

## Intelligent Wi-Fi Solutions Deliver Unmatched Flexibility

### Customized, Enhanced Wireless Drivers and Licensed Firmware IP

You need a trusted Wi-Fi solutions partner that can take you to the next level of connectivity, security, and reliability. Intelligraphics (IGX Wireless) is the provider of choice for the most technically advanced and innovative mobile, mission-critical, and IoT Wi-Fi device driver IP and development services. Our fast, seamless Wi-Fi roaming solutions for TI WiLink™ and select Qualcomm® chipsets allow you and your customers to see more and do more, while keeping your wireless connections protected.



### Solutions and Services

- Customized Wi-Fi device driver, firmware, and licensed IP for TI WiLink™ and Qualcomm® chips
- Wi-Fi packet sniffing, injection, and monitoring
- Advanced wireless features including 802.11e, 802.11i, and 802.11h
- Implementation of 802.11k, 802.11r, 802.11s, 802.11u, 802.11ai, and 802.11v
- FIPS support and enterprise-level Security protocols including WPA, WPA2, 802.1x, and EAP TTLS
- Cisco CCX support and pre-certification testing
- Wi-Fi Alliance pre-certification development
- Advanced RF noise mitigation, antenna diversity and coexistence
- Advanced diagnostics

### Industries and Use Cases

- **Industrial** – M2M, asset tracking, mobile robotics and data acquisition, mobile printing
- **Medical** – wireless devices including patient monitoring, diagnostic systems, infusion pumps, X-ray, and ultra-sound machines
- **Warehousing and logistics** – wearable and mobile devices for asset tracking, pick/put-away
- **Enterprise** – mesh networking, access points, wireless VoIP
- **IoT, retail, and consumer** – wearables, smart appliances and devices, beaconing
- **Government and security** – packet sniffing/injection, network characterization
- **Transportation** – security/tracking, inter-train, intra-train, and train-station communication



# Advanced Roaming and Bloodhound Sniffer/Injector IP

## IGX Wireless Advanced Roaming

Organizations and businesses today rely on a wide range of data-driven insights for proactive decision-making. Acting on data in a timely fashion first requires that all assets, including wireless devices, maintain persistent connectivity to the organization's IT backplane. Having an "always on" Wi-Fi connection helps organizations make decisions faster, continuously improve efficiencies, and reduce costs. IGX Wireless Advanced Roaming supports all types of 802.11 access points (APs), allowing customers to quickly integrate their wireless devices, while maintaining compatibility with their existing IT infrastructure..

IGX Advanced Roaming software uses proprietary scanning algorithms and decision-making logic to significantly reduce the time it takes for wireless devices to connect to an AP, boosting device availability and connection reliability. The software provides fast, seamless roaming along with optional enterprise-class security to unleash the full benefits of Qualcomm® and TI Wi-Fi chips. It delivers superior connectivity for achieving Industry 4.0 automation goals, improving medical system wireless performance, expanding the adoption of wireless autonomous robotics in manufacturing, and deploying wireless devices to help streamline logistics operations.

### Key Benefits

- Maintain persistent AP connections, regardless of network load
- Ensures both mobile and stationary wireless devices stay connected, boosting device availability
- Roaming times of tens of milliseconds, depending on the hardware configuration and application
- Support for multiple hardware platforms and OS's including Linux, Android, Windows 7/10, and WEC7

## IGX Wireless Bloodhound Sniffer/Injector

Analysts, agencies, and security experts are all in agreement that threats to public safety, critical infrastructure, and data will rapidly escalate. The widespread proliferation of IoT and other wireless devices create enormous numbers of vectors and entry points for malicious activities including keylogging, malware, DDoS, IP spoofing, man-in-the middle (MiTM), man-on-the-side (MoTS), and other attacks.

IGX Wireless Bloodhound Sniffer/Injector allows users to passively listen, inject, and record packet information exchanged within a targeted Wi-Fi channel. It features a single Wi-Fi driver that can either act as a Wi-Fi sniffer for big data traffic collection, surveillance, or as a regular Wi-Fi driver. Organizations can use IGX Bloodhound to target and proactively surveil Wi-Fi communications in real-time, more effectively identify and evaluate threats, help improve public safety, and protect critical infrastructure.

### Key Benefits

- Single Wi-Fi driver that can either act as a Wi-Fi sniffer/injector, or as a standard Wi-Fi driver
- Multi Wi-Fi module/adaptor support enables sniffing/injection on multiple channels
- Remote wireless monitoring reduces risk of being noticed or compromised
- Enables customers to create a solution stack for a truly portable, mobile wireless sniffer/injector

## Enterprise Security Suite and CCXv5/v5 Extensions IP

### IGX Wireless Enterprise Security Suite for Qualcomm® QCA401x Chipsets

Securing critical infrastructure including manufacturing, transportation, medical, and industrial is not only essential—it's also extremely challenging. While it's clear that Wi-Fi IoT devices allow organizations to operate more efficiently and reduce costs, not enough consideration is given to their potential security risks. The solution is to ensure that the IoT devices being deployed contain strong Wi-Fi (AES/WEP/WPA2) and internet-level Transport Layer Security (TLS)/Secure Sockets Layer (SSL) encryption, along with all the other supported standards including the variations of EAP-FAST, PEAP, and LEAP.

Enterprise Security Suite from Intelligraphics provides robust security provisions that leverage the strength of the existing security standards plus EAP-TLS capabilities including encrypted password generation, authentication, and client/server handshake. Security keys are generated at runtime based on a handshake process between the server and the IoT device. It leverages public key infrastructure (PKI) certificates, which provides a secure way to authenticate and authorize users for network access. Passwords are not stored in the IoT device and are randomly generated during connection to the Wi-Fi infrastructure, providing a method for organizations to quarantine unsecure or infected devices from their network.

#### Key Benefits

- Relies on the strength of EAP-TLS v1.1/v1.2 libraries for authentication secrecy
- Wi-Fi passwords are not stored in the IoT device, eliminating stored password vulnerabilities
- Passwords are randomly generated at runtime during connection with the Wi-Fi infrastructure
- Optimized for the [Qualcomm® QCA4010/12](#) chipset

### IGX Wireless CCXv5/v5 Extensions

802.11-based wireless devices contain radios that must provide secure and reliable connectivity. IEEE and industry standards define how a Wi-Fi radio operates with a wireless LAN infrastructure, and the Wi-Fi CERTIFIED™ seal ensures interoperability. For many devices, however, Wi-Fi CERTIFIED is not enough. These devices need to operate with a Cisco wireless LAN infrastructure and support Cisco wireless LAN innovations for enhanced security, mobility, quality of service, and network management.

The CCX specification is a superset of the one used for Wi-Fi certification. Medical, mission critical, and industrial-grade devices requiring extra security are tested for CCX version 4 (CCXv4), and now the new CCXv5 standard. However, not all Wi-Fi chipsets ship with baseline driver and firmware that supports CCX by default. Meeting this challenge, Intelligraphics has developed IP that allows us to deliver CCX support and also pre-certify your product, saving you time and effort.

#### Key Benefits

- Certification is essential for any device that need to use CCX features and connect to Cisco-based WLAN APs
- IGX Wireless pre-certification lab ensures compliance with CCXv4/v5 requirements
- Available as licensed IP and customized configurations