WINC1500 Software

Release Notes

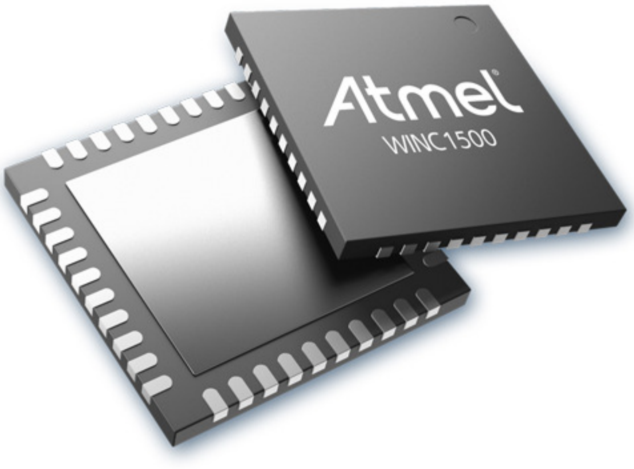
VERSION : 19.5.2
DATE : JAN 26 2017

Abstract

This document presents an overview of the WINC1500 software release version 19.5.2.

The following topics will be covered:

- Changes since previous release.
- Test information.
- New features & enhancements.



1. Introduction

This document describes the WINC1500 version 19.5.2 revision 14274 firmware release package. This is a release containing Wi-Fi functionality.

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

The released firmware binary information is:

Firmware Version	19.5.2 revision 14274
Minimum driver version	19.3.0
SVN URL	trunk
Build date	Jan 26 2017 22:13:34

2. Changes since the last release (version 19.4.4)

- WLAN Features:
  - Add WPA/WPA2 security to AP mode.
  - Add passive scan support.
  - Power saving improvements under different traffic conditions.
  - Removed WLAN sniffer mode feature.
- Network Stack Features:
  - Add TLS v1.2 server mode support.
  - Add SHA384 and SHA512 support in X509 certificates processing.
  - Add TLS client authentication support.
  - Add X509 certificate revocation support.
  - Integration with ATECC508 (Add ECDSA/ECHE support).
  - Add device name feature in DHCP requests.
  - Add X509 certificate revocation check feature.
  - Add device name in DHCP requests.
- Various bug fixes.

The table below compares the features of 19.5.x to 19.4.4 release:

Features in 19.4.x	**Changes in 19.5.x**
Wi-Fi STA	
• IEEE 802.11 b/g/n. • OPEN, WEP security. • WPA Personal Security (WPA1/WPA2). • WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLS/MS-Chapv2.0 authentication with RADIUS server.	No change.
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN and WEP security modes. • The device could not work as a station in this mode (STA/AP Concurrency is not supported).	Added WPA/WPA2 security mode.
WPS	
The WINC1500 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change

Features in 19.4.x	**Changes in 19.5.x**
TCP/IP Stack	
The WINC1500 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 11 divided as: • 7 TCP sockets (client or server). • 4 UDP sockets (client or server).	No change.
Transport Layer Security	
• TLS protocol version 1.0 TLSv1.0 • TLS v1.2 Client operation only. • RSA is the only supported Public Key Algorithm with AES and is the only supported Encryption technique. • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256	• Support TLS v1.2. • Client and server modes. • Mutual authentication. • X509 certificate revocation scheme. • Add SHA384 and SHA512 support in X509 certificates processing. • Integration with ATECC508 (Add ECDSA/ECHE support). • Certificate revocation check API. • Disable Support of DH groups larger than 2048 bits. • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ECC508) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)
Networking Protocols	
DHCPv4 (client/server) DNS Resolver	Add device name feature in DHCP requests.

Features in 19.4.x	**Changes in 19.5.x**
IGMPv1, v2.	
Power saving Modes	
• M2M_PS_MANUAL • M2M_PS_AUTOMATIC • M2M_PS_H_AUTOMATIC • M2M_PS_DEEP_AUTOMATIC	Same list of power saving modes. Optimized power saving state machine which reduced power consumption during: • Idle disconnected. • Beacon monitoring. • Intermittent traffic.
Device Over-The-Air (OTA) upgrade	
Wi-Fi credentials provisioning via built-in HTTP server	
Built-in HTTP provisioning using AP mode	HTTPS support (needs TLS server) on WPA2 secured AP mode.
Ethernet Mode (TCP/IP Bypass)	
Allow WINC1500 to in WLAN MAC only mode and let the host to send/receive Ethernet frames.	No change.
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU.	No change.

3. Test Information

This section summarizes the tests conducted for this release.

Testing was performed against the release candidate 19.5.2 revision 14274 against the following configuration(s):

H/W Version:	WINC1500 module
Host MCU:	ATSAMD21-XPRO
Test Request Info:	#8914 and #8940

Testing was performed in both open air and shielded environments. The following testing has been performed:

- **General functionality.**
  - HTTP Provisioning.
  - Station Mode.
  - AP Mode.
  - IP Client (TCP and UDP).
  - IP Server (TCP and UDP).
  - Security (TLS).
  - WPS (PIN and PushButton methods).
  - Over-The-Air (OTA) update functionality.
  - Stability
  - Longevity.
  - Interoperability.
- **Performance under interference.**

4. Terms and Definitions

Term	Definition
ARP	Address Resolution Protocol
ASD	Application Specific Device
BLE	Bluetooth Low Energy
BSS	Basic Service Set
CPU	Central Processing Unit
CSPI	Configurable SPI
EAPOL	Extensible Authentication Protocol over LAN
e.g.	*exempli gratia*, for example
EEPROM	Electrically Erasable Programmable Read Only Memory
ESS	Extended Service Set (infrastructure network)
ESD	Electrostatic Discharge
Etc	*et cetera*, and the rest, and so forth
IC	Integrated Circuit
i.e.	*id est*, that is
IBSS	Independent BSS (ad-hoc network)
IEEE	Institute of Electronic and Electrical Engineers
MIB	Management Information Base
NDIS	Network Driver Interface Specification
OS	Operating System
OTA	Over The Air update
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PMK	Pairwise Master Key
PSK	Pre-shared Key
QoS	Quality of Service
RSN	Robust Security Network
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
RSSI	Receive Signal Strength Indicator
WEP	Wired Equivalent Privacy
Wi-Fi®	Wireless Fidelity (IEEE 802.11 wireless networking)
WLAN	Wireless Local Area Network
WMM™	Wi-Fi Multimedia
WMM-PS™	Wi-Fi Multimedia Power Save
WoWLAN	Wake On WLAN
WPA™	Wi-Fi Protected Access
WPA2™	Wi-Fi Protected Access 2 (same as IEEE 802.11i)

Enabling Unlimited Possibilities®

Atmel Corporation
1600 Technology Drive
San Jose, CA 95110
USA
Tel: (+1)(408) 441-0311
Fax:(+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax:(+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax:(+49) 89-3194621

Atmel Japan G.K.
16F Shin-Osaki Kangyo Bldg.
1-6-4 Osaki, Shinagawa-ku
Tokyo 141-0032
JAPAN
Tel: (+81)(3) 6417-0300
Fax: (+81)(3) 6417-0370

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and products descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.