WINC3400 Software

Release Notes

VERSION : 1.4.4

DATE : 4 AUG, 2022

Abstract

This document presents an overview of the WINC3400 firmware release version 1.4.4, and corresponding driver.

1 Introduction 3
1.1 Highlights of the release 3
1.2 Firmware readiness 3
2 Release summary 4
2.1 Auditing information 4
2.2 Version information 4
2.3 Released components 5
2.4 Release Comparison 6
3 Test Information 9
3.1 Internal testing 9
4 Known Issues 11
5 New Features 14
6 Fixes and Enhancements 15
6.1 Issues Fixed 15
6.2 Enhancements 17
7 Appendix A – TLS Root certificates 18
7.1 TLS root certificates 18

1 Introduction

This document describes the WINC3400 version 1.4.4 firmware release package. This is a release containing Wi-Fi functionality with basic BLE support including an on-chip provisioning profile and custom BLE profiles using the Atmel BLE API and BluSDK.

The release package contains all the necessary components (binaries and tools) required to make use of the latest features including tools, and firmware binaries.

1.1 Highlights of the release

- Fixed:
    - TLS Subject Alternative Name support
    - TLS Server Name Indication support for OTA
    - Numerous fixes and enhancements (see section 6)

1.2 Firmware readiness

Microchip Technology Inc. considers version 1.4.4 firmware to be suitable for production release.

2 Release summary

2.1 Auditing information

Master Development Ticket : `https://jira.microchip.com/projects/W3400/versions/70420`

Wi-Fi:

Release Repository Branch : /chn-vm-svnrepo01.microchip.com/repo/wsg/Wifi_M2M/branches/rel_3400_1.4.4
Subversion Revision : **`20290`**

BLE:

Release Repository Branch : `/svn/Bluetooth/branches/ATWILC3400_BT_BLE_API`
Subversion Revision : **`r7651`**

BLE API:

Release Repository Branch : `/svn/Bluetooth/branches/ATWILC3400_BLE_API`
D21 Subversion Revision : **`r7650`**
SAM4 Subversion Revision : **`r7650`**

2.2 Version information

WINC Firmware version : 1.4.4
Host Driver version : 1.3.1
Host Interface Level : 1.6

RF version: 1.0

2.3 Released components

The release contains documentation, sources and binaries.

2.3.1 Documentation overview

The Application manuals, Release notes and Software API guides can be found in the `doc/` folder of the release package.

Release Notes:

This document

Software APIs:

WINC3400_IoT_SW_APIs.chm

WINC3400_BLE_APIs.chm

2.3.2 Binaries and programming scripts

The main 3400 firmware binary is in the `firmware` directory and named `m2m_image_3400.bin`. This can be flashed to a WINC device using, for example, a serial bridge application available from ASF.

An OTA image is provided in the `ota_firmware` directory named `m2m_ota_3400.bin`.

2.3.3 Sources

Source code for the host driver can be found under the `src/host_drv` directory.

Source code for the tools, including crypto_lib) can be found under the `src/Tools` directory.

2.4 Release Comparison

Features in 1.4.3	Changes in 1.4.4
Wi-Fi STA	
• IEEE 802.11 b/g/n. • OPEN (WEP protocol is deprecated, attempts to configure it will result in error). • WPA Personal Security (WPA1/WPA2), including protection against key re-installation attacks (KRACK) and countermeasures for 'Fragattack' vulnerabilities. • WPA Enterprise Security (WPA1/WPA2) supporting: EAP-TTLSv0/MS-Chapv2.0 EAP-PEAPv0/MS-Chapv2.0 EAP-PEAPv1/MS-Chapv2.0 EAP-TLS EAP-PEAPv0/TLS EAP-PEAPv1/TLS • Simple Roaming Support	• Added driver API to allow enable/disable specific phase-1 Enterprise methods. • Increased fragmentation threshold and improved outer layer PEAP and TTLS fragmentation.
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN security mode (WEP protocol deprecated). • The device cannot work as a station in this mode (STA/AP Concurrency is not supported). • Includes countermeasures for 'Fragattack' vulnerabilities.	No change
WPS	
The WINC3400 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change
TCP/IP Stack	
The WINC3400 has a TCP/IP Stack running in firmware side. It supports TCP and UDP full socket operations (client/server). The maximum number of supported sockets is currently configured to 12 divided as: • 7 TCP sockets (client or server). • 4 UDP sockets (client or server). • 1 RAW socket	• Added support for B.A.T.M.A.N. ethernet packets (EtherType 0x4305)

Transport Layer Security	
• The WINC3400 supports TLS v1.2, 1.1 and 1.0. • Client mode only. • Mutual authentication. • SHA384 and SHA512 support in X509 certificates processing. • Integration with ATECC508 (ECDSA and ECDHE support). • Multi-scream TLS RX operation with 16KB record size • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128 _CBC_SHA256 (requires ATECC508) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ECC508) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)	• Improved server authentication, with support for cross-signed certificate chains. • TLS client mode works with Subject Alternative Names in server certificate
Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • SNTP	No change
Power saving Modes	
• The WINC3400 supports these powersave modes: o M2M_NO_PS o M2M_PS_DEEP_AUTOMATIC • BLE powersave is always active	No change
Device Over-The-Air (OTA) upgrade	
• The WINC3400 has built-in OTA upgrade. • Firmware is backwards compatible with driver 1.0.8 and later. • Driver is backwards compatible with firmware 1.2.0 and later (though the functionality will be limited by the firmware version in use).	• Allow OTA to use SSL options such as SNI and server name verification
Wi-Fi credentials provisioning via built-in HTTP server	
The WINC3400 has built-in HTTP provisioning using AP mode (Open only - WEP support has been removed).	• Fixed multithread race condition during provisioning connection teardown.

WLAN MAC only mode (TCP/IP Bypass, or Ethernet Mode)	
Allow WINC3400 to operate in WLAN MAC only mode and let the host send/receive Ethernet frames.	No change
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU.	No change
Miscellaneous features	
	• Removal of obsolete python scripts in release package, as image_tool now natively supports the functionality.
BLE functionality	
BLE 4.0 functional stack	• Fixed BLE issues related to connection parameters messages exchange between controller and peripherals

3 Test Information

This section summarizes the tests conducted for this release

3.1 Internal testing

Please refer to ticket W3400-767 for full details.

Testing was performed against the release candidate 1.4.4 against the following configuration(s):

H/W Version	:	WINC3400 XPRO module
Host MCU	:	ATSAMD21-XPRO

For Elliptic Curve cryptography support verification, a CRYPTOAUTH XPLAINED PRO board (containing an ECC508A chip) was inserted into the EXT2 socket on the ATSAMD21-XPRO board.

Testing was performed in both open air and shielded environments.

The following testing has been performed:

1. General functionality including:
    1. HTTP Provisioning
    2. BLE API verification
    3. Station Mode
    4. AP Mode
    5. IP (TCP and UDP client and server)
    6. HTTP POST/GET
    7. WPS (PIN and PushButton methods)
    8. Over-The-Air (OTA) update functionality and robustness (with and without TLS)

2. TLS functionality including:
    1. RSA ciphersuites:
        i. TLS_RSA_WITH_AES_128_CBC_SHA
        ii. TLS_RSA_WITH_AES_128_CBC_SHA256
        iii. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        iv. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        v. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

        Testing uses a 1024 bit server certificate, with a chain of 7 certificates of varying key lengths (1024,2048 and 4096 bit) leading to a 2048 bit root certificate.
    2. ECDSA ciphersuites:
        i. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

        Testing uses a NIST standard ECC P256 prime curve server certificate with two chains, one leading back to an ECC root certificate and the other leading to an RSA root certificate.
    3. SNI Client Hello extension
    4. Server certificate name validation
    5. Client authentication
    6. Amazon AWS IoT environment with client authentication and ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. MQTT connection, publishing and subscribing all succeed.
3. Performance under interference
4. Wi-Fi AP interoperability testing
5. Regression and longevity tests
6. TCP/IP stack robustness testing
    a. Using an internal implementation of IPerf.
    b. Verification of multi socket functionality

Known issues are declared in Section 4

4 Known Issues

Jira	Severity	Description
W3400-605	Medium	Prolonged heavy IP traffic load can result in the SPI becoming unusable between the WINC3400 and the host. Observed with SAMD21 host and WINC powersave disabled. Could potentially occur with other host platforms, but not yet observed. Recommended workaround: On SAMD21 host, the frequency of the issue can be minimized by using M2M_PS_DEEP_AUTOMATIC when transferring IP traffic. The issue could be detected by checking the return value of an API such as m2m_get_system_time(). A negative return value indicates that the SPI is unusable. If this occurs, reset the system via system_reset(). Alternatively, m2m_wifi_reinit() can be used to reset just the WINC. In this case, the different driver modules also need to be initialized (m2m_ota_init(), m2m_ssl_init(), socketInit()).
W3400-621	Medium	The AP initiated group rekey process sometimes fails when the WINC is processing a high volume of receive traffic. Recommended workaround: Reconnect the Wi-Fi connection to the AP if a disconnection occurs due to this issue
W3400-102	Medium	During HTTP provisioning, if applications are running on the device being used to provision the WINC3400, they will not be able to access the internet during provisioning. Furthermore, if they attempt to do so, then the WINC3400 can become flooded with DNS requests and crash. This applies to HTTP provisioning only; BLE provisioning is unaffected. Also, this only applies if powersave is enabled. Recommended workarounds: (1) Use M2M_NO_PS when WINC3400 is in HTTP provisioning mode. (2) Close other internet applications (browsers, skype etc) before HTTP provisioning. If crash occurs, reset system via system_reset(). Alternatively, m2m_wifi_reinit() can be used to reset just the WINC. In this case, the different driver modules also need to be initialized (m2m_ota_init(), m2m_ssl_init(), socketInit()).
W3400-40	Medium	The WINC3400 occasionally fails to proceed with 4-way handshake in STA mode, when using 11N WPA2. It does not send M2 after receiving M1. Recommended workaround: Retry the Wi-Fi connection.
W3400-293	Medium	1% of Enterprise conversations fail due to the WINC3400 not sending an EAP response. The response is prepared and ready to send but does not appear on the air. After 10 seconds the firmware times-out the connection attempt and the application is notified of the failure to connect.

		Recommended workaround: Configure the authentication server to retry EAP requests (with interval < 10 seconds). The application should retry the connection request when it is notified of the failure.
W3400-298	Medium	70% of Enterprise connection requests fail with a TP Link Archer D2 access point (TPLink-AC750-D2). The access point does not forward the initial EAP Identity Response to the authentication server. The issue is bypassed by PMKSA caching (WPA2 only), so reconnection attempts will succeed. Recommended workaround: The application should retry the connection request when it is notified of the failure.
W3400-708	Medium	When the WINC3400 is operating in M2M_PS_DEEP_AUTOMATIC powersave mode, and is receiving two concurrent TLS streams, one of which consists of 16KB record sizes, the other has record sizes smaller than 16KB, the WINC3400 can occasionally leak memory buffers when the streams are closed. If sockets in this configuration are opened and closed repeatedly, eventually it will not be possible to open any further TLS sockets, and a restart of the WINC3400 will be needed to restore TLS functionality. Recommended workaround: The leak can be avoided by disabling powersave when receiving two concurrent TLS streams in this configuration.
W3400-461	Low	Sometimes the WINC3400 fails to see ARP responses sent from certain APs at 11Mbps. Recommended workaround: None. The ARP exchange will be retried several times and the response will eventually get through to the WINC3400.
W3400-60	Low	During BLE provisioning, the AP list is not cleaned up at the start of each scan request. As a result, the AP scan list can sometimes display duplicate or old scan entries. Recommended workaround: Only use one scan request during BLE provisioning.
W3400-59	Low	APIs at_ble_tx_power_get() and at_ble_max_PA_gain_get() return default values which do not correspond to the actual gain settings. Recommended workaround: None. Do not use these APIs.
W3400-30	Low	If the TLS server certificate chain contains RSA certificates with keys longer than 2048 bits, the WINC takes several seconds to process it. A Wi-Fi group rekey occurring during this time can cause the TLS handshake to fail. Recommended workaround: Retry opening the secure connection.

W3400-64	Low	at_ble_tx_power_set() needs special handling. Return values 0 and 1 should both be interpreted as successful operation. Refer to WINC3400_BLE_APIs.chm for more detail. Recommended workaround: Process the return value with care, according to the API documentation.
W3400-240	Low	After writing new firmware to the WINC3400, the first Wi-Fi connect attempt in STA mode takes an extra 5 seconds. Recommended workaround: Allow longer for the Wi-Fi connection to complete.
W3400-451	Low	When running in AP mode, the WINC3400 DHCP Server sometimes takes 5 to 10 seconds to assign an IP address. Recommended workaround: Allow longer for DHCP to complete.

5 New Features

New SSL options for OTA from an https server.

It is now possible to configure SSL related options for use by the WINC when it conducts an OTA from a server using TLS (via https).

The configuration is performed using the new API:

```
sint8 m2m_ota_set_ssl_option(tenuOTASSLOption enuOptionName, const void *pOptionValue, size_t OptionLen);
```

The configurable options defined in `tenuOTASSLOption` are:

`WIFI_OTA_SSL_OPT_BYPASS_SERVER_AUTH`

Bypass the authentication of the remote server.

Type is `int`, value 1=bypass server authentication, 0=authenticate the server.

`WIFI_OTA_SSL_OPT_SNI_VALIDATION`

Check the server name in the received subject name against the server name specified with `WIFI_OTA_SSL_OPT_SNI_SERVERNAME`.

Type is `int`, value 1=perform the check, 0=do not perform the check.

`WIFI_OTA_SSL_OPT_SNI_SERVERNAME`

Server name to send in the TLS SNI extension.

Type is null terminated string.

The options set via `m2m_ota_set_ssl_option` will be used for every subsequent OTA, and will be reset when the board restarts.

It is possible to get the currently configured options using the function `m2m_ota_get_ssl_option()`.

Further details can be found in the API documentation provided with the release.

6 Fixes and Enhancements

These are the fixes and enhancements since the previous released version (1.4.3)

6.1 Issues Fixed

Jira ID	Description
W3400-735	**Incorrect timestamp on first day of the year** The internal time maintained by the WINC3400 becomes incorrect for the duration of the first day of non-leap years. Fixed: The algorithm has been rewritten to perform correctly for all dates.
W3400-638	**Probe requests always sent to broadcast SSID** Probe requests sent by the WINC1500 are always sent to the broadcast SSID, even when scanning for a specific AP. Fixed: Probe requests are sent to a specific SSID set, when required.
W3400-717	**Cross-signed TLS certificate chains are rejected once the original root certificate expires.** If the WINC has an expired entry in its root certificate store, it rejects any certificate chains which lead to it, even if it also has a non-expired entry which could be used to verify the chain. Fixed: When an expired root certificate is encountered, continue to search for a different, valid root certificate.
W3400-719	**WINC1500 responds to TCP SYN on port 0** If a TCP SYN is sent to the WINC on port 0, it responds with SYN/ACK. There should be no response sent to a SYN on port 0. Fixed: Send no response if a SYN is received on port 0.
W3400-730	**Firmware crash when using defragmentation.** A race condition when defragmenting a frame at the 802.11 layer can result in a firmware crash. Fixed: Rework the code to remove the race condition.
W3400-723	**Race condition between timer delete and timer start can cause the timer not to start** A rare race condition can occur in WINC firmware when internal timers are used, which can result in the internal timer failing to start. If this occurs the effect can be wide ranging, depending on where the timer is being used. Fixed: Checks in the code are now improved, and the race condition is closed.
W3400-656	**NULL BSSID set in frames that follow a deauthentication** After a deauthentication frame has been sent to the WINC3400, there is a short window where the

	WINC3400 may attempt to send subsequent frames with a NULL destination address until it has processed the deauthentication and send out its own deauthentication frame in response. Fixed: Modifications made to the firmware to close the window in which this can happen.
W3400-763	**WINC3400 fails to notify the host of a BLE disconnect in some scenarios** If a connected client has its connection parameters updated, then the WINC3400 doesn't notify the host when that client disconnects. Fixed: Fixed the connection parameter message exchanged between the controller and the client to ensure the host is notified when it disconnects.

6.2 Enhancements

W3400-82	**Consider Subject Alternative Names when verifying TLS server name** If server name verification is enabled (via SO_SSL_ENABLE_SNI_VALIDATION or WIFI_OTA_SSL_OPT_SNI_VALIDATION), the verification succeeds if the server name matches the Common Name or any of the Subject Alternative Names in the server certificate.
W3400-718	**Removal of python helper scripts** The image_tool image creation utility has been enhanced which removes the need for two python helper scripts which are now removed from the release package: image_tool now reads the gain table directly without having to convert into a supported format, so gain_converter.py is obsolete and removed. image_tool now natively reads the xo offset from flash to compute the PLL table, which renders the extract_xo_offset.py and update_pll_table.bat scripts obsolete. These changes are mostly internal and do not affect the usage of the prepare_image.cmd script. For the remaining python scripts, checking of the correct version of python has been improved, with a relevant warning given if the wrong version is found.
W3400-751	**Improved connection option API to allow enable/disable phase 1 Enterprise Method** Added WIFI_1X_PHASE1_METHOD option to force specific phase 1 Enterprise methods to be used. The API to set and get the connection options are m2m_wifi_1x_set_option and m2m_wifi_1x_get_option. Please refer to API Documentation for more information. FreeRadius v3.0.20 is known to have issues with PEAPv0/TLS. If the user is not able to reconfigure or update their Enterprise server, then this API can be used to allow the application to choose a different method.

7 Appendix A – TLS Root certificates

The WINC3400 1.4.4 module comes with a preselected selection of TLS root certificates that will allow a TLS connection to be established with a range of internet TLS servers out of the box.

These preselected certificates are described in 7.1

7.1 TLS root certificates

Issuer	Filename	Expiry	Public Key	Signature Alg.	Notes
Amazon Root CA 1	AmazonRootCA1.cer	17 January 2038 01:00:00	RSA (2048 bits)	SHA256RSA	AWS Cloud
Baltimore CyberTrust Root	BaltimoreCyber-TrustRoot.cer	13 May 2025 00:59:00	RSA (2048 bits)	SHA1RSA	Azure Cloud
DigiCert High Assurance EV Root CA	DigiCert.cer	10 November 2031 01:00:00	RSA (2048 bits)	SHA1RSA	
DigiCert High Assurance EV Root CA	DigiCertSHA2.cer	22 October 2028 13:00:00	RSA (2048 bits)	SHA256RSA	
Entrust Root Certification Authority	EnTrust.cer	27 November 2026 21:53:42	RSA (2048 bits)	SHA1RSA	
GlobalSign Root CA	GlobalSignRoot.cer	28 January 2028 13:00:00	RSA (2048 bits)	SHA1RSA	
Internet Security Research Group Root X1	isrgrootx1.cer	04 June 2035 12:04:38	RSA (4096 bits)	SHA256RSA	LetsEncrypt
QuoVadis Root CA 2	QuoVadis_Root.cer	24 November 2031 19:23:33	RSA (4096 bits)	SHA1RSA	
VeriSign Class 3 Primary Certification Authority	VeriSign.cer	17 July 2036 00:59:59	RSA (2048 bits)	SHA1RSA	

Term	Definition
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
BSS	Basic Service Set
CBC	Cyclic Block Chaining
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name Server
DTIM	Directed Traffic Indication Map
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESS	Extended Service Set (infrastructure network)
GAP	Generic Access Profile
HTTP	Hypertext Transfer Protocol
IBSS	Independent BSS (ad-hoc network)
IEEE	Institute of Electronic and Electrical Engineers
MIB	Management Information Base
MQTT	Message Queuing Telemetry Transport
NDIS	Network Driver Interface Specification
OTA	Over The Air update
PCI	Peripheral Component Interconnect
PMK	Pair-wise Master Key
PSK	Pre-shared Key
RSA	Rivest-Shamir-Adleman (public key cryptosystem)
RSN	Robust Security Network
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
RSSI	Receive Strength Signal Indicator
TIM	Traffic Indication Map
TLS	Transport Layer Security
WEP	Wired Equivalent Privacy
WINC	Wireless Network Controller
WLAN	Wireless Local Area Network
WMM™	Wi-Fi Multimedia
WMM-PS™	Wi-Fi Multimedia Power Save
WPA™	Wi-Fi Protected Access
WPA2™	Wi-Fi Protected Access 2 (same as IEEE 802.11i)