

Worldpay Wi-Fi Connected Solutions

Network and Device Best Practices

Introduction

This document describes best practices for using TCP/IP connected payment devices with Worldpay TCP/IP connection solutions which include:

Solution	Location	Description
triPOS Cloud	US	
IPS Cloud	UK	
triPOS Direct	US	
triPOS Mobile iOS and Android	US	

Stable network

Must have a stable network that permits long-lived, persistent socket connections:

- Less-than-optimal connectivity options (cell-based networks, poor wifi set-ups/meshes, hotspots, etc) are strongly discouraged, and have been shown to be problematic. Networks that have intermittent connectivity patterns can work ok with more traditional “make/break” connections (e.g, typical web browser↔web site use cases, where connection are made and broken rapidly, each being relatively short-lived). However, these less-than-ideal network setups may not work well with these processing platforms as there must be an always-on, reliable, and persistent connection between the platform and the device.
- Reliable, always up behavior: robust ISP, good wiring, a properly equipped and configured WiFi-mesh (if needed), high-quality and properly configured hardware.
- The network must not interrupt TCP keep-alive traffic, like regular heartbeats or pings.
- Guidance for the minimal network speed characteristics are:
 - 10Mega-bits per second, upload and download
 - Latency less than 30milliseconds
 - 0% packet loss

Hotspots

Do not use hotspots via iOS and Android devices. These devices have known behaviors that shut down connections aggressively to save on bandwidth, etc.

- Prefer more stable hotspots that permit long-lived, and non-chatty, connections to persist.

Router and Firewall configurations

Router and Firewall configurations must open the port for device connections:

Solution	Port (primary)	Port (backup)
triPOS Cloud	9001	443
IPS Cloud	443	
triPOS Direct	N/A	
triPOS Mobile iOS and Android	N/A	

Firewall rules

Firewall rules must be written using domain names; using IP-address is not allowed as IPs may change.

- Multiple IPs may be used for redirection traffic / load balancing / DR purposes. Do not use static IP.

Security scanning

Eliminate and/or remove any security scanning and/or any packet sniffing.

- These scans can interfere with the persistent connections, and have been demonstrated to break the connectivity between the platform and the terminal device.

Quality-of-Service (QOS) configurations

Properly applied Quality-of-Service (QOS) configurations might help to prioritize device traffic, but QOS has not been shown to reliably address other flaws in the setup.

- QOS configuration requires packet inspection to shape the traffic, and this can interfere with always-up sockets.
- "Automatic", "intelligent" or similar QOS options are not effective, as they will often prioritize other types of traffic and can make the situation worse.

Roaming

Roaming allows you to freely move from room to room while your device automatically roams from one access point to another as necessary, intuitively choosing the strongest access point without dropping its Wi-Fi signal, providing seamless connectivity. While there's always a brief interruption when switching between networks (around half a second) when roaming, the duration of that interruption can be reduced to a minimum if the devices use the same Wi-Fi network names (SSID's), Wi-Fi channels, and network keys or passcodes. Ideally, environments where ability to roam is critical will leverage dedicated mesh hardware that is designed for seamless handoff of connections between meshed access points.

Dedicated Network, Frequency options

If issues persist on-site in getting devices to establish and maintain a reliable connection to the platform, some merchants have had success creating a separate, dedicated WiFi network for just the payments platform, to avoid complications from the unpredictable bandwidth sharing characteristics that can result from shared WiFi ecosystem.

Similarly, some merchants have experienced better results when using the 5GHz channels for their WiFi devices (vs 2.4GHz, which can suffer from increased interference as more devices share this band). However, there is a potential tradeoff, as using 5GHz channels may shorten the effective range the devices can be from the router and still maintain a reliable connection.

Device health

It is of course critical to take care of the device, and ensure the battery is properly charged (and holding charge), and is in good working order. If all other avenues have been explored, the culprit could be a defective device. If available, confirming behavior with a second (ideally, known working) device can help determine if the pin-pad hardware is in play.