Release note

Topic **u-connectXpress software v2.1.0 for NINA-W13**
UBX-19047541

Author Erik Carlberg

Date 21 November 2019

Contents

1 Software

1.1 General Information

1.1.1 Scope

This release note describes the u-connectXpress software v2.1.0 for NINA-W13.

1.1.2 Related documentation

Document	UBX number	Audience	Updates
AT Commands manual	UBX-14044127	Public	Updated with NINA-W13 u-connectXpress v2.1.0
NINA-W13 Product Summary	UBX-16029109	Public	Updated with new features
NINA-W13 Data Sheet	UBX-17006694	Public	Updated with new features
u-connectXpress MQTT	UBX-19005066	Public	NINA-W13 added as supported product
u-connectXpress IoT Cloud Connectivity	UBX-19010078	Public	NINA-W13 added as supported product
Open Source Software Licenses	UBX-15022695	Public	Updated with MQTT license for NINA-W13

1.1.3 Released software image

The NINA-W13 software image is available on the NINA-W13 series page at u-blox.com. The table below lists the binary and configuration files included in the package.

File	Description
NINA-W13X-SW-2.1.0-017.bin	Software binary
NINA-W13X-CF-1.0.json	Manifest that defines the memory addresses for the binary
NINA-W13X-SI-2.1.0-017.txt	u-connectXpress software signature

1.1.4 s-center evaluation software

s-center version 4.9.0 is available and can be used with NINA-W13.

1.2 Features and improvements

1.2.1.1 End-to-end security

Connections using Transport Layer Security (TLS) enabling encrypted end-to-end communication over TCP is supported. The TLS versions 1.0, 1.1, and 1.2 are supported.

1.2.1.2 MQTT protocol

NINA-W13 can be set up as an MQTT client allowing the host to transmit and receive MQTT data directly over the UART.

This feature has been tested against IBM IoT Platforms, AWS IoT Core, Azure IoT Hub and Eclipse Mosquitto.

1.2.2 Vendor specific information elements

The possibility to include vendor specific information in Wi-Fi Access Point probe responses and beacons has been added.

1.3 Known limitations

Area	Description	Reference
Application	After upgrade to this version of u-connectXpress a downgrade to a version older than 2.1.0 may cause the module to assert immediately after startup. Workaround: Execute the following procedure 1. Enter bootloader mode See data sheet chapter 2.5.2 System control IO signals for instructions. *Note that access to pin 7(SWITCH_1) and pin 18(SWITCH_2) is required!* 2. While in bootloader mode, send the following sequence on UART to the module: e 0x001E0000 0x0001FFFF 3. Reset module	UCS_DEV-908
Wi-Fi	RMII/Ethernet to Wi-Fi Station bridge, requires use of a dummy IP-address with AT+UBRGC=0,100,1 and AT+UBRGC=0,101.	UCS_DEV-626
Wi-Fi	Configuring as Wi-Fi Access Point with PPP causes the module to reset if Access Point is activated while in PPP mode. Workaround: Configure AP before going into PPP mode.	UCS_DEV-687
Wi-Fi	Configuring as Wi-Fi Access Point with PPP, it is not possible to connect to the server on the host using its published gateway IP from the station. Workaround: Connect to PPP IP address instead.	UCS-DEV-706

1.4 Solved issues

Area	Description	Reference
Application	Reading back a default TCP peer that is set up with a hostname will return the wrong IP address. The same applies when using +UDLP to list peers until the TCP peer has been connected.	UCS_DEV-9
Application	Incorrect configuration of Ethernet will return ERROR. The next attempt will then result in a reset of the module.	UCS_DEV-380
Wi-Fi	AT+UWSCANIE does not report vendor specific Microsoft OUI (00:50:F2) IEs. Resolution: UWSCANIE command will not support to return internal Information Elements (IEs).	UCS_DEV-57
Wi-Fi	When scanning for a specific SSID with AT+UWSCANIE, the report may include other networks as well. Resolution: Not possible to exclude unwanted networks, filtering to be done on the host side.	UCS_DEV-69
Wi-Fi	Wi-Fi scanning while sending data can cause Wi-Fi driver to hang and should be avoided.	UCS_DEV-374
Wi-Fi	AT+UWCFG=2 returns OK, despite the command is not supported by NINA-W13.	UCS_DEV-678
Wi-Fi	AT+UWCFG returns ERROR.	UCS_DEV-679
Wi-Fi	EAP-TLS authentication with server validation does not work.	UCS_DEV-813