SendSuite® Shipping 6.80:

Security Overview

September 2012

Purpose

This document details the permissions required by SendSuite® Shipping version 6.80.

Document Contents

SendSuite Shipping Installation and Upgrade

Directories

SendSuite Shipping requires read and write permission to the following directories:

- ☐ If the default install paths were used:
  - On 32-bit operating system - C:\Program Files\Pitney Bowes\SendSuite Shipping\
  - On 64-bit operating system - C:\Program Files (x86)\Pitney Bowes\SendSuite Shipping\
    The system also requires permission to all of its subdirectories.
    The system installs the Administrative Component and Internet Browser COM+ Components in these directories (DLLs, OCXs, EXEs, TLBs, etc.).
- ☐ If the default install paths were NOT used, the directory can be found in the registry key:
  - 32-bit - HKLM\Software\pbtranscape\Conquest\Version 1.0\ConquestInstallPath
  - 64-bit - HKLM\Software\Wow64 32 Node\pbtranscape\Conquest\Version 1.0\ ConquestInstallPath
- ☐ C:\WINDOWS\system\
- ☐ On 32-bit operating system - C:\Windows\System32
- ☐ On 64-bit operating system - C:\Windows\SysWOW64

  The system installs runtime VB and VC DLLs in this directory.
- ☐ If the default install paths were used:
  - C:\inetpub\wwwroot\eQuest
    The system installs the ASP files needed for the Web browser in this directory
  - C:\inetpub\wwwroot\eTMSStatus
    The system installs the ASP files for shipment planning in this directory.
- ☐ If the default install paths were NOT used, the directory can be found in the registry key:
  - 32-bit - HKLM\Software\pbtranscape\Equest\EquestWebPath
  - 64-bit - HKLM\Software\Wow64 32 Node\pbtranscape\Equest\EquestWebPath

Registry

SendSuite Shipping requires read and write permission to the following registry hives:

- ☐ HKEY_USERS\DEFAULT\Software\UPS\UPSL32
- ☐ HKEY_CURRENT_USER\Software\PBTranscape
- ☐ On 32-bit operating system:
  - HKEY_LOCAL_MACHINE\SOFTWARE\PitneyBowes\
  - HKEY_LOCAL_MACHINE\SOFTWARE\PBTranScape\eQuest
  - HKEY_LOCAL_MACHINE\SOFTWARE\PBTranScape\Conquest\Version 1.0
- ☐ On 64-bit operating system:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PitneyBowes\
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PBTranScape\eQuest
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PBTranScape\Conquest\Version 1.0

SendSuite Shipping Processing

Directories

The execution of the program requires read and write permission to the following directories:

- ☐ On Windows XP and 2003 (all sub-folders in these directorires must have read/write access):
  - ■ C:\Document and Settings\All Users\Pitney Bowes\SendSuite Shipping\
  - ■ C:\Documents and Settings\<login name.computer name>\Local Settings\Temp\
- ☐ On Windows 7 and 2008 (all sub-folders in these directorires must have read/write access):
  - ■ C:\Users\Public\Pitney Bowes\SendSuite Shipping\
  - ■ C:\Users\<login name.computer name>\AppData\Local\Temp\
- ☐ C:\Temp\
- ☐ On 32-bit operating system: C:\Program Files\UPS\
- ☐ On 64-bit operating system: C:\Program Files (x86)\UPS\
- ☐ C:\inetpub\wwwroot\eQuest

  The system writes temporary report files in this directory.

SendSuite Shipping Setup Admin for Password Reset Situations

When SendSuite Shipping is installed, there is a "user" that is registered with its components and a password that is associated with this user on the configured identity for the website, com+ components, and so on.

If this password needs to be changed (for example, if the customer's network requires password updates every 90 days), then after the password change the system must be synchronized by the SendSuite Shipping administrator with the same password so that the SendSuite Shipping components will continue to have network access. This password change is accomplished through the SendSuite Shipping Setup Administrator program, which is accessed via the **Start** > **Programs** menu. (The desktop icon for this program was removed because it was confusing for users.)

Installation Notes

IIS Setup

The installation for SendSuite Shipping requires the creation of a user on the IIS server with local administrator rights. This user is also used for the identity of various Windows' services and COM+ objects. This user must be configured in the local security policies to run as a service.

Microsoft® SQL Server

Installation
The installation of the database components of SendSuite Shipping requires using the SA login on the Microsoft SQL database server. Due to the method of installation, extended characters cannot be used in the password during the installation process.

Up to 5 databases are created on the SQL server (see table below). Database chaining needs to be enabled on the SQL server to support the carrier rating engines.

The install process creates two default users in the Master database. These users have strong passwords that can be modified after the installation (Use caution when changing these passwords). Upon installation, these users will be set as database owners and database administrators for the databases in the table below.

Getting Started with SendSuite Shipping

The installation for SendSuite Shipping on Windows Server 2008 R2, Windows Server 2008, or Windows 7 machines requires the following:

1. You must be logged on to a computer as a member of the local administrators group
2. Right-click on an application installation file **setup.exe** and select **Run this program as an administrator**.

Upgrades
During an upgrade, SendSuite Shipping will update the ConquestDB database on your SQL server. Below is the ownership and password information.

NOTE: Upgrades from older versions of SendSuite Shipping will preserve **transcape** as the password for the **ConquestUser** account.

Databases Created By SendSuite Shipping

- ☐ ConquestDB

Users Created in Microsoft SQL Server During SendSuite Shipping Installation Process

ConquestDB Database	
Database owner: **ConquestUser**	Password: **s@ndsu1te**

SQL Security Options

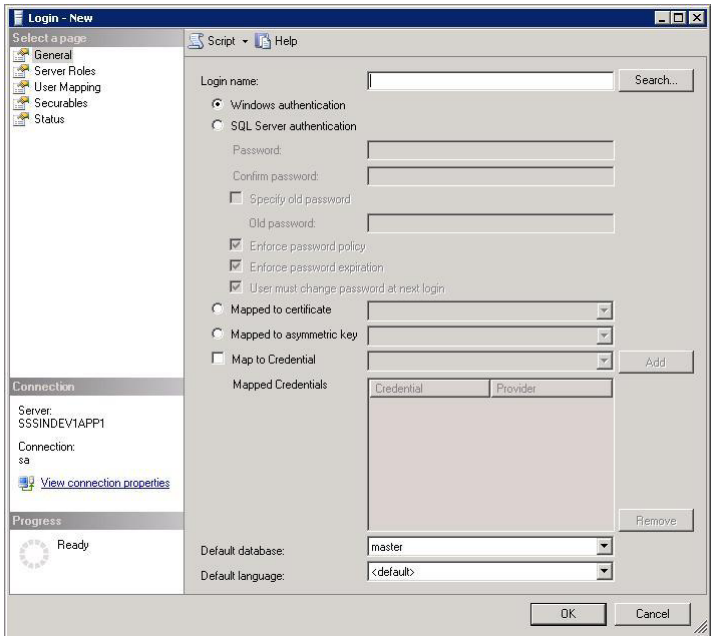
- SQL Server Secure Socket Layer — When enabled, traffic to the SQL server is encrypted using a certificate for added security. You need to first create a certificate on your server before using this option. See the following Microsoft support article for creating the certificate:

  http://support.microsoft.com/kb/316898

- SQL Server Integrated Security — Allows access to the database with a Windows Account rather than SQL logins such as **sa**. Use the following procedure to configure Server Integrated Security.

> **NOTE:** The **sa** user name and password will still be used during the installation.

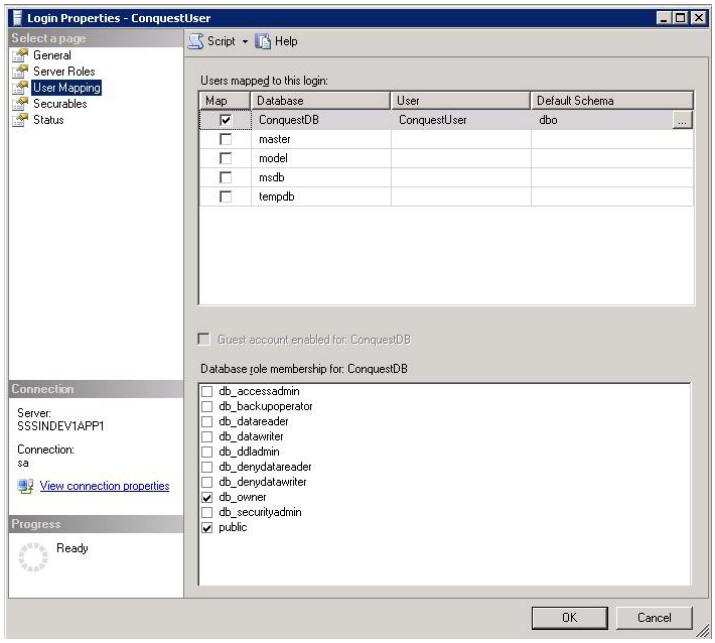
1. Click Start **> Programs > Microsoft SQL Server 2008 > SQL Server Management Studio Express**.
2. Log into to Microsoft SQL Server Management Studio Express.
3. Open the **Security** folder.
4. Right-click **Logins** and select **New Login…**.
5. Type your domain and Windows login name in the **Login name** field.
6. Select **Windows authentication**.
7. Under the left pane, click **User Mapping**.



8. Select **db_owner**.
9. Click **OK**.

NOTE: If you have Server Integrated Security enabled and you get login errors, verify that the user is correctly defined in the SQL database.

NOTE: If you are using a remote Admin client, the Windows user on the remote Admin client must be setup in the SQL database.



Microsoft Internet Explorer

Active X controls and Plug-ins must be enabled in Microsoft Internet Explorer in order to access the scale during processing.

Ports

SendSuite Shipping will access the following ports. Additional ports may be required by carrier communication. See the specific carriers on the pages that follow.

- ☐ TCP and UDP ports 135-139 — These ports are used for Microsoft file and print sharing.
- ☐ Port 445 — This port is used for direct-hosted SMB traffic without network basic input/outputs system (NetBIOS).
- ☐ Port 1433 — Default port used by Microsoft SQL Server. However, this can be changed to any other non-used port.

Web Access

PB Secure Archive
SendSuite Shipping will need to access the following Web addresses through port 80:

- ☐ PBSecure Download Path — http://err.pb.com
- ☐ PB My Account URL — http://www.pb.com/cgi-bin/pb.dll/jsp/Home.do

E-Track
The workstation running the feature or task needs access to the following sites:

- ☐ FedEx — http://www.fedex.com/cgi-bin/tracking — TCP port 80
- ☐ USPS — http://www.usps.com/shipping/epstrac.htm — TCP port 80

HTS Enterprise

HTS Enterprise requires read and write permission to the following directories:

- ☐ C:\Inetpub\wwwroot
- ☐ C:\Inetpub\wwwroot\HTS

SendSuite Shipping Digital Dashboard

The SendSuite Shipping Digital Dashboard requires read and write permission to the following directories on the client (local) machine:

- ☐ On 32-bit operating system: C:\Program Files\pbTranScape\eQuest
- ☐ On 64-bit operating system: C:\Program Files (x86)\pbTranScape\eQuest

  The system also requires permission to all of its subdirectories.

SendSuite Shipping Carrier Installation and Upgrade

- ☐ C:\inetpub\wwwroot\eTMSStatus

  The system installs the ASP files for shipment planning in this directory.

Carrier Supplied Software

In general, the data transmitted over the Internet is not specific or sensitive data for the customer. For example, no credit card information is transmitted. Pitney Bowes does recommend use of firewalls between the web and database servers.

SendSuite Shipping uses stored procedures to open some ports:

- ☐ **FTP** — SendSuite Shipping uses stored procedures to open the FTP ports 20 and 21. The data is transmitted and then the port is shut. The stored procedure will time out and shut the port if a problem occurs.
- ☐ **HTTP** — No high risk data is moving through the session. This data generally consists of package data (weight and dimensions) and recipient data (name, address, phone number).
- ☐ **HTTPS** — Uses port 443 and is a secure port.

Golden State Overnight

Ports

- ☐ The machine must be able to hit the following Web address through port 80: http://wsa.gso.com/gsowebserv/3.0/gsowebserv.asmx

OnTrac

Ports

- ☐ The machine must be able to communicate to 12.38.237.20 through port 80.

Eastern Connection™

When using the Eastern Connection carrier, SendSuite Shipping must be able to hit the following sites:

Web Track URL
https://pod.easternconnection.com/

Tracking URL
http://ecship.easternconnection.com/BOLTrack/68F5068E-8ACE-432A-9BC9-23BB7FAA57A8/PODInfo.xml?BOLNumber=test

Communications URL
ftp://ecftp.easternconnection.com/

DHL®

Directories
The Cyclone® Activator™ requires access to a shared directory on a SendSuite Shipping Server. The name of this directory is determined by the Customer or the Pitney Bowes representative installing the software. Full read and write access must be allowed to this directory.

Ports
SendSuite Shipping, PBDS, and Cyclone Activator will actively communicate with DHL using Internet connections. These communications are transported using both HTTP and HTTPS which means that ports 80 and 443 must be accessible through the Customer's firewall.

URLs that the system may need to reach include the following:

- ☐ The machine running Cyclone Activator must be able to reach **IP Address 216.138.89.46** through port 80.
- ☐ The machine running Cyclone Activator must be able to reach https://b2bgwyadm.dhl.com/idk through port 443.
- ☐ The machine running Cyclone Activator must be able to reach http://b2bgwyadm.dhl.com/servlet/rpcrouter through port 80.
- ☐ The machine running Cyclone Activator must be able to reach http://b2bgwy.dhl.com:80/pb/UNITID through port 80.
- ☐ The machine running the PBDS application must be able to reach http://dhlconnect.dhl-usa.com/dhlconnect through port 80.

SNS

SNS Production URL: http://xmlpi.dhl-usa.com/XMLShippingServlet

SNS Test URL: http://xmlshippingtest.dhl-usa.com/XMLShippingServlet

xmlpi.dhl-usa.com = 165.72.192.229

/xmlshippingtest.dhl-usa.com/ = 165.72.192.240

FedEx® Ship Manager Server (FSMS)

Directories
The FedEx Ship Manager Server software requires read and write permission to the following directories:

- ☐ C:\Program Files\JavaSoft\JRE\1.1
- ☐ C:\FedEx and its sub directories
- ☐ C:\FedEx\FedEx_Reports

Ports
FSMS uses an Internet protocol for external communication. FSMS also uses UNC paths for internal communication. Existing installations can also use an FTP protocol for internal communication.

- ☐ The tunnel gateway server is through port 443.
- ☐ FSMS communicates externally with the following sites:
  - ■ 199.81.196.27
  - ■ 199.81.197.140
  - ■ 199.81.216.140
  - ■ 199.81.217.140
- ☐ FTP setup is used so FSMS can send reports to SendSuite Shipping; no external communication is going out or coming in through FTP connection.
  - ■ FSMS on systems other than the application server require the use of FTP (or a shared path) on the FedEx server, accessible by the application server.

UPS® UPSlinkHTTP

UPS software requires read and write permission to the following directories:

Ports
- ☐ The machine transmitting the manifest must be able to send and receive information through port 443.
- ☐ The machine must be able to hit the following Web address: https://www.upslinkvendor.ups.com.
- ☐ If there is a proxy server on the network, then the proxy server must support SSL tunneling.
  - ■ UPSLinkHTTP establishes a TCP socket connection to Proxy Server.com via port 8080
  - ■ UPSlinkHTTP issues an HTTP CONNECT commands to connect

UPS OnLine Tools

Use the following information when configuring UPS OnLine Tools:

1. Protocol: HTTPS, SSL
2. Port: 443
3. Method: HTTPS POST
4. URLs:

```
LICENSE_URL_TEST = "https://wwwcie.ups.com/ups.app/xml/License"
LICENSE_URL_PRODUCTION = "https://www.ups.com/ups.app/xml/License"
REGISTRATION_URL_TEST = "https://wwwcie.ups.com/ups.app/xml/Register"
REGISTRATION_URL_PRODUCTION = "https://www.ups.com/ups.app/xml/Register"
UPSTEST_TRNST_URL = "https://wwwcie.ups.com/ups.app/xml/TimeInTransit"
UPSPRDC_TRNST_URL = "https://www.ups.com/ups.app/xml/TimeInTransit"
UPS_QUANTUM_VIEW_URL = "https://www.ups.com/ups.app/xml/QVEvents"
```

USPS® Delivery Confirmation™

FTP Information

- ☐ **Upload Path** — USPS ftp server upload Delivery Confirmation (ftp-in.usps.gov)
- ☐ **Download Path** — USPS ftp server download Delivery Confirmation directory (ftp-out.usps.gov)

USPS IOP

Production

The customer should add the following to their firewall exception list:

https://idswebp0-ext.pb.com
https://idswebp1-ext.pb.com
https://idswebp2-ext.pb.com
https://idswebp3-ext.pb.com
https://idswebp4-ext.pb.com
https://idswebp5-ext.pb.com
https://idswebp6-ext.pb.com
https://idswebp7-ext.pb.com
https://idswebp8-ext.pb.com
https://idswebp9-ext.pb.com

Domestic

URL_DOMESTICRATE = https://ibdsravp-partner-nv.pb.com/WebService/RatesAVService.asmx

URL_DOMESTICDISPENSE = https://ibdswebp-partner-nv.pb.com/WebService/Transaction.asmx

URL_DOMESTICRETRY = https://ibdswebp-re-partner-nv.pb.com/WebService/Transaction.asmx

URL_DOMESTICREPRINT = https://ibdswebp-re-partner-nv.pb.com/WebService/Transaction.asmx

International

URL_INTLRATE = https://ibdsravp-partner-nv.pb.com/WebService/GlobalRatesAVService.asmx

URL_INTLDISPENSE = https://ibdswebp-partner-nv.pb.com/WebService/GlobalTransaction.asmx

URL_INTLRETRY = https://ibdswebp-re-partner-nv.pb.com/WebService/GlobalTransactionRe.asmx

URL_INTLREPRINT = https://ibdswebp-re-partner-nv.pb.com/WebService/GlobalTransactionRe.asmx

Tracking

Production: https://ibdstrkp.pb.com/WebService/TrackingAPI.asmx

Test: http://bnbusprt2trk2.pb.com/WebService/TrackingAPI.asmx

Test – Sales and Service

Domestic

TEST_URL_DOM_RATE = https://bnbusPrt2rav.test.pb.com/WebService/RatesAVService.asmx

TEST_URL_DOM_RETRY = https://bnbusPrt2web-re.test.pb.com/WebService/Transaction.asmx

TEST_URL_DOM_DISPENSE = https://bnbusPrt2web.test.pb.com/WebService/Transaction.asmx

TEST_URL_DOM_REPRINT = https://bnbusPrt2web-re.test.pb.com/WebService/Transaction.asmx

International

TEST_URL_INT_RATE = https://bnbusPrt2rav.test.pb.com/WebService/GlobalRatesAVService.asmx

TEST_URL_INT_DISPENSE = https://bnbusPrt2web.test.pb.com/WebService/GlobalTransaction.asmx

TEST_URL_INT_RETRY = https://bnbusPrt2web-re.test.pb.com/WebService/GlobalTransactionRe.asmx

TEST_URL_INT_REPRINT = https://bnbusPrt2web-re.test.pb.com/WebService/GlobalTransactionRe.asmx

Tracking

Production: https://ibdstrkp.pb.com/WebService/TrackingAPI.asmx

Test: http://bnbusprt2trk2.pb.com/WebService/TrackingAPI.asmx

USPS Web Tools

USPS Web-service URL = http://production.shippingapis.com/shippingapi.dll

☎ **Need more help?** Call Pitney Bowes Technical Support at **1-800-692-0003.** ☎

Documents are available on the GMS Customer Service Website at:
http://pb1field.pbi.global.pvt/gms/service/products-mvs/product.asp?id=499&sect=tab2