Data sheet

pitney bowes

Shipping & Mailing
Technology platform

# Pitney Bowes Shipping 360® Platform

Login Security Data Sheet

# Introduction

**The Pitney Bowes Shipping 360® platform** offers both **SSO (Single Sign-On)** and **MFA (Multi-Factor Authentication)** as log in security measures. Each application, Shipping, Lockers, Tracking and Analytics, is supported by both login security measures.

# 01. Single Sign On

## 1.1 What is Single Sign-On?

Single sign-on (SSO) is an authentication method that enables users to securely authenticate multiple applications and websites by using a single set of credentials.

## 1.2 Why Single Sign-On needed by an organization?

Organizations use Single Sign-On (SSO) to make it easier for their employees to access different systems with a single login. It improves user experience and security by reducing the number of passwords users must remember and simplifies how IT teams manage user access to applications.

## 1.3 How does Single Sign On (SSO) work?

SSO works based upon a trust relationship set up between an application, known as the service provider, and an identity provider. This trust relationship is often based on a certificate that is exchanged between the identity provider and the service provider.

## 1.4 Shipping 360 Single Sign On (SSO) features

**Protocols Supported**:

- **SAML 2.0 (Security Assertion Markup Language)**: Enables secure single sign-on (SSO) across different applications by exchanging authentication and authorization data between identity providers and service providers.
- **OIDC (OpenID Connect)**: Builds on OAuth 2.0 protocol to allow authentication and information about users to be passed securely. It provides additional features like user identity information in JSON format.

**SAML Metadata File Integration**:

- Customers can share their SAML Metadata file with Pitney Bowes. This file includes necessary configuration details such as endpoint URLs, encryption keys, and attribute mappings.
    - **NOTE**: Based on the request of customer we can also share the sample Metadata file with them for better understanding.
- **Customizable Attributes**: Customers can specify required values like User Role, Location, Cost Account, etc., within the SAML Metadata file. This customization ensures that the Shipping 360 applications receive essential user attributes during authentication.

**User Management Options**:

- **JIT (Just In Time) Provisioning**: Users can be dynamically created in the Shipping 360 applications upon their first login attempt.
    - We support location and role optional attributes mapping under the token.
    - We don't support any API or SCIM (System for Cross-domain Identity Management) to provision users or manage users in the Shipping 360 applications.
- **Add Federated User**: Customers have the flexibility to manually add user mappings directly within the application interface. This option is useful for managing users who may not be provisioned via JIT.
    - **NOTE**: We don't support importing federated users in the application yet.

**TA Device User Support**:

- **Non-SSO Users for TA Devices**: Specifically for TA (Transaction Advisor) Device users, who are added as non-SSO users. This ensures compatibility and usability within SSO-enabled subscriptions.

**Multiple Subscriptions Management**:

- **Single Domain, Multiple Subscriptions**: Allows multiple subscriptions to be associated with a single domain name. This feature supports organizations that manage multiple instances or versions of the Shipping 360 applications under a unified domain.
    - NOTE: Creation of Non-SSO users and TA Device users is not supported in this case.

# 02. Multi-Factor Authentication (MFA)

## 2.1 What is Multi-Factor Authentication (MFA)?

**Multi-Factor Authentication (MFA)** is a security method that requires users to provide **two or more different types of verification** before gaining access to an account, system, or application. This additional layer of security helps ensure that only authorized users can access sensitive information or perform critical actions.

## 2.2 Why Multi-Factor Authentication needed by an organization?

Multi-Factor Authentication (MFA) is key for organizations because it adds extra security checks to prevent unauthorized access, protect sensitive data, and meet legal standards. It also helps prevent cyberattacks and strengthens trust with customers.

## 2.3 How Does Multi-Factor Authentication (MFA) Work?

We offer two Multi-Factor Authentication (MFA) options for your security. You can choose to use the Okta Verify App in combination with your email for an added layer of protection, or you can opt for MFA using only the Okta Verify App.

It's important to note that when SSO is enabled, the MFA functionality will not be active. This means that users will not be prompted for additional authentication factors beyond their initial login when accessing applications through SSO.

**United States**
3001 Summer Street
Stamford, CT 06926-0700

For more information, please contact your Pitney Bowes sales representative.

Pitney Bowes, the Corporate logo, and SendPro are trademarks of Pitney Bowes Inc. or a subsidiary. All other trademarks are the property of their respective owners.
© 2024 Pitney Bowes Inc. All rights reserved.