmware releases:

Firmware Release Number	Release Date	See Page
11z48	25 June 2013	page 1
11z47	09 July 2012	page 1
11z42	15 April 2011	page 2
11z31	30 November 2010	page 5
11t22	14 November 2008	page 7

Hardware Requirements

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

- P4T (P4D-0XXXXXXX-XX)
- RP4T (P4D-XXXXXXXX-XX)

11z48

Release Date: 25 June 2013

Enhancements

- Implemented `bluetooth.connected_security_mode` SGD

Note • 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 following SGD command:

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

11z47

Release Date: 09 July 2012

Enhancements

- WLAN: Update 802.11 radio firmware

- WLAN: Added SHA2 support for EAP authentication methods
- ZPL: add support for Swiss721 Cyrillic font
- Avalanche: does not list "G" radio as WPA2-compatible
- Avalanche auto-run does not update correctly with multiple packages enable
- PRINT: Dropped characters followed by the '!' character in line-print mode
- PRINT: I2 of 5 barcode calculates incorrect checksum if using field justification
- PRINT: Correct media.width_sense.enable parameter to update width when enabled
- TT: Ribbon sticking at cold temperatures
- USB: SGD parameter usb.device.device_unique_id should default to off
- WLAN: Certificates with version 1 and 2 are rejected
- WLAN: EAP authentication 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 (see below for more details)
- ZPL: not handling out of paper condition correctly
- ZPL: vertical alignment failure in peel mode

Additional information regarding the WEP issue

The problem is only present with the new "G" radio configuration (P4D-xxGxxxxx-xx). Older radios, (P4D-xxKxxxxx-xx), are not affected.

11z42

Release Date: 15 April 2011

Enhancements

- RFID: Increased maximum size of EPC length from 96 to 496 bits
- Mirror: Added support for encrypted command files (see below for description)
- Avalanche: Custom property not working correctly after a reset
- BT: Unable to save multiple files to flash over Bluetooth
- PRINT: Vertical alignment failure if label height is > physical media height
- TT: Non-uniform print darkness of Datamatrix barcodes using ribbon
- TT: False ribbon out indication
- TT: Motor continues to run when an out of ribbon condition occurs
- TT: Poor print quality with resin ribbon
- RFID: Potential printer lockup on encode

- WLAN: "G" radio incompatible with Symbol 4131 access point

- ZPL: `^JUS` setting reverting back to full page width after reset

- ZPL: Printing human readable data behind Micro-PDF-417 barcode output

- ZPL: Printer delays 2nd label if sent immediately after 1st label

- ZPL: Vertical label alignment issues occur after ZPL paper out condition

- ZPL: Default value for parameter `device.languages` changed from "`epl-zpl`" to "`zpl`" for new printers from the factory (note -- downloading this image to a printer with a previous firmware release will not by itself change the setting)

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.

11z31

Release Date: 30 November 2010

Enhancements

- Add compressed firmware download, see details below

- Add failsafe download, see details below

- Add support for "G" radio, part numbers P4D-xxGxxxxx-xx and P4D-xxJxxxxx-xx

- Add print adjust Set/Get/Do parameter to adjust tone setting, see below for details

- Improve smart battery behavior (power up messages and battery charge state)

- RFID: Added support for relative program position (in the forward direction only). Relative position is specified in mm, and represents the movement required to line up the RFID tag with the transponder, once the leading edge of the media is at the print line. See the `^RS` command in the latest ZPL manual for more details.

- WLAN: Add EAP session resumption (see below for description)

- WLAN: Removed VPN firmware

- WLAN: Removed MSP 2.x support

Issues Corrected

- CPCL: PACE command not functioning properly for labels

- LCD: When `display.flip_display` is set to `"on"` the left and right arrows move the wrong way in the WML menus

- PRINT: Removed delay after closing media cover, not needed on P4T

- WLAN: Authentication failed with PEAP on NPS2008 server

- WLAN: not properly responding to duplicate SYNs

- WLAN: improper TCP handshake, occasionally not setting SYN flag in acknowledgement packets

- WLAN: radio can occasionally lock up

- WLAN Unable to receive broadcast messages after TKIP key rotation
- WLAN Difficulty re-authenticating after roaming
- WLAN Initial PEAP connection fails
- WLAN; User was allowed to turn the unsupported 802.1 d feature on which resulted in wireless communication interruptions
- ZPL ~JC or ~JL command inside ^XA and ^XZ tags hangs printer
- ZPL: Incorrect behavior when using multiple ^PO commands in one label file
- 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)
- ZPL label with embedded ~SD command causes printer to hang
- ZPL ~JS or ~SD commands causes printer to hang
- ZPL graphic only prints 15 times then stops

Enhancements

Compressed Application

Benefit Improved memory utilization and file transfer times.

Summary Starting with the 1 z31 release, the firmware is stored on the printer in compressed 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

Benefit Improved robustness for application updates.

Summary Starting with the 1 z31 release a new feature has been added that protects the printer from transmission failures during firmware download. The printer retains the current version in flash while downloading the new version. If the download suc- ceeds 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.

In order to activate this feature, the user must first download the 1 z31 image to the printer and then send the following command:

```
! U1 setvar "device.dual_programming.enable" "on"
```

Perform another download of the 1 z31 image to the printer.

Then reboot the printer (turn power off and then back on). At this point any subse- quent firmware downloads will be protected.

Print Adjust

Benefit Assists in darkness compatibility across printer generations or models. Summary: The purpose of the print adjust parameter is to provide an offset to the printer tone that is settable and readable remotely. This offset is additive to any TONE command settings.

Syntax ! U1 setvar "print.print_adj" "value"

where value = -30 to +30 An example setting the print adjust parameter to 10 is shown below:

```
! U1 setvar "print.print_adj" "10"
```

EAP Session Resumption

Benefit Enables faster roaming when using EAP-based protocols.

Summary 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 • Release 11t22 is not compatible with the new "G" radio, part numbers P4D-xxGxxxxx- xx and P4D-xxJxxxxx-xx, released in November 2010.

11t22

Release Date: 14 November 2008

Enhancements

Original release on P4D

Issues Corrected

None