pitney bowes

Shipping & Mailing
Stamp Duty Meters

B700® Version 2.0

Connectivity Guide

Connectivity Guide
SV63189-in Rev. A
Indian Stamp Duty Edition
16 July 2020

Introduction

The B700 Version 2.0 Stamp Duty Franking machine from Pitney Bowes uses a LAN or Wi-Fi connection to synchronize machine performance data and compliance related data and downloading of funds. If you have extensive network security restrictions at your site, you may need assistance from your IT or network specialist. In this case, refer to the *Advanced Network Requirements* section of this document for more information.

Basic Installation Requirements

In most cases, you connect your machine as described in the installation instructions included in the box. If you use the direct LAN connection, you just plug the network cable into the back of the machine. If you use Wi-Fi, a wizard will take you through the procedure for setting up the Wi-Fi connection.

Advanced Network Requirements

B700 Version 2.0 initiates all communication (via HTTP or TLS), so it can safely sit behind most corporate firewalls

- High-speed network connection.
- B700 Version 2.0 supports 802.11n WiFi WPA, WPA-2 PSK, WPA-802.1x (LEAP) protocols.
- Due to security issues, WEP Wireless Security Protocol is not supported.
- Both 2.4 and 5 GHz frequency band wireless is supported.
- B700 Version 2.0 communicates to external web services via HTTP over Port 80.
- B700 Version 2.0 communicates to PB secure server(s) via TLS over port 443.
- B700 Version 2.0 uses Port 53 for DNS lookup.
- Pitney Bowes requires a minimum network bandwidth of 384 kbps (upstream and downstream) to operate, but we recommend 1 Mbit/sec for best performance.
- Pitney Bowes recommends that DSL or cellular devices are not shared across multiple B700 Version 2.0 systems.
- Customer owned web filtering devices or software, as well as SSL packet inspection should be disabled for these ports as they can affect performance or could prevent functionality.
- B700 Version 2.0 internal base and tablet communication uses a subnet that consists of IPs from the 192.168.10.240 to 192.168.10.255 and 192.168.10.96 to 192.168.10.111 ranges. When the B700 Version 2.0 is connected to a network that has a default gateway which uses any address in these ranges, the B700 Version 2.0 will not be able to communicate on the network because messages can not be routed properly.
- Wireless Routers that support IPv6 are supported if IPv6 has been properly configured. Recently, ISPs are remotely activating IPv6 as a feature, but are not yet fully supporting the protocol. This can cause the display to repeatedly reboot once the Wi-Fi connection is established. Please ensure your network is not configured this way.

Ports and Communication Requirements

The B700 Version 2.0 connection uses these ports and protocols. The system will require access through your network and firewall.

Communications

- All communication is initiated from the system via ports 80 (HTTP) and 443 (TLS)
- All communications from the system to the back end system are in the form of XML messages.

Ports

Port 80 (HTTP)

- Web Services.
- TeamViewer (remote access software).

Port 443 (TLS)

- B700 Version 2.0 sends requests to refill or audit its PSD (Postal Security Device) when the user requests it or an inspection is required. Audits occur if the PSD inspection date has expired.
- On PSD replacement the system will automatically request the configuration data for the replacement PSD.
- Transaction records from the B700 Version 2.0 are automatically uploaded when a user message appears (within three days of the mail being generated).
- O/S updates and PB Application Software and Rates Data updates.

Port 53

- DNS lookup.

IMPORTANT:

IT departments that use a "rules based" method for allowing specific ports to pass traffic on their network for port 53, allow for both UDP and TCP traffic to this port.

URL Information

These URLs must be accessible from the device, without any obstructions. This includes being free of any SSL packet inspection, web filtering devices or software monitoring.

Required URLs

- **Distributor** - main PB Server that authenticates machine for access to other PB web services
  - *http://distservp1.pb.com/csd/dstproduct* (Port 80)
  - *https://distservp1.pb.com/csd/dstproduct* (Port 443)
- **Funds (Funds Management & Refills)** - funds are managed through a separate Funds Server
  - *https://incometp4.pb.com/csd/t3cometserver_35.aspx* (Port 443)
  - *https://aucometdr4.pb.com/t3cometserver_14.asp* (Port 443)
- **Rates and Updates (Download Services)** - Downloads new software
  - *Main Download Services entry*
    - *https://dlsdlp1.pb.com* (Port 443)
    - *https://dlsdlp1b.pb.com* (Port 443)
  - *File Processing*
    - *https://pbdlsp1.pb.com* (Port 443)
    - *https://pbdlsp1t.pb.com* (Port 443)
    - *https://pbdlsp1k.pb.com* (Port 443)
    - *https://pbdlsp1b.pb.com* (Port 443)
    - *https://pbdlsp1z.pb.com* (Port 443)
  - *OS Updates*
    - *https://pb-ota.redbend.com* (Port 443)
- **Health Data Update** - machine health Information upload
  - *https://s3.amazonaws.com* (Port 443)
- **Network Connectivity Test Site** - used by tablet's Android O/S to confirm connectivity
  - *http://connectivitycheck.gstatic.com/generate_204* (Port 80)
  - **Note**: Connectivity tests also use Google DNS explicitly (8.8.8.8 Port 53)
- **PB Web Services Support** - used by several PB applications
  - *https://api.pitneybowes.com* (Port 443)
  - *https://pitneybowes.okta.com* (Port 443)
  - *http://microsoft.com/SoftwareDistribution/Server/SimpleAuthWebService* (Port 80)
  - *http://mail.o365.pb.com* (Port 80)
  - *https://cdn.sendprocare.pitneycloud.com/* (Port 443)
  - *https://play.vidyard.com/* (Port 443)
  - *https://www.youtube.com/* (Port 443)
  - *https://s3-us-west-2.amazonaws.com/* (Port 443)

Recommended URLs

We recommend these URLs are left open, but if this presents a security issue, they can remain blocked. They are enabled by default.

Remote Access

TeamViewer is an application that lets Pitney Bowes Service access your device remotely, when you authorise it. *(A TeamViewer session can only be initiated by someone on your end, therefore the system cannot be accessed without your knowledge.)* There are two ways to unblock TeamViewer:

- General unblocking of Port 5938 TCP for outgoing connections (recommended). *Port 5938 is only used by a few applications and therefore there is no security risk. This traffic should be filtered or cached.*
- Unblocking URLs of the following formats (to any server) GET:
  - /din.aspx?s=…&client=DynGate…GET
  - /dout.aspx?s=…&client=DynGate…POST
  - /dout.aspx?s=…&client=DynGate…

Note:

Regardless of which method you choose to unblock TeamViewer, verify there are no content filters or anything similar blocking one of these URLs:

- *.TeamViewer.com
- *.dyngate.com

- **Device Management**(uses Port 443 or 80 unless otherwise stated).
  - *https://smb.pitneybowes.com*
  - *https://prov.mdm.pitneybowes.com*
  - *https://api.mdm.pitneybowes.com*
  - *https://cn977.awmdm.com*
  - *https://ds977.awmdm.com*
  - *https://play.google.com*
  - *https://gate.hockeyapp.net*
  - *https://e.crashlytics.com*
  - *https://android.googleapis.com*
  - *http://mobile-gtalk.l.google.com* (Port 5228)
  - *https://csd-indiataxmeter-transaction.s3.ap-south-1.amazonaws.com*
  - *a21iywh40b72eh-ats.iot.us-west-2.amazonaws.com*
  - *alt2-mtalk.google.com*
  - *alt5-mtalk.google.com*
  - *alt6-mtalk.google.com*
  - *alt8-mtalk.google.com*
  - *android.clients.google.com*

- *android-safebrowsing.google.com*
- *api.crashlytics.com*
- *apis.google.com*
- *app-measurement.com*
- *aws.amazon.com*
- *captive.apple.com*
- *cloudconfig.googleapis.com*
- *cognito-identity.us-east-1.amazonaws.com*
- *content.googleapis.com*
- *csd-error-logs.s3.amazonaws.com*
- *csd-error-logs.s3-us-west-1.amazonaws.com*
- *csd-launcher.s3.amazonaws.com*
- *csd-launcher.s3-us-west-1.amazonaws.com*
- *csd-mailing.s3.amazonaws.com*
- *csd-mailing.s3-us-west-1.amazonaws.com*
- *csd-remote-config.s3.amazonaws.com*
- *csd-remote-config.s3-us-west-1.amazonaws.com*
- *csd-translations.s3.amazonaws.com*
- *csd-translations.s3-us-west-1.amazonaws.com*
- *digitalassetlinks.googleapis.com*
- *dl.google.com*
- *docs.google.com*
- *ES-MAD-ANX-R010.teamviewer.com*
- *firebaseinstallations.googleapis.com*
- *fonts.googleapis.com*
- *fonts.gstatic.com*
- *GB-LON-ANX-R008.teamviewer.com*
- *hshh.org*
- *in.appcenter.ms*
- *lh3.googleusercontent.com*
- *master3.teamviewer.com*
- *mdh-pa.googleapis.com*
- *mtalk.google.com*
- *pagead2.googlesyndication.com*
- *phonedeviceverification-pa.googleapis.com*
- *ping3.teamviewer.com*
- *play.googleapis.com*
- *pool.ntp.org*
- *r1---sn-8pgbpohxqp5-auol.gvt1.com*
- *r2---sn-8pgbpohxqp5-auol.gvt1.com*
- *r3---sn-8pgbpohxqp5-auol.gvt1.com*
- *r3---sn-8pgbpohxqp5-auos.gvt1.com*
- *r6---sn-8pgbpohxqp5-auol.gvt1.com*

- *r7---sn-8pgbpohxqp5-auol.gvt1.com*
- *r8---sn-8pgbpohxqp5-auol.gvt1.com*
- *redirector.gvt1.com*
- *registrar.iot.pitneycloud.com*
- *reports.crashlytics.com*
- *safebrowsing.googleapis.com*
- *settings.crashlytics.com*
- *ssl.gstatic.com*
- *time.apple.com*
- *www.google.com*
- *www.googleapis.com*
- *www.gstatic.com*
- *www.pitneybowes.com*

Proxy

The B700 Version 2.0 supports a proxy feature to tunnel network traffic to a Proxy Server's IP address and port using HTTP CONNECT Tunneling method.

Overview

When using proxy on your B700 Version 2.0 it will send network traffic to the proxy over the specified port. The Proxy Server will then establish a TCP connection to the specified destination on behalf of the B700 Version 2.0 using the protocol and port requested by the B700 Version 2.0. When the connection is made, the Proxy Server responds to the original HTTP request with an HTTP response to the B700 Version 2.0 allowing it to send the data to the destination.

To setup the proxy complete the following:

1. Tap **Settings** (gear icon).
2. Tap the network option in use; either **Wired (Ethernet)** or **Wi-Fi.**
3. In the Proxy Setting drop-down select **Manual**.
4. For Proxy Hostname enter the IP address of your proxy server.
5. For Proxy Port, enter the port the B700 Version 2.0 should use to send network traffic to the Proxy Server.
6. If your Proxy Server requires authentication, select the box and additional fields will be displayed.
    a. Enter the Proxy Username.

        Note: This may be case sensitive for some proxy servers.

    b. Enter the Proxy Password Note:

        Note: This is case sensitive for proxy servers.

What is not supported:

The proxy does not support allowing exceptions or exclusions. All communication must tunnel through the proxy when enabled. Also, Socket Secure (SOCKS) protocol is not supported.

FAQs

Question	Answer
What OS does this device run?	Android 7.0
How are updates to the Android Operating System performed?	PB uses a 3rd party Over The Air (OTA) tool that securely downloads updates to registered machines.
Why are both ports 80 and 443 in use? Please detail what information is being sent over port 80 and if it is required	ALL critical funds related or core services only use port 443. Some of the non-critical services use port 80 (examples: online read-only Help System content, or non-PB sites for tracking services site)
What controls are in place to protect this device against network-based malware threats?	Controls include: • White list of URLs • TLS • Only executes services needed to perform activities • OS distribution has been optimized and locked down
What information is being sent and presumably stored at Pitney Bowes?	PB collects usage data that is required for state government reporting. This includes items such as use of services and date of impressions etc. No Personal Identifiable Information (PII) is collected or used. We also collect machine health information such as Software version numbers, errors reported etc.
If information is being stored, how is it being stored? Please describe the protections in place.	Usage information is stored in a special application and database, which is reviewed by the state government prior to our Meter Approval. Machine Health information is stored in Amazon Web Services, but is uploaded through a TLS connection and authenticated using machine resident credentials. Again, no PII information is collected or stored there.
Does it have a firewall?	No
Who controls the firewall rules?	Not applicable
How are the firewall rules configured?	Allow only the ports Http, TLS and DNS
What is the security patch process?	B700 Version 2.0 security patches are applied by emergency updates via PB only, and on a regular schedule through PB services.
What is the software update process, and how often does this occur?	As required with periodic feature additions and bug fixes

Question	Answer
• What is the network traffic flow to and from the B700 Version 2.0 systems? • What firewall rules need to be in place to allow the necessary communication?	• Outgoing contact initiated (no push) utilizing TLS, URLs provided by PB services • Outgoing - transactional data • Incoming is both transactional data and files and Web Services
Can you identify suspicious activity affecting B700 Version 2.0 machines?	Yes. An audit process exists to validate the financial integrity of the system. Error logs are available and can be uploaded to the PB data centre.
What are the access controls in place to secure B700 Version 2.0 machines?	The application access is managed by the customer using an access code. The system operates in a Kiosk mode where access to the underlying Android operating system is prevented.
Are there audit trails in place?	Yes. PSD transactional audits, extensive logs and all financial transactions are audited by the PB infrastructure. The B700 Version 2.0 logs all error conditions, and maintains ink usage logs, print usage logs, etc.
Is data stored on the device?	Yes. The B700 Version 2.0 stores transactional data, customer profiles and settings etc.). Transactional usage data is uploaded and then deleted when confirmed upon receipt by PB Infrastructure over TLS channel.
What controls protect the data?	All files and data interface utilizing TLS. Incoming data and files are signed and verified prior to use. If consumed by the printer, it is verified on each use. If used by the application, it is verified on load.
Do the B700 Version 2.0 machines allow remote administration?	Pitney Bowes will use TeamViewer to troubleshoot system problems remotely. The end user will initiate the session using a special session code which is generated by the TeamViewer application and changes each session.
Is TeamViewer required?	No, it is not required, but it is recommended. It is configured to **not run until the end user activates it with a special one-time session code**. The session code changes for each system and each activation. The special session code is provided by the call centre to the end user, once they have called the centre and provided specific information that also changes for the session.