Laird™
CONNECTIVITY

AT Command Guide

Sterling-EWB

Version 1.0

REVISION HISTORY

Version	Date	Notes	Contributors	Approver
1.0	16 Mar 2021	Initial version	Kurt Furlong Bob Monroe	Jonathan Kaye

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

CONTENTS

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

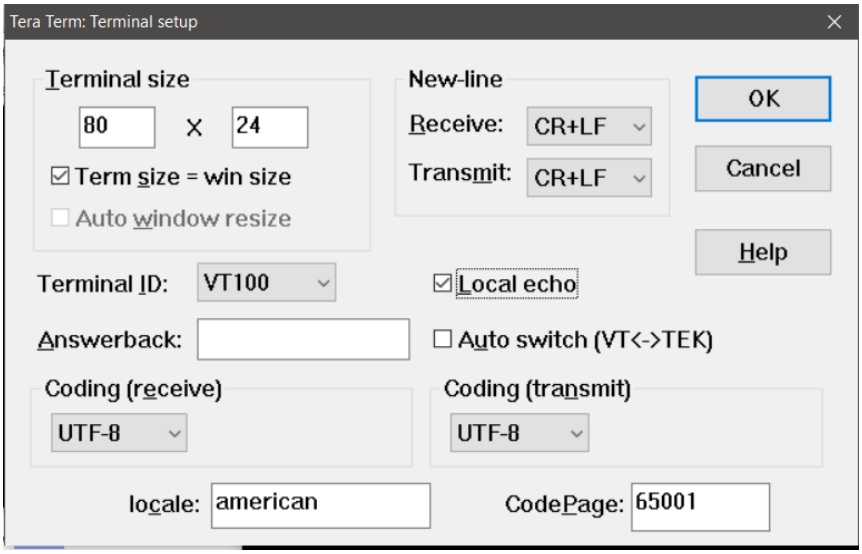
1 INTRODUCTION

1.1 Overview

This document describes all of the available Laird Connectivity Sterling-EWB AT commands.

1.2 Command Syntax

Each command ***must*** end in *\r\n (CR+LF) and Local Echo. It is recommended to use a Terminal Emulation software program that supports CF and LF like Tera Term VT, RealTerm, or UwTerminal. The default version of PuTTY does not have an option for CF+LF. Here is an example of the Terminal Setup screen in Tera Term VT:*



The following are the default for UART communication:

- 115200 baud rate
- 8 data bits
- No flow control
- No parity
- 1 stop bit

1.2.1 Escape Characters

The following are reserved characters that must be escaped with a \ when used within a string parameter to an AT command:

\

,

"

For example, if you want to send a URI parameter to AT+HTTPCONFIG containing a comma, the raw data sent over UART should look like the following:

AT+HTTPCONFIG="api.openweathermap.org",443,0,"/data/2.5/weatherq=Syracuse\,NY\,US&appid=APIKEYGOESHERE"

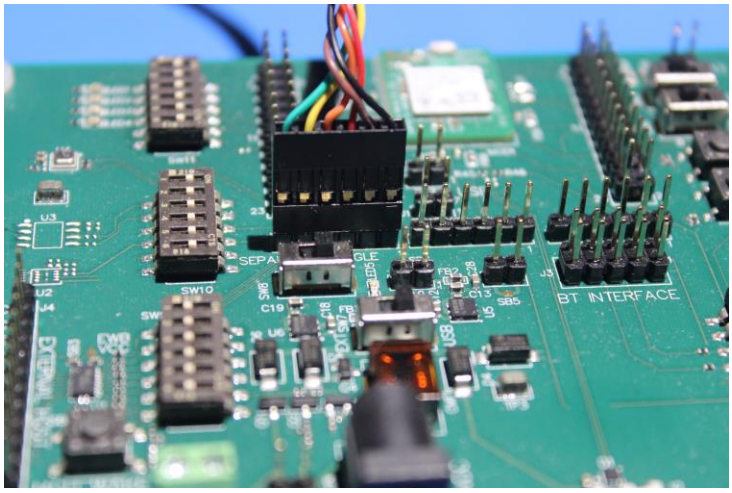
Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

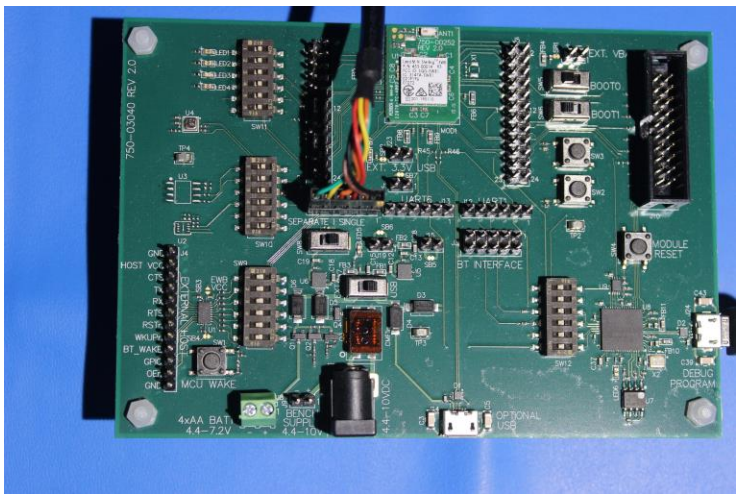
1.3 Sterling-EWB Development Kit Usage

To connect the Sterling-EWB devkit (part number 455-00030 or 455-00031) you must use the UART3 (J7) port to send the commands. You need a USB-FTDI cable to connect to your computer. The pin on the right, closest to UART6 (J13) is ground.

There are debug commands for troubleshooting that come out of the DEBUG/program port so it is a good idea to connect that up as well.

Both of the ports by default are set to 115200,N,8,1. The UART3 (J7) port requires that your terminal application is set to CR+LF for Receive and Transmit as well as Local Echo. The following images are cable connection references.





Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

1.4

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

1.5 Firmware Update

This module supports firmware updates via UART.

1.5.1 Factory Reset

1.5.1.1 Setting the Factory Image

When initially flashing the Laird AT commands firmware please use the flash_AT.bat file from one of the three “full image” zip files (where x.x.x.x is the version number you want to install:

- laird-ewb-at-eu-full-x.x.x.x.zip
- laird-ewb-at-jp-full-x.x.x.x.zip
- laird-ewb-at-us-full-x.x.x.x.zip

This flashes the image as the factory image. This needs to be done at least once to get the correct firmware and application files installed.

1.5.2 Firmware Update Procedure

To update the firmware, follow these steps, where x.x.x.x is the version number you wish to install:

1. You will need one of these three files depending on the region the device is to be used in:
    a. laird-ewb-at-eu-upgrade-x.x.x.x.elf from the laird-ewb-at-eu-upgrade-x.x.x.x.zip file.
    b. laird-ewb-at-jp-upgrade-x.x.x.x.elf from the laird-ewb-at-jp-upgrade-x.x.x.x.zip file.
    c. laird-ewb-at-us-upgrade-x.x.x.x.elf from the laird-ewb-at-us-upgrade-x.x.x.x.zip file.
2. Send **AT+FWBEGIN** and specify the size of your firmware.
3. Break the .elf file into chunks no larger than 2048 bytes.
4. Send each chunk sequentially with **AT+FWCHUNK**, waiting until the module responds with OK before sending the next chunk.
5. When all chunks are sent, send **AT+FWDONE** to finalize.
6. Reboot the module manually or with **AT+RESET**.

Note: The fw_update.py file in the ATCommands_SampleApps.zip file shows how to accomplish this programmatically.

1.6 Reset Procedure

To reset Sterling-EWB development kit, follow these steps:

1. Press and hold SW2 (PC13) button.
2. While holding SW2, press and release the MODULE RESET (MODULE_RESET) button. The blue LED (LED3/PB15) begins flashing.
3. Keep holding SW2 until LED3 stops flashing.

    Once SW2 is released, it takes ten seconds or so for the bootloader to switch to the factory image. After this, the module boots from the factory image.

1.7 Asynchronous Messages

The term *message* refers to data sent from the module to the host. Some messages may be sent based on asynchronous events as opposed to a received command. These messages always start with **+**.

1.7.1 +READY

This message is sent whenever the module starts up or wakes up from a deep sleep.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

1.7.2 +IPD

This message is sent whenever a TCPIP packet is received by the module. See the +IPD manual for more information on the syntax of this message.

1.7.3 +MQD

This message is sent whenever a MQTT packet is received by the module. This does not also send a +IPD message. See the +MQD manual for more information on the syntax of this message.

1.7.4 +HTTPD

This message is sent whenever an HTTP packet is received by the module. This does not also send a +IPD message. See the +HTTPD manual for more information on the syntax of this message.

1.7.5 +WIFI CONNECTED

This message is sent when the module connects to an access point. This does not mean that the module has an IP address; only that it has connected.

1.7.6 +WIFI GOT IP

This message is sent when the module receives an IP address from its connected access point.

1.7.7 +WIFI DISCONNECTED

This message is sent when the module disconnects from an access point.

1.7.8 +IP

These two messages **+IP,<connection id> CONNECTED** and **+IP,<connection id> DISCONNECTED** are sent in response to TCP socket state changes in both client and server mode.

1.8 Command Responses

Unless otherwise specified, all commands either return **OK** or **ERROR <code>** where the code is:

Number	Code	Meaning
0	SUCCESS	Success
1	PENDING	Pending
2	TIMEOUT	Timeout
3	PARTIAL_RESULTS	Partial results
4	ERROR	Error
5	BADARG	Bad Arguments
6	BADOPTION	Mode not supported
7	UNSUPPORTED	Unsupported function
8	OUT_OF_HEAP_SPACE	Dynamic memory space exhausted
9	NOTUP	Interface is not currently Up
10	UNFINISHED	Operation not finished yet
11	CONNECTION_LOST	Connection to server lost
12	NOT_FOUND	Item not found
13	PACKET_BUFFER_CORRUPT	Packet buffer corrupted
14	ROUTING_ERROR	Routing error

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

15	BADVALUE	Bad value
16	WOULD_BLOCK	Function would block
17	ABORTED	Operation aborted
18	CONNECTION_RESET	Connection has been reset
19	CONNECTION_CLOSED	Connection is closed
20	NOT_CONNECTED	Connection is not connected
21	ADDRESS_IN_USE	Address is in use
22	NETWORK_INTERFACE_ERROR	Network interface error
23	ALREADY_CONNECTED	Socket is already connected
24	INVALID_INTERFACE	Interface specified in invalid
25	SOCKET_CREATE_FAIL	Socket creation failed
26	INVALID_SOCKET	Socket is invalid
27	CORRUPT_PACKET_BUFFER	Packet buffer is corrupted
28	UNKNOWN_NETWORK_STACK_ERROR	Unknown network stack error
29	NO_STORED_AP_IN_DCT	DCT contains no AP credentials
30	STA_JOIN_FAILED	Join failed
31	PACKET_BUFFER_OVERFLOW	Packet buffer overflow
32	ALREADY_INITIALIZED	Module has already been inited
33	UNINITIALIZED	Module not inited

If a command returns additional data, it still ends with **OK**.

1.9 Persistent Storage

The following commands save data to persistent storage:

Command	Data
AT+UART_DEF	All UART parameters
AT+CWJAP	Access point configuration (SSID/key)
AT+CIPDHCP	DHCP configuration (enabled/disabled)
AT+CIPSTA	Static IP, Netmask, Gateway

You can clear the storage by using **AT+RESTORE**.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

2 System Commands

2.1 AT+UART_CUR – Current UART Configuration (Not Saved in Flash)

Query Command	AT+UART_CUR	
Response	+UART_CUR,<baudrate>,<stopbits>,<parity>,<flow control> OK	
Set Command	AT+UART_CUR=<baudrate>,<stopbits>,<parity>,<flow control>	
Parameters	<baudrate>	UART baud rate
	<stopbits>	1 – 1 stop bit 2 – 2 stop bits
	<parity>	0 – None 1 – Odd 2 – Even
	<flow control>	0 – None 1 – Enable RTS 2 – Enable CTS 3 – Enable both RTS and CTS
Notes	The configuration is **NOT** saved in flash.	
Example	Configure Baud 115200, 1 stop bit, no parity, enable RTS/CTS **AT+UART_CUR=115200,1,0,3**	

2.2 AT+UART_DEF – Default UART Configuration (Saved in Flash)

Query Command	AT+UART_DEF	
Response	+UART_DEF,<baudrate>,<stopbits>,<parity>,<flow control> OK	
Set Command	AT+UART_DEF=<baudrate>,<stopbits>,<parity>,<flow control>	
Parameters	<baudrate>	UART baud rate
	<stopbits>	1 – 1 stop bit 2 – 2 stop bits
	<parity>	0 – None 1 – Odd 2 – Even
	<flow control>	0 – None 1 – Enable RTS 2 – Enable CTS 3 – Enable both RTS and CTS
Example	Configure Baud 115200, 1 stop bit, no parity, enable RTS/CTS **AT+UART_DEF=115200,1,0,3**	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

2.3 AT+GMR – Version Information

Execute Command	AT+GMR	
Response	<WICED SDK Version info> <WLAN Driver Version info> <AT Command Firmware Version info> OK	
Parameters	<WICED SDK Version Info>	Information about the WICED SDK version used to build the firmware
	<WLAN Driver Version Info>	Information about the 43364 WLAN driver version
	<BT Version Info>	Information about the 43364 Bluetooth driver version
	<AT Command Firmware Version Info>	Information about the AT command firmware version

2.4 AT+RESET – Reset the Module

Execute Command	AT+RESET
Response	No response. The module resets

2.5 AT+PWRSAVE – Enable/Disable Power-Saving Features

If you are enabling MCU powersave mode, the MCU does not respond to UART AT commands unless it is woken up by rising edge on *PA0*. On the Laird EWB development kit, this is the MCU WAKE push-button.

Set Command	+PWRSAVE,<wifi mode>,<mcu mode>	
Query Command	AT+PWRSAVE	
Response	AT+PWRSAVE:<wifi mode>,<mcu mode> OK	
Parameters	<wifi mode>	0 – Wi-Fi power-saving disabled (default) 1 – Wi-Fi power-saving enabled
	<mcu mode>	0 – STM32 power-saving disabled (default) 1 – STM32 power-saving enabled

2.6 AT+RESTORE – Reset Persistent Storage to Factory

Execute Command	AT+RESTORE
Response	The module sends OK before rebooting

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

2.7 AT – Communication Check

This is a simple command that always responds with OK.

Execute Command	AT
Response	OK

3 Wi-Fi Commands

3.1 AT+CWLAP – List Available Access Points

Execute Command	AT+CWLAP[=<ssid>,<mac>,<channel>] **Note:** All parameters are optional. AT+CWLAP can be used to query for all available access points	
Response	OK	
Parameters	<sec>	Encryption method as user readable string
	<ssid>	SSID of the access point
	<rssi>	Signal strength
	<mac>	MAC address of the access point in *aa:bb:cc:00:11:22* format
Examples	Search for specific SSID, MAC, and channel: **AT+UART_DEF=115200,1,0,3** Query for all available access points: **AT+CWLAP**	

3.2 AT+CWN – Enable/Disable 11n Mode

Set Command	AT+CWN=<enabled>	
Query Command	AT+CWN	
Response	+CWN,<enabled> OK	
Parameters	<enabled>	Is 11n mode enabled 0 – Disabled 1 – Enabled
Examples	Disable 11n mode: **AT+CWN=0**	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.3 AT+CWJAP – Join Access Point as STA

Notes: This command saves to persistent storage.

This command is not synchronous. It only begins the join process. Use AT+CIPSTATUS to check the connection status or wait for the asynchronous +WIFI GOT IP message.

Execute Command	AT+CWJAP=<ssid>,<password>[,<bssid>]	
Parameters	<ssid>	Access point SSID
	<password>	Access point password. Ignored this if the access point is open with no security
	<bssid>	Optional access point MAC. Used if multiple access points have the same SSID.
Examples	Join AP with SSID, Password, and BSSID: **AT+CWJAP="MyNetwork","password123","00:11:22:33:44:55"** Join AP without BSSID: **AT+CWJAP="MyNetwork","password123"**	

3.4 AT+CWQAP – Disconnect from the Access Point

Execute Command	AT+CWQAP

3.5 AT+CWCCODE – Get Country Code

Query Command	AT+CWCCODE
Response	+CWCCODE,<country code> OK

3.6 AT+CWBLECONF – Start Bluetooth LE Wi-Fi Configuration

This command starts a Bluetooth LE Wi-Fi configuration session, which can be accessed through any central device that can discover and interact with the services outlined in section 8. Once Wi-Fi is configured, the module stops advertising until this command is issued again. There is a Python script in the ATCommands_SampleApps.zip file called ble_join.py to test this command and show how to connect to a Wi-Fi network using BLE.

Execute Command	AT+CWBLECONF

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.7 TCP/IP Commands AT+CIPSTA – Set STA IP Address Set

Command	AT+CIPSTA=<ip>,<netmask>,<gateway>	
Response	OK	
Query Command	AT+CIPSTA	
Response	+CIPSTA,<ip>,<netmask>,<gateway> OK	
Parameters	<ip>	Desired IP address of STA
	< netmask>	Optional netmask
	<gateway>	Optional gateway
Example	AT+CIPSTA="192.168.6.100","255.255.255.0","192.168.6.1"	

3.8 AT+CIPSTATUS – Get Current Connection Status

Query Command	AT+CIPSTATUS	
Response	+STATUS,<stat>[,<local ip>,<ssid>] +CIPSTATUS,<connection id>,<type>,<remote ip>,<remote port>,<local port>,<tetype> OK	
Parameters	<stat>	Status of the STA interface 0 – The STA is connected to an access point and its IP is obtained 1 – The STA is NOT connected to an access point
	< local ip>	Local IP address
	<ssid>	SSID of connected AP
	<connection id>	The ID of the connection; used for multiple connections
	<type>	TCP/UDP
	<remote ip>	Remote IP address
	<remote port>	Remote port number
	<local port>	Local port number
	<tetype>	0 – Connected as a client 1 – Connected as a server
Example	> AT+CIPSTATUS < STATUS:0,"192.168.1.234","LairdNet" < +CIPSTATUS:0,"TCP","192.168.1.123",2345,4567,0 // Client connection < +CIPSTATUS:1,"TCP","192.168.1.345",3432,4568,0 // Client connection < +CIPSTATUS:2,"TCP","192.168.1.345",4054,8080,1 // Server connection < OK	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.9 AT+CIPDHCP – Enable/Disable DHCP

If enabled, the IP address is determined from the DHCP server. If disabled, the setting set via AT+CIPSTA determines the IP address.

Set Command	AT+CIPDHCP=<enabled>	
Response	OK	
Query Command	AT+CIPDHCP	
Response	+CIPDHCP,<enabled> OK	
Parameters	<enabled>	0 – Disabled 1 – Enabled

3.10 AT+CIPSTART – Establishes TCP Connection, UDP Transmission, or SSL Connection

Execute Command	AT+CIPSTART=<connection id>,<type>,<remote IP>,<remote port>[,<enable keepalive]	
Parameters	<connection id>	Integer connection ID
	<type>	Connection type: TCP, UDP, or SSL
	<remote ip>	Remote IP address
	<remote port>	Remote port number
	<enable keepalive>	TCP keepalive. disabled by default 0 – Disable 1 – Enable
Server Mode Behavior	When in TCP/UDP server mode, the +CIPSTART,<connection id>,<type>,<remote IP>,<remote port> message is sent whenever a client connects.	
Example	AT+CIPSTART=0,"TCP","192.168.1.123",8080	

3.11 AT+CIPSEND – Sends Data

Execute Command	AT+CIPSEND=<connection id>, <length>	
Response	After sending this command, write data matching the length specified as the <length> parameter. Once <length> bytes are written, transmission begins. After data is sent, the module responds with the normal **OK/ERROR** message.	
Parameters	<connection id>	Integer connection ID
	<length>	Length of data to be written. Max 2048 bytes
Example	See full examples at the end of this document.	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.12 AT+CIPCLOSE – Closes Existing TCP, UDP, SSL Connection

Execute Command	AT+CIPCLOSE=<connection id>	
Parameters	<connection id>	Integer connection ID
Example	AT+CIPCLOSE=0	

3.13 AT+CIPSSLCONF – Configure SSL Client

Set Command	AT+CIPSSLCONF=<connection id>,<verify host>,<SSL CA Slot>	
Response	OK	
Query Command	AT+CIPSSLCONF	
Response	+CIPSSLCONF,<connection id><verify host>,<SSL CA Slot> OK	
Parameters	<connection id>	Integer connection ID
	<verify host>	Verify host certificate. Must load a CA cert using CIPSSLCALOAD if this is enabled. 0 – Disable 1 – Enable
	<SSL CA slot>	SSL CA certificate slot (0 - 3)

3.14 AT+CIPSSLCALOAD – Load CA SSL Cert

Execute Command	AT+CIPSSLCALOAD=<slot>,<length> Once you send this command, you can then send a .pem formatted CA certificate	
Parameters	slot	Slot number of certificate (0-3)
	length	Length of the certificate in bytes

3.15 AT+CIPSSLCLILD – Load SSL HTTPS/MQTT Client Certificate

Execute Command	AT+CIPSSLCLILD=<length> Once you send this command, you can then send a .pem formatted client certificate	
Parameters	length	Length of the certificate in bytes

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.16 AT+CIPSSLCLIKEYLD – Load SSL HTTPS/MQTT Private Key

Execute Command	AT+CIPSSLCLIKEYLD=<length> Once you send this command, you can then send your client private key	
Parameters	length	Length of the key in bytes

3.17 AT+CIPSERVER – Create/Delete TCP/UDP Server

TCP Server Behavior	After creating a TCP server, a +CIPSTART message is sent asynchronously from the module when a client connects. This message contains information about the client, including the connection ID. Using this connection ID, data can be sent to the client via AT+CIPSEND.	
Execute Command	AT+CIPSERVER=<mode>,<port>	
Query Command	AT+CIPSERVER	
Response	+CIPSERVER,<mode>,<port> OK	
Parameters	<mode>	0 – Delete/Idle 1 – TCP *2 - UDP
	<port>	Local port

3.18 AT+CIPPING – Ping Target Server

Execute Command	AT+CIPPING=<remote host>[,<timeout>]	
Response	+CIPPING,<response time> OK	
Parameters	<remote host>	Remote host (can be hostname or IP)
	<timeout>	Ping timeout in seconds. Defaults to 10 seconds
	<response time>	Response time in milliseconds

3.19 AT+CIPDNS – Set User-Defined DNS Server

Execute Command	AT+CIPDNS=<enable>[,<dns server>]	
Query Command	AT+CIPDNS	
Response	+CIPDNS,<enabled>[,<dns server>] OK	
Parameters	<enabled>	0 – Disabled 1 – Enabled
	<dns server>	0 – Delete/Idle 1 – TCP *2 - UDP

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

3.20 AT+CIPSTO – Set TCP Server Timeout

Execute Command	AT+CIPSTO=<timeout in seconds>	
Query Command	AT+CIPSTO	
Response	+CIPSTO,<timeout in seconds> OK	
Default	The default value for this parameter is 60 seconds.	
Parameters	<timeout in seconds>	Timeout in the range of 0-7200s. A value of 0 never times out (this is not recommended)

3.21 AT+CIPCERTSTAT – Get Current Certificate Status

Query Command	AT+CIPCERTSTAT	
Response	+CERTSTAT,<CA slot 0>,<CA slot 1>,<CA slot 2>,<CA slot 3>,<Client Cert>,<Client Priv Key>,<Enterprise Wi-Fi Clie OK	
Parameters	Each parameter is either 0 or 1	0 – Slot not filled 1 – Slot filled

3.22 +IPD – Receive Network Data

Overview	This message is sent by the module to the host via serial asynchronously when data is received over the network	
Message	+IPD,[<connection id>,]<length>,<remote ip>,<remote port>:<data>	
Parameters	<connection id>	Integer connection ID
	<length>	Length of data received
	<remote ip>	Remote IP
	<remote port>	Remote port
	<data>	Data received
UDP Transmissions	If operating in UDP server mode, received packets do contain a connection ID. If you wish to reply to a received UDP packet, you must create a new UDP transmission.	
Data Format	The data parameter is raw binary, not a hex string. For example, if the module receives 0x78, the byte 0x78 is transmitted over UART	
Example	See full examples at the end of this document.	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

4 HTTP(S) COMMANDS

4.1 AT+HTTPCLEAR – Clear HTTP Configuration

This command clears the configuration for the previous HTTP transaction. It is not required in order to execute an HTTP transaction.

Execute Command	AT+HTTPCLEAR
Response	OK

4.2 AT+HTTPCONFIG – Configure HTTP Transaction

Set Command	AT+HTTPCONFIG=<host>,<port>,<method>,<uri>,<version>	
Response	OK	
Query Command	AT+HTTPCONFIG	
Response	+HTTPCONFIG,<host>,<port>,<method>,<uri>,<version> OK	
Parameters	<host>	HTTP server hostname or IP
	<port>	HTTP server port
	<method>	HTTP method 0 – GET 1 – POST 2 – PUT 3 – DELETE
	<uri>	Universal Resource Identifier or URI (normally starts with */*)
	<version>	HTTP Version. Defaults to HTTP 1.1 0 – HTTP 1.0 1 – HTTP 1.1 2 – HTTP 2
Example	Set up a non-SSL GET transaction to /version at ip 192.168.1.123 on port 8080 AT+HTTPCONFIG="192.168.1.123",8080,0,"/version",1	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

4.3 AT+HTTPADDHDR – Add an HTTP Header

Execute Command	AT+HTTPADDHDR=<key>,<value>	
Parameters	<key>	Header key
	<value>	Header value
Example	Add a content type header for application/json AT+HTTPADDHDR="Content-Type","application/json"	

4.4 AT+HTTPRSPHDR – Show Headers in HTTP Response

If enabled, the full HTTP packet is included in the response. If not, only the status code and body are returned.

Set Command	AT+HTTPRSPHDR=<enabled>	
Query Command	AT+HTTPRSPHDR	
Response	+HTTPRSPHDR,<enabled> OK	
Parameters	<enabled>	Show HTTP headers in response data? 0 – Disabled 1 – Enabled

4.5 AT+HTTPEXEC – Execute HTTP Transaction

Begin the execution of an HTTP transaction. This command returns immediately. Any received data is sent via the +HTTPD message.

Execute Command	AT+HTTPEXEC=<length>	
Response	After sending this command, write data matching the length specified as the <length> parameter. Once <length> bytes are written, transmission begins. If no body is required, length may be either omitted or set to 0.	
Parameters	<length>	Length of request body to be written. Max 2048 bytes. Must be 0 if not sending data.
Example	See full examples at the end of this document.	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

4.6 AT+HTTPSSLCONF - Configure HTTP SSL

Set Command	AT+HTTPSSLCONF=<mode>[,<SSL CA Slot>]	
Response	OK	
Query Command	AT+HTTPSSLCONF	
Response	+HTTPSSLCONF,<mode>,<SSL CA Slot> OK	
Parameters	<mode>	0 – SSL disabled 1 – SSL enabled (*no* host verification) 3 – SSL enabled (*with* host verification)
	<SSL CA Slot>	Slot for SSL CA certificate

4.7 +HTTPD – Receive HTTP Data

Overview	This command is sent by the module to the host via serial asynchronously when HTTP data is received over the network. If AT+HTTPRSPHDR is set to 0, HTTP headers are omitted. Otherwise, the data output is identical to +IPD.	
Command	+HTTPD,<length>,<response code>:<data>	
Parameters	<length>	Length of data received
	<response code>	HTTP integer response code
	<data>	Data received
Example	See full examples at the end of this document.	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

5 BLUETOOTH LE COMMANDS

5.1 AT+BLESCN – Scan for Bluetooth LE Advertisements

This command initiates a single Bluetooth LE advertising scan.

Execute Command	AT+BLESCN	
Response	OK	
Response	+BLESCN,<rssi>,<mac addr>,<length>:<hex advertisement> ***Note:*** *This command is synchronous.* A *+BLESCN is sent for every detected beacon.*	
Parameters	<hex advertisement>	Advertisement data in raw hex
	<mac addr>	MAC address of found device
	<rssi>	RSSI of advertisement

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

6 MQTT COMMANDS

6.1 AT+MQCONN – Connect to MQTT Message Broker

Execute Command	AT+MQCONN=<hostname or ip>,<port>,<client ID>[,<username>,<password>]	
Parameters	<hostname or ip>	The hostname or IP address of the MQTT broker
	<port>	Broker port. Set to 0 to use defaults
	<client ID>	Client ID string
	<username>	Username for authentication. Username/password may be left out if authenticating via certificate
	<password>	Password for authentication

6.2 AT+MQDISCONN – Disconnect from MQTT Broker

Execute Command	AT+MQDISCONN

6.3 AT+MQPUB – Publish an MQTT Message to a Topic

Execute Command	AT+MQPUB=<topic>,<qos>,<length>	
Response	After sending this command, write data matching the length specified as the parameter. Once bytes are written, transmission begins.	
Parameters	<topic>	MQTT topic
	<qos>	(0 - 2) MQTT Quality of Service (QOS)
	<length>	Length in bytes of the message

6.4 AT+MQSUB – Subscribe to an MQTT Topic

Execute Command	AT+MQSUB=<topic>,<qos>	
Messages	Once subscribed, any received messages are sent in the +MQD format	
Parameters	<topic>	MQTT topic
	<qos>	(0 - 2) MQTT Quality of Service (QOS)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

6.5 AT+MQUNSUB – Unsubscribe from an MQTT Topic

Execute Command	AT+MQUNSUB=<topic>	
Messages	Once subscribed, any received messages are sent in the +MQD format	
Parameters	<topic>	MQTT topic

6.6 AT+MQSTATUS – Get Current MQTT Connection Status

Query Command	AT+MQSTATUS	
Response	+STATUS,<stat> OK	
Parameters	<stat>	Status of the MQTT service 0 – Connected 1 – Disconnected

6.7 AT+MQSSLCONF – Configure MQTT SSL

Set Command	AT+MQSSLCONF=<mode>[,<SSL CA Slot>]	
Response	OK	
Query Command	AT+MQSSLCONF	
Response	+MQSSLCONF,<mode>,<SSL CA Slot> OK	
Parameters	<mode>	0 – SSL disabled 1 – SSL enabled (*no* host verification) 2 – SSL enabled (*with* host verification)
	<SSL CA Slot>	Slot for SSL CA certificate

6.8 +MQD – Receive MQTT Message Data

Overview	This command is sent by the module to the host via serial asynchronously when MQTT data is received over the network.	
Command	+MQD,<topic>,<length>:<data>	
Parameters	<topic>	MQTT topic
	<length>	Length of data in bytes
	<data>	Message data received
Example	See full examples at the end of this document.	

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

7 FIRMWARE UPDATE

7.1 AT+FWBEGIN - Begin FW Update Process

Execute Command	AT+FWBEGIN=<image size>	
Parameters	<image size>	Size of the image in bytes

7.2 AT+FWCHUNK – Send Firmware Chunk

After sending AT+FWBEGIN, the .elf can then be sent in chunks no larger than 2048 bytes. You must wait for the OK response from the module before sending another chunk.

Execute Command	AT+FWCHUNK=<chunk size> Once sending this command, you can then send your binary chunk data. For detailed progress information, see the debug output of the module.	
Parameters	<chunk size>	Size of the chunk in bytes

Note: The fw_update.py file in the ATCommands_SampleApps.zip file shows how to accomplish this programmatically.

Note: Laird Connectivity recommends that you add debug UART on your prototype/test builds or your device to be able to debug during development.

7.3 AT+FWDONE – Finalize Firmware

After all chunks are sent, the AT+FWDONE command saves firmware metadata and configures the module to boot from the new firmware on next boot.

If the firmware does not boot properly, it will fall back to the factory image.

Execute Command	AT+FWDONE

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

8 Bluetooth LE Interface

The AT+CWBLECONF – Start Bluetooth LE Wi-Fi Configuration command initiates Wi-Fi provisioning via the Bluetooth LE interface. This section describes the details of the GATT services supported by the radio to integrate Wi-Fi provisioning into a mobile application, gateway, or other central application.

When the command is issued, the radio starts advertising as connectable with the following advertising format. A scan can be performed and filtered on the name *EWB* to filter out non-EWB devices.

The following is the raw advertisement packet data format:

```
0x020106110700000000000000000000000000000000000040945574204FFFF0200
```

This raw advertisement packet data is broken down by AD type in the following table (Table 1).

Table 1: Bluetooth advertising format

Length	AD Type	AD Data
0x02	0x01	0x06
0x11	0x07	0x00000000000000000000000000000000
0x04	0x09	0x455742
0x04	0xFF	0xFF0200

The Sterling-EWB implements the GATT services listed in the following sections.

8.1 Wi-Fi Scanning Service

UUID: 78c8adfd-a21c-4297-bd34-7477eefa97a0/

Characteristics:

Name	UUID	Description
Scanning Mode	8ac32d3f-5cb9-4d44-bec2-ee689169f627	A one-byte characteristic used to start scanning and determine the state of an active scan. Writing a value 1 to the characteristic starts a scan. The characteristic reads as follows: 0 – Not scanning 1 – Scan in progress 2 – Scan complete
AP Count	8ac32d3f-5cb9-4d44-bec2-ee689169f628	Unsigned 8-bit integer containing the number of APs found during the most recent scan (or ongoing scan).
AP Details	8ac32d3f-5cb9-4d44-bec2-ee689169f629	A 41-byte value holding information about an access point from the scan. The contents are laid out as follows: ▪ 1 byte of state ▪ 1 byte of channel number ▪ 1 byte of frequency band ▪ 1 signed byte of RSSI ▪ 4 bytes of security mode ▪ 1 byte of SSID length ▪ 32 bytes of SSID (padded with zeros if the SSID is shorter than 32 bytes)

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

The scanning mode characteristic is read/write. The others are read-only. All three support notifications.

In order to successfully use this service, the central role device should register for notifications for the AP Details characteristic prior to starting the scan. As scan results are found, a notification is sent with each result.

8.2 Wi-Fi Configuration Service

UUID: c59d3c56-0d2c-4860-a0ca-1d2aa6342630

Characteristics:

Name	UUID	Description
Connection State	3ee26ddd-ca51-472f-9091-436ce9ba4356	A one-byte characteristic representing the state of the Wi-Fi connection: 0 – Not provisioned 1 – Disconnected 2 – Connecting 3 – Connected 4 – Disconnecting
AP Parameters	98ed0280-23b9-4934-ab21-600cb2033593	A 101-byte value holding the parameters of the network to which the device should join: ▪ 4 bytes of security mode ▪ 1 byte of SSID length ▪ 32 bytes of SSID ▪ 1 byte of passphrase length ▪ 63 bytes of passphrase The lengths of each of the fields must match the above lengths; SSID and passphrase should be zero-padded to make up any difference in length.

The state characteristic is read-only and supports notifications. The AP parameters are read/write.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

9 EXAMPLES

9.1 Basic TCP Connection

```
> AT+CWJAP="MyAp","password123" // Connect to Access Point
< OK
> AT+CIPSTART=0,0,"192.168.1.123",8080 // Connect to remote server
< CONNECT
> AT+CIPSEND=0,11
> hello world
< SEND OK
< +IPD,0,17,”192.168.1.123”,8080:hello from server
> AT+CIPCLOSE
< OK
```

9.2 Basic HTTPS Transaction

```
> AT+CWJAP=”MyAp”,”password123” // Connect to Access Point
< OK
> AT+HTTPCLEAR // Optionally clear the current HTTP config
< OK
> AT+HTTPCONFIG=”mytestserver.com”,443,0,”/version”,1 // GET mytestserver.com/version using SSL
< OK
> AT+HTTPSSLCONF=1
< OK
> AT+HTTPRSPHDR=0 // Don’t show the header in the response, just the body
< OK
> AT+HTTPEXEC=0
< SEND OK
< +HTTPD,6,200:v1.2.3
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

9.3 Basic MQTT Transaction

9.3.1 Publish to a Topic

```
> AT+CWJAP=”MyAp”,”password123” // Connect to Access Point

< OK

> AT+MQCONN=”mybroker.mysite.com”,1883,”SomeClient”,”myuser”,”mypassword” // Connect without SSL

< CONNECT

> AT+MQPUB=”temperature”,1,4

> 75.3

< SEND OK
```

9.3.2 Subscribe to a Topic

```
> AT+CWJAP=”MyAp”,”password123” // Connect to Access Point

< OK

> AT+MQCONN=”mybroker.mysite.com”,1883,”SomeClient”,”myuser”,”mypassword” // Connect without SSL

< CONNECT

> AT+MQSUB="temperature",1

< OK

< +MQD,"temperature",4:75.3
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

9.4 Configure SSL

```
> AT+CIPSSLCONF=0,1,0 // verify SSL host on transaction
< OK
> AT+CIPSSLCALOAD=0,1188 // Load root certificate
> [Raw PEM File Data]
< LOAD OK
> AT+CWJAP=”MyAp”,”password123” // Connect to Access Point
< OK
> AT+HTTPCLEAR // Optionally clear the current HTTP config
< OK
> AT+HTTPCONFIG=”mytestserver.com”,80,0,”/version”,1,1 // GET mytestserver.com/version
using SSL
< OK
> AT+HTTPRSPHDR=0 // Don’t show the header in the response, just the body
< OK
> AT+HTTPEXEC
< SEND OK
< +HTTPD,6,200:v1.2.3
```


Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

10 Additional Assistance

Please contact your local sales representative or our support team for further assistance:

Laird Connectivity
Support Centre: https://www.lairdconnect.com/resources/support
Email: wireless.support@lairdconnectivity.com
Phone: Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610
Web: https://www.lairdconnect.com/products