TSI® IoT Devices

Communication to TSI® Cloud Platform

Application Note TSI-168 (US)

Security and Protocols that are Supported

- 2.4 GHz Wi-Fi® frequency
- WEP/WPA-TKIP/WPA2-CCMP & Protected Management Frames
- Cellular Modems or Smartphone Wi-Fi® hotspots
- Enhanced Wi-Fi® security MAC address filtering/MAC filtering
- IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (Wi-Fi 1, Wi-Fi 3, Wi-Fi 4)
- Encryption via MQTT/SSL
- IPv4

Not Supported

- Guest Wi-Fi® Networks with captive portal (aka splash page or terms and conditions page) that require a user to authenticate themselves and/or register to the Wi-Fi® network.
- WPA2-Enterprise is not supported. *The device is capable, but TSI® would need to enable it and test.*
- IPv6 is not supported. *Device is capable, but TSI would need to enable and test.*

Enterprise Firewall Setting

Following ports need to be Enabled:

- DNS: 53 (UDP)
- SNTP: 123 (UDP)
- HTTPS: 443 (TCP)
- MQTT: 8883 (TCP)

Hostnames

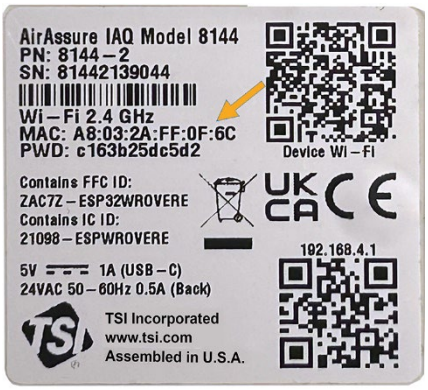
- mqtt.tsilink.com (for the Device communication to **TSI Link™** software)
- tsi-prd.appspot.com (Device firmware over the air updates)
- tsilink.com (Device firmware over the air updates)
- time.google.com (default SNTP server)
- tsi-prd.auth0.com (M2M token retrieval)

Frequently Asked Questions

1. Not able to connect to Wi-Fi®, getting a solid white light.

LED	Wi-Fi®	Cloud
Pulse Yellow	Set up Mode	
Pulse White	Connecting	
Pulse Blue	Connected	Connecting
Solid Blue	Connected	Connected
Solid White	No connection	No connection

   - Verify the Wi-Fi® channel is 2.4 GHz Wi-Fi® frequency and supports WPA2-Personal Security.
   - The most common issue is an incorrect password for your Wi-Fi®. To double check the Wi-Fi® password try connecting to the same network using your phone. Once you have confirmed the password is correct, try again with the device.
   - Check if your Wi-Fi® router has MAC address filtering/MAC filtering enabled. If so you will need to add your device MAC address on the approved Wi-Fi® router whitelist. See diagrams for where they are placed on the labels.



   - If you are connecting to GUEST network, verify if it has a captive portal (aka, splash page. For example when you have to accept the terms and conditions or login to a public Wi-Fi®). If so, that is currently not supported and you will not be able to connect the device to the GUEST network.

2. I am able to get a blue solid light, but still unable to connect to the internet.
   - Most likely your Wi-Fi® router/Cellular modem is having issues connecting to the internet.
     - Try power cycling your Wi-Fi® router/Cellular modem
     - Try connecting another device to that Wi-Fi® router/Cellular modem/hotspot
   - If you are trying to connect to a corporate/enterprise network, most likely it is due to a firewall setting/rule.
     - Request the IT/Firewall security team enable required ports and hostnames on the firewall settings

3. Is any communication initiated from the cloud to monitors?

   Yes*, communication can be done in both directions.*

4. Is data pulled from monitors by application running in the cloud or are data pushed by monitors into the cloud?

   Data is currently being pushed by device.

5. How is data moved into the cloud, what protocols or applications are used by software running on monitors?

   IoT device communicates via MQTT.

6. Are your applications, systems, and networks run on robust, reliable hardware and software supported by appropriate backup hardware and facilities where necessary?

   Yes.

7. Does **TSI Link™** software require the utilization of a special browser?

   Google® Chrome® browser is recommended, but it will also work with Safari®, Edge® and Firefox® browsers.

8. Is sensitive information/PII encrypted from the device to the cloud and from the cloud to the Applications?

   Yes we do encrypt our data, regarding the process / different components:

   a. Data moving from the device to the cloud is encrypted using TLS/SSL and compression of JSON formatted payloads, under a secure connection using public/private key authentication and TLS encryption.
   b. Data in our cloud requires proper certification using 2 factor authentications to access and the data is stored unencrypted in our databases which are secured and only allowed from specific IP addresses we manually add to a white list.
   c. from the cloud to the application? Uses standard TLS/SSL encryption and compression as per REST standards, requires valid JWT from the customer as well which is provided by Auth0 using proper OAuth flow.
   d. From the cloud / API to the customer? Uses standard TLS/SSL encryption and compression as per REST standards, protected via client id and secret as per OAuth machine2machine client credentials flow, requires valid subscription and account_id for access.

9. Do you have an information security risk assessment program?

   Yes.

10. Do you maintain a process to document non-compliance with any statutory, regulatory, or contractual requirements?

    Yes.

11. Do you perform regular security audits/reviews by internal or qualified third-party assessors?

    Yes.

12. Where is the data stored?

    Our **TSI Link™** data is currently hosted in Google® Cloud Platform, specifically using Google's us-central1 location (physically in Iowa).

®Chrome is a registered trademark of Google LLC, Safari is a registered trademark of Apple Inc., Edge is a registered trademark of Microsoft Corporation, Firefox is a registered trademark of Mozilla Foundation.

Knowledge Beyond Measure.

TSI Incorporated – Visit our website **www.tsi.com** for more information.

USA	**Tel:** +1 800 680 1220	**India**	**Tel:** +91 80 67877200
UK	**Tel:** +44 149 4 459200	**China**	**Tel:** +86 10 8219 7688
France	**Tel:** +33 1 41 19 21 99	**Singapore**	**Tel:** +65 6595 6388
Germany	**Tel:** +49 241 523030		

TSI-168 Rev C (4/1/2026) US Printed in U.S.A.