Agile FleetCommander
Kiosk and Key Box VPN Communications Specification

Communications Specification for Kiosks and Key Boxes

CONTACT: FleetCommander Support
EMAIL: fcsupport@agilefleet.com

Disclaimers

Privacy Information

This document may contain information of a sensitive nature. This information should not be given to persons other than those specifically designated in your software use agreement.

Table of Contents

Introduction

This document serves the purpose of detailing the data flow and order of operations for how an Administrative Workstation, FleetCommander Kiosk, and FleetCommander Key Box communicate with Agile Fleet's cloud hosting platform using the key box VPN connection method. Network requirements are provided for each piece of equipment.

As always, if you have any questions or concerns, please reach out to FleetCommander Support at FCSupport@agilefleet.com or 571-498-7555 x2.

Data Flow and Order of Operations

Administrative Workstation

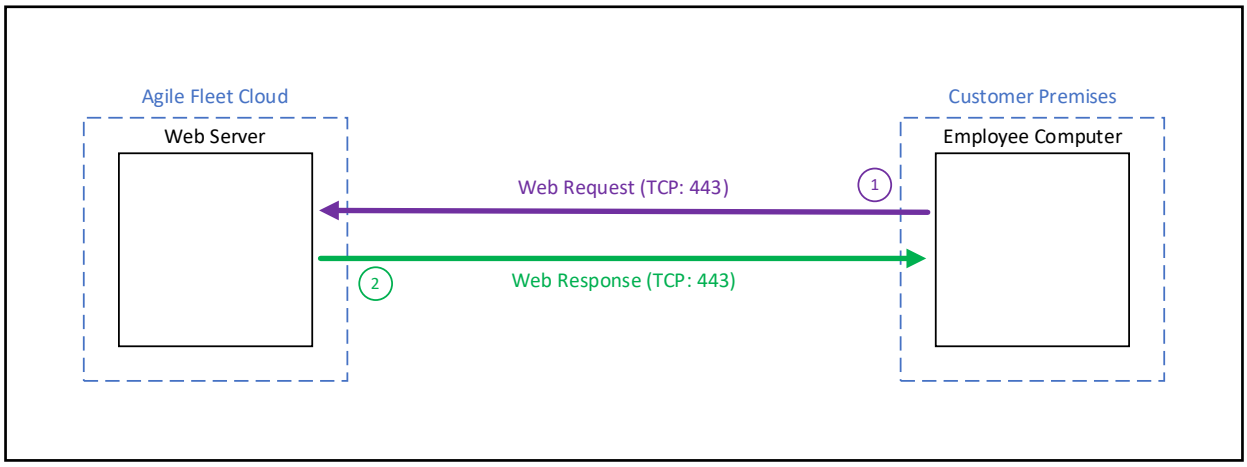

Figure 1: Administrative Workstation Data Flow

Administrative Workstation Data Flow:

1. Fleet administrators and drivers can access the FleetCommander administrative site from any computer using a web browser. Web page requests are sent to an Agile Fleet web server via HTTPS (TCP: 443).
2. Response to the web page request is returned to the user's web browser via HTTPS (TCP: 443).

FleetCommander Kiosk and Key Box

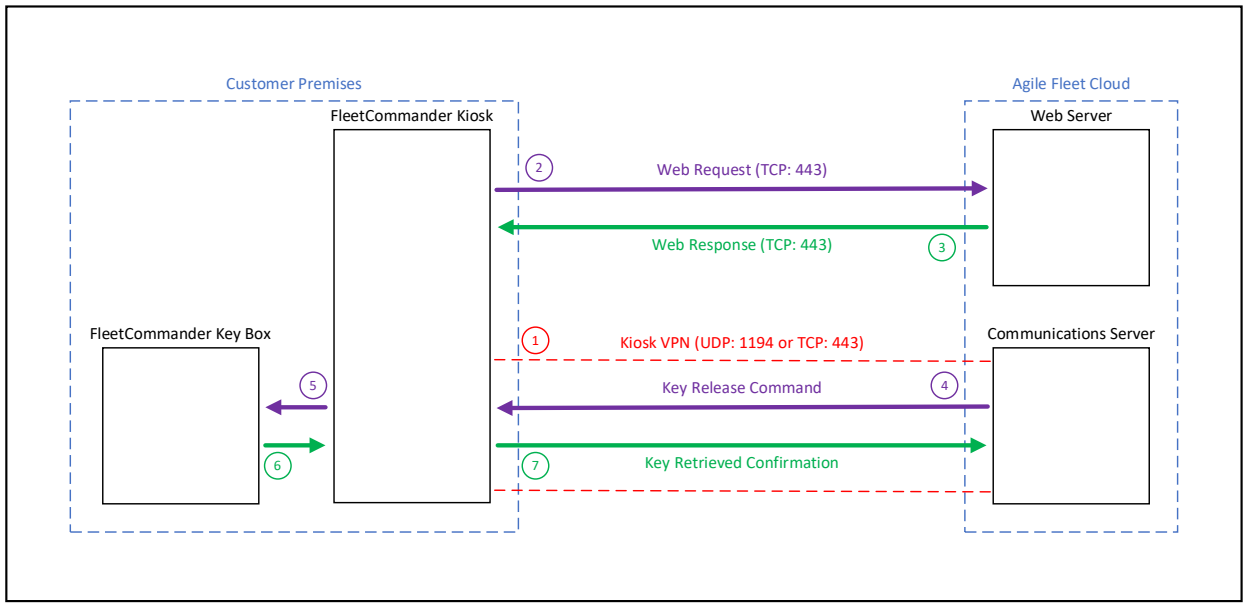

Figure 2: Kiosk and Key Box Data Flow

Kiosk and Key Box Data Flow:

1. Upon kiosk startup a VPN client installed on the kiosk as a Windows service initiates and establishes a VPN connection with Agile Fleet's communications server via UDP: 1194 or TCP: 443. The VPN connection is used as a secure communication for sending commands to the key box.
2. Drivers will use a FleetCommander kiosk to check out a vehicle and obtain vehicle keys. Web page requests are sent from the kiosk to an Agile Fleet web server via HTTPS (TCP: 443).
3. Response to the web page request is returned to the kiosk via HTTPS (TCP: 443).
4. Upon completing the vehicle check out process, a Key Release Command is sent from Agile Fleet's communications server to the kiosk via the VPN connection established in step 1.
5. The kiosk relays the Key Release Command to the key box, allowing the driver to retrieve the vehicle keys.
6. The key box will send a confirmation back to the kiosk.
7. The kiosk relays the confirmation to Agile Fleet's communications server via the VPN connection, indicating if the key box was open and if the vehicle key was retrieved.

Requirements

Administrative Workstation:

- DNS[i]
- Outbound Internet Access[ii]

FleetCommander Kiosk:

- One (1) Physical Network Connection
- Two (2) Network Interface Cards (NIC)[iii]
- DHCP or Static IP Address[iv]
- DNS[i]
- Outbound Internet Access[ii]
- TCP: 443 (Web Traffic for Kiosk)
- UDP: 1194 or TCP: 443 (VPN Traffic for Key Box)[v]
- UDP: 123 (NTP Time Synchronization)[vi]
- OpenVPN Connect v3 or higher[vii]
- IP Forwarding Enabled in Windows OS

FleetCommander Key Box:

- Network Cable connected directly to Kiosk NIC #2

[i] DNS must be able to resolve agilefleet.com and any of its subdomains. Example: acme.agilefleet.com DNS for the kiosk must be able to resolve agilefeet.com and any of its subdomains and openvpn.com and any of OpenVPN's subdomains. Example: us-lax.gw.openvpn.com

[ii] Outbound Internet must allow access to agilefleet.com any of its subdomains and openvpn.com and any of OpenVPN's subdomains. Example: acme.agilefleet.com and us-lax.gw.openvpn.com

[iii] The first NIC is required for the LAN connection, and the second NIC is required to connect the key box to the kiosk. A USB based network adaptor may be used if a second NIC is unavailable.
[iv] DHCP is preferred, but a static IP address can be used. The IP Address, Subnet Mask, Default Gateway, and DNS address information is required for the static IP option.
[v] UDP: 1194 is the default protocol the VPN client installed on the kiosk. The VPN client will automatically fallback to TCP: 443 if UDP: 1194 is unavailable.
[vi] The default NTP source is time.windows.com but may be changed.
[vii] Data Channel Encryption:

- Algorithm: AES (Advanced Encryption Standard)
- Key Length: 256 bits
- Mode: CBC (Cipher Block Chaining)

Control Channel Encryption:

- Protocol: TLS (Transport Layer Security)
- Key Exchange: RSA-2048
- Session Key Exchange: Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) for Perfect Forward Secrecy (PFS)
- Cipher Suites: AES

Message Authentication:

- Algorithm: HMAC (Hash-based Message Authentication Code)
- Hash Function: SHA256

