WINCS02

Supplemental User Guide

**Version: 2.0**

**Date: April , 2024**

**Abstract**

This document provides extra information on specific features contained within the 2.0 firmware release.

[1 Introduction 4](#_Toc164931309)

[2 Features 5](#_Toc164931310)

[2.1 Multiple Wi-Fi region Support 5](#_Toc164931311)

[2.1.1 Overview 5](#_Toc164931312)

[2.1.2 Usage 5](#_Toc164931313)

[2.2 Simple Roaming 5](#_Toc164931314)

[2.2.1 Overview 5](#_Toc164931315)

[2.2.2 Usage 6](#_Toc164931316)

[2.3 Autorate 6](#_Toc164931317)

[2.3.1 Overview 6](#_Toc164931318)

[2.3.2 Usage 6](#_Toc164931319)

[2.4 Powersave 6](#_Toc164931320)

[2.4.1 Overview 6](#_Toc164931321)

[2.4.2 Usage 7](#_Toc164931322)

[2.5 Bluetooth/Wi-Fi Coexistence 7](#_Toc164931323)

[2.5.1 Overview 7](#_Toc164931324)

[2.5.2 Usage 7](#_Toc164931325)

[2.6 Configuring TLS 7](#_Toc164931326)

[2.6.1 Overview 7](#_Toc164931327)

[2.6.2 Usage 7](#_Toc164931328)

[2.7 Secure Signing 8](#_Toc164931329)

[2.7.1 Overview 8](#_Toc164931330)

[2.7.2 Usage 8](#_Toc164931331)

1. Introduction

This document provides supplemental information on features and functionality contained within the WINCS02 2.0 firmware release.

1. Features
   1. Multiple Wi-Fi region Support
      1. Overview

An improper combination of transmit power level and antenna gain can result in Equivalent Isotropic Radiated Power (EIRP) that exceeds the amount allowed for the regulatory domain in which the device is operating. Regulatory authorities set the maximum transmit power of Wi-Fi devices for the region they govern; for example, the FCC and the CE regulatory authorities govern the US and Europe regions, respectively.

In short, the maximum transmit power is limited according to the regulatory region under which the device is known to be operating. The IC’s “gain tables” allow the maximum transmit power to be controlled for up to 6 different regulatory domains/regions in WINCS02 devices.

* + 1. Usage

Refer to sections 1.1.20.1 and 1.1.20.2 for information on viewing the installed regulatory gain tables and selecting the desired region.

* 1. Simple Roaming
     1. Overview

802.11 roaming is a feature in which a WLAN station may transition between a multitude of Access Points within an Extended Service Set (ESS). An ESS is formed when a collection of Access Points share the same wired network and provide the same Wi-Fi network name (Service Set Identifier or SSID). The purpose of roaming is to automatically connect to another AP within the ESS when the existing AP connection becomes unusable due to issues such as the station ‘moving out of range’.

As mentioned earlier, an AP participating in an ESS is expected to share not only the same Wi-Fi network name, but also to be on the same LAN. Thus, roaming enables a station to change its Access Point while remaining connected to the IP layer network.

In release 2.0, the WINCS02 will roam on detection of link-loss with the existing AP; link-loss is detected by tracking the beacons of the associated Access Point; a prolonged absence of beacons is used to trigger the roaming function in the WINCS02. The WINCS02 station will also send keep-alive (NULL) frames to the Access Point to maintain the link during periods of network inactivity.

Note: ISO/OSI Layer 2 roaming occurs when the WINCS02 roams from one AP to another AP, both of which are inside the same IP subnet. Layer 3 roaming occurs when the WINCS02 roams from one AP to another AP which is in a different subnet.

Note: In version 2.0 the WINCS02 will always attempt to refresh or update its IP address by sending out a DHCP Renew message. As a result of layer 3 roaming, any existing network connections will be interrupted, and it will be the responsibility of upper layer protocols to re-establish an IP connection if such is required at layers 4 and above.

* + 1. Usage

Simple roaming is always enabled in this release.

* 1. Autorate
     1. Overview

The ability to dynamically adjust the transmission rate to reflect the conditions of the wireless environment is an important feature of any Wi-Fi device as dynamically adjusting the transmit rate can make a significant difference in overall performance. The aim of rate adaptation is to select the highest-performing modulation and coding scheme that can allow reliable data exchange in the current radio environment.

Radio environments may be subject to frequent changes in ‘quality’. In the case where the environment is ‘degrading’ (e.g. signal-to-noise ratio is decreasing), and frames are being lost, the device will select a more robust (lower transmission rate) modulation/coding scheme to improve link reliability.

Similarly, in an environment where radio conditions improve (e.g. signal-to-noise ratio increases), the device will attempt to step up to a higher rate while looking for a new balance with the new radio conditions in order to make the most efficient use of the wireless medium and allow for higher overall throughput.

* + 1. Usage

This feature is implemented in firmware and will always run automatically.

* 1. Powersave
     1. Overview

The WINCS02 implements the 802.11 Protocol Power Save functionality.

When operating as a station, the device will notify the Access Point when it is unavailable to receive data (i.e. when the WINCS02 has been configured to disable its receiver when idle to save power). During such periods, the Access Point will temporarily store any traffic for any ‘sleeping’ station and indicate in its beacons (TIM/DTIM element) that data for the station has been buffered.

A WINCS02 station in powersave mode, will wake periodically to listen for the beacons from the Access Point, and in the case where data has been buffered, the station will inform the Access Point that it is now ‘awake’ and available to receive.

Note: In version 2.0, the WINCS02 will wake every beacon interval to check for buffered traffic.

* + 1. Usage

Refer to sections 1.1.20 for information on configuring (or reading) the powersave settings.

* 1. Bluetooth/Wi-Fi Coexistence
     1. Overview

Bluetooth and Wi-Fi share the same 2.4GHz ISB Band. These wireless protocols have different modulations schemes, channel frequencies and bandwidths but may nevertheless interfere with one another, particularly when co-located. Signals from one wireless protocol look like unwanted noise for the other protocols, causing performance degradation. The WINCS02 implements Bluetooth/Wi-fi coexistence, compliant with the recommendations in IEEE 802.15.2. Supporting 2- and 3-wire PTA interfaces, the WINCS02 can be configured to assign priorities for WLAN and Bluetooth traffic to ensure collisions and corruption of frames is avoided. The WINCS02 supports both shared (switching) antenna and separate Bluetooth/Wi-Fi antennas.

* + 1. Usage

Refer to sections 1.1.20 for information on configuring (or reading) the Bluetooth/Wi-Fi Coexistence settings.

* + - 1. Sample command sequence

To configure Bluetooth/Wi-Fi Coexistence on WINCS02, the driver API calls would be:

WDRV\_WINC\_STATUS **WDRV\_WINC\_WifiCoexConfSet**(DRV\_HANDLE handle, WDRV\_WINC\_COEX\_CFG \*pCoexCfg)

WDRV\_WINC\_STATUS **WDRV\_WINC\_WifiCoexEnableSet**(DRV\_HANDLE handle, bool enableCoexArbiter)

* 1. Configuring TLS
     1. Overview

TLS behaviour is controlled via TLS contexts. A context is opened using WDRV\_WINC\_TLSCtxOpen, and then updated using other WDRV\_WINC\_TLSCtx APIs.

* + 1. Usage

The minimal set of WDRV\_WINC\_TLSCtx APIs which must be called in order to make a TLS context ready for use are:

* WDRV\_WINC\_TLSCtxCACertFileSet, to either:
  + set the file of CA certificates to be used for authenticating the peer; or
  + disable authentication of the peer (not recommended for a TLS Client).
* WDRV\_WINC\_TLSCtxHostnameCheckSet, to either:
  + set the hostname of the peer, for verifying the peer certificate’s subject name; or
  + disable verification of the peer certificate’s subject name peer (not recommended for a TLS Client).

Other WDRV\_WINC\_TLSCtx APIs may be called to control other aspects of the TLS behaviour.

Refer to section 1.1.19 for full details of TLS APIs.

* 1. Secure Signing
     1. Overview

TLS client authentication allows a server to verify the identity of a client that connects using the Transport Layer Security (TLS) protocol. The server requests the client to sign a message with its private key which is verified against the public key in the X.509 certificate. WINCS02 enables TLS client authentication secure signing via the on-module ATECC608 secure element, or an external device capable of secure ECDSA signing, leveraging hardware-based private key storage and accelerated signing. The on-module secure element is the ATECC608A-TNGTLS, the Trust-and-Go pre-provisioned variant of the ATECC608, featuring ECDSA P-256 signing, ECC Private Key secure storage, and X.509 compressed certificate storage. Access to the secure element is made through I2C or SWI.

* + 1. Usage

To leverage the crypto device for secure signing, the host application needs to follow these steps:

* Retrieve from the crypto device the X.509 certificate that includes the public key corresponding to the securely stored private key:

ATECC608\_ReadDeviceCert(<CERT\_NAME>, <CERT\_SIZE>)

* Send the certificate to the Wi-Fi companion chip using the WDRV\_WINC\_File APIs.
* Set the certificate filename in the TLS context with the WDRV\_WINC\_TLSCtxCertFileSet API.
* Register a signing callback function of type WDRV\_WINC\_EXTCRYPTO\_SIGN\_CB, using the WDRV\_WINC\_TLSCtxSetSignCallback API.
* Implement the above signing callback function, to request a signing operation from the crypto device and send the result to the Wi-Fi companion chip via the WDRV\_WINC\_EXTCRYPTOSign API.

Refer to section 1.1.8 for full details of these APIs.