Network Requirements for Internet, POS & mPOS

Version 1.73 03/01/2016

Introduction

KWI requires a firewall, which can filter (block) both incoming and outgoing services by IP address/Protocol/Port and also by URL and (not just specific IP address, protocol, port number combinations). All firewalls can block incoming services, but not all firewalls can block outgoing traffic by URL address.

It is important to filter outgoing traffic by URL to limit the applications which the POS is allowed to connect to externally, and to stop any Trojans or viruses which do make it inside the security perimeter from phoning home (remote control). Outgoing traffic filtering helps to prevent your site from being used as a spam relay or to spread infections to others.

You should treat the requirements detailed in this document as a baseline security policy for traffic entering and leaving the store. If your business requires an "Intranet" between your store and corporate locations you should enhance this policy to prevent rogue traffic between sites within your own internal network.

Standardized Store/Internet Configurations

In order to provide standardized services, KWI needs to connect to stores using IP over the public Internet. KWI cannot provision individual VPNs to each store.

KWI also requires simultaneous access from its Help Desk to all clients' stores. KWI cannot utilize a pcAnywhere or Ultra VNC gateway where effectively only a single connection is granted from KWI to be shared across all stores. A "single session gateway" prevents KWI from having multiple Help Desk technicians working on stores simultaneously creating a bottleneck where only one technician can access a single store at a time.

Standardized Store/Internet Configuration Goals

The only TCP/IP access that should be allowed are the addresses & services listed below (in addition to any access that is needed for the Client's day to day business). This policy is designed to limit Spyware and Virus programs from the Internet.

1. Outbound SSH (secure shell) allows access to KWI's SFTP polling. SSH/SFTP requires TCP port 22 outbound to kligerweiss.net, ftp1.kligerweiss.net, ftp2.kligerweiss.net , ftp3.kligerweiss.net, ftp4.kligerweiss.net, ftp5.kligerweiss.net, ftp6.kligerweiss.net, ftp7.kligerweiss.net, ftp8.kligerweiss.net, ftp9.kligerweiss.net, ftp10.kligerweiss.net.

2. Inbound PC Anywhere for KWI help desk support. UDP & TCP ports 56xx-56xx inbound from 65.206.45.0/26, 65.51.69.64/26.

PCanywhere's port numbering convention is as follows and increases incrementally to match register quantity on site.

Example: 5631/5632 = Reg-1. 5633/5634 = Reg-2.
*Ports will need to point to the IP of the corresponding register

For stores that will be utilizing Port Forwarding, please refer to section #7a and 7b.

Example:

Ports to be Used	Corresponding Register
5631/5632	1
5633/5634	2
5635/5636	3

2.1. Inbound Ultra VNC for KWI help desk support. TCP Port 561xx inbound from:

65.206.45.0/26
65.51.69.64/26
65.51.37.192/28

Ultra VNC's port numbering convention is as follows and increases incrementally to match register quantity on site.
Format: 561xx where xx = Register number.

For stores that will be utilizing Port Forwarding, please refer to section #7a and 7b.

Example:

Port to be Used	Corresponding Register
56101	1
56102	2
56103	3

3. Microsoft's File sharing (CIFS/SMB shared drives) from the POS terminals to external locations must be blocked. KWI does use shared drives within the store for application & support purposes (selected files & directories are shared between registers within a store). This requirement can be met by blocking UDP ports 137 & 138 and TCP ports 139 & 445 (both in and out) at the firewall.

4. The below URL's must be accessible to properly run Symantec NAV Live Updates & NAV Cloud.

   hb.lifecycle.norton.com
   www.norton.com
   liveupdate.symantecliveupdate.com
   ratings-wrs.symantec.com
   stats.qalabs.symantec.com
   shasta-rrs.symantec.com
   sasmain.symantec.com
   sas1alt.symantec.com
   www.symantec.com
   ssaw.symantec.com
   siaw.symantec.com
   heartbeat.s2.spn.com
   message.s2.spn.com
   hostedendpoint.spn.com
   ins.spn.com
   https://manage.symanteccloud.com
   https://activate.symanteccloud.com
   backup.sp1.symanteccloud.com through backup.sp15.symanteccloud.com

   Websites for Symantec NAV Live Updates:
   http://liveupdate.symantecliveupdate.com (Primary)
   http://liveupdate.symantec.com (Secondary)
   ftp://update.symantec.com (Last)

5. Firewall openings for access to KWI Merchandising system website:

URL	IP Range	Port	Protocol
http://*.kligerweiss.net https://*.kligerweiss.net	65.206.45.0/26	80, 8080, 443, 8443	TCP, UDP
http://*.kligerweiss.net https://*.kligerweiss.net	65.51.69.64/26	80, 8080, 443, 8443	TCP, UDP
http://*.kligerweiss.net https://*.kligerweiss.net	65.51.37.192/28	80, 8080, 443, 8443	TCP, UDP
http://*.kligerweiss.net https://*.kligerweiss.net	66.35.45.128/26	80, 8080, 443, 8443	TCP, UDP

6. For Internet credit card processing on the First Data North and South platforms using Datawire IPN, KWI requires the following DNS addresses accessible:

URL	IP Address	Port
https://vxn.datawire.net	216.220.36.75	443
https://vxn1.datawire.net	205.167.140.10	443
https://vxn2.datawire.net	64.243.142.36	443
https://vxn3.datawire.net	206.112.91.167	443
https://vxn4.datawire.net	63.240.199.76	443
https://Vf2.datawire.net	205.167.140.11	443
https://support.datawire.net	66.241.131.100 69.46.100.78 205.167.141.100	443

To access the First Data "test" systems using Datawire IPN, KWI requires the following DNS addresses accessible:

URL	IP Address	Port
https://staging1.datawire.net	65.110.169.83	443
https:// staging2.datawire.net	69.46.100.76	443
https://stagingsupport.datawire.net	66.241.131.101 69.46.100.81	443

7. KWI needs the Static IP address info with unique subnets for the stores. Every location will need to have a public NAT (or have a range of publics) for KWI help desk to be able to access the terminals for support.

   7a. Port forwarding: For stores using a Single Public IP address that will have multiple registers, the pcAnywhere/UltraVNC port(s) for each register will need to be listening on the External IP and forwarded to the corresponding register and port(s) on the Local LAN.

   7b. Port forwarding: For stores using Multiple Public IP addresses configured for individual registers, the pcAnywhere/UltraVNC port(s) for each register will need to be listening on the External IP and forwarded to the corresponding register and port(s) on the Local LAN.

8. DNS must be enabled on the POS devices. The POS must be able to gain access to a DNS server to allow address resolution. KWI will not support manually created static host table entries at POS where specific DNS filtering is not available. This will allow easy access to your desired Internet resources using traditional "www.kligerweiss.net" type names and/or migration once specific rotating IP change.

9. To sync the time IP address 192.5.41.209 UDP port 123 needs to be available and open to NTP traffic.

10. For Internet gift card processing to Profit Point, KWI requires the following sites and services accessible:

URL	Port
https://www.wa.rewardforloyalty.com:8417/NetConnect/controller2	80
http://crl.verisign.net	80

SNAP External Services			
Service	Host	IP address	Ports
Raw IP Transactions	ipgw.profitpointinc.com	68.234.43.47	443
Web site	snap.profitpointinc.com	68.234.43.48	443
Web site	merchants.profitpointinc.com	68.234.43.49	443
Web site	admin.profitpointinc.com	68.234.43.50	443
API Interfaces	api.profitpointinc.com	68.234.43.51	443
Balance Checker	checkbalance.rewardforloyalty.com	68.234.43.39	80, 443
User Registration	register.rewardforloyalty.com	68.234.43.36	80, 443

Profit Point Outbound IP Traffic

Profit Point requires the store firewall to allow the following IP addresses for outbound traffic:

54.209.94.133
54.208.192.16
54.84.32.103
54.208.179.137

To connect to the Profit Point "test" system, KWI requires the sites are accessible:

URL	Port
https://www.wa.rewardforloyalty.com:8417/NetConnect/controller	80
http://crl.verisign.net	80

11. For clients utilizing AJB credit/debit/check/gift card engine, we recommend the router at the store level have Internet failover capabilities as AJB uses strictly IP connections to all processors. i.e. Wireless Broadband or Secondary ISP.
12. Versions of the Java run time plug-in for Internet Explorer will need to be upgraded from time to time to compliment new functionality being added to the back office system. For this: http://java.sun.com should also be left open.
13. E-mail from KWI to customers may come from two domains: kwi.com and kligerweiss.net. Generally, human e-mail will come from the kwi.com domain, while automated e-mail (reports, etc.) will come from one of two addresses: DoNotReply@kwi.com (display name "KWI") or files@kligerweiss.net. Both domains should be trusted and excluded from spam filtering to prevent reports and general correspondence from failing to be received by the intended user base.
14. To allow Microsoft Windows services (e.g. Activation), KWI requires the below domains accessible. Add the below domains to the firewall allow list.

https://*.microsoft.com
http://*.microsoft.com

15. The following web addresses will allow access to Microsoft Update. While this is not a KWI requirement, it is recommended that all registers are allowed access to receive important Windows Security Updates.

http://windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com
https://*.windowsupdate.microsoft.com
http://*.update.microsoft.com
https://*.update.microsoft.com
http://*.windowsupdate.com
http://download.windowsupdate.com
http://download.microsoft.com
http://*.download.windowsupdate.com
http://wustat.windows.com
http://ntservicepack.microsoft.com
https://*.ws.microsoft.com
http://*.ws.microsoft.com

Enterprise Class Cloud Platform

mPOS

Outbound and Inbound Communications

The mPOS system requires access to the following links for production and support services.

https://*.kligerweiss.net:90
https://*.kligerweiss.net
https://*.airwatchportals.com
https://*.awmdm.com
https://.awmdm.com
https://cn700.awmdm.com
https://ds700.awmdm.com

1. Communication with *.airwatchportals.com and *.awmdm.com on TCP port 80, 443, 8087 for device services. IP address ranges are below.
   US: 205.139.50.0/23, 209.208.230.0/23, 199.106.140.0/23, 63.128.72.0/24, 63.128.76.0/24, 192.30.64.0/20, 216.253.141.0/24.
   CANADA: 207.2.204.0/22, 206.152.33.0/24, 206.152.32.0/21.
   UK: 185.45.163.200 – 185.45.163.234, 213.86.109.144, 213.86.109.37, 46.244.37.28, 206.101.38.112/29, 206.132.43.0/24, 206.151.160.0/22.

2. Communication with the public Apple Push Notification Service (gateway.push.apple.com) on TCP port 5223. IP address range is 17.*.*.* (17.0.0.0/8)

3. Communication with public Apple OCSP and iTunes (IP address ranges are hosted by Akamai and vary)

   a. *.apple.com TCP port 80, 443
   b. phobos.apple.com TCP port 80, 443
   c. ocsp.apple.com TCP port 80, 443
   d. ax.itunes.apple.com TCP port 80, 443
   e. ax.init.itunes.apple.com TCP port 80, 443
   f. *.mzstatic.com TCP port 80,443

   Optional:

   d. mesu.apple.com.

   The iOS checks for new versions of the OS by polling this server.

   Clients can block this URL on their firewall to block the iOS update pop-up. Clients can unblock when prepared to update to a newer iOS.

4. Communication between the mPOS devices and KWI use the following URL's and port number.
   kwigbsrv.kligerweiss.net, kwigbsrv2.kligerweiss.net, kwigbsrv3.kligerwiess.net.
   65.206.45.41, 65.51.69.83, 65.51.37.205, 66.35.45.149, port 90 TCP.

5. mPOS peripherals and services
   a. mPOS payment server – mPOS stores with an AJB payment server communicate with the mPOS devices through internal ports 24900 TCP & 24910 TCP.
      The AJB payment server can reside on Register-1 or on a dedicated laptop/desktop.
      mPOS stores that use ONLY Verifone sleds DO NOT need to open ports 24900 & 24910 TCP.

   b. mPOS Cash Drawers (Wired Ethernet) - use internal port 30998 TCP/UDP.
   c. mPOS Epson Receipt Printers (Wireless & Wired Ethernet)
      For mPOS versions 4.2.16 and lower, use internal port 9100 TCP/UDP.
      For mPOS versions 4.218 and higher, use internal ports 9100 TCP/UDP & 3289 TCP/UDP.

6. KWI remote support services for stores using mPOS require reservations on the store router. Refer to section "Network Requirements for Internet, POS & mPOS" sections 2.1, 7, 7a, 7b.
   mPOS stores that use a dedicated AJB payment server or a Register-1 require access through remote access reservations.
   mPOS stores that use ONLY Verifone sleds do not need to apply remote access reservations.

WAN Recommendations for mPOS-Only Stores

For WAN (Wide Area Network) redundancy in an mPOS-Only store, KWI recommends a backup Internet connection. A 4G Cellular Internet service can serve as an adequate backup Internet connection. KWI recommends that the Primary WAN Internet Service Provider be different from the Secondary WAN Internet Service Provider.

Traffic Management Recommendations for Stores with mPOS

To improve bandwidth quality, KWI recommends the use of Traffic Shaping. Traffic Shaping will optimize performance and increase available bandwidth. KWI highly recommends that dedicated bandwidth be allocated to the mPOS system (mPOS Handheld, Receipt Printer, Cash Drawer, mPOS Payment Server). It is recommended that the bandwidth allocated to the mPOS system not be shared with other network devices in the store such as the security system, cameras or any devices that have streaming video & audio.

Enterprise Class Cloud Platform

mPOS

Network Requirements and Recommendations

The store network for mPOS must comply with the below requirements and recommendations.

1. Wireless Frequency Requirements

   The 2.4 GHz frequency is compatible with all wireless KWI mPOS devices and peripherals.

   Option-1 If the store has a mixed environment of wireless devices where some mPOS devices and peripherals support 2.4 GHz frequency ONLY and other devices support both 2.4 and 5 GHz, enable Simultaneous Dual-Band on your wireless access point. Simultaneous Dual-Band allows devices on the 2.4 GHz and 5 GHz frequencies to connect to the access point simultaneously. If the store enables the 5 GHz frequency in a mixed environment, it is a requirement that the access point support Simultaneous Dual-Band.

   Option-2 For optimal performance and if all mPOS devices and peripherals (mPOS Handheld, Receipt Printer, Cash Drawer) in the store support 5GHz wireless frequency. Connect all the mPOS devices and peripherals to the 5 GHz frequency. Less interference is expected on 5 GHz frequency.

   Note: To re-configure the wireless receipt printer frequency (2.4 & 5 GHz), contact KWI.

2. Wireless Network Protocol Requirements

   The 2.4 GHz frequency with 802.11b protocol is compatible with all wireless KWI mPOS devices/peripherals.

   Option-1 If the store has a mixed environment of wireless devices with preferred network protocols, you can apply the below to support all wireless devices.

   If the access point utilizes 2.4 GHz frequency, enable 802.11 b/g/n protocols.

   If the access point utilizes 5 GHz frequency, enable 802.11 a/n protocols.

   If the access point has Simultaneous Dual-Band enabled to support both frequencies, apply all of the above.

   Option-2 If all wireless devices in the store support 802.11a or 802.11b you can apply the below configurations for optimal performance. Limiting the number of protocols on a frequency will reduce the number of channels the radio has to scan.

   If the access point utilizes 5GHz frequency and ALL wireless devices support protocol 802.11a, configure 5GHz for 802.11 a-only.

   If the access point utilizes 2.4GHz frequency and ALL wireless devices support protocol 802.11b, configure 2.4GHz for 802.11 b-only.

   If the access point has Simultaneous Dual-Band enabled to support both frequencies, apply all of the above.

3. Wireless Channel Bandwidth
   Requirements
   a. In order to support and maintain a consistent connection to all devices, it is a requirement that the below Channel Bandwidths be enabled.
      If the access point has 2.4 GHz frequency enabled, enable 20 MHz Only.
      If the access point has 5 GHz frequency enabled, enable 20 MHz Only.

4. Wireless Channels
   Recommendations
   a. The wireless access point channels will vary based on the store environment. It is recommended that the wireless access point be set to the channel or parameter with the least interference. Scanning for channel interference within the store is highly recommended.

5. Wireless Security Mode
   Recommendations
   a. The stores wireless security mode works best with WPA2-PSK (AES).
   b. WEP is not a secure mode.

6. Wireless Key
   Recommendations
   a. The Passphrase should be a minimum of 8 characters. Use non-dictionary based words. Include letters (at least one uppercase letter) and numbers.

7. Wireless SSID (Service Set Identifier)
   Recommendations
   a. Change the default SSID. Routers out-of-box are pre-configured with a default SSID.
   b. SSID Broadcast should remain enabled.

8. Wireless Access Point Positioning
   Requirement
   a. The wireless access point should be mounted and positioned properly to provide optimal WiFi coverage throughout the store. Conduct a site survey after the wireless access point is installed to ensure consistent signal strength throughout the store and minimal to no WiFi dead spots. The mPOS device and peripherals should be positioned near the wireless access point.

9. DHCP (Dynamic Host Configuration Protocol)
   Requirements
   a. mPOS Handheld devices require a static IP.
   b. Peripherals such as the Cash Drawer and Receipt Printer require a static IP.
   Recommendations
   c. If the DHCP server is enabled on the router, it is recommended that the DHCP IP address range be as small as possible for increased security.

10. MAC Address Filtering
    Recommendations
    a. MAC Address Filtering should remain disabled.

11. Router Management
    Recommendations
    a. Remote Management should remain disabled.
    b. Enable “HTTPS” for management access of the Router.
    c. Keep your router firmware up to date. The firmware is provided by the device vendor.
    d. Change the default management password of the router. Use non-dictionary based words. Include letters & numbers.
    e. It is recommended to not use the default IP scheme that is commonly pre-configured on the router.

12. mPOS Handheld Device Network Settings
    Requirements
    a. A static IP is required for proper functionality.
    Recommendations
    b. Turn-off WiFi “Auto-Join”.

Client Review and Sign Off

We acknowledge that we have reviewed the above documentation and agree to meet the requirements and specifications as outlined.

Name (Print)

Signature

Date

Change History

Version	Date	Item	Change
1.68	11-07-2014	mPOS Outbound and Inbound..	5. All mPOS… 24900 & 24910.
1.69	02-04-2015	Network Requirements..	Network Requirements… 4. The below URL's.. 6. For Internet credit card… ------- mPOS Outbound and..
		MPOS Outbound and ..	3. Communication with public Apple.. TCP Port 80, 443 5. All mPOS systems.. mPOS-Only stores 6. KWI remote support.. Recommendations mPOS-Only stores
1.70	05/29/2015	5. mPOS peripherals and services	ports 9100 TCP/UDP & 3289 TCP/UDP.
1.71	07/20/2015	mPOS Recommended Configuration of Network Security	mPOS_Network Requirements and Recommendations Added Additional requirements and recommendations.
1.72	12/29/2015	Network Requirements for Internet POS & mPOS	"2. Inbound PC Anywhere for KWI help desk support." IP removed 65.51.37.192/28. ------ "10. POS health monitoring software.." This section on health monitoring has been removed.
1.72	12/29/2015	mPOS Outbound and Inbound Communications	"1. Communication with *.airwatchportals.com.." IP's of the URL's added to this document. ------ "3. Communication with public Apple OCSP.." Added optional address to this section. -------- "Traffic Management Recommendations.." Added a section on Traffic Management.
1.72	12/29/2015	Network Requirements and Recommendations.	"1. Wireless Frequency. 2. Wireless Network Protocol." These sections have been updated with requirements.
1.73	03-01-2016	MS Update Communication For POS	1. MS Update Addresses – POS 15
