

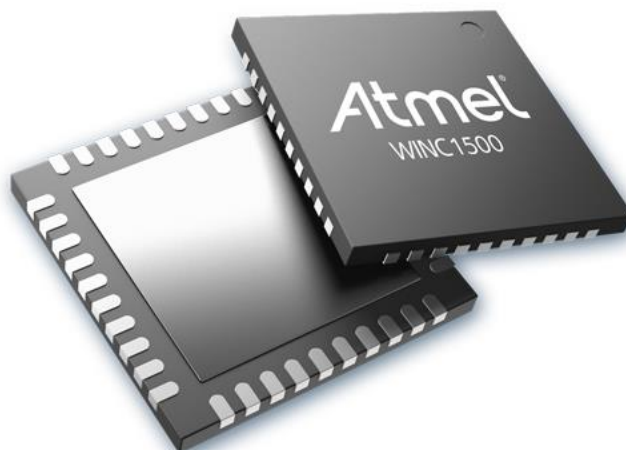
VERSION :	19.4.4
DATE :	10/13/2015

### Abstract

This document presents an overview of the WINC1500 software release version 19.4.4.

The following topics will be covered:

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



## 1. Introduction

This document describes the WINC1500 version 19.4.4 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.

**Important Note: During doing OTA from release 19.3.0 to release 19.4.1 a 5 second delay will exists due to flash dynamic remapping.**

## 2. Changes since the last release (version 19.3.0)

- [GES] connect and disconnect while growl produce E3 and buffer is free.
- [JIRA] (WINCSP-181) spurious receive callback when using TLS and doing open - send - receive - close in a loop.
- [Sigma] merge certification branch.
- [JIRA] (WINCSP-132) WINC1500 communication of broadcast frames between host and WINC.
- Restore downloader\_firmware for low power boot without efuse ROM programming.
- [JIRA] (WINCSP-122) WINC1500 Demo Loop Overnight Test.
- PMK Caching is not implemented for WPA-Enterprise security.
- [TLS\_BASELINE]Add support for DHE\_RSA cipher suites in TLS.
- [TLS\_BASELINE]Change the current TLS Design to support more cipher suites.
- Galois Counter Mode (GCM) mode of operation.
- [JIRA] (WINCSP-145)WINC1500 TLS loop crashes after 20mins connect/get/post/disconnect.
- [TRAC]#7457 TLS Buffer Full blocking the system and OTA.
- One byte corruption in shared memory.
- [GES]TCP/UDP host TX consume all memories while mac restart.
- [GES]UDP TX memory leakage in GES tests.
- Repeated connection to "https://www.un.org" causes scratch memory leak.
- Memory Corruption while TLS Connection with DHE\_RSA server with a bad-sign certificate.
- Although certificate is expired TLS session continues if it was cached from previous successful connection.
- Allow the host application to control the TLS Session caching by a socket option.
- Eliminate data copying in the TLS TX data path.
- [JIRA](WINCSP-180) WINC1500 does not support SHA2 extended certificate.
- [JIRA](WINCSP-183) m2m\_wifi\_set\_sytem\_time issue.
- [TRAC] #7365 WINC1500 - First Ping to WINC after connect always fails.
- [JIRA] (WINCSP-158) [WINC1500] SAMW25 Download failed in 19.3.0.
- [JIRA] (WINCSP-159) [WINC1500] Build error missing CORTUS\_APP feature in 19.3.0.
- [JIRA] (WINCSP-161) [WINC1500] Check SPI define in 19.3.0.
- Potential problem with the TCP packet drop condition.
- [JIRA](wincsp-163)SSID/PSK special characters are not handled correctly during provisioning.
- [TRAC] #7400 WINC1500 - DUT SoftAP does not acknowledge loss of client connection.
- Problems with multicast addresses.
- Missing check on the pau8M2mCustInfoElement len before copying to gau8M2mCustInfoElement.
- [JIRA](WINCSP-174) WPS failing on TP-Link Routers.
- Dynamic bypass mode.
- [Sigma] merge Sigma fixes from WINC3400 repo.
- Integrate new RF setting for WINC1500B (1003a1).
- [JIRA] (WINCSP-152) Stuck with error -14 after some time.
- Add TX stuck check to all data queues.
- [GES] TCP TX window wrap around.
- 1003 adjust power seq that cause Poc fixes.

- [TRAC]#7175 WINC1500 - 1503A1 - DUT does not recognize channel change on AP.
- Fix duration interval for NULL & normal priority frames.
- [JIRA](WINCSP-160) Cannot connect the AP mode with WEP in 19.3.0.
- [TRAC] expose the aes-prng to the host.
- [GES] Winc1500 mode change.
- [GES] Channel descriptor corrupted.
- [GES] TCP RX Crash.
- Set number of users to one for Descriptors.
- [JIRA] (WINCSP-143) WINC1500 G55 Xplained Pro Image downloader issue.
- [JIRA] (WINCSP-149) WINC1500 - Crypto APIs while WINC1500 FW running.
- Cortus app hangs in "Reset MAC" after provisioning.
- De-authentication is not handled while connect.
- [JIRA](WINCSP-165) Packet Sniffer: zero length payload.
- WINC1500 - 1503A1 - WPS tests - Failure to timeout if DUT is powercycled or reset.
- [JIRA](WINCSP-168) [WINC1500] When we set the CortusEFuse (no-wait) can't download F/W.
- [JIRA](WINCSP-173) WINC header files and error codes.
- B0 code size exceed the 2M flash.
- Authentication timeout while overnight test.
- [JIRA] (WINCSP-175) OTA set the invalid URL parameter - no response.
- Get OTA firmware version.
- Fix P2P on sigma branch.
- [TRAC] #7560 WINC1500 - 1503A1 - OTA Error - Invalid Info Sector.
- [TRAC]#7420 WINC1500-1503A1 - BRx7 (TKIP REPLY Attack) after connection.
- [JIRA](WINCSP-167) WINC1500 firmware 19.3.0 monitor mode and enable receive mac header, after switch channel, it cannot capture a packet.
- Disable cortus app on 2M flash to increase the firmware size.
- [JIRA](WINCSP-133) WINC1500 Null frame transmission time.
- [TRAC]#7580 replenish\_rx\_queue could result in allocation of more RX buffers than intended.
- Buffer is free on mdns app.
- Ethernet Mode: Host app did not set RX Done.
- [JIRA] (WINCSP-151) WINC1500 SAMG55 Crypto API SPI Read Error.
- [TRAC] expose the aes-prng to the host.
- [JIRA] (WINCSP-149) WINC1500 - Crypto APIs while WINC1500 FW running.
- [JIRA] (WINCSP-152) Stuck with error -14 after some time.
- Fix duration interval for NULL & normal priority frames.
- Get OTA firmware version.
- [JIRA] (WINCSP-175) OTA set the invalid URL parameter - no response.
- Dynamic SPI flash map.
- Allow the host application to control the TLS Session caching by a socket option.
- Eliminate data copying in the TLS TX data path.
- Ethernet Mode: Host app did not set RX Done.

- [JIRA] (WINCSP-132) WINC1500 communication of broadcast frames between host and WINC.
- Integrate new RF setting for WINC1500B (1003a1).
- Set number of users to one for Descriptors.
- [TRAC]#7420 WINC1500-1503A1 - BRx7 (TKIP REPLY Attack) after connection.
- [JIRA](WINCSP-133) WINC1500 Null frame transmission time.
- [TRAC]#7580 replenish\_rx\_queue could result in allocation of more RX buffers than intended.
- SPI flash current leakage.
- [TRAC] (#7175) WINC1500 - 1503A1 - DUT does not recognize channel change on AP.
- GES: TCP RX CRASH.
- [TRAC] #7560 WINC1500 - 1503A1 - OTA Error - Invalid Info Sector.
- Enable ARP table update in the arp request.
- Wrong GPIO names in disable\_pullups() and unset mux and wrong gpios in m2m\_periph module.
- Disable SPI flash before turning off the chip to minimize leakage.
- [TRAC]#7175 WINC1500 - 1503A1 - DUT does not recognize channel change on AP.
- The 19.4.0 host driver must be backward compatible with 19.3.0 driver.
- [JIRA](WINCSP-196)Abnormal operation of power saving mode.
- AES HW fail while repeat OTA test case.
- Requirement to investigate TLS throughput.
- Update ATE APP to use high and low power mode.
- [JIRA](WINCSP-195) Wi-Fi connection fail and no response.
- [TRAC]#7400 AP: STA disconnects and re-connects before link loss timer is up.
- [JIRA] (WINCSP-130) WINC1500 SSL Connection in Automatic Sleep Mode.
- [JIRA](WINCSP-204)WINC1500 Efuse application problems.
- Implement an API in ATE FW to read the prod FW version from flash.
- [JIRA](WINCSP-195) Wi-Fi connection fail and no response.
- [TRAC]#7400 AP: STA disconnects and re-connects before link loss timer is up.
- [JIRA] (WINCSP-130) WINC1500 SSL connection in Automatic Sleep Mode.
- Implement an API in ATE FW to read the prod FW version from flash.
- Fix 11b long preamble.
- Install external flash to WILC1000 fails on 19.4 pre-release.
- GES fixes.
- OTA 19.3.0 fail to upgrade to 19.4.0.
- [JIRA] (WINCSP-210) WINC1500 CW Tone Embedded ATE.
- [JIRA] (WINCSP-230) WINC1500 Unable to connect to WPA network with a 64 digit key.
- Change default mode to high power.

### 3. Test Information

This section summarizes the tests conducted for this release.

Testing was performed against the release candidate 19.4.4 against the following configuration(s):

H/W Version	:	WINC1500 module
Host MCU	:	ATSAMD21-XPRO

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. Known Issues

Bug ID	Description
6244	[JIRA] (WINCSP-139) WINC1500 - Support multiple regions with unique FW/Image.

## 5. New Features

This section describes the new features that have been introduced since the previous release.

Bug ID	Description
6077	Integrate new RF setting for WINC1500B (1003a1).
6184	Get OTA firmware version.
6113	[JIRA] (WINCSP-149) WINC1500 - Crypto APIs while WINC1500 FW running.
6169	[TRAC] expose the aes-prng to the host.
6171	Dynamic bypass mode.
6198	[JIRA](WINCSP-180) WINC1500 does not support SHA2 extended certificate.
6196	Allow the host application to control the TLS Session caching by a socket option.
6036	[TLS_BASELINE]Change the current TLS Design to support more cipher suites.
6035	[TLS_BASELINE]Add support for DHE_RSA cipher suites in TLS.
5996	PMK Caching is not implemented for WPA-Enterprise security.



## 6. Enhancements

This section describes the enhancements and/or investigations that have been made since the previous release.

Bug ID	Description
6168	[JIRA](WINCSP-173) WINC header files and error codes.
6197	Eliminate data copying in the TLS TX data path.
6153	[JIRA](wincsp-163) SSID/PSK special characters are not handled correctly during provisioning.
6255	[JIRA] (WINCSP-210) WINC1500 CW Tone Embedded ATE.
6271	[JIRA] (WINCSP-230) WINC1500 Unable to connect to WPA network with a 64 digit key.

## 7. 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.	<i>exempli gratia</i> , for example
EEPROM	Electrically Erasable Programmable Read Only Memory
ESS	Extended Service Set (infrastructure network)
ESD	Electrostatic Discharge
Etc	<i>et cetera</i> , and the rest, and so forth
IC	Integrated Circuit
i.e.	<i>id est</i> , 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](http://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  
Parking 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

© 2015 Atmel Corporation. All rights reserved.

Atmel®, Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, and others are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.

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.