

---

---

**ATWINC15x0 Software Release Notes**

---

---

**Release Overview**

---

This document describes the ATWINC15x0 version 19.7.3 release package. The release package contains all the necessary components (binaries and tools) required for the latest features including tools, and firmware binaries.

**Software Release Details**

The following table provides the software release details.

**Table 1. Software Version Information**

Parameter	Description
Software Name	WINC15x0 Firmware
WINC Firmware Version	19.7.3
Host Driver Version	19.7.3
Minimum Driver Version	19.3.0

**Release Impact**

The newly added features in ATWINC15x0 v19.7.3 release are:

- Address “Amnesia” vulnerabilities
- Improvements to socket closing code
- Improvements to TCP Rx windowing
- TLS ALPN support
- Add WPA/WPA2 Enterprise option for TLS handshake certificate expiry checking mode
- Gain Table Update

**Notes:**

1. For more information, refer to Wi-Fi Network Controller Software Design Guide (DS00002389).
2. For more details on release note information, refer to ASF firmware upgrade project doc folder.

**Related Information**

- Ordering Information
  - Customers who would like to order ATWINC15x0 with Firmware 19.7.3, contact Microchip marketing representative.
- Firmware Upgrade
  - Firmware 19.7.3 is supported in ASF version 3.51. This is available for customers to update the ATWINC15x0-MR210xB module and supporting demo and evaluation boards. Download the latest firmware package from [gallery.microchip.com/packages/4CE20911-D794-4550-8B94-6C66A93228B8/3.51.0.2344](https://gallery.microchip.com/packages/4CE20911-D794-4550-8B94-6C66A93228B8/3.51.0.2344).
  - Firmware 19.7.3 is supported in latest Harmony3. This is available for customers to update the ATWINC15x0-MR210xB module and supporting demo and evaluation boards.
    - Download the latest firmware package and driver from: [github.com/Microchip-MPLAB-Harmony/wireless\\_wifi/](https://github.com/Microchip-MPLAB-Harmony/wireless_wifi/)

- Download latest applications from: [github.com/Microchip-MPLAB-Harmony/wireless\\_apps\\_winc1500](https://github.com/Microchip-MPLAB-Harmony/wireless_apps_winc1500)
- Harmony 3 release notes available at [github.com/Microchip-MPLAB-Harmony/wireless\\_apps\\_winc1500/blob/master/release\\_notes.md](https://github.com/Microchip-MPLAB-Harmony/wireless_apps_winc1500/blob/master/release_notes.md)

**Notes:** The references to the ATWINC15x0-MR210xB module include the module devices listed in the following:

- ATWINC1500-MR210PB
  - ATWINC1500-MR210UB
  - ATWINC1510-MR210PB
  - ATWINC1510-MR210UB
- Refer to the reference documents.

**Note:** For more information, refer to Microchip product webpage:  
[www.microchip.com/wwwproducts/en/ATWINC1500](http://www.microchip.com/wwwproducts/en/ATWINC1500).

---

---

## Table of Contents

---

Release Overview.....	1
1. Release Details.....	4
1.1. Changes in Version 19.7.3, with respect to Version 19.6.1.....	4
1.2. Changes in Version 19.6.1, with respect to Version 19.5.4.....	6
1.3. Changes in Version 19.5.4, with respect to Version 19.5.3.....	8
1.4. Changes in Version 19.5.3, with respect to Version 19.5.2.....	11
1.5. Changes in Version 19.5.2, with respect to Version 19.4.4.....	13
1.6. Version 19.4.4, Initial Release.....	15
2. Known Problems and Solutions.....	16
The Microchip Web Site.....	18
Customer Change Notification Service.....	18
Customer Support.....	18
Microchip Devices Code Protection Feature.....	18
Legal Notice.....	19
Trademarks.....	19
Quality Management System Certified by DNV.....	19
Worldwide Sales and Service.....	20

## 1. Release Details

### 1.1 Changes in Version 19.7.3, with respect to Version 19.6.1

The following table compares the features of 19.6.1 to 19.7.3 release.

**Table 1-1. Comparison of Features between 19.6.1 and 19.7.3 Release**

Features in 19.6.1	Changes in 19.7.3
<b>Wi-Fi STA</b>	
<ul style="list-style-type: none"> <li>IEEE802.11 b/g/n</li> <li>OPEN, WEP security</li> <li>WPA Personal Security (WPA1/WPA2)</li> <li>WPA Enterprise Security (WPA1/WPA2) supporting :                             <ul style="list-style-type: none"> <li>EAP-TTLSv0/MS-Chapv2.0</li> <li>EAP-PEAPv0/MS-Chapv2.0</li> <li>EAP-PEAPv1/MS-Chapv2.0</li> <li>EAP-TLS</li> <li>EAP-PEAPv0/TLS</li> <li>EAP-PEAPv1/TLS</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Add WPA/WPA2 Enterprise option for TLS handshake certificate expiry checking mode</li> </ul>
<b>Wi-Fi Hotspot</b>	
<ul style="list-style-type: none"> <li>Only ONE associated station is supported. After a connection is established with a station, further connections are rejected</li> <li>OPEN and WEP, WPA2 security modes</li> <li>The device cannot work as a station in this mode (STA/AP concurrency is not supported)</li> </ul>	<ul style="list-style-type: none"> <li>Fix to ensure DHCP offered address is consistent when STA disconnects/reconnects</li> <li>Fix to close race condition when a STA disconnects and reconnects that could cause the WINC to disallow all further connection attempts.</li> </ul>
<b>Wi-Fi Direct</b>	
Wi-Fi direct client is not supported	No change
<b>WPS</b>	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
<b>TCP/IP Stack</b>	
<p>The ATWINC15x0 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:</p> <ul style="list-style-type: none"> <li>7 TCP sockets (client or server)</li> <li>4 UDP sockets (client or server)</li> </ul>	<ul style="list-style-type: none"> <li>Improvements to socket closing code</li> <li>Improvements to TCP Rx windowing</li> <li>Address "Amnesia" vulnerabilities</li> </ul>
<b>Transport Layer Security</b>	

.....continued	
Features in 19.6.1	Changes in 19.7.3
<ul style="list-style-type: none"> <li>Support TLS v1.2</li> <li>Client and server modes</li> <li>Mutual authentication in client mode.</li> <li>X509 certificate revocation scheme.</li> <li>SHA384 and SHA512 support in X509 certificates processing.</li> <li>Integration with ATECC508 (ECDSA and ECDHE support).</li> <li>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 ATECC508)            TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256            (requires ATECC508)</li> </ul>	<ul style="list-style-type: none"> <li>Added TLS ALPN support</li> <li>Fix verification of certificate chains which include ECDSA signatures</li> </ul>
<b>Networking Protocols</b>	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	<ul style="list-style-type: none"> <li>SNTP server allocated from DHCP is now cleared when switching between networks</li> </ul>
<b>Power saving Modes</b>	
<ul style="list-style-type: none"> <li>M2M_PS_MANUAL</li> <li>M2M_PS_DEEP_AUTOMATIC</li> </ul>	No change
<b>Device Over-The-Air (OTA) upgrade</b>	
<ul style="list-style-type: none"> <li>Built-in OTA upgrade available</li> <li>Backwards compatible as far as 19.4.4, with the exception of:               <ul style="list-style-type: none"> <li>Wi-Fi Direct (removed in 19.5.3)</li> <li>Monitor mode (removed in 19.5.2)</li> </ul> </li> </ul>	No change
<b>Wi-Fi credentials provisioning via built-in HTTP server</b>	
Built-in HTTP/HTTPS (TLS server mode) provisioning using AP mode (Open, WEP or WPA2 secured)	No change
<b>Ethernet Mode (TCP/IP Bypass)</b>	

.....continued	
Features in 19.6.1	Changes in 19.7.3
Allow ATWINC15x0 to operate in WLAN MAC only mode and let the host send/receive Ethernet frames.	<ul style="list-style-type: none"> <li>• Ensure broadcast frames contain correct destination MAC address</li> <li>• Ensure NULL frames are sent to keep the AP connection alive during periods of low activity.</li> </ul>
<b>ATE Test Mode</b>	
Embedded ATE test mode for production line testing driven from the host MCU	No change
<b>Miscellaneous Features</b>	
	No change

## 1.2 Changes in Version 19.6.1, with respect to Version 19.5.4

The following table compares the features of 19.5.4 to 19.6.1 release.

**Table 1-2. Comparison of Features between 19.5.4 and 19.6.1 Release**

Features in 19.5.4	Changes in 19.6.1
<b>Wi-Fi STA</b>	
<ul style="list-style-type: none"> <li>• IEEE802.11 b/g/n</li> <li>• OPEN, WEP security</li> <li>• WPA Personal Security (WPA1/WPA2)</li> <li>• WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLSv0/MSCHAPv2 authentication with RADIUS server</li> </ul>	<p>Same features along with the following:</p> <ul style="list-style-type: none"> <li>• WPA/WPA2 Enterprise new methods: <ul style="list-style-type: none"> <li>– EAP-PEAPv0/MSCHAPv2</li> <li>– EAP-PEAPv1/MSCHAPv2</li> <li>– EAP-PEAPv0/TLS</li> <li>– EAP-PEAPv1/TLS</li> <li>– EAP-TLS</li> </ul> </li> <li>• WPA/WPA2 Enterprise other new features <ul style="list-style-type: none"> <li>– Phase 1 TLS session caching</li> <li>– Option to specify domain</li> <li>– Option to send actual identity in phase 1</li> </ul> </li> <li>• Simple Roaming support</li> <li>• Improved connection API, allowing connection via BSSID as well as SSID</li> <li>• Option to encrypt connection credentials that are stored in ATWINC15x0 flash</li> </ul>
<b>Wi-Fi Hotspot</b>	
<ul style="list-style-type: none"> <li>• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected</li> <li>• OPEN and WEP, WPA2 security modes</li> <li>• The device cannot work as a station in this mode (STA/AP concurrency is not supported)</li> </ul>	No change
<b>Wi-Fi Direct</b>	
Wi-Fi direct client is not supported	No change

.....continued	
Features in 19.5.4	Changes in 19.6.1
<b>WPS</b>	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
<b>TCP/IP Stack</b>	
The ATWINC15x0 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: <ul style="list-style-type: none"> <li>• 7 TCP sockets (client or server)</li> <li>• 4 UDP sockets (client or server)</li> </ul>	No change
<b>Transport Layer Security</b>	
<ul style="list-style-type: none"> <li>• Support TLS v1.2</li> <li>• Client and server modes</li> <li>• Mutual authentication</li> <li>• Custom scheme for X509 certificate revocation</li> <li>• X509 certificate support including SHA1, SHA256, SHA384 and SHA512</li> <li>• Integration with ATECC508 (adds support for ECDSA/ ECHE)</li> <li>• Supported cipher suites are: <ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</li> <li>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</li> <li>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</li> <li>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_128_GCM_SHA256</li> <li>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</li> <li>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)</li> <li>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (requires ATECC508)</li> <li>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)</li> </ul> </li> </ul>	No change
<b>Networking Protocols</b>	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	SNTP servers are fully customizable

.....continued	
Features in 19.5.4	Changes in 19.6.1
<b>Power saving Modes</b>	
<ul style="list-style-type: none"> <li>M2M_PS_MANUAL</li> <li>M2M_PS_AUTOMATIC</li> <li>M2M_PS_H_AUTOMATIC</li> <li>M2M_PS_DEEP_AUTOMATIC</li> </ul>	No change
<b>Device Over-The-Air (OTA) upgrade</b>	
<ul style="list-style-type: none"> <li>Built-in OTA upgrade available</li> <li>Backwards compatible as far as 19.4.4, with the exception of:               <ul style="list-style-type: none"> <li>Wi-Fi Direct (removed in 19.5.3)</li> <li>Monitor mode (removed in 19.5.2)</li> </ul> </li> </ul>	No change
<b>Wi-Fi credentials provisioning via built-in HTTP server</b>	
Built-in HTTP/HTTPS (TLS server mode) provisioning using AP mode (Open, WEP or WPA2 secured)	<ul style="list-style-type: none"> <li>Improved provisioning user experience</li> <li>Default gateway and subnet mask can now be customized when in AP mode</li> </ul>
<b>Ethernet Mode (TCP/IP Bypass)</b>	
Allow ATWINC15x0 to in WLAN MAC only mode and let the host to send/receive Ethernet frames	No change
<b>ATE Test Mode</b>	
Embedded ATE test mode for production line testing driven from the host MCU	No change
<b>Miscellaneous Features</b>	
	<ul style="list-style-type: none"> <li>Addition of host file download capability, allowing the host MCU to download and retrieve files from the ATWINC1510 flash</li> <li>Multiple Gain Table support - Support upto 4 gain tables</li> <li>Simple Roaming feature</li> <li>Encrypted credential storage in ATWINC15x0 flash</li> </ul>

### 1.3 Changes in Version 19.5.4, with respect to Version 19.5.3

The following table compares the features of 19.5.3 to 19.5.4 release.

**Table 1-3. Comparison of Features between 19.5.3 and 19.5.4 Release**

Features in 19.5.3	Changes in 19.5.4
<b>Wi-Fi STA</b>	

.....continued	
Features in 19.5.3	Changes in 19.5.4
<ul style="list-style-type: none"> <li>IEEE802.11 b/g/n</li> <li>OPEN, WEP security</li> <li>WPA Personal Security (WPA1/WPA2)</li> <li>WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLS/MS-Chapv2.0 authentication with RADIUS server</li> </ul>	<ul style="list-style-type: none"> <li>Protect against key re-installation attacks forcing NONCE re-use</li> <li>Fix <code>m2m_wifi_set_tx_power()</code> to work in all cases</li> <li>Fix interoperability issues with ARRIS TG862G/CT (Xfinity) access point</li> </ul>
<b>Wi-Fi Hotspot</b>	
<ul style="list-style-type: none"> <li>Only ONE associated station is supported. After a connection is established with a station, further connections are rejected</li> <li>OPEN and WEP, WPA2 security modes</li> <li>The device cannot work as a station in this mode (STA/AP concurrency is not supported)</li> </ul>	No change
<b>Wi-Fi Direct</b>	
Wi-Fi direct client is not supported	No change
<b>WPS</b>	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
<b>TCP/IP Stack</b>	
<p>The ATWINC15x0 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:</p> <ul style="list-style-type: none"> <li>7 TCP sockets (client or server)</li> <li>4 UDP sockets (client or server)</li> </ul>	No change
<b>Transport Layer Security</b>	

.....continued	
Features in 19.5.3	Changes in 19.5.4
<ul style="list-style-type: none"> <li>• Support TLS v1.2</li> <li>• Client and server modes</li> <li>• Mutual authentication</li> <li>• X509 certificate revocation scheme</li> <li>• Add SHA384 and SHA512 support in X509 certificates processing</li> <li>• Integration with ATECC508 (add ECDSA/ECHE support)</li> <li>• Certificate revocation check API</li> <li>• Disable Support of DH groups larger than 2048 bits</li> <li>• 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 ATECC508)            TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256            (requires ATECC508)</li> </ul>	No change
<b>Networking Protocols</b>	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2 SNTP	Use NTP server pools instead of specific servers
<b>Power saving Modes</b>	
<ul style="list-style-type: none"> <li>• M2M_PS_MANUAL</li> <li>• M2M_PS_AUTOMATIC</li> <li>• M2M_PS_H_AUTOMATIC</li> <li>• M2M_PS_DEEP_AUTOMATIC</li> </ul>	No change
<b>Device Over-The-Air (OTA) upgrade</b>	
<ul style="list-style-type: none"> <li>• Built-in OTA upgrade available</li> <li>• Backwards compatible as far as 19.4.4, with the exception of:               <ul style="list-style-type: none"> <li>– Wi-Fi Direct (removed in 19.5.3)</li> <li>– Monitor mode (removed in 19.5.2)</li> </ul> </li> </ul>	No change
<b>Wi-Fi credentials provisioning via built-in HTTP server</b>	

.....continued	
Features in 19.5.3	Changes in 19.5.4
Built-in HTTP/HTTPS (TLS server mode) provisioning using AP mode (Open, WEP or WPA2 secured)	No change
<b>Ethernet Mode (TCP/IP Bypass)</b>	
Allow ATWINC15x0 to in WLAN MAC only mode and let the host to send/receive Ethernet frames	No change
<b>ATE Test Mode</b>	
Embedded ATE test mode for production line testing driven from the host MCU	No change

## 1.4 Changes in Version 19.5.3, with respect to Version 19.5.2

The following table compares the features of 19.5.2 to 19.5.3 release.

**Table 1-4. Comparison of Features between 19.5.2 and 19.5.3 Release**

Features in 19.5.2	Changes in 19.5.3
<b>Wi-Fi STA</b>	
<ul style="list-style-type: none"> <li>• IEEE802.11 b/g/n</li> <li>• OPEN, WEP security</li> <li>• WPA Personal Security (WPA1/WPA2)</li> <li>• WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLS/MS-Chapv2.0 authentication with RADIUS server</li> </ul>	Same features along with the following: <ul style="list-style-type: none"> <li>• Improved automatic rate selection algorithm for optimized TCP upload experience</li> <li>• Supports SAMW55 module</li> <li>• Firmware does not print WLAN passcode in the WINC firmware log</li> </ul>
<b>Wi-Fi Hotspot</b>	
<ul style="list-style-type: none"> <li>• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected</li> <li>• OPEN and WEP, WPA2 security modes</li> <li>• The device cannot work as a station in this mode (STA/AP concurrency is not supported)</li> </ul>	No change
<b>Wi-Fi Direct</b>	
<ul style="list-style-type: none"> <li>• The device can operate only as a Wi-Fi Direct client (group owner function is not supported)</li> <li>• The device could not work as a station in this mode (STA/P2P concurrency is not supported)</li> </ul>	Wi-Fi direct client is not supported
<b>WPS</b>	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
<b>TCP/IP Stack</b>	

.....continued	
Features in 19.5.2	Changes in 19.5.3
<p>The ATWINC15x0 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:</p> <ul style="list-style-type: none"> <li>• 7 TCP sockets (client or server)</li> <li>• 4 UDP sockets (client or server)</li> </ul>	<p>Implement fast TCP re-transmission for improved TCP upload in busy radio environments</p>
<b>Transport Layer Security</b>	
<ul style="list-style-type: none"> <li>• Support TLS v1.2</li> <li>• Client and server modes</li> <li>• Mutual authentication</li> <li>• X509 certificate revocation scheme</li> <li>• Add SHA384 and SHA512 support in X509 certificates processing</li> <li>• Integration with ATECC508 (add ECDSA/ECHE support)</li> <li>• Certificate revocation check API</li> <li>• Disable Support of DH groups larger than 2048 bits</li> <li>• 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 ATECC508)            TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256            (requires ATECC508)</li> </ul>	<p>Fix an issue where SHA384 and SHA512 are not present in the list supported signature algorithms in the ClientHello message</p>
<b>Networking Protocols</b>	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2	<ul style="list-style-type: none"> <li>• Fix DHCP client renew never timeout issue</li> <li>• Add client identifier to DHCP request</li> <li>• Various DHCP client improvements to confirm to RFC 2131</li> </ul>
<b>Power saving Modes</b>	
<ul style="list-style-type: none"> <li>• M2M_PS_MANUAL</li> <li>• M2M_PS_AUTOMATIC</li> <li>• M2M_PS_H_AUTOMATIC</li> <li>• M2M_PS_DEEP_AUTOMATIC</li> </ul>	<p>Improved initialization time (reduced by about 70 ms)</p>
<b>Device Over-The-Air (OTA) upgrade</b>	

.....continued	
Features in 19.5.2	Changes in 19.5.3
	Improve WINC HTTPS client to allow it to work with HTTP servers which do not provide "content-length" HTTP header field (e.g. openssl s_server)
<b>Wi-Fi credentials provisioning via built-in HTTP server</b>	
Built-in HTTP/HTTPS (TLS server mode) provisioning using AP mode (Open, WEP or WPA2 secured)	No change
<b>Ethernet Mode (TCP/IP Bypass)</b>	
Allow ATWINC15x0 to in WLAN MAC only mode and let the host to send/receive Ethernet frames	No change
<b>ATE Test Mode</b>	
Embedded ATE test mode for production line testing driven from the host MCU	No change

## 1.5 Changes in Version 19.5.2, with respect to Version 19.4.4

The following table compares the features of 19.4.4 to 19.5.2 release.

**Table 1-5. Comparison of Features between 19.4.4 and 19.5.2 Release**

Features in 19.4.4	Changes in 19.5.2
<b>Wi-Fi STA</b>	
<ul style="list-style-type: none"> <li>IEEE802.11 b/g/n</li> <li>OPEN, WEP security</li> <li>WPA Personal Security (WPA1/WPA2)</li> <li>WPA Enterprise Security (WPA1/WPA2) supporting EAP-TTLS/MS-Chapv2.0 authentication with RADIUS server</li> </ul>	No change
<b>Wi-Fi Hotspot</b>	
<ul style="list-style-type: none"> <li>Only ONE associated station is supported. After a connection is established with a station, further connections are rejected</li> <li>OPEN and WEP security modes</li> <li>The device cannot work as a station in this mode (STA/AP concurrency is not supported)</li> </ul>	Added WPA/WPA2 security mode
<b>WPS</b>	
The ATWINC15x0 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods	No change
<b>TCP/IP Stack</b>	
<p>The ATWINC15x0 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:</p> <ul style="list-style-type: none"> <li>7 TCP sockets (client or server)</li> <li>4 UDP sockets (client or server)</li> </ul>	No change

.....continued	
Features in 19.4.4	Changes in 19.5.2
<b>Transport Layer Security</b>	
<ul style="list-style-type: none"> <li>• TLS protocol version 1.0 TLSv1.0</li> <li>• TLS v1.2 Client operation only</li> <li>• RSA is the only supported Public Key Algorithm with AES and is the only supported Encryption technique</li> <li>• 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</li> </ul>	<ul style="list-style-type: none"> <li>• Support TLS v1.2</li> <li>• Client and server modes</li> <li>• Mutual authentication</li> <li>• X509 certificate revocation scheme</li> <li>• Add SHA384 and SHA512 support in X509 certificates processing</li> <li>• Integration with ATECC508 (add ECDSA/ECHE support)</li> <li>• Certificate revocation check API</li> <li>• Disable Support of DH groups larger than 2048 bits</li> <li>• 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 ATECC508)            TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)</li> </ul>
<b>Networking Protocols</b>	
DHCPv4 (client/server) DNS Resolver IGMPv1, v2	Add device name feature in DHCP requests
<b>Power saving Modes</b>	
<ul style="list-style-type: none"> <li>• M2M_PS_MANUAL</li> <li>• M2M_PS_AUTOMATIC</li> <li>• M2M_PS_H_AUTOMATIC</li> <li>• M2M_PS_DEEP_AUTOMATIC</li> </ul>	Same list of power saving modes. Optimized power saving state machine which reduced power consumption during: <ul style="list-style-type: none"> <li>• Idle disconnected</li> <li>• Beacon monitoring</li> <li>• Intermittent traffic</li> </ul>
<b>Device Over-The-Air (OTA) upgrade</b>	

---

---

<b>.....continued</b>	
<b>Features in 19.4.4</b>	<b>Changes in 19.5.2</b>
<b>Wi-Fi credentials provisioning via built-in HTTP server</b>	
Built-in HTTP provisioning using AP mode	HTTPS support (needs TLS server) on WPA2 secured AP mode
<b>Ethernet Mode (TCP/IP Bypass)</b>	
Allow ATWINC15x0 to in WLAN MAC only mode and let the host to send/receive Ethernet frames	No change
<b>ATE Test Mode</b>	
Embedded ATE test mode for production line testing driven from the host MCU	No change

## **1.6 Version 19.4.4, Initial Release**

Initial release of version 19.4.4 to public.

## 2. Known Problems and Solutions

The following table provides the list of known problems and solutions.

Additional known issues information can be found at [github.com/MicrochipTech/WINC15x0-known-issues](https://github.com/MicrochipTech/WINC15x0-known-issues)

**Table 2-1. Known Problems and Solutions**

Problem	Solution
Occasionally ATWINC15x0 fails to receive an individual UDP broadcast frame when in M2M_PS_DEEP_AUTOMATIC powersave mode.	Use M2M_NO_PS Power Save mode if reliability is preferred for UDP broadcast frames. Otherwise ensure the overlying protocol can handle the odd missing frame.
The ATWINC15x0 cannot handle two simultaneous TLS handshakes, due to memory constraints.	When attempting to open two secure sockets in STA mode, the application should wait to be notified of the first one completing (succeeding or failing) before attempting the second one.
1% of Enterprise conversations fail due to the ATWINC15x0 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.	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.
When connected to certain access points, the ATWINC15x0 sometimes fails to roam when the access point changes channel. The issue is seen with these access points: Linksys E2500, Linksys E4200, Linksys 6500. The failures to roam are due to two issues: <ul style="list-style-type: none"> <li>Sometimes the access point takes a long time to start sending beacons or probe responses on the new channel, so it is not discoverable.</li> <li>Sometimes the access point does not initiate the 4-way handshake (for WPA/WPA2 PSK reconnection).</li> </ul>	On reception of M2M_WIFI_DISCONNECTED event, the application should attempt to discover the access point using <code>m2m_wifi_request_scan()</code> API.
If an AP uses an 802.11 ACK policy of “No Ack”, then the ATWINC15x0 sometimes fails to receive 802.11b frames.	Avoid using an ACK policy of “No Ack”. If “No Ack” is used, ensure frames are sent at 802.11g or higher rates.
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 Re-sponse to the authentication server. The issue is bypassed by PMKSA caching (WPA2 only), so reconnection attempts will succeed.	The application should retry the connection request when it is notified of the failure.
Occasionally during AP provisioning, after entering the credentials of the AP to connect to and pressing “connect”, an error will be returned even though provisioning was successful and the connection proceeds.	Add a delay in the application between receiving the provisioning info and connecting to the AP. Ignore the “Request Failed” message
Using TLS Server mode with a server certificate that is signed with a key size which differs from the key size contained within the certificate can cause the WINC to crash.	Only use a TLS Server certificate that is signed using the same key size as the key contained within the certificate.

# ATWINC15x0

## Known Problems and Solutions

.....continued

Problem	Solution
When using a driver pre – 19.6.1 with 19.7.3 firmware, upon failure to obtain a DHCP address the WINC will not trigger a WiFi Disconnection and notify the driver of the failure.	In this case of an older driver running with later firmware, the application should monitor the time taken to obtain a DHCP address, if it takes too long then it can decide whether to disconnect and try again.

## The Microchip Web Site

---

Microchip provides online support via our web site at [www.microchip.com/](http://www.microchip.com/). This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

## Customer Change Notification Service

---

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at [www.microchip.com/](http://www.microchip.com/). Under "Support", click on "Customer Change Notification" and follow the registration instructions.

## Customer Support

---

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: [www.microchip.com/support](http://www.microchip.com/support)

## Microchip Devices Code Protection Feature

---

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

## Legal Notice

---

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

## Trademarks

---

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, memBrain, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2018, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN:

## Quality Management System Certified by DNV

---

### ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

## Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
<p><b>Corporate Office</b> 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: <a href="http://www.microchip.com/support">http://www.microchip.com/support</a> Web Address: <a href="http://www.microchip.com">www.microchip.com</a></p> <p><b>Atlanta</b> Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455</p> <p><b>Austin, TX</b> Tel: 512-257-3370</p> <p><b>Boston</b> Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088</p> <p><b>Chicago</b> Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075</p> <p><b>Dallas</b> Addison, TX Tel: 972-818-7423 Fax: 972-818-2924</p> <p><b>Detroit</b> Novi, MI Tel: 248-848-4000</p> <p><b>Houston, TX</b> Tel: 281-894-5983</p> <p><b>Indianapolis</b> Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380</p> <p><b>Los Angeles</b> Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800</p> <p><b>Raleigh, NC</b> Tel: 919-844-7510</p> <p><b>New York, NY</b> Tel: 631-435-6000</p> <p><b>San Jose, CA</b> Tel: 408-735-9110 Tel: 408-436-4270</p> <p><b>Canada - Toronto</b> Tel: 905-695-1980 Fax: 905-695-2078</p>	<p><b>Australia - Sydney</b> Tel: 61-2-9868-6733</p> <p><b>China - Beijing</b> Tel: 86-10-8569-7000</p> <p><b>China - Chengdu</b> Tel: 86-28-8665-5511</p> <p><b>China - Chongqing</b> Tel: 86-23-8980-9588</p> <p><b>China - Dongguan</b> Tel: 86-769-8702-9880</p> <p><b>China - Guangzhou</b> Tel: 86-20-8755-8029</p> <p><b>China - Hangzhou</b> Tel: 86-571-8792-8115</p> <p><b>China - Hong Kong SAR</b> Tel: 852-2943-5100</p> <p><b>China - Nanjing</b> Tel: 86-25-8473-2460</p> <p><b>China - Qingdao</b> Tel: 86-532-8502-7355</p> <p><b>China - Shanghai</b> Tel: 86-21-3326-8000</p> <p><b>China - Shenyang</b> Tel: 86-24-2334-2829</p> <p><b>China - Shenzhen</b> Tel: 86-755-8864-2200</p> <p><b>China - Suzhou</b> Tel: 86-186-6233-1526</p> <p><b>China - Wuhan</b> Tel: 86-27-5980-5300</p> <p><b>China - Xian</b> Tel: 86-29-8833-7252</p> <p><b>China - Xiamen</b> Tel: 86-592-2388138</p> <p><b>China - Zhuhai</b> Tel: 86-756-3210040</p>	<p><b>India - Bangalore</b> Tel: 91-80-3090-4444</p> <p><b>India - New Delhi</b> Tel: 91-11-4160-8631</p> <p><b>India - Pune</b> Tel: 91-20-4121-0141</p> <p><b>Japan - Osaka</b> Tel: 81-6-6152-7160</p> <p><b>Japan - Tokyo</b> Tel: 81-3-6880-3770</p> <p><b>Korea - Daegu</b> Tel: 82-53-744-4301</p> <p><b>Korea - Seoul</b> Tel: 82-2-554-7200</p> <p><b>Malaysia - Kuala Lumpur</b> Tel: 60-3-7651-7906</p> <p><b>Malaysia - Penang</b> Tel: 60-4-227-8870</p> <p><b>Philippines - Manila</b> Tel: 63-2-634-9065</p> <p><b>Singapore</b> Tel: 65-6334-8870</p> <p><b>Taiwan - Hsin Chu</b> Tel: 886-3-577-8366</p> <p><b>Taiwan - Kaohsiung</b> Tel: 886-7-213-7830</p> <p><b>Taiwan - Taipei</b> Tel: 886-2-2508-8600</p> <p><b>Thailand - Bangkok</b> Tel: 66-2-694-1351</p> <p><b>Vietnam - Ho Chi Minh</b> Tel: 84-28-5448-2100</p>	<p><b>Austria - Wels</b> Tel: 43-7242-2244-39 Fax: 43-7242-2244-393</p> <p><b>Denmark - Copenhagen</b> Tel: 45-4450-2828 Fax: 45-4485-2829</p> <p><b>Finland - Espoo</b> Tel: 358-9-4520-820</p> <p><b>France - Paris</b> Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79</p> <p><b>Germany - Garching</b> Tel: 49-8931-9700</p> <p><b>Germany - Haan</b> Tel: 49-2129-3766400</p> <p><b>Germany - Heilbronn</b> Tel: 49-7131-67-3636</p> <p><b>Germany - Karlsruhe</b> Tel: 49-721-625370</p> <p><b>Germany - Munich</b> Tel: 49-89-627-144-0 Fax: 49-89-627-144-44</p> <p><b>Germany - Rosenheim</b> Tel: 49-8031-354-560</p> <p><b>Israel - Ra'anana</b> Tel: 972-9-744-7705</p> <p><b>Italy - Milan</b> Tel: 39-0331-742611 Fax: 39-0331-466781</p> <p><b>Italy - Padova</b> Tel: 39-049-7625286</p> <p><b>Netherlands - Drunen</b> Tel: 31-416-690399 Fax: 31-416-690340</p> <p><b>Norway - Trondheim</b> Tel: 47-7289-7561</p> <p><b>Poland - Warsaw</b> Tel: 48-22-3325737</p> <p><b>Romania - Bucharest</b> Tel: 40-21-407-87-50</p> <p><b>Spain - Madrid</b> Tel: 34-91-708-08-90 Fax: 34-91-708-08-91</p> <p><b>Sweden - Gothenberg</b> Tel: 46-31-704-60-40</p> <p><b>Sweden - Stockholm</b> Tel: 46-8-5090-4654</p> <p><b>UK - Wokingham</b> Tel: 44-118-921-5800 Fax: 44-118-921-5820</p>