ATWINC3400 Software Release Notes

WINC3400

Release Overview

This document describes the ATWINC3400 version 1.4.6 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	WINC3400 Firmware
WINC Firmware Version	1.4.6
Host Driver Version	1.3.2
Host Interface Level	1.6.0

Release Impact

The newly added features in ATWINC3400 v1.4.6 release are:

- Added EAPOL v3 support for WPA Enterprise connections.
- Fixed connection parameter saving code to ensure it doesn't make unnecessary flash writes
- Correctly parse and handle the "critical" field of x.509 certificate extensions
- Check CA Basic Constraint in TLS certificate chain
- Improvements and bugfixes to the BLE API
- BLE MAC address generation code no longer requires WiFi MAC to be even

Notes:

1. For more information, refer to ATWINC3400 Wi-Fi® Network Controller Software Design Guide (DS50002919).
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 ATWINC3400 with Firmware 1.4.6, contact Microchip marketing representative.
- Firmware Upgrade
  - To upgrade the ATWINC3400-MR210xA module with latest 1.4.6 release. Customers needs to follow the steps available in the salesforce knowledge base article: microchipsupport.force.com/s/article/How-to-update-the-firmware-of-WINC3400-module.

  - **Notes:** The references to the ATWINC3400-MR210xA module include the module devices listed in the following:
    - ATWINC3400-MR210CA
    - ATWINC3400-MR210UA

- Refer to the reference documents.

Note: For more information, refer to Microchip product webpage: www.microchip.com/wwwproducts/en/ATWINC3400.

Table of Contents

1. Release Details

1.1 Changes in Version 1.4.6, with respect to Version 1.4.4

The following table compares the features of 1.4.6 to 1.4.4 release.

Table 1-1. Comparison of Features between 1.4.6 and 1.4.4 Release

Features in 1.4.4	Changes in 1.4.6
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN (WEP protocol is deprecated, attempts to configure it will result in error). • WPA Personal Security (WPA1/WPA2), including protec-tion against key re-installation attacks (KRACK) and coun-termeasures 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 EAPOLv3 support to WPA Enterprise Security. • Fixed code that saves connection info to WINC flash upon successful connection to ensure it doesn't perform unnec-essary flash writes.
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN security mode • 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. 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	No change
Transport Layer Security	

.....continued

Features in 1.4.4	Changes in 1.4.6

• The WINC 3400 supports TLS v1.2, 1.1 and 1.0.
• Client mode only.
• Mutual authentication.
• 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_RSA_WITH_AES_128_GCM_SHA256`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA256`
`TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`
`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (requires host-side ECC support eg ATECC508)`
`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECC508)`
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECC508)`
	• The “critical” field of x.509 certificate extensions is now correctly handled.
	• Ensure Basic Constraint is checked in server certificate chain.

Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • SNTP	No change
Power saving Modes	
• The WINC3400 supports these powersave modes: – M2M_NO_PS – 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)	No change
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).	No change
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	
	No change
BLE functionality	

.....continued	
Features in 1.4.4	**Changes in 1.4.6**
• BLE 4.0 functional stack	BLE API improvements/fixes

1.2 Changes in Version 1.4.4, with respect to Version 1.4.3

The following table compares the features of 1.4.4 to 1.4.3 release.

Table 1-2. Comparison of Features between 1.4.4 and 1.4.3 Release

Features in 1.4.3	Changes in 1.4.4
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN (WEP protocol is deprecated, attempts to configure it will result in error). • WPA Personal Security (WPA1/WPA2), including protec-tion against key re-installation attacks (KRACK) and coun-termeasures 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	

.....continued

Features in 1.4.3	Changes in 1.4.4

• The WINC 3400 supports TLS v1.2, 1.1 and 1.0.
• Client mode only.
• Mutual authentication.
• Supported cipher suites are:
`TLS_RSA_WITH_AES_128_CBC_SHA`
`TLS_RSA_WITH_AES_128_CBC_SHA256`
`TLS_RSA_WITH_AES_128_GCM_SHA256`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA256`
`TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`
`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (requires host-side ECC support eg ATECC508)`
`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECC508)`
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg 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: – M2M_NO_PS – 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	

.....continued	
Features in 1.4.3	**Changes in 1.4.4**
• BLE 4.0 functional stack	• Fixed BLE issues related to connection parameters messages exchange between controller and peripherals

1.3 Changes in Version 1.4.3, with respect to Version 1.4.2

The following table compares the features of 1.4.3 to 1.4.2 release.

Table 1-3. Comparison of Features between 1.4.2 and 1.4.3 Release

Features in 1.4.2	Changes in 1.4.3
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN, WEP security • WPA Personal Security (WPA1/WPA2), including protection against key re-installation attacks (KRACK). • 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	• Support for the WEP protocol is deprecated in 1.4.3. Attempts to configure it will result in error. • Countermeasures for 'Fragattack' vulnerabilities. • Ensure PMKSA caching is attempted for WPA2 Enterprise connections.
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 cannot work as a station in this mode (STA/AP Concurrency is not supported).	• Support for the WEP protocol is deprecated in 1.4.3. Attempts to configure it will result in error. • Countermeasures for 'Fragattack' vulnerabilities. • Fixed handling of source address when forwarding ARP packets out from the host.
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	No change
Transport Layer Security	

.....continued

Features in 1.4.2	Changes in 1.4.3

• The WINC 3400 supports TLS v1.2, 1.1 and 1.0.
• Client mode only.
• Mutual authentication.
• Supported cipher suites are:
`TLS_RSA_WITH_AES_128_CBC_SHA`
`TLS_RSA_WITH_AES_128_CBC_SHA256`
`TLS_RSA_WITH_AES_128_GCM_SHA256`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA256`
`TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`
`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (requires host-side ECC support eg ATECC508)`
`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECC508)`
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECC508)`
	• Improved operation of multi-stream TLS RX with 16KB record size
	• Fix to TLS Alert handling.
	• Fixed TLS RX memory leak when closing socket.

Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • SNTP	No change
Power saving Modes	
• The WINC3400 supports these powersave modes:M2M_NO_PSM2M_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)	No change
Wi-Fi credentials provisioning via built-in HTTP server	
• The WINC3400 has built-in HTTP provisioning using AP mode (Open or WEP secured)	• WEP support has been removed
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	
	Improved gain tables for module antenna
BLE functionality	
• BLE 4.0 functional stack	No change

1.4 Changes in Version 1.4.2, with respect to Version 1.3.1

The following table compares the features of 1.4.2 to 1.3.1 release.

Table 1-4. Comparison of Features between 1.4.2 and 1.3.1 Release

Features in 1.3.1	Changes in 1.4.2
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN, WEP security • WPA Personal Security (WPA1/WPA2), including protection against key re-installation attacks (KRACK). • 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	• Add option to stop scanning on first result
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 cannot work as a station in this mode (STA/AP Concurrency is not supported).	• Fix to ensure DHCP offered address is consistent when STA disconnects/reconnects. • Fix to close race condition when a STA disconnects and reconnects that could cause the WINC to disallow all further connection attempts.
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	• Fix TCP RX window leak • Address “Amnesia” vulnerabilities
Transport Layer Security	

.....continued

Features in 1.3.1	Changes in 1.4.2

• The WINC 3400 supports TLS v1.2, 1.1 and 1.0.
• Client mode only.
• Mutual authentication.
• Supported cipher suites are:
`TLS_RSA_WITH_AES_128_CBC_SHA`
`TLS_RSA_WITH_AES_128_CBC_SHA256`
`TLS_RSA_WITH_AES_128_GCM_SHA256`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA`
`TLS_DHE_RSA_WITH_AES_128_CBC_SHA256`
`TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`
`TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (requires host-side ECC support eg ATECCx08)`
`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECCx08)`
`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECCx08)`
• TLS ALPN support
	• Fix verification of certificate chains which include ECDSA signatures
	• SHA224, SHA384 and SHA512 verification capability added

Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • IGMPv1, v2 • SNTP	No change
Power saving Modes	
• The WINC3400 supports these powersave modes:M2M_NO_PSM2M_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)	No change
Wi-Fi credentials provisioning via built-in HTTP server	
• The WINC3400 has built-in HTTP provisioning using AP mode (Open or WEP secured)	No change
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.	• Ensure broadcast frames contain correct destination MAC address. • Ensure NULL frames are sent to keep the AP connection alive during periods of low activity
ATE Test Mode	
• Embedded ATE test mode for production line testing driven from the host MCU.	• Ensure ATE image is included in compound image • Fix TX test in demo application
Miscellaneous Features	

.....continued	
Features in 1.3.1	**Changes in 1.4.2**
• Host FLASH API – allows a host to store and retrieve data on the WINC stacked flash.	• I/Q calibration values read and applied from efuse
BLE functionality	
• BLE 4.0 functional stack	• Allow capture of RSSI of received advertising frames • Improve BLE powersave • Fix BLE pairing with iOSv13.x • Allow a device to reprovision the WINC without having to re-pair.

1.5 Changes in Version 1.3.1, with respect to Version 1.2.2

The following table compares the features of 1.3.1 to 1.2.2 release.

Table 1-5. Comparison of Features between 1.3.1 and 1.2.2 Release

Features in 1.2.2	Changes in 1.3.1
Wi-Fi STA	
• IEEE802.11 b/g/n • OPEN, WEP security • WPA Personal Security (WPA1/WPA2), including protection against key re-installation attacks (KRACK).	Same features along with the following: • 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 • WPA/WPA2 Enterprise options for phase 1 TLS handshake: Bypass server authentication Specify root certificate Time verification mode Session caching • Option to encrypt connection credentials that are stored in WINC3400 flash. • Improved connection API, allowing connection via BSSID as well as SSID. • Simple Roaming support.
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN and WEP, WPA2 security modes • The device cannot work as a station in this mode (STA/AP Concurrency is not supported).	• Ability to specify the default gateway, DNS server and subnet mask
WPS	
• The WINC3400 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change
Wi-Fi Direct	
Wi-Fi direct client is not supported	No change

.....continued

Features in 1.2.2	Changes in 1.3.1
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 11 divided as: • 7 TCP sockets (client or server) • 4 UDP sockets (client or server)	• New socket type "Raw Socket" added, raising the total socket count to 12. • Ability to configure the TCP keepalive settings via Socket Options. • Ability to specify the NTP servers.
Transport Layer Security	

• The WINC 3400 supports TLS v1.2, 1.1 and 1.0.
• Client mode only.
• Mutual authentication.
• 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_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (requires host-side ECC support eg ATECCx08)`
	• Added ALPN support.
	• Added cipher suites:
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires host-side ECC support eg ATECCx08)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA 256 (requires host-side ECC support eg ATECCx08)

Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • IGMPv1, v2 • SNTP	• SNTP servers are fully customizable.
Power saving Modes	
• The WINC3400 supports these powersave modes:M2M_NO_PSM2M_PS_DEEP_AUTOMATIC	If M2M_PS_DEEP_AUTOMATIC mode is selected the power consumption will be significantly lower than in previous releases, when both BLE and WIFI subsystems are idle
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)	No change
Wi-Fi credentials provisioning via built-in HTTP server	
• The WINC3400 has built-in HTTP provisioning using AP mode (Open or WEP secured)	• Improved provisioning user experience • Default gateway and subnet mask can now be customized when in AP mode
WLAN MAC only mode (TCP/IP Bypass, or Ethernet Mode)	
The WINC3400 does not support WLAN MAC only mode.	• The WINC3400 can be restarted in WLAN MAC only mode, letting the host send/receive Ethernet frames
ATE Test Mode	
	• Embedded ATE test mode for production line testing driven from the host MCU.
Miscellaneous Features	

.....continued	
Features in 1.2.2	**Changes in 1.3.1**
	• New APIs to allow host applications to read, write and erase sections of WINC3400 flash when the WINC3400 firmware is not running. • Removed previous m2m_flash APIs which allowed access to WINC3400 flash for specific purposes.

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/WINC3400-known-issues

Table 2-1. Known Problems and Solutions

Problem	Solution
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.	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()).
The AP initiated group rekey process sometimes fails when the WINC is processing a high volume of receive traffic.	Reconnect the Wi-Fi connection to the AP if a disconnection occurs due to this issue.
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.	(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()).
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.	Retry the Wi-Fi connection.
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.	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.
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.	The application should retry the connection request when it is notified of the failure.
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.	The leak can be avoided by disabling powersave when receiving two concurrent TLS streams in this configuration.
Sometimes the WINC3400 fails to see ARP responses sent from certain APs at 11Mbps.	None. The ARP exchange will be retried several times and the response will eventually get through to the WINC3400.

.....continued

Problem	Solution
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.	Only use one scan request during BLE provisioning.
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.	None. Do not use these APIs.
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.	Retry opening the secure connection.
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.	Process the return value with care, according to the API documentation.
After writing new firmware to the WINC3400, the first Wi-Fi connect attempt in STA mode takes an extra 5 seconds.	Allow longer for the Wi-Fi connection to complete.
When running in AP mode, the WINC3400 DHCP Server sometimes takes 5 to 10seconds to assign an IP address.	Allow longer for DHCP to complete.
When performing intensive crypto operations, the WINC3400 can become unresponsive to host interactions for up to 5 seconds. Specifically, when performing PBKDF2 passphrase to PMK hashing during WPA/WPA2 WiFi connects, or TLS certificate verification using 4096-bit RSA keys, the WINC3400 can take up to 5 seconds to perform the necessary calculations. During this time, it does not service it's event queues, so any host interactions, and expected responses can be delayed.	Host code should be written to expect a delay in responses from the WINC3400 of up to 5 seconds in the rare cases that it is busy performing the scenarios described above.

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legal-information/microchip-trademarks.

ISBN:

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications 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. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. 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 ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP’S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

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.

Microchip Devices Code Protection Feature

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

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.