



Shipping & Mailing
Outbound and Inbound Package Management

SendSuite[®] Tracking

Technical Specifications

Introduction

The SendSuite[®] Tracking Package Tracking and Delivery Management system is a robust and scalable solution for organizations requiring a large-scale computing environment for accountable mail and package tracking. SendSuite[®] Tracking consists of web-enabled programs operating within generic PC-based hardware platforms. In addition, SendSuite[®] Tracking supports special purpose computing equipment, such as portable data collection devices (Tracking Assistants) and barcode printers, to facilitate automation and information processing functions associated with the recording of package movement within an organization.

This document is intended to provide an overview of the technical details and systems requirements necessary for installation.

This document outlines the technical requirements for the most current release of SendSuite[®] Tracking. For previous versions, please refer to the SendSuite[®] Tracking Platform Compatibility Matrix.

Service Collateral
SVTS3183 Rev.AC
August 2025

Document Information

Document Name	SendSuite® Tracking Technical Overview
Document Version	v.AC
Region	United States; Canada; Europe; A-Pac
Document Owner	Michael Beausoleil, Service Designer – Office Shipping
Document Reviewers	Michael Beausoleil; Simon Cook
Document Author	Michael Beausoleil, Service Designer – Office Shipping
Document Audience	Technical Internal & External
Document Creation Date	August 12 th , 2023

Revision History

Seq. #	Date	Description	Version	Author/Modifier
1	08/12/2023	Document re-authored; updated OS & SQL support; updated MSMQ requirement.	Z	Michael Beausoleil
2	01/24/2024	Grammar and spelling corrections.	AA	Michael Beausoleil
3	06/12/2025	Added Mobile Device Management section	AB	Michael Beausoleil
4	08/22/2025	Updates in support of 15.1 release	AC	Michael Beausoleil

Table of Contents

Introduction	1
Document Information	2
Revision History	2
Table of Contents.....	3
Architecture	4
Administrator	4
Client	4
Designer.....	4
SendSuite® Link	4
Dependencies.....	4
Development Languages	4
System Configurations & Requirements.....	5
Deployment Models	5
System Requirements.....	6
Supported Browsers	7
Product Installation Requirements.....	7
Software and Feature Dependencies	7
Supporting Files.....	8
SQL Server Security Requirements	9
SQL Login for Installation and Upgrades	9
SST_User SQL Login.....	9
Default Language	9
Supported Collations.....	10
Communications Requirements.....	10
Licensing Considerations.....	10
Networking & Firewall Requirements	10
Network communication ports.....	10
Firewall Whitelist	10
Android Tracking Assistant Networking Considerations	11
Virtual Machine Considerations	11
Authentication	12
Mobile Device Management.....	13

Architecture

The SendSuite® Tracking solution is comprised of a collection of components:

Administrator

The SendSuite® Tracking Administrator module is a web-based application used by administrators to configure and administer the product.

Client

SendSuite® Tracking Client is the application leveraged by users to process transactions within the product. The life cycle of an item is managed by this application. All reports are acquired through the Client. No business logic resides on the workstation. The Client is based on .NET technology and does not require ActiveX controls.

Designer

SendSuite® Designer is the application used to create and modify screens, email templates, and label templates as well as to write application business logic via the Powerlogic.net tool.

SendSuite® Link

Required for Tracking Assistant integrations, SendSuite® Link provides the following:

- Facilitate data synchronization between SendSuite® Tracking and SendSuite® Mobile on Tracking Assistants.
- Third-party API integration.

Dependencies

Installing SendSuite® Link will also install the following:

- WildFly - A flexible, lightweight, managed application runtime extending REST based data access.
- OpenJDK – Open-source Java platform.
- JDBC Driver – Java Database Connectivity Driver

Development Languages

The following development languages are employed:

- SendSuite® Tracking Software – C# .NET
- SendSuite® Mobile (Android mobile app) – Xamarin

System Configurations & Requirements

SendSuite® Tracking may be installed in a variety of configurations to suit organizational requirements. The actual configuration of workstations, file servers, and database servers can vary depending upon enterprise circumstances. Listed in this document are minimum and recommended requirements for hardware and software for each computer component of the system. Use the *Deployment Models* table below as a guide to determining the most appropriate configuration.

Deployment Models

This table describes the various deployment models for SendSuite® Tracking.

Model	Appropriate For:
Turn-key – SendSuite® Tracking software and database are installed together on in a single workstation-grade environment.	<ul style="list-style-type: none"> • 1-5 local processing workstations • 1-5 concurrent users • Centralized user environment • Low transaction volume (~100/day) • ~1k possible recipients
Self-hosted – SendSuite® Tracking software and database are installed and hosted in a customer-provided environment.	<ul style="list-style-type: none"> • 5+ dispersed processing workstations • 5+ concurrent users • High transaction volume (>100/day) • >1k possible recipients • Geographically dispersed user environments • Separate application and database servers • Campuses to enterprises
AWS-hosted* – SendSuite® Tracking and related software are installed and hosted in a Pitney Bowes-provided cloud-based AWS environment.	<ul style="list-style-type: none"> • 5+ workstations • 10+ users • High transaction volume (>100/day) • >1k possible recipients • Reduced technical administration and financial overhead • Campuses to enterprises

*AWS hosting is restricted to limited countries

System Requirements

Model	Architectures	Requirements
Turn-key	<ul style="list-style-type: none"> Stand-alone single workstation. Single workstation peer-to-peer (5 workstations maximum, including the host). 	<p>Hardware</p> <ul style="list-style-type: none"> 2 GHz or higher CPU 4 GB RAM (minimum) Network Interface 1024 x 768 (minimum) display 40 GB available hard disk space Sufficient ports for peripherals <p>Operating System</p> <ul style="list-style-type: none"> Windows 8.1; Windows 10; Windows 11 <p>Database</p> <ul style="list-style-type: none"> SQL/SQL Express Server 2012; 2014; 2016; 2017; 2019
Self-hosted	<ul style="list-style-type: none"> Single-server (same for database and application) Multi-server (separate for database and application) Web farm Clustered 	<p>Hardware (Servers)</p> <ul style="list-style-type: none"> 2 GHz or higher Dual-Core or Quad-Core CPU 8 GB RAM Network Interface 40 GB available hard disk space <p>Operating System (Servers)</p> <ul style="list-style-type: none"> Microsoft Windows Server 2012; 2012R2; 2016; 2019; 2022 <p>Database (Servers)</p> <ul style="list-style-type: none"> SQL/SQL Express Server 2012; 2014; 2016; 2017; 2019 <p>Hardware (Clients)</p> <ul style="list-style-type: none"> 2 GHz or higher CPU 4 GB RAM (minimum) Network Interface 1024 x 768 (minimum) display 20 MB available hard disk space
AWS-hosted*	<ul style="list-style-type: none"> Cloud hosting 	<p>Hardware (Clients)</p> <ul style="list-style-type: none"> 2 GHz or higher CPU 4 GB RAM (minimum) Network Interface 1024 x 768 (minimum) display 20 MB available hard disk space

NOTE: The product installer will automatically install SQL Server Express 2019 if a remote SQL server is not selected during product installer configuration. The maximum database size permitted by SQL Server Express is 10 GB.

Supported Browsers

The SendSuite® Administrator web-based application supports the following browsers:

- IE (9-11); Edge
- FireFox
- Chrome

Product Installation Requirements

The IT administrator should provide the Pitney Bowes Service Professional installing the product with temporary Windows administrator permissions to the target servers and workstations. This is required to execute the SendSuite® Tracking installation package which uses the Windows Installer (MSI) engine.

Software and Feature Dependencies

Item	Server/Turn-key Host	Client Workstation	Notes
Internet Information Services (IIS)	Yes	No	
IIS 6 Management Compatibility	Yes	No	Must be installed: <ul style="list-style-type: none"> • IIS 6 Metabase Compatibility • IIS 6 WMI Compatibility
Microsoft Active Server Pages (ASP.Net) 3.5	Yes	No	
Microsoft Message Queuing (MSMQ)	Mandatory for Installation	No	Required by the product installer only and may be disabled upon successful installation/upgrade.
Microsoft Distributed Transaction Coordinator (MSDTC)	Yes, if database and application are installed on separate servers	No	
Microsoft .NET Framework 4/8	Yes	Yes	
.NET Ajax Support	Yes	No	

Supporting Files

The following Visual FoxPro runtime files are installed to ...\\Windows\\System during product installation:

File name	Description
VFP9R.DLL	VFP9 Runtime Library
VFP9RENU.DLL	VFP9 Runtime Library Resource
VFP9RUN.EXE	VFP9 Runtime Executable (Displays Current Version of VFP Runtime)

NOTE: VFP libraries are in use to support legacy business logic but are being deprecated over the course of multiple releases.

SQL Server Security Requirements

This section defines the minimum SQL permissions required to install, upgrade, or operate SendSuite® Tracking.

SQL Login for Installation and Upgrades

While use of the *sa* login is preferred, product installation and upgrades may be executed with a SQL login having at least the following Server Roles:

Role	Justification
dbcreator	This role allows the product installer to execute scripts to create the following databases: <ul style="list-style-type: none"> SSAdmin SST TAPlusRepository
Public	n/a
securityadmin	Allows the product installer to create and configure the SST_User SQL login

Furthermore, the SQL login used for installation must be assigned to the public role on the master database.

SST_User SQL Login

By default, the product installer creates the SST_User login with the following configuration:

Database	Server Role	User Mapping: Role Membership	Explicit Permission
SSAdmin	public	<ul style="list-style-type: none"> db_datareader db_datawriter public 	Grant: execute
SST	public	<ul style="list-style-type: none"> db_datareader db_datawriter public 	Grant: execute
TAPlusRepository	Public	<ul style="list-style-type: none"> db_datareader db_datawriter public 	Grant: execute

Default Language

Because all date formats in the SendSuite® Tracking databases are *mm/dd/yyyy*, the default language for SST_User must be English (us-English) and must never be altered.

Supported Collations

The following collations are supported:

- SQL_Latin1_General_CP1_CI_AS
- SQL_Latin1_General_CI_AS

Communications Requirements

The default SQL port is TCP-1433, but this is configurable in SQL Server.

Licensing Considerations

Microsoft SQL Server is licensed by Microsoft in a variety of configurations. For self-hosted environments, it is the obligation of the customer to ensure proper licensing.

Networking & Firewall Requirements

SendSuite® Tracking may be installed with HTTP or HTTPS. When implementing HTTPS in a turn-key or self-hosted environment, it is the customer’s responsibility to provide the necessary certificates. When deploying the SendSuite® Mobile Android App, certificates must be issued by a Certificate Authority (CA); self-signed certificates are not supported.

Consider the following default port assignments when configuring firewalls:

Network communication ports

Protocol	Ports
HTTP	<ul style="list-style-type: none"> • 80 – Admin; Clients • 8080 – SendSuite® Link • 9990 – WildFly
HTTPS	<ul style="list-style-type: none"> • 443 – Admin; Clients • 8443 – SendSuite® Link • 9990 – WildFly

Firewall Whitelist

Administrators of self-hosted implementations must configure their firewall whitelist. Those having AWS-hosted systems will be provided whitelist URLs upon the launch of the project.

If implementing the optional SMS feature, the following URL must be whitelisted:

- <https://api.twilio.com/2010-04-01>

Android Tracking Assistant Networking Considerations

Android OS Jelly Bean 4.1.2 and Marshmallow 6.0.1 are not capable of resolving hostnames to IP addresses in certain LAN/WAN environments. Due to this constraint, it is advisable that the SendSuite® Link application server be assigned a reserved IP address (Static IP). Often, the SendSuite® Link application server is the same as the SendSuite® Tracking application server. This constraint is not applicable to AWS-hosted solutions nor is it likely to be applicable in situations where the SendSuite® Link server is otherwise made public.

Virtual Machine Considerations

Virtual Machines can be used for the SendSuite® Tracking Application Server. These virtual machine images should be configured just like their physical counterparts according to the published hardware and software requirements in this document. Additional tuning of these requirements may be needed, depending on environment variables. Performance of the SendSuite® Tracking VM should be monitored over the first 6 months of deployment to ensure that the VM is performing optimally. Shared VM environments can often impact the performance of other VMs depending on the usage and I/O. If users are experiencing poor performance with a VM server, consideration should be made to migrate the VM to a less active host.

While it is technically feasible to host the application database on a virtual machine, it is not recommended. This is because DBMS software is very I/O intensive, and it is much easier to tune a physical machine than a virtual machine.

NOTE: Any VM product desired may be employed, however, it is the customer's full responsibility for setup, configuration, and maintenance of the environment. Pitney Bowes does not test SendSuite® Tracking in virtual environments.

Authentication

SendSuite® Tracking supports various authentication methods.

Authentication Type	Installation Model	Description
Product Authentication	Turn-key; Self-hosted; AWS-hosted	This is the standard means of logging into the product. User IDs and passwords are stored and validated by the application.
Auto-logon	Turn-key; Self-hosted	Supported by Windows Authentication, .NET is leveraged to acquire the credential of an authenticated user. The password verification is disabled when the user is successfully authenticated by the operating system. The user's ID in the product must match their Windows user ID.
LDAP	Turn-key; Self-hosted	Active Directory. Interactive login is not validated by the product. Users are validated only by the LDAP server.
Key Exchange	AWS-hosted	This is restricted to AWS-hosted environments. The product generates a customer key for each software instance during the installation of the software. The enterprise is provided with their key to use during deployment. The product generates an access code based on the user ID, a unique token, and customer key, then grants access if matching.

NOTE: A valid user account must first be created or already exist within the product for any user to access the system. Passwords are validated by the product while in Product Authentication mode. In LDAP mode, the user ID and password are validated against the configured LDAP host system. In Auto-Logon or Key Exchange authentication modes, the product only validates the user ID but not the password. Key Exchange makes use of a unique access token that, when configured, is automatically provided by the customer workstation.

Mobile Device Management

Pitney Bowes implements a robust MDM framework using Omnisia Workspace ONE UEM (<https://www.omnissa.com/products/workspace-one-unified-endpoint-management>) to ensure that all Zebra devices are secure, compliant, and restricted to authorized usage only.

The key aspects of this policy are outlined below:

1. Device Usage Restrictions

The Omnisia Workspace ONE UEM policy is configured to limit the functionality of Zebra mobile devices to Pitney Bowes-authorized applications only, including:

- SendSuite® Tracking
- ParcelPoint™ Smart Lockers & PitneyLockers® (where applicable)
- Any associated system utilities essential to solution performance

To achieve this, the following controls are enforced:

- Application Whitelisting: Only approved applications are permitted to run; all other apps are blocked.
- App Store Restrictions: Access to Google Play and installation of third-party applications are disabled.
- Kiosk Mode: Devices operate in either single- or multi-app kiosk mode to prevent users from navigating outside the authorized application environment.
- Settings Lockdown: Access to developer options, system settings, and other potentially vulnerable areas is restricted or disabled.

2. Security and Network Protection

To safeguard both the device and the client's internal network, the MDM policy incorporates the following security controls:

- Secure Wi-Fi Configuration: Devices are provisioned to connect only to designated SSIDs using enterprise-grade encryption protocols (e.g., WPA2/WPA3 with EAP authentication).
- Data Encryption: All device data is encrypted at rest, protecting sensitive information in the event of loss or theft.
- Remote Lock/Wipe Capability: Devices can be remotely locked or wiped if reported lost, stolen, or found to be non-compliant.
- Threat Detection and Compliance Monitoring: Continuous monitoring ensures that rooted or compromised devices are immediately flagged, and access is revoked.
- Network Isolation Options: Devices can operate within a segregated VLAN or VPN if required, minimizing exposure to internal networks.

Pitney Bowes' Omnisia Workspace ONE UEM policy provides a secure, locked-down mobile environment that supports operational needs while aligning with client security requirements. It ensures that Zebra devices are:

- Used exclusively for approved Pitney Bowes applications
- Protected against tampering and misuse
- Isolated from and not capable of compromising internal client networks