Shipping & Mailing
Outbound and Inbound Package Management

Shipping 360™ SSO Technical Overview

Single Sign-on for Shipping 360™, inclusive of PitneyShip™ Pro, PitneyShip™ Enterprise, PitneyTrack™ Inbound, and PitneyAnalytics™

Introduction

This document overviews the technical aspects and configuration requirements for SAML & OIDC Single Sign-on (SSO) in the Shipping 360™ platform.

NOTE: This document applies to version Shipping 360™ v1.63 and higher. Also, please be advised that in SSO configurations completed before the v1.58 release, the Attribute Mapping values ***will not be visible*** in the SSO configuration page.

Service Collateral
Shipping 360™ SSO. Rev C
August 2023

Document Information

Document Name	Shipping SSO Technical Overview
Document Revision	C
Platform Version	V1.63
Region	United States; Canada
Document Owner	Michael Beausoleil, Product Engineer – Office Shipping
Document Reviewers	Christopher Lore; Sam Morkos; John Rortvedt; John Paul Cruz; Jonathon Anderson; Jonathon Jiovani; Chris Gorgas
Document Author	Michael Beausoleil, Product Engineer – Office Shipping
Document Audience	Technical Internal & External
Document Original Creation Date	June 5th, 2023

Revision History

Seq. #	Date	Description	Document Revision	Platform Version	Author/Modifier
1	05/31/2023	Document authored	A	v1.61	Michael Beausoleil
2	06/06/2023	Editorial corrections; applied trade markings.	B	v1.61	Michael Beausoleil
3	8/18/2023	Added steps for contacting Tech Ops; added troubleshooting steps; multiple domain support.	C	v1.63	Michael Beausoleil

Approvals

Approver	Signature
Michael Beausoleil (Product Engineer)	Michael Beausoleil Michael Beausoleil (Aug 18, 2023 10:55 PDT)
Jonathon Jiovani (Sr. Director)	Jonathon Jiovani Jonathon Jiovani (Aug 21, 2023 10:15 EDT)

Table of Contents

What is Single Sign-On?

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

How does SSO Work?

SSO works based upon a trust relationship set up between an application, known as the Service Provider (SP), and an Identity Provider (IdP). This trust relationship is often based upon a certificate that is exchanged between the IdP and the SP.

Supported Protocols

SAML (Security Assertion Markup Language)

Frequently used in large enterprise cloud deployments, SAML is an XML based data format for exchanging authentication and authorization data (assertions) between an IdP and an SP (Shipping 360™). IdPs - entities that manage and store user credentials - exchange digitally signed XML documents (SAML Assertions) allowing an end-user to access a requested resource or service such as Shipping 360™.

OIDC (OpenID Connect)

OIDC is an interoperable authentication protocol based on the OAuth 2.0 framework of specifications (IETF RFC 6749 and 6750). It simplifies the way to verify the identity of users based on the authentication performed by an Authorization Server and to obtain user profile information in an interoperable and REST-like manner. OpenID Connect enables application and website developers to launch sign-in flows and receive verifiable assertions about users across Web-based, mobile, and JavaScript clients.

Authentication Process Overview

Shipping 360™ supports ***service provider-initiated*** authentication. Below outlines the process:

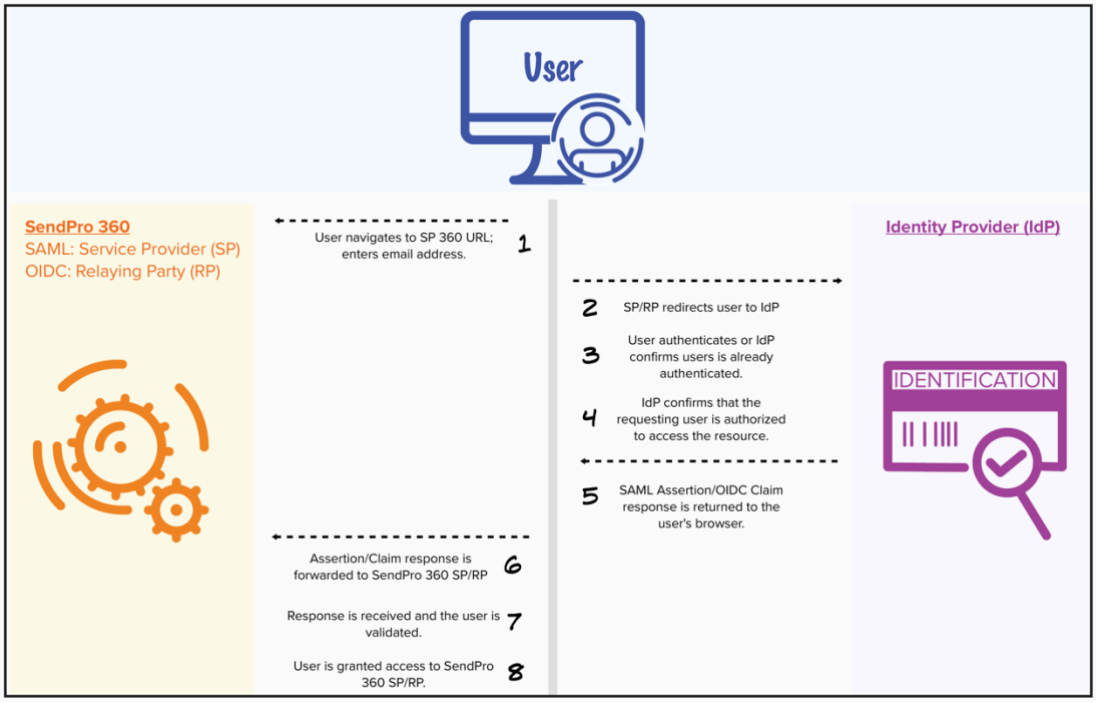
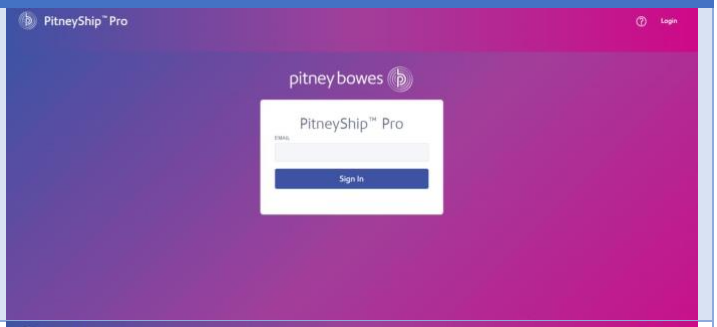
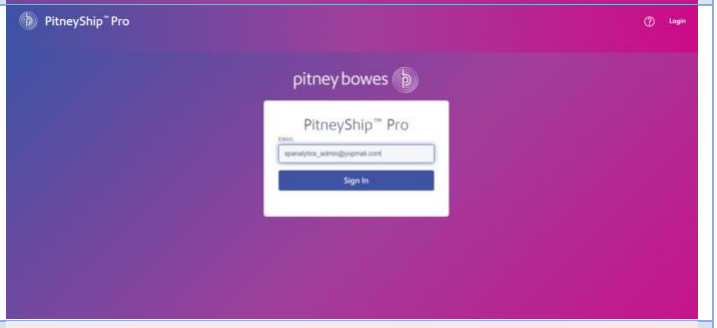
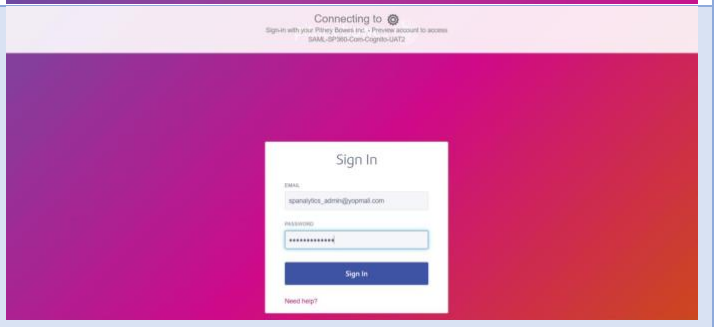
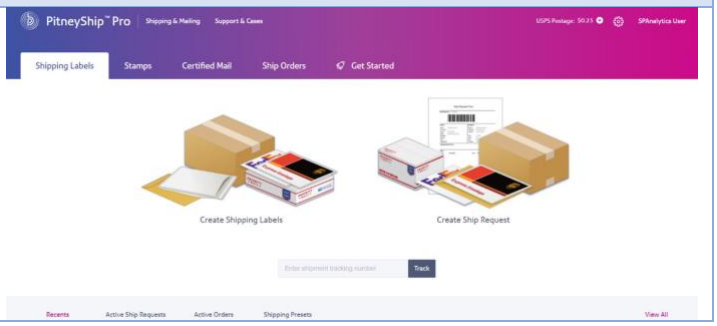


Figure 1: Graphical representation of the Shipping 360™ SSO Authentication Process

Shipping 360™ SSO Authentication Behavior

The following table describes and illustrates the SSO authentication application behavior from the user's perspective:

#	Desc.	Illustration
1	Visit the Shipping 360™ URL provided by the Installation Professional.	
2	Enter your email address and select Sign In.	
3	Shipping 360™ detects that the user must be authenticated by an external provider and redirects to the correct login page based on the email domain; user enters their credentials. (Note: this image is for example purposes only. Your login page may look different.)	
4	Upon successful authentication, user is redirected to the Shipping 360™ home page (PitneyShip™ Pro is illustrated in this example).	

Empty page?

Configuring your IdP for Shipping 360™ SSO

You'll be required to provide Pitney Bowes with a metadata file containing embedded certificate(s). Use the following information when configuring your IdP:

Region	Configuration Values
US	1. **EntityID (US):** urn:amazon:cognito:sp:us-east-1_jnFR1tyn8 2. **Reply URL:** https://sso-us.shipping360.pitneybowes.com/saml2/idpresponse 3. **Login URL:** https://sendpro360.pitneybowes.com
Canada	1. **EntityID (Canada):** urn:amazon:cognito:sp:ca-central-1_CTEzvam32 2. **Reply URL:** https://sso-ca.shipping360.pitneybowes.com/saml2/idpresponse 3. **Login URL:** https://app-ca.shipping360.pitneybowes.com

Providing your Metadata

Here is what you need to know about providing your metadata to Pitney Bowes:

1. Provide the file ***after*** configuring your IdP with the EntityID and URLs provided in this document.
2. May be provided by public URL.
3. May be provided by email attachment.
4. All certificates must be embedded in the metadata.

User Pool Attribute Mapping

Please observe the following User Attribute mappings:

User Pool Attribute	SAML/OIDC Attributes (provided by client)
UniqueID	**Required**. Examples: • Email address • Employee number • Employee network id • Etc.
Email	**Required**. Email address
Given Name	**Required**. First Name
Family Name	**Required**. Last Name
Location	**Optional**. The user's location name (***case-sensitive***)
Role	**Optional**. The use's assigned role name (***case-sensitive***)

IMPORTANT:

1. In all fields, the following special characters are prohibited:
   ~ ` ' ^ & – = \ | { } [ ] " ; < >
2. Locations and Roles are ***case-sensitive*** and *must be present before using SSO*.

User Provisioning

Onboarding users in Shipping 360™ requires two attributes associated with the user:

1. User Location
2. User Role

Three user provisioning methods are supported:

1. **Just In Time (JIT) Provisioning** (with ***defined*** role/location): With this method, administrators configure an SSO connection between the IdP and Service Provider, ensuring the required Location and Role attributes are present. These attributes can be included in the User Token.
2. **Just In Time (JIT) Provisioning** (with ***empty*** role/location): The user will be assigned to the '**Default**' location and '**Default**' role.
3. **Manual/Scheduled Import**: Importing users is done via the Manage Users screen. ***This will not directly create users***; .It will create user mappings and update existing users that have already logged in. Upon first login, the user mapping is disabled and can no longer be edited.

IMPORTANT:

Before configuring SSO, the **Default** location and role records must ***always*** be created, ***regardless of whether the values are provided***. If the defaults do not exist and a user logs in without them already assigned, they will see an error message.

Shipping 360™ SSO Configuration Process

Successful configuration of SSO for Shipping 360™ relies upon the collaboration of two entities:

1. Client IdP Administrator
2. Pitney Bowes Service Professional

In brief, the process for SSO configuration is:

Seq.	Action	Owner
1	Configure IdP	Client IdP Administrator
2	Provide metadata with embedded certificates and email domain name(s).	Client IdP Administrator
4	Configure Shipping 360™ (see Configuration Steps)	Pitney Bowes Service Prof.
5	Test authentication	Client IdP Administrator

Configuration Prerequisites

Before proceeding with configuration as the Pitney Bowes Service Professional, be sure to have the following information available:

- Client IdP administrator contact information
- Enterprise Identifier
- Protocol (OIDC or SAML)
- Domain(s)*
    - *See chart below for the supported quantity of domains
- Metadata
    - File
    - URL
- User Pool Mappings

Domain Support

Product	Qty of Domains Supported
PitneyShip Pro (Domestic); PitneyAnalytics; PitneyTrack Inbound	1
PitneyShip Pro (International)	1
PitneyShip Enterprise	3*

*The quantity of supported domains may be increased for additional fees.

SAML Configuration Steps

IMPORTANT: Before proceeding, take note of the following:

- Once enabled:
  - **SSO cannot be disabled**.
  - **Auth Provider cannot be changed**.
  - The **Create Identity Provider (IdP)** button will be relabeled **Update Attribute Mapping**.
- The Federated Client checkbox cannot be changed.

Note: Be sure to have created the Default location and role records before proceeding.

The installing Pitney Bowes Service Professional must complete the following steps:

1. Log into **360 Admin**.
2. Select the **client's enterprise**.
3. Select **Manage** under **Sign In Security**.
4. Set **Single Sign On (SSO)** toggle switch to **On**.
5. Select **SAML** from the **Auth Protocol** drop-down box.
6. Input the **Domain**. This must be the email domain, e.g., pb.com.
7. **Optionally** enter additional values in the **ADDITIONAL DOMAIN** field.
8. Introduce the metadata by selecting one of the methods below:
   a. **Upload Metadata File**
      i. Select the **Upload Metadata File** radio button.
      ii. Select **Browse**.
      iii. Using the file browser, navigate to and select the **metadata file** to be uploaded.
      iv. Select **Upload**.
   b. **Provide Metadata URL**
      i. Select the **Provide Metadata URL** radio button.
      ii. Input the **metadata URL**.
9. Map each **User Pool Attribute** to the appropriate **SAML Attribute**.
   a. UniqueID (**required**)
   b. Email (**required**)
   c. Given Name (**required**)
   d. Family Name (**required**)
   e. Location (optional)
   f. Role (optional)
10. Select **Create Identity Provider (IDP)**.
11. The platform will automatically send an email to STS-Support@pb.com requesting SSO domain activation, along with a carbon copy to the installing service professional, which may be used for acquiring progress updates as well as for maintaining a dialog with Tech Ops during SSO onboarding.

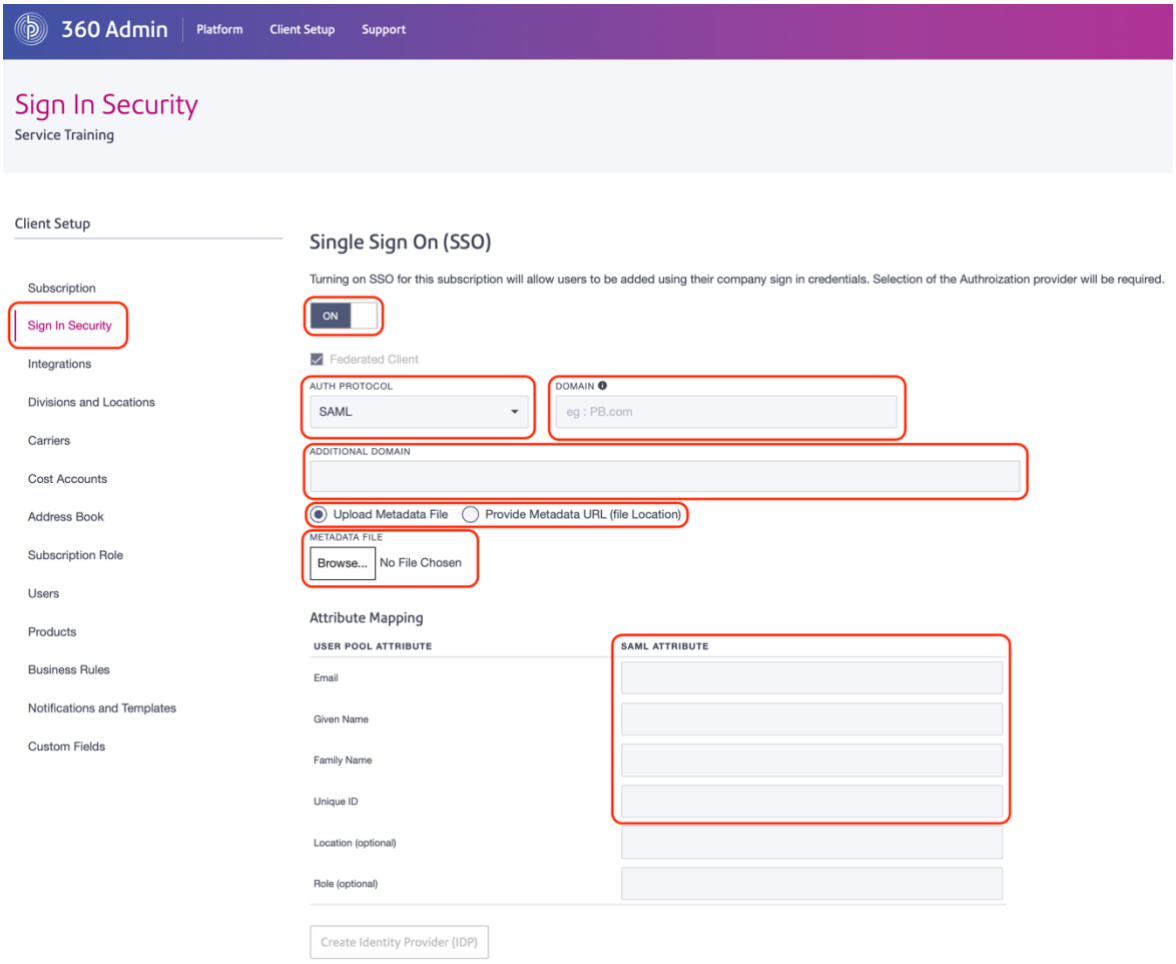


Figure 2:360 Platform Sign In Security SAML Configuration Form

OIDC Configuration Steps

IMPORTANT: Before proceeding, take note of the following:

- Once enabled:
  - **SSO cannot be disabled**.
  - **Auth Provider cannot be changed**.
  - The **Create Identity Provider (IdP)** button will be relabeled **Update Attribute Mapping**.
- The Federated Client checkbox cannot be changed.

Note: Be sure to have created the Default location and role records before proceeding.

The installing Pitney Bowes Service Professional must complete the following steps:

1. Log into **360 Admin**.
2. Select the **client's enterprise**.
3. Select **Manage** under **Sign In Security**.
4. Set **Single Sign On (SSO)** toggle switch to **On**.
5. Select **OIDC** from the **Auth Protocol** drop-down box.
6. Input the **Domain**. This must be the email domain, e.g., pb.com.
7. **Optionally** enter additional values in the **ADDITIONAL DOMAIN** field.
8. Enter the **Authentication Credentials** in the fields provided:
   a. CLIENT ID
   b. SECRET KEY
9. Input the **Issuer URL** in the provided text box.
10. Map each **User Pool Attribute** to the appropriate **OIDC Attribute**.
    a. UniqueID (**required**)
    b. Email (**required**)
    c. Given Name (**required**)
    d. Family Name (**required**)
    e. Location (optional)
    f. Role (optional)
11. Select **Create Identity Provider (IDP)**.
12. The platform will automatically send an email to STS-Support@pb.com requesting SSO domain activation, along with a carbon copy to the installing service professional, which may be used for acquiring progress updates as well as for maintaining a dialog with Tech Ops during SSO onboarding.

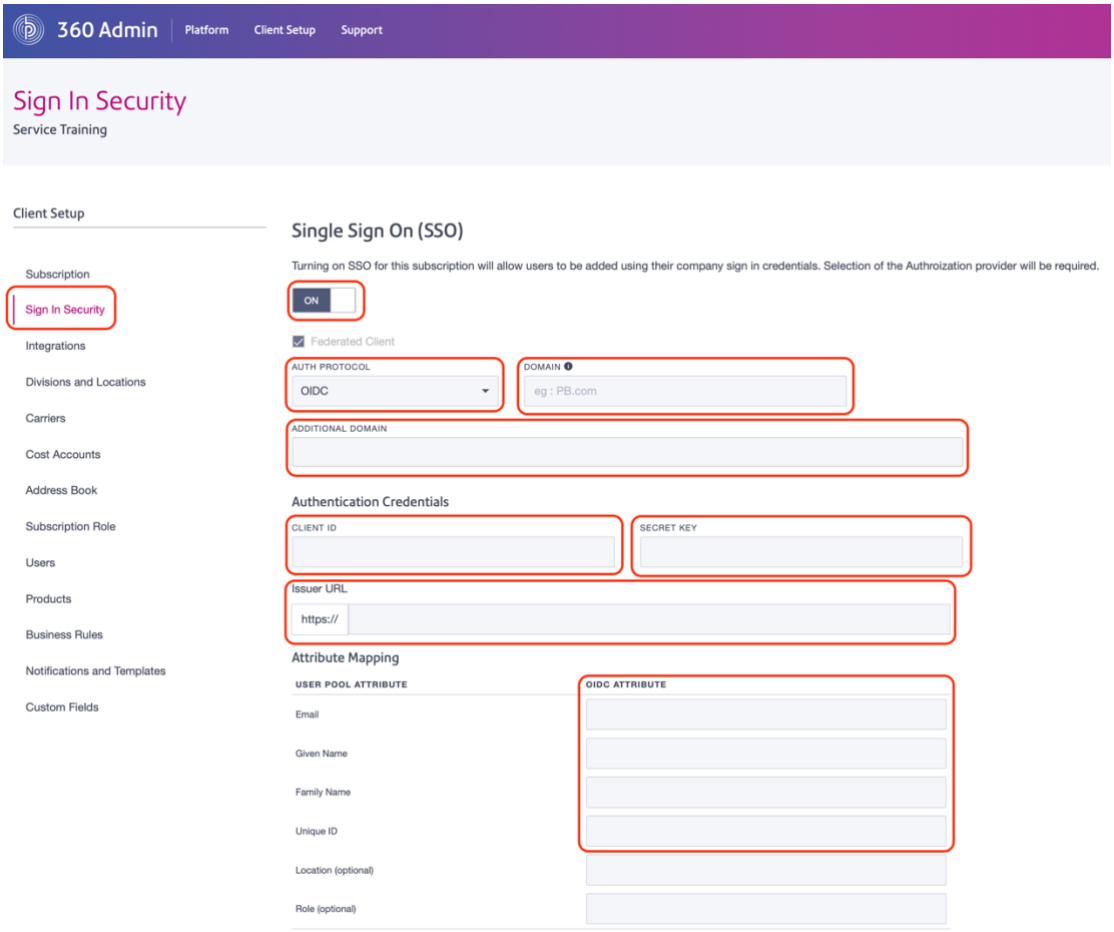


Figure 3:360 Platform Sign In Security OIDC Configuration Form

SAML Troubleshooting

For troubleshooting Shipping 360™ SSO authentication issues, Pitney Bowes recommends installing the "SAML Chrome Panel" for the Google Chrome browser. Refer to the following resource for installation and usage instructions:

How to gather a SAML trace.

Provide to your Pitney Bowes Service Professional the trace logs captured by the "SAML Chrome Panel".

Validating Assertion/Claim Attributes

Customers may have provided user pool attribute values that differ from what is in the actual assertion/claim. If after creating the IdP users are not able to log in, review the assertion to discover any differences between the actual assertion/claim and the data provided by the customer before escalating to DevOps.

Other troubleshooting resources:

- SAML-tracer Chrome Extension