

Networking Technical Specification

Connect+ Series

Introduction	1
Network Requirements.....	1
Port/Communication Requirements	1
Port 80 (HTTP).....	1
Port 443 (HTTPS)	1
Port 53	2
URLs	2
Download Services	2
Accounting	2
More than a Mailing Machine.....	2
FAQs	3

Introduction

This document details the networking technical considerations for the Connect+ Series.

Network Requirements

- The Connect+ System will require a high-speed network connection.
- The Connect+ System will initiate all communication.
- The Connect+ System will initiate all communication (via HTTP or HTTPS), so it can safely sit behind most corporate firewalls.
- The Connect+ System will communicate to external Web Services via HTTP over Port 80.
- The Connect+ System will communicate to PB secure server(s) via HTTPS over port 443.
- The Connect+ System will use Port 53 for DNS lookup.

Port/Communication Requirements

All communication is initiated from the Connect+ System via ports 80 (HTTP) and 443 (HTTPS). All communication from the Connect+ System to the back end system is in the form of XML messages.

Port 80 (HTTP)

- OS Update
- AV Updates
- Web Browsing (Help)

Port 443 (HTTPS)

- Connect+ will send requests to refill or audit its PSD (Postal Security Device) based on a low funds or inspection date. (Refills currently occur when the PSD funds drop below \$xxx.xx. Audits occur if the PSD inspection date has expired.)
- During initial install, the system will automatically request an Operational Block, from the infrastructure, for the PSD.
- On PSD replacement the System will automatically request the configuration data for the replacement PSD.

This document is a publication of Pitney Bowes. The use of this information by the recipient or others for purposes other than the repair, adjustment or operation of Pitney Bowes equipment may constitute an infringement of patent and/or other intellectual property rights of Pitney Bowes or others. Pitney Bowes assumes no responsibility for any such use of the information. Except as provided in writing, duly signed by an officer of Pitney Bowes, no license, either express or implied, under any Pitney Bowes or any third party's patent, copyright, or other intellectual property rights is granted by providing this information.

- Transaction Records from the Connect+ System are automatically uploaded when:
- The System has been idle for a period of 10 minutes
- While powering down the system.
- Web Accounting Services.
- On power up the System freshens the Web Service (Supplies, My Account, Tracking etc.) configuration data.
- Software, Rates and Graphic updates.

Port 53

DNS lookup

URLs

The following URL's must be accessible from the Connect+ system, without any obstructions.

- Connect+ Help: <http://www.pitneyworks.com/ms1/>
(Domain www.pitneyworks.com; IP=199.231.44.16)
- Distributor:
 - <http://distservp1.pb.com/dstproduct.asp>
 - <https://distservp1.pb.com/dstproduct.asp>
(Domain distservp1.pb.com; IP=152.144.128.244)
- Comet Server:
 - http://cometservp1.pb.com/T3cometserver_03.asp
 - https://cometservp1.pb.com/T3cometserver_03.asp
(Domain cometservp1.pb.com; IP=199.231.44.36)

Download Services

- Misc. Data Upload:
<https://pbgdspp1.pb.com/MS1ConfigurationUpload/MS1ProductConfigurationUpload.svc>
(Domain pbgdspp1.pb.com; IP=199.231.44.222)
- ClamAV: <http://clamserver.pb.com>
(Domain clamserver.pb.com; IP=199.231.45.165)
- Error Log uploads: <https://pbdlsp1.pb.com/UploadService/service.svc>
(Domain pbdlsp1.pb.com; IP=199.231.44.30)
- Configuration web page: <https://MyMS1Configuration.pb.com>
(Domain MyMS1Configuration.pb.com; IP=152.144.128.48)
- OS updates: <http://SMT.pb.com>
(Domain SMT.pb.com; IP=199.231.44.54)
- File Updates: <https://pbgdspp1.pb.com/MS1/DlaService.svc>
(Domain pbgdspp1.pb.com; IP=199.231.44.222)
- Orders (CCD): <https://pbgdspp1.pb.com/MS1CCD/DlaCCDService.svc>
(Domain pbgdspp1.pb.com; IP=199.231.44.222)

Accounting

- Accounting Web Application: <https://ms1app.pb.com/>
(Domain ms1app.pb.com; IP=199.231.44.149)
- Accounting Web Services: <https://ms1app.pb.com/services/>
(Domain ms1app.pb.com; IP=199.231.44.149)

More than a Mailing Machine

- Verify Address (Address cleansing):
<https://creativemailings2.pb.com/usertx.web/asp/AddressVerification.aspx>
(Domain creativemailings2.pb.com; IP=199.231.44.50)
- My Account at PB.com:
<https://www.pb.com/cgi-bin/pb.dll/jsp/Login.do?lang=en&country=US&ga1=MS1>
(Domain www.pb.com; IP=199.231.44.12)
- Discounts & Presort Services: <http://us.stage.pb.com/mstest/mailing-services/>
- Buy Supplies:
<http://pbstage.ct.pb.com/cgi-bin/pbstage.dll/jsp/supplies/SuppliesListShowHtml/-23085.html>
(Domain pbstage.ct.pb.com; IP=152.144.132.65)
- Track a Package (Web tracking – Boxo Generic package tracking service): <http://pb.boxoh.com/>
(Domain pb.boxoh.com; IP=72.47.250.186)
- Postal Tools: <http://us.stage.pb.com/mstest/postal-tools/>
(Domain us.stage.pb.com; IP=152.144.132.65)

FAQs

1. What OS does this device run?
 - SUSE Linux Sled 11
2. What controls are in place to protect this device against network-based malware (viruses/worms) threats?
 - White list of URL's
 - HTTPS
 - Anti Virus Software
 - Only executes services needed to perform activities
 - OS distribution has been optimized and locked down
3. Does it have a firewall?
 - Yes
 - a. Who controls the firewall rules?
 - Pre-configured and not modifiable
 - b. How are the firewall rules configured?
 - Allow only the ports Http, Https and DNS
4. Describe the security patch process.
 - Emergency updates via PB only
 - Regular schedule through PB services
5. Describe the anti-virus controls in place.
 - ClamAv installed on every system, AV signature updates regularly updated
6. Describe the software update process.
 - a. How often does this occur?
 - As required, in some cases monthly
7. Describe the network traffic flow to/from this device.
 - a. What firewall rules need to be in place to allow the necessary communication?
 - Outgoing contact initiated (no push) utilizing HTTPS, URLs provided by PB services
 - Outgoing - transactional data
 - Incoming is both transactional data and files and Web Services
8. Can you identify suspicious activity with respect to this device?
 - a. If so, please describe in detail.
 - An audit process exists to validate the financial integrity of the system
 - Error logs are available and can be uploaded to the PB data center
 - Regularly scheduled physical visits from PB Service
9. What are the access controls in place to secure this device?
 - Unique passwords for each machine - cryptographically strong - restricts access the o/s
 - Application access managed by the customer userid and password available

10. How do you authenticate an individual? A service?

- See 9, above, for individual
- Machine does not provide services over a network so authentication not required

11. Are there audit trails in place?

a. If so, what types of events are audited?

- PSD transactional audits, extensive logs all financial transactions are audited by the PB infrastructure.
- Logs for all error conditions
- Ink usage logs, print usage logs etc.

12. Is data stored on the device?

a. If so, what type of data?

- Transactional data, graphic images, customer profiles and settings, files (rates etc.)

b. Describe the controls in place to protect the data.

- All files and data interface utilizing HTTPS
- 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 is verified on load

13. Does this device allow remote administration?

a. Describe the controls in place to enable remote administration.

- Remote administration not allowed.