

Release Notes

Topic:	Software 5.0.1 for ODIN-W2
	UBX-18006009
Author:	Erik Carlberg
Date:	23-Jan-2018

We reserve all rights in this document and in the information contained therein. Reproduction, use or disclosure to third parties without express permission is strictly prohibited.

© 2018, u-blox ag.

1 General Information

1.1 Released software image

File: ODIN-W26X-FW5.0.1-002.bin

1.2 Updated documentation

Document	Audience	Updates
ODIN-W2 Data Sheet	Public	Updated with new features
Short Range AT Commands Manual	Public	Updated with new features
ODIN-W2 Product Summary	Public	Updated with new features
ODIN-W2 System Integration Manual	Public	Updated with new features
Open Source Software Licenses	Public	Updated with new licenses
ODIN-W2 series - Using u-blox connectivity software Application Note	Public	Updated with new features

1.3 Released tools

1.3.1 s-center v4.2.0

s-center supports the AT commands needed to operate and configure ODIN-W2. s-center also supports software updates from the previous versions of the ODIN-W2 modules.

2 New features in Software 5.0.1

2.1 Wi-Fi 802.11n and MIMO

Support for the IEEE standard 802.11n has been added. This includes Multiple Input Multiple Output (MIMO) functionality. MIMO is supported only on the ODIN-W260 module and on the 2.4 GHz band.

2.2 Wi-Fi roaming

Possibility to roam in a Wi-Fi network has been included by adding scanning functionality that maintains a list of alternative access points in the vicinity. The device can then connect to another access point when the signal strength from the current declines, but before the connection is lost.

2.3 Protected Management Frames (802.11w)

IEEE 802.11w provides encryption of the network management information sent between the access point and station. This feature protects the module from spoofing attacks.

2.4 Bluetooth PAN

With the Personal Area Networking (PAN) Profile, up to 8 Bluetooth devices can form an adhoc network or access a remote network through an access point. ODIN-W2 can act both as a Network Access Point (NAP) or Personal Area Network User (PANU).

2.5 PEAP and EAP-TLS server certificate validation

The handling of certificates for secure authentication in the Wi-Fi network using Enterprise Security has been improved. With the v5 of the u-blox connectivity software, ODIN-W2 is able to validate the remote server certificate before sending any credentials over the link.

3 Issues

3.1 Solved issues in 5.0.0

Area	Description
Application	Wrong byte order for port number in Extended Data Mode (EDM)
Bluetooth	Latency is higher than expected (too much jitter) when acting as Bluetooth slave. Solved by configure active poll.
Application	Memory leak in PEAP
Wi-Fi	Long PEAP connection times
Wi-Fi	Wi-Fi scan and connection stability issues
Bluetooth	Bluetooth connection drops when using Wi-Fi
Bluetooth	SPP connection failure during Wi-Fi activation
Wi-Fi	Resolution on remaining KRACK issue (CVE-2017-13080)
Application	8th UPD link does not transfer data
Application	Can't mix ipv4 and ipv6 connection to the same TCP service
Bluetooth	Connection problem with SPS when configured a remote peer
Bluetooth	SPS on ODIN-W2 without flow control (credits disabled) not supported.
Bluetooth	ACL LE can disconnect

3.2 Solved issues in 5.0.1

Area	Description
Application	UART hangs when an UART error is detected
Application	Module hangs when doing factory restore by pressing SWITCH_0 and SWITCH_1 pins

3.3 Known issues in 5.0.1

Area	Description
Application	Only 669 bytes packet allowed on EDM for IP connections
Wi-Fi	4k certificates for EAP-TLS will make the module crash
Wi-Fi	Scan for a specified SSID can fail on 5 GHz channels
Wi-Fi	Connection to ODIN-W2 in AP mode using WPA sometimes fails
Wi-Fi	Unbalanced throughput for AP, bridged connections. Incoming throughput higher than outgoing
Bluetooth	Module resets if the SPP connection is received from an OS X device
Bluetooth	Duplicate incoming connections from same peripheral device results in watchdog reset
Application	Low TCP throughput when using Active at startup when setting up Wi-Fi and Ethernet as a bridge
Application	AT+UBTD reports multiple responses for the same device
Application	Default remote peer in EDM mode fails for always connected configuration
Application	AT+UDCP accepts too long host names but connection will fail
Application	Sending too many AT commands without waiting for ok could cause a crash

4 Changed behavior

Customers upgrading a module that uses older software to v5.0 will lose the settings stored in the module.

To decrease the time to first connection after startup, ODIN-W2 will start in the pre-defined World Mode that uses a channel list that is approved in all certified countries. If there is a need to use Wi-Fi channels not included in this list, the user must disable the Force World Mode using AT+UWCFG=11,0 which will enable 802.11d to discover allowed channels.

When activating Wi-Fi enterprise security with PEAP or EAP-TLS, the server certificate validation functionality is enabled by default. This requires a certificate to be uploaded to ODIN-W2. If no certificate is available, there will be an error upon activation. To disable the server certificate validation, use AT+UWSC=<id>,15,0 command.

5 Revision History

R01	Initial release for software version 5.0.1
-----	--