SendPro® US – Commerce Cloud, Security and Compliance

January 2018

Thank you for inquiring about the security and compliance for the Pitney Bowes SendPro® online shipping software and its related solutions. This document is formatted as Frequently Asked Questions to help you search topics specific to your interests. Due to the technical nature of this document, information here will be updated regularly and is subject to change. Please inquire with your Pitney Bowes account representative before making significant decisions that rely on this information.

1. **Which browser (version) do I need in order to access SendPro® online shipping solution?**
   - Chrome (Google)
   - Safari (Apple MAC)
   - Firefox (Mozilla)
   - Microsoft IE 11
   - Microsoft Edge

2. **Is there any encryption between the client and the web application?**
   All traffic between the client and web application is encrypted using TLS 1.2.

3. **What is the login security?**
   Username / Password authentication.

4. **Is there any Physical and Environment Security?**
   - Fire detection monitoring? Yes
   - Climate and temperature monitoring? Yes
   - Physical access to the system? Yes
     Please see Addendum for info specific to what AWS offers relative to security.

5. **Where is the location of the database?**
   Northern Virginia, USA

6. **Business Continuity Management?**
   - Availability – What is the calculated uptime? 99.9%
   - How is the backup functionality working? Duplicate, active, hosted clusters ensure seamless and immediate failover if any outages occur.

7. **How are versions implemented?**
   AWS Rolling Updates. Installed on Instance 1 first. When this happens, clients will automatically be routed to active Instance 2. Once upgrade is done on Instance 1, clients will be re-routed back to Instance 1, and Instance 2 is upgraded. No downtime is experienced.

8. **Are security updates installed on a regular basis?**
   Pitney Bowes SendPro online shipping software is deployed in the Amazon AWS Cloud. The Amazon AMI EC2 instances are all 'hardened' versions of RedHat Linux, which is actively monitored and security patched by Amazon.

9. **What happens if a user hasn't been active for the last 30 min?**
   Users will be automatically logged-out for security purposes.

10. **Which port is using for external communication?**
    Port 443

11. **Can SendPro Shipping Application work with a Proxy Server?**
    Yes

12. **What is AWS?**
    Amazon Web Services

13. **How can we be sure that only we have access to our data?**
    Each client receives an enterprise account which is used to logically separate the data. Each client and its users are also given their own username and password with 256-bit salt. A salt is simply added to make a common password uncommon. In password protection, salt is a random string of data used to modify a password hash. Salt is added to make it more difficult for an attacker to break into a system by using password hash-matching strategies, because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system. The underlying database is a MySQL database, which has been hardened.

    Access to the database is restricted to Pitney Bowes' (PBI) Operations staff and Amazon. PBI uses a principle of separation of duties, in which software development staff has no access to production systems or database. The PBI Operations staff managing the production system are all PBI employees. Access to the system is limited to ONLY the team that is dedicated to the SendPro online shipping software. Amazon has no way to see our data. PBI Operations Staff is limited, and requires a special access key even to SSH into the database (SSH is a UNIX-based command interface and protocol for securely getting access to a remote computer).

    All access is logged. All data passing either outside of AWS to the end-customer, or internal with the AWS VPC, is encrypted via TLS.

14. **When we end our SendPro contract with Pitney Bowes, can we get our data?**
    The user can export package data to CSV.

15. **Who will own the data in the database?**
    The data belongs to the client, and will be accessible for as long as they maintain their subscription.

16. **Can I use a standard smartphone with the SendPro online shipping software?**
    No. The application is available through a web browser.

17. **Are system admin rights required to install the hardware – in the case where security has the system locked-down, making hardware installation difficult?**
    Not Applicable

18. **How frequently will you be updating product functionality and am I obliged to utilize the new features (can I stay at an earlier version)**
    SendPro online shipping software is a SaaS application and, therefore, will be updated frequently. Depending on your subscription, you may or may not see new features. Some of these features may not be user facing, and considered as performance updates. No users can remain on older versions of the application.

19. **How secure is our online environment / how safe is my information?**
    The application is hosted by Amazon Web Services, and is consistently backed up and monitored against virus intrusions and external access. Client information can be considered as safe (if not safer) compared to hosting the application on their own dedicated servers. AWS are certified ISO27001, providing both excellent physical and digital security.
    AWS provides highly secure data centers which use state of the art electronic and multi-factor access control systems including:
    - Highly secure facility with 24x7 guard protection, closed circuitry, alarmed doors with secure card-key access, biometric scanner, and restricted access to the data floor
    - Building and environmental control alarms which are constantly monitored.

    In addition, PB employee and staff security follows these procedures:
    - Prior to hire, all employees must clear a thorough back ground check and drug screening.
    - All staff members are required to participate in an annual Information Security Training that covers our policies on Acceptable Use, Information Security, and Data Protection.
    - Multi-factor authentication required for all remote user access.
    - There is a separation of duties or other compensating controls to prevent development access to the production systems.
    - At termination, all accounts are deactivate for a user and all equipment is collected by manager (inventory of equipment is supplied and must be checked off).

20. **What are the language settings required in the Web Browser to ensure you see the correct local language version?**
    The browsers in those markets should automatically render the application in the appropriate language. If this does not occur, the language can be selected in the settings menu for each browser

21. **How long does Pitney Bowes store the data for the client?**
    Data is stored for a period of 2 years as long as the client maintains an active subscription.

22. **What printers are supported?**
    There are two thermal label printers supported: Brother QL-1050 and Datamax W1110. You can also print to

LaserJet and Inkjet plain paper printers. Application produces shipping labels and other forms in PDF format. These are sent to the browser's built-in PDF reader.

23. **What scales are supported for weight retrieval?**

The SendPro online shipping software supports the use of PBI provided XJ Scales (5 LB, 10 LB, 30 LB, 70 LB). It is optional to use a scale. If a scale is used the client is required to download and install a small application so that the browser can retrieve the weight from the scale.

24. What personally identifiable data does SendPro store?

Client Name, Street Address, Email Address, Telephone Number – information required for a shipping label. Payment method (including credit card if required) is processed by PB.com's billing system.

ADDENDUM

AWS Security and Compliance

Excerpts below taken from Overview of Amazon Web Services, Sajee Mathew, November 2014

Security

The AWS cloud infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It provides an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

With the AWS cloud, not only are infrastructure headaches removed, but so are many of the security issues that come with them. AWS's world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation.

Compliance

AWS Compliance enables our customers to understand the robust controls in place at AWS to maintain security and data protection. As you build systems on top of the AWS cloud infrastructure, the compliance responsibilities will be shared: AWS Compliance provides assurance related to the underlying infrastructure, and your organization owns the compliance initiatives related to anything placed on the AWS infrastructure. The information provided by AWS Compliance helps you to understand our compliance posture and to assess your organization's compliance with your industry and/or government requirements.

The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 27001
- ISO 9001
- ITAR
- FIPS 140-2

Location of Data contained in AWS

Important information for European clients on European Data Security

Resources:

- **Overview of Amazon Web Services, Sajee Mathew, November 2014- https://d0.awsstatic.com/whitepapers/aws-overview.pdf.**
- **Whitepaper - Security AWS, June 2016 - https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf.**
- **General AWS Solutions overview - https://aws.amazon.com/solutions/?nc2=h_ql_ny_livestream_blu**

Amazon Web Services serves hundreds of thousands of customers in more than 190 countries. They are steadily expanding their global infrastructure to help customers achieve lower latency and higher throughput, and to ensure that data resides *only* in the regions specified by the application's solution provider.

AWS is available in multiple locations worldwide. These locations are composed of regions and Availability Zones. A region is a named set of AWS resources in the same separate geographic area. Each region has multiple, isolated locations known as Availability Zones. AWS enables the placement of resources, such as instances, and data in multiple locations. Resources *aren't* replicated across regions unless you chose to do so.

Each region is *completely independent* and is designed to be *completely isolated* from the other regions. This achieves the greatest possible fault tolerance and stability. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links.

Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure.

Availability Zones are all redundantly connected to multiple tier-1 transit providers.