



# **Point-to-Point Encryption (P2PE) Manager User Guide**

Document Date: October 26, 2020

## **Legal Notice**

Copyright © 2020 Bluefin Payment Systems LLC.

Bluefin Payment Systems LLC is a registered ISO of Wells Fargo Bank, N.A., Walnut Creek, CA.

Bluefin Payment Systems LLC is a registered ISO/MSP of Deutsche Bank AG, New York, New York.

Bluefin Payment Systems LLC is a registered MSP/ISO of the Canadian branch of U.S. Bank National Association and Elavon, Inc. Georgia, a wholly owned subsidiary of U.S. Bancorp, Minneapolis, MN.

Decryptx® is a registered trademark of Bluefin Payment Systems LLC in the United States and/or other countries.

P2PE Manager® is a registered trademark of Bluefin Payment Systems LLC in the United States and/or other countries.

PayConex™ (Gateway) is a trademark of Bluefin Payment Systems LLC.

PayConex™ (for Salesforce) is a trademark of Bluefin Payment Systems LLC.

PayConex™ (Plus) is a trademark of Bluefin Payment Systems LLC.

QuickSwipe® (Mobile POS) is a registered trademark of Bluefin Payment Systems LLC in the United States and/or other countries.

ShieldConex® is a registered trademark of Bluefin Payment Systems LLC in the United States and/or other countries.

# Table of Contents

---

<b>Overview</b>	<b>6</b>
Audience	6
Terminology	6
Contacting Support	7
Response Times	7
Subscribe to System Updates	8
<b>Getting Started</b>	<b>9</b>
Logging In	9
Dashboard	9
Menu Options At A Glance	11
Receiving and Activating Your Device	12
Batch Receiving Devices	12
Receiving Device with Special Serial Number Requirements	13
Accessing Online Help Documentation	14
Downloading and Viewing PDF Files	15
Downloading and Viewing Video Files	15
<b>Transactions</b>	<b>16</b>
<b>Reporting</b>	<b>17</b>
Creating the Chain of Custody Report	17
Creating a Client Transaction Summary Report	17
Creating the Inventory Summary Report	18
User Report	18
Device Activity Report	19
Device Receipt	19
Daily Report	19
Decryption Totals	20
Exporting a Report	20
<b>Administration</b>	<b>22</b>
Managing Users	22
Adding a User	23
Updating a User	23
Resetting a User's Password	24
Managing Your Personal Settings	24
Resetting Your Password (Forgotten Password)	25
Adding Locations	25
Removing Locations	26
Editing Locations	26
<b>Device Management</b>	<b>27</b>
Device Activation Process Flow	27
Updating Devices	28
Device State Definitions	29

---

Viewing Device Details .....	30
Chain of Custody .....	30
Device State History .....	31
Lifecycle Report - Detailed Device History .....	31
Return Merchandise Authorization Process .....	31
Checking on Device Shipment and Tracking .....	32
Checking Tracking Number .....	32
Checking Device Status .....	33
Checking Order Status .....	34
Transferring a Device between Custodians or Locations .....	34
Transferring Multiple Device Locations .....	35
Equipment .....	36
Deploying Equipment .....	36
Opt Out of Bluefin Program .....	38
<b>Device Inspections and Attestations .....</b>	<b>39</b>
Inspecting a Device .....	39
Inspections Report: Viewing Details of Past Inspections .....	39
Device Attestations .....	40
Changing Device Attestation Date .....	42
Batch Process: Change Device Attestation Date .....	43
Viewing Future Scheduled Attestations .....	44
Device Tampering Detection .....	44
<b>Appendix: User Roles .....</b>	<b>45</b>
Client / Merchant Roles .....	45
Partner Roles .....	45
<b>Appendix: Receiving and Activating Your Device .....</b>	<b>46</b>
Overview .....	46
Step 1: Access the P2PE Manager Online .....	46
Step 2: Log Receipt of the Shipment .....	47
Step 3: Activate Your Device .....	49
Reporting a Tampered Device .....	50
<b>Appendix: Partners .....</b>	<b>51</b>
Client Merchant Communications .....	51
Customizing Email Templates .....	52
Adding Data Tokens .....	52
Deleting Email Templates .....	53
Administration .....	53
Adding a Partner Record (Sub-Partner) .....	54
Adding a Client / Merchant .....	56
Editing a Client's Contact Person .....	58
Client Import .....	59
Managing Devices .....	60
Partner Device Types .....	60
Shared Devices .....	61

---

Device Transfer .....	61
Single Sign-On (SSO) .....	61
Benefits .....	61
Setup Process .....	61
Frequently Asked Questions .....	62
What is SAML? .....	62
Who establishes SAML / SSO in P2PE Manager? .....	63
What are the SSO setup requirements? .....	63
What will I receive from Bluefin to establish SSO? .....	63
What does the Identity Provider need to do? .....	63
How many Identity Providers are supported? .....	63
Information Identity Providers Need .....	63
Sample IDP Setup .....	64
IDP Configuration .....	64
IDP User Configuration .....	65
Azure Setup Overview .....	67
Single Sign-On Request Form (Sample) .....	69

## Overview

Bluefin was the first payment security provider in the United States to receive Payment Card Industry (PCI) validation for a Point-to-Point Encryption (P2PE) payments solution in March 2014. Bluefin's P2PE solution encrypts cardholder data at the Point of Interaction (POI) in a PCI-approved P2PE device and decryption is done off-site in an approved Bluefin Hardware Security Module (HSM). Our solution prevents clear-text cardholder data from being present in a merchant or enterprise's system or network where it could be accessible in the event of a data breach.

**P2PE Manager** is a web-based management system provided in conjunction with Bluefin's P2PE solution. P2PE Manager assists merchants by facilitating the chain-of-custody transfers required for PCI compliance. It also supports ordering new devices and remotely disabling devices.

For a comprehensive system overview, you can download and watch **P2PE Manager Overview.mp4** from the **Documentation** tab. Additional videos are available.

## Audience

This user guide is intended for Clients / Merchants and authorized Partners. Clients and partners share many system capabilities. (Exceptions are noted in the sections below.)

**IMPORTANT:** All capabilities are described in this guide. Depending on your role, you might or might not have access to certain capabilities.

Related Information: [Appendix User Roles](#).

Oftentimes the only difference between how clients/partners access information is in setting certain parameters. Partners must populate the Partner and Client fields by selecting an option from a drop-down list.

Capabilities restricted to Partners are described in [Appendix: Partners](#).

## Terminology

Key terms used throughout this guide are defined below:

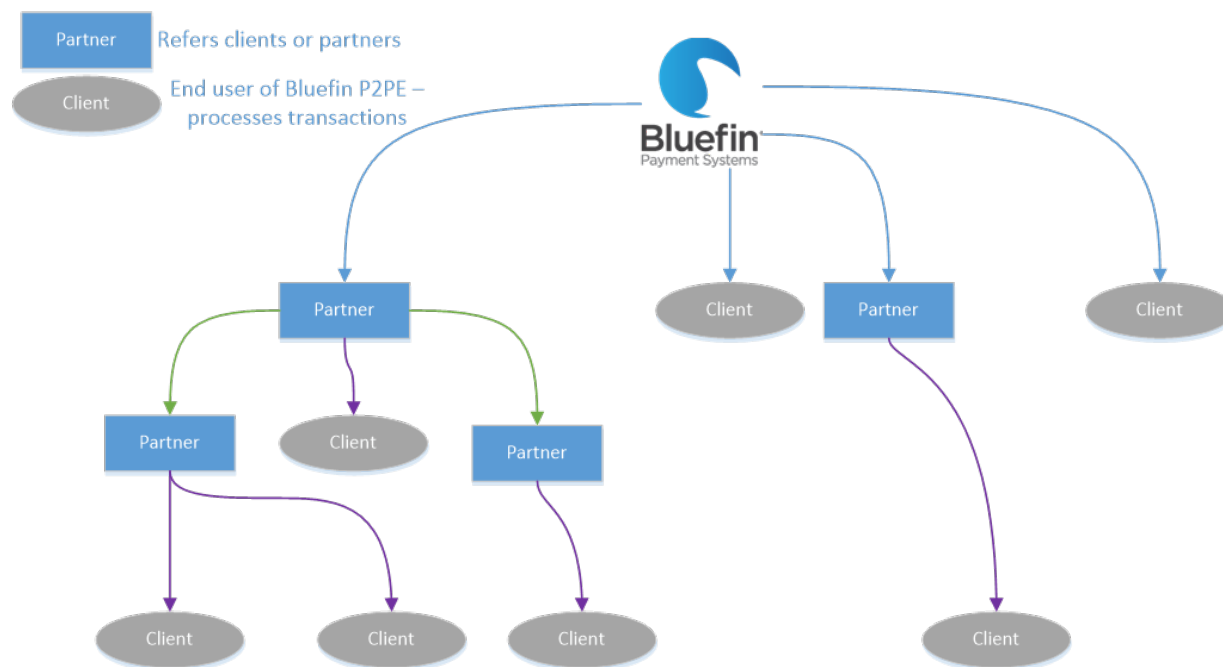
A **partner** is an entity that resells devices and services to merchants.

A **client** is the end user (merchant) who uses devices to process transactions.

**Locations** can be based on physical location (Atlanta Office, Chicago Office) or internal departments (Front Desk, Cafeteria, Gift Shop). Locations can be used to "partition" a client.

A **custodian** is the person who takes responsibility for device compliance (and not necessarily the primary person interacting with the device.)

The following diagram illustrates how partners and clients are related to the Bluefin ecosystem.



## Contacting Support

**PHONE:** 800-675-6573

Available 24 /7 (24 Hours/Day and 7 days a week.)

Option 2 for Technical Support

Option 4 for Customer Service

**EMAIL:** [service@bluefin.com](mailto:service@bluefin.com)

**WEB PORTAL:** Click the **Contact Support** tab within P2PE Manager.

## Response Times

**VOICEMAIL:** Call back within four hours during business hours.

**EMAIL:** Response within 24 hours.

## Subscribe to System Updates

You can subscribe and get automated email notifications whenever Bluefin Payment Systems creates, updates or resolves an incident.

1. Access <https://status.bluefin.com/> and click **Subscribe To Updates**.
2. Enter your email address and then click **Subscribe**.
3. Select the product of your choice.
4. Click **Save** when you're done.





**Notifications**

☐ You have an open device shipment that needs to be checked in. When you receive the device(s), please click [here to begin](#).

[Dismiss](#) [Continue](#)

---

Date From: 10/17/2018 00:00:00 [📅](#) Date To: 10/17/2019 23:59:59 [📅](#) [Apply](#)

**Summary Information** [🔗](#)

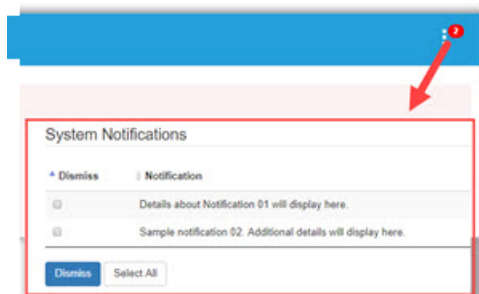
<b>Devices</b> Stored: 0 Activated: 0 Tampered: 1 Malfunctioning: 0 Rma: 0 Total: 1	<b>Shipped devices by type</b> PAX D210: 7 Augusta S: 1 Total: 8	<b>Attestations Due on 2 Devices:</b> Serial No. 30358 30360	<b>User Count</b> 8 (Total Users) 8 (Users 2018) Jan: 0 Feb: 0 Mar: 0 Apr: 0 May: 0 Jun: 0 Jul: 0 Aug: 1 Sep: 7 Oct: 0 Nov: 0 Dec: 0 2018 (8)
---	---	---	---

**Device Locations**  
[View](#)

The information displayed is dynamic based on the date range specified and includes the following information:

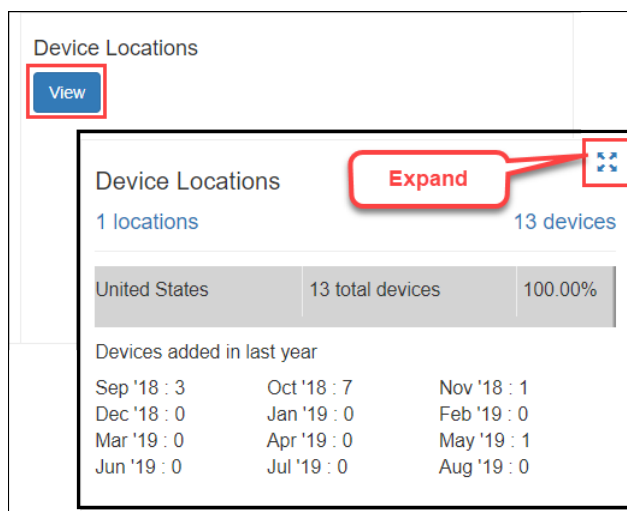
- Number of Devices by State
- Number of Shipped devices by Device Type
- Number of Devices due for Attestation
- Number of P2PE Manager Users in your account monthly - User Count
- Number of Devices by Location (active devices by country)
- Number of Transactions (Partners user only)
- Number of Clients (Partners user only)

The Notifications banner displays as needed when alerts from the administrator are published. After reading a notification, you can select it and then click **Dismiss** to remove it. To hide the banner, click **Continue**. To review unread notifications, click the red notifications icon in the top right corner to see a list.

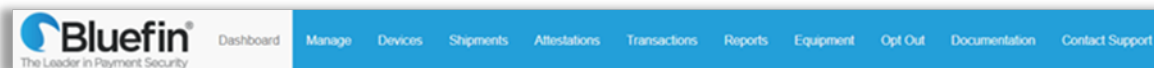


From **Manage > System Notifications** you can also review notifications and **Dismiss** them.

**NOTE:** If there's a lot of data to summarize in any "tile", click the **View** button to populate the tile. Click the **Expand** icon, when applicable, to enlarge a tile.



## Menu Options At A Glance



From the tabs at the top of the screen, you can access the following options.

**NOTE:** Depending on your access level, you might or might not have access to all options. Refer to the [Appendix: User Roles](#) for details.

Tab	Description
<b>Manage</b>	Manage Users, Locations and Device Transfers.
<b>Devices</b>	Displays a summary of all devices.
<b>Shipments</b>	Displays incoming shipments.
<b>Attestations</b>	Displays Current Attestations, History and Future Attestations.
<b>Transactions</b>	Displays a summary of transactions including encryption and decryption status
<b>Reports</b>	POI Chain of Custody, Client Transaction Summary, Inventory Summary, User Report, Device Activity, Device Receipt, Daily Report and Decryption Totals.  <b>NOTE:</b> Partners can run additional reports. Refer to <a href="#">Appendix: Partners</a> for details.
<b>Equipment</b>	Deploy equipment (order equipment and check device status.)
<b>Opt Out</b>	Retire all devices in your account so they cannot conduct transactions.

Tab	Description
	<b>IMPORTANT:</b> This option is restricted to Client Administrators.
<b>Documentation</b>	Help files and videos. Refer to <a href="#">Accessing Online Help Documentation</a> for details.
<b>Customer Support</b>	Submit a help request online and review help contact information.

## Receiving and Activating Your Device

For detailed information, refer to the [Appendix: Receiving and Activating Your Device](#).

**NOTE:** You can also access this information from within P2PE Manager by clicking the **Documentation** tab and downloading the **Device Activation Guide**.



**Video Tutorial:** Watch a video from the **Documentation** tab.

### Related Information:

- See [Accessing Online Documentation](#).
- See [Batch Receiving Devices](#) for information about scanning multiple devices into P2PE Manager.
- See [Receiving Device with Special Serial Number Requirements](#) when appropriate.

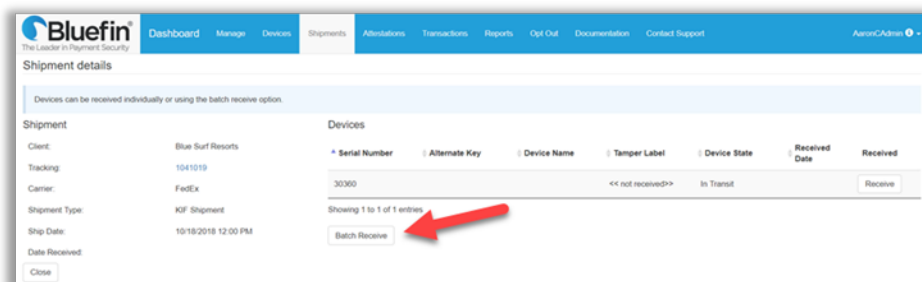
## Batch Receiving Devices

With P2PE Manager, you can **Batch Receive** devices by scanning them into the system. Any scanner connected via USB/Serial or Ethernet will work with P2PEManager.

**NOTE:** Partners need to use the drop-down options at the top of the page and select a **Partner** and **Client** first.

**TIP:** At the top of the **Shipments** page, the you can filter the list of shipments from the drop-down list: All, In-transit, Received

1. From the **Shipments** tab, select a shipment and then click **Batch Receive**.



2. Optional: Click **Auto Activate device** only if you are ready to activate and start using the device now.  
**TIP:** To take advantage of this time saving option, you must select it before scanning your devices.
3. Scan the **Serial Number**. The whole serial number will be displayed.  
**NOTE:** For Ingenico devices, P2PEManager will automatically find a match based on the input from the Key Injection Facility (KIF.)
4. Scan the **security seal number**. (This number might also be called the tamper seal.) Wait for the green success message.
5. If you selected **Auto Activate device**, you're done! The **Device State** will display as **Activating**.  
If you did not select Auto Activate device, then the **Device State** will display as **Received**. To continue, follow the actions in **Step 3: Activate Your Device** in the [Appendix: Receiving and Activating Your Device](#).

## Receiving Device with Special Serial Number Requirements

In special circumstances, P2PE Manager will also support the ability to configure how to match a device's serial number.

1. From the **Shipments** tab, select a shipment and then click **Batch Receive**.
2. Enter the serial number. (manual entry or scanner)
3. Select **Matching Pattern** based on your solution requirements.

- a. Full Match
  - b. Partial Match from Start: Configure the Matching Length by counting from the beginning of the serial number.
  - c. Partial Match from End: Configure the Matching Length by counting from the End of the serial number
4. Select a **Padding Pattern** based on your solution requirements.
  - a. Pad on the Left: Configure the extra character length in the "Padding Length" and then enter in the values in the "Character" field.
  - b. Pad on the Right: Configure the extra character length in the "Padding Length" and then enter in the values in the "Character" field.
5. Review the **Matching options** that display based on your configurations.

**Receiving device**

Scan or enter device serial number and tamper label if present. If device is matched proceed next device.

**Matching options**

Matching pattern \*  
Partial Match From Start

Matching length \*  
5

Padding pattern \*  
Pad on the left

Padding length \*  
1

Character \*  
0000000

Serial number (searching: 12345) \*  
123456789

Tamper label  
Tamper label

☐ Auto Activate device

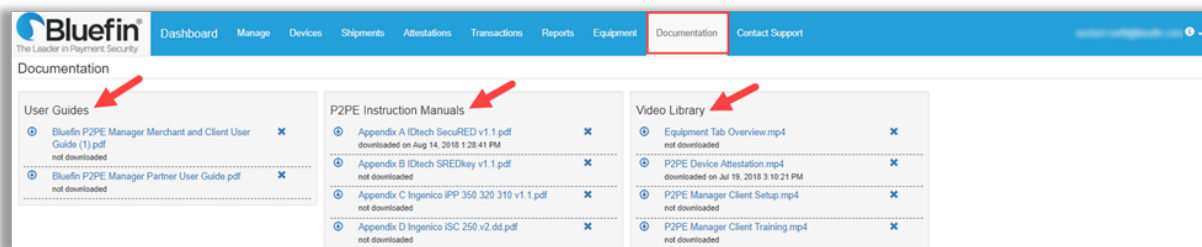
Progress

Close

6. Wait for the green success message. The device will be marked as **Received** and the progress bar will be completed.

## Accessing Online Help Documentation

Click the **Documentation** tab to access PDF files and videos.



## Downloading and Viewing PDF Files

To download the file, click the download icon to the left of the document name:

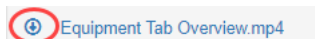


Depending on your browser, the file will automatically download to your local drive, or you will be prompted to **Open/Save** the file.

View the file from your local **Downloads** folder or depending on your browser, view it directly from the browser.

## Downloading and Viewing Video Files

To download a video, click the download icon to the left of the file name:



**NOTE:** Video file types are: .mp4 or .wav.

Depending on your browser, the video will automatically download to your local drive, or you will be prompted to **Open/Save** the file. (**NOTE:** Some browsers might have the option to **Save link as . . .** or **Save target as . . .** )

You can watch the video by launching the file from your local **Downloads** folder or depending on your browser, view it from the browser.

# Transactions

Transactions

A2Z Partner

Blue Surf Resorts

Select a location in the list or search it by name, address

Any

01/01/2020 00:00:00

05/29/2020 23:59:59

☐ Search based on UTC

Skip sorting (fast performance)

Apply

Click "Apply" button in order to get transactions

25 entries on page

Search:

CSV

Partner	Direct Partner	Client	Transaction Client ID	MID	Serial Number	Alternate Key	Device Name	Message ID	Reference	Method	# Encrypted	# Decrypted	Success	Completed Date	Virtual
No data available in table															

Previous

Next

You can run a transaction report to troubleshoot transaction problems or to verify that billing is correct.

The Transaction Summary lists transactions including encryption and decryption status.

To create this report, do the following:

1. Click the **Transactions** tab.
2. Select a **Location** from the drop-down list.
3. (Partner users only: Select partner name, client name, and location from the drop-down lists.)
4. Enter the date range.
5. Click **Apply**. The report will display.
6. Optional. Click a transaction to view report details.

**Related Information:** See [Exporting a Report](#).



# Reporting

## Creating the Chain of Custody Report

To generate a report that shows every device with a custodian affiliated with your organization, do the following:

1. Select **Reports > POI Chain of Custody Report**.  
(Point of Interaction = POI)

**Bluefin**  
The Leader in Payment Security

Dashboard Manage Devices Shipments Attestations Transactions **Reports** Equipment Opt Out Documentation Contact Support AaronCAdmin

Report  
**POI Chain of Custody**  
 Client Transaction Summary  
 Inventory Summary

**POI Chain of Custody Report**

Date From  Date To

<< All POIs >>  
 << All Custodians >>  
 Blue Surf Resort, Florida

Apply

PDF CSV

Model	Serial Number	Alternate Key	Date of Event	Location	Address	City	State / Province	Postal Code	Country	Custodian	Status
-------	---------------	---------------	---------------	----------	---------	------	------------------	-------------	---------	-----------	--------

2. Enter a date range, select a POI, custodian or location based on your preference.

Date From  08/01/2018 12:00:00 Date To  08/31/2018 12:00:00

<< All POIs >>  
 << All Custodians >>  
 << All Locations >>

Apply

3. Click **Apply**.

**Related Information:** See [Exporting a Report](#).

## Creating a Client Transaction Summary Report

**Bluefin**  
The Leader in Payment Security

Dashboard Manage Devices Shipments Attestations Transactions **Reports** Equipment Opt Out Documentation Contact Support

Report  
 POI Chain of Custody  
**Client Transaction Summary**  
 Inventory Summary  
 User Report  
 Device Activity  
 Device Receipt  
 Daily Report  
 Decryption Totals

**Client Transaction Summary**

Date From  Date To  ☐ Search based on UTC Apply

Search:  PDF CSV

Partner	Direct Partner	Client	Location	MID	Total Messages	Total Decrypt	3DES / CBC Good	3DES / ECB Good	BPS Good	RSA-2048 Good	AES-128 Good	3DES / CBC Bad	3DES / ECB Bad	BPS Bad	RSA-2048 Bad	AES-128 Bad	Total Device Validate
No data available in table																	

Showing 0 to 0 of 0 entries

To create this report, do the following:

1. Click the **Reports** tab.
2. Click **Client Transaction Summary** in the left column.
3. Enter the date range.
4. (Partner users only: Select partner from the drop-down list.)
5. Click **Apply**. The report will display.

## Creating the Inventory Summary Report

To generate a report that shows totals by device type and organization, do the following:

1. Click the **Reports** tab.
2. Click **Inventory Summary** in the left menu.
3. (Partner users only: Select partner and client from the drop-down lists.)
4. The report shows your inventory by device type (total number per device type) and by status (total number of devices by status):

Inventory By Type	
Device Type	Total
SecuRED	1
SREDKey	17
Showing 1 to 2 of 2 entries	
Inventory By Status	
Device Status	Total
Activated	12
Activating	5
Lost	1

**Related Information:** See [Exporting a Report](#).

## User Report

Select **Reports > User Report** to track user activity. The information displayed includes: user contact info, partner and client relationship, individual role, path and the user's active/inactive status.

## Device Activity Report

The Device Activity Report displays serial number, model (device type), device location, status, date/time of first use, date/time of last use and device custodian.

To create this report, click **Reports > Device Activity**.

Serial No.	Alternate Key	Model	Location	Partner	Status	MID	Address	Country	First Use	Custodian Name
WPC20202901686		WisePad 2	Kiljohn	A22 Partner	Activating		1234 big street, Atlanta, Georgia, 30338	US		
DeviceDelete		Augusta S	Blue Surf Resort, Florida	A22 Partner	In Transit		1234 Main St, Capliva, Florida, 33924	US		Suri Surfe
30360		PAX D210	Blue Surf Resort, North Carolina	A22 Partner	Activating		1212 Central St, Nags Head, North Carolina, 27959	US		Suri Surfe
30359		PAX D210	Blue Surf Resort, Florida	A22 Partner	Tampered		1234 Main St, Capliva, Florida, 33924	US		Suri Surfe
30358-20190925143308 CXFER		PAX D210	Blue Surf Resort, Florida	A22 Partner	Corp Transfer		1234 Main St, Capliva, Florida, 33924	US		AaronC Admin
30358-20190923161283 CXFER		PAX D210	Blue Surf Resort, North Carolina	A22 Partner	Corp Transfer		1212 Central St, Nags Head, North Carolina, 27959	US		ChrisC Custodian

**NOTE:** You can display All devices and then export the list for inventory purposes.

## Device Receipt

Select **Reports > Device Receipt**. The information displayed includes: your total device count, number of missed devices (count of devices that have not been checked in after the selected number of days) and date of last shipment.

## Daily Report

Select **Reports > Daily Report**. The information displayed includes: decryption requests for the specified time based on your preference.

## Daily Report

A2Z Partner  << Select Client >> Date From: 05/28/2020 12:00:00 Date To: 05/29/2020 12:00:00 ☐ Search based on UTC

Daily Report

25 entries on page

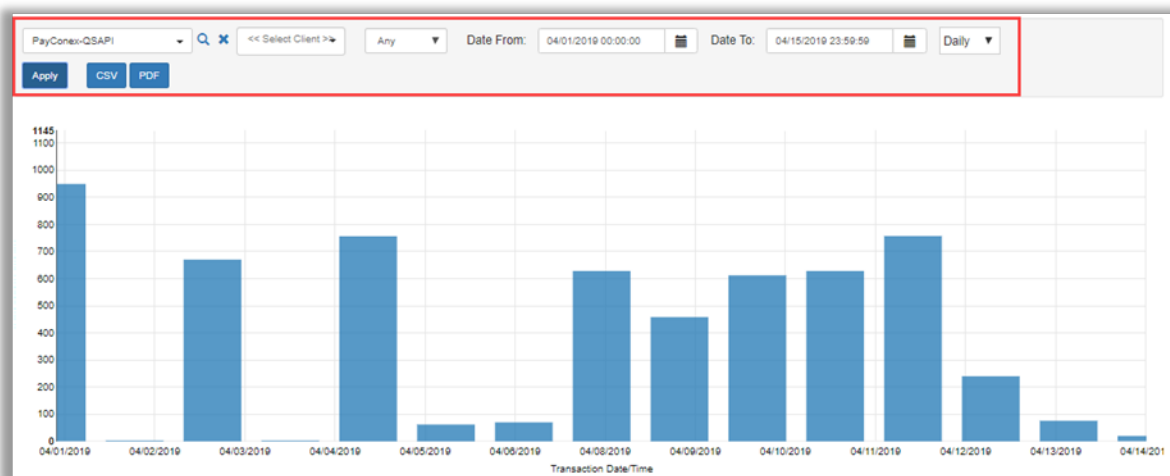
Search:

Client Name	Message ID	Reference	MID	Method	Encrypted	Decrypted	Success	Date	Virtual	Serial Number	Alternate Key	Device Name	Partner Name	Direct Partner Name
No data available in table														

Showing 0 to 0 of 0 entries

## Decryption Totals

You can use the Decryption Totals report to audit your monthly invoice.



Select **Reports > Decryption Totals**. The information displayed summarizes decryption totals in a bar chart. You can filter by type of decryption and specify a date range. This information is dynamic and based on the parameters set at the top of the page.

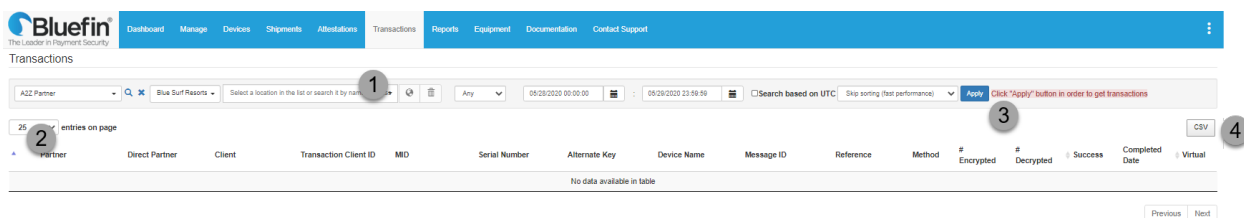
**TIP:** You can hover your mouse over a bar in the chart to see information at-a-glance.

Partner users only: Options display at the top to select partner / sub-partner and client.

## Exporting a Report

You can export report data to a **PDF** or **CSV** file from various tabs. Look for these options on the right side of the screen and above the column headings.

To export data, do the following:



1. Set the parameters at top of page based on your preference.
2. Set the number of entries based on your preference.  
**IMPORTANT:** Only the information displayed will be exported.
3. Click **Apply**.
4. Click **CSV** for a spreadsheet, or click **PDF** based on the options available. The report is automatically downloaded to your default local drive.

# Administration

**IMPORTANT:** Administrative functions from the **Manage** tab are restricted to Client Administrators.

Manage
<b>Users</b>
Locations
Device Transfer
System Notifications

## Managing Users

Select **Manage** and then click **Users** in the left column. A list of users displays.

Users

25 entries on page [Create](#) Search:  [CSV](#)

	First Name	Last Name	Email	Phone	User Name	Role
	AaronC	Admin	p2pemanagerusername@gmail.com	+1 800-675-6573	AaronCAdmin	Client Admin
	ChrisC	Custodian	p2pemanagerusername@gmail.com	+1 800-675-6573	ChrisCCustodian	Client Custodian
	Francis	Surfe	p2pemanagermerchantuser@gmail.com	+1 800-675-6573	Francis_BlueSurfResorts	Client Procurement
	Niel	Surfe	p2pemanagermerchantuser@gmail.com	+1 800-675-6573	Niel_bluesurfresorts	Client Custodian
	PatC	Procurement	p2pemanagerusername@gmail.com	+1 800-675-6573	PatCProcurement	Client Procurement
	Suri	Surfe	p2pemanagerusername@gmail.com	+1 800-675-6573	Suri_BlueSurfResorts	Client Admin
	UmaC	User	p2pemanagerusername@gmail.com	+1 800-675-6573	UmaCUser	Client User
	Your	Name	youremail@example.com	+1 800-675-6573	yourname	Client User

Use the filters at the top to sort the list by partner, client, and status.

## Adding a User

1. Select **Manage > Users** and then click **Create**.
2. Enter the user's information.

3. Check the **Active** check box.

4. Select a **Role**. Refer to [Appendix: User Roles](#).
5. Click **Send welcome email**. (The user will receive an email with a link to access the system. They will be prompted to update their password.)
6. Click **Save** when you're done.

## Updating a User

To update a user's information, click edit (the pencil icon) next to the appropriate name. Edit the fields as needed and click **Save** when you're done.

**NOTE:** To deactivate a user, deselect the **Active** checkbox.

## Resetting a User's Password

To reset a user's password, do the following:

1. Select **Manage > Users**.
2. Locate the user in the list and click **Edit**.
3. Select the checkbox next to **Send welcome email**. (The user will receive an email with a link to access the system. They will be prompted to update their password.)
4. Click **Save**.

**NOTE:** Users can also reset their own passwords from the login screen by clicking **Forgot password**.

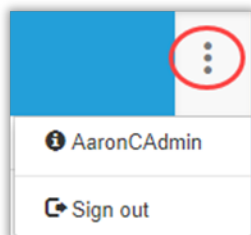
## Managing Your Personal Settings

Your Personal Settings include:

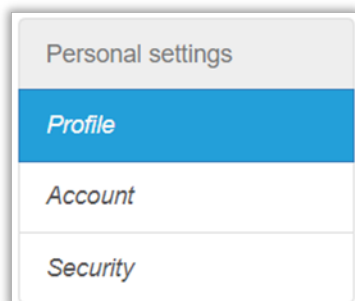
- Profile: Update your name, email address or your default login landing page (**NOTE:** Landing Page options are based on your user role.)
- Account: Update your password
- Security: Set up two-factor authentication

To access your personal settings, do the following:

1. In the top right corner, click the menu icon and select your name.



2. Select an option in the left column based on your preference.



3. Follow the prompts to update the information based on the option selected.



## Resetting Your Password (Forgotten Password)

If you forget your password, do the following:

1. From the login screen, enter your user name and then click **Forgot password**.

Portal Login

User Name \*

Password \*

2. Follow the prompts to reset your password.

## Adding Locations

You can use locations to “partition” a client. **Example:** Locations could be based on physical location (Atlanta Office, Chicago Office) or internal departments (Front Desk, Cafeteria, Gift Shop).

If a merchant wants location-based information to remain confidential, then separate clients should be created so users in one location cannot see information about another location.

**IMPORTANT:** Decisions about adding a location or creating a separate client do not have to consider whether a separate merchant ID or gateway ID is tied to these entities.

To add a location, do the following from the **Manage** tab:

1. Select **Locations** in the left column and then click **Create**.
2. Complete the information requested.

Field	Description
<b>Partner</b>	Required
<b>Client</b>	Required
<b>Location Type</b>	Required. Select an option from the drop-down list.
<b>Location Name</b>	Required. Enter a name for the location to easily identify it. This name will be used in reports.
<b>Name of Business</b>	Optional
<b>Address</b>	Required. Street address, City, Postal code, Country, State Province

Field	Description
Mail Address	Optional
Contact Person	Required. Enter First Name, Last Name, Email, Phone  <b>NOTE:</b> The contact person does <u>not</u> have to be the device custodian.

3. Check **Active** to enable the location.
4. Click **Save** when you're done.

## Removing Locations

To remove a location, click the edit icon next to the location of your choice and then **deselect Active**. Click **Save** when you're done.







## Editing Locations

To edit a location, click the edit icon next to the location of your choice and then make your changes. Click **Save** when you're done.

## Device Management

Click the **Devices** tab to see a summary of devices including serial number, name, device type, device state, client, location, activation date, MID, virtual, and notes. To search for a device, enter your search criteria in the Search field and then click **Search**.

**NOTE:** Shared devices display with a “sharing” icon: 

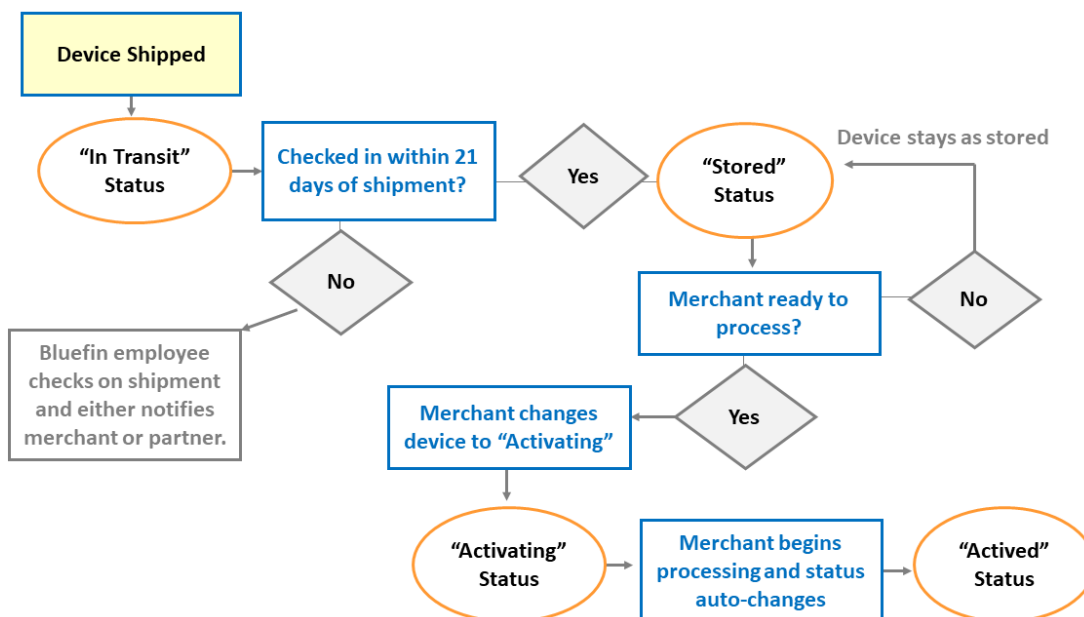
Devices										
<div> <div>AZZ Partner</div> <div>Blue Surf Resorts</div> <div>&lt;&lt; Any State &gt;&gt;</div> <div>Apply</div> <div>Click "Apply" button in order to get devices</div> </div>										
<div> <div>25 entries on page</div> <div>Search: <input type="text"/></div> <div>Search</div> <div>CSV</div> </div>										
Serial Number	Alternate Key	Name	Device Type	Device State	Client Name	Location Name	Activation Date	Mid	Virtual	Notes
 000030350		Registration	PAX S300	Activating	Blue Surf Resorts	Blue Surf Resort: Florida			No	
 000030351		Restaurant	PAX D210	Activating	Blue Surf Resorts	Blue Surf Resort: Florida			No	
 000030352			PAX S500	In Transit	Blue Surf Resorts	Blue Surf Resort: North Carolina			No	
 000030353			PAX S500	Injected	Blue Surf Resorts	KIF			No	
 000030354			PAX S500	Stored	Blue Surf Resorts	Blue Surf Resort: North Carolina			No	
 000030355			PAX S500	Injected	Blue Surf Resorts	KIF			No	

You can filter the list by device state: Any State, Active States (default), or Non Active States.



## Device Activation Process Flow

The following diagram describes the device activation flow.



## Updating Devices

From the **Devices** tab, click **Edit** (pencil icon) next to the device you want to update.

The following fields can be updated. Click **Save** when you're done.

Field	Description
<b>Name</b>	<p>Enter a short name that allow you to easily identify the device.</p> <p><b>Example:</b> "Lisa's desk", "Register 10", or "front desk."</p> <p><b>TIP:</b> Device names do not affect processing.</p>
<b>Device State</b>	<p>Select an option from the drop-down list.</p> <div> <div>&lt;&lt; Change Device State &gt;&gt;</div> <div>           Damaged            Retired            Tampered            Malfunctioning            Lost            RMA            Stored         </div> </div> <p>See <b>Device State Definitions</b> below for additional details.</p>
<b>Attestation Period</b>	Refer to <a href="#">Changing Device Attestation Date</a> for details.
<b>Audit Next Date</b>	Select a date for device inspections. Refer to <a href="#">Changing</a>

	<a href="#">Device Attestation Date</a> for details.
--	--

**Related Information:** For instructions for activating a brand-new device, see [Batch Receiving Devices](#).

## Device State Definitions

The following is a summary of all device states. For more details about device status and the impact of making various updates, refer to the P2PE Instruction Manuals (PIM). (Click **Documentation** and download a manual or an appendix as needed.)

STATE	CAN PROCESS?	DEFINITION
<b>Activated</b> (Automatic)	YES	Device is in hands of merchant and processing of cards has begun (state change from "activating" to "active" occurs automatically.)  <b>NOTE:</b> In <u>Branded</u> versions of P2PE Manager, if <b>Allow External Device Activation Mode</b> is enabled by the system administrator, then system users, partner supervisors and client administrators can change a device's state to <b>Activated</b> manually and via batch upload.
<b>Activating</b>	YES	Device is in hands of merchant and ready to begin processing cards
<b>Damaged</b>	NO	Unit is inoperable due to physical damage.
<b>Destroyed</b>	NO	Unit is inoperable and cannot be recovered. <b>NOTE:</b> System admins and users only.
<b>DOA by KIF</b>	NO	Device needs to be removed from service for destruction. <b>NOTE:</b> Key Injection Facility (KIF) use only.
<b>In Repair</b>	NO	Device needs to be removed from service for repair.
<b>In Transit</b> (Automatic)	NO	Device has been shipped to the merchant. <b>NOTE:</b> KIF use only.
<b>Injected</b>	NO	Encryption key has been injected into the unit. <b>NOTE:</b> KIF use only.
<b>KIF Test</b>	NO	Used by the KIF to do an end-to-end test prior to shipping. <b>NOTE:</b> KIF use only.
<b>Lost</b>	NO	Merchant does not know where device is.
<b>Malfunctioning</b>	NO	Unit is inoperable or inconsistently operable for unknown reasons.  The state is automatically triggered when the system detects 10 consecutive decryption failures. Additionally,

		an email alert is sent to the device custodian so they can address this issue with Bluefin or their service provider.
<b>Quarantined (by KIF)</b>	NO	Unit was discovered to be malfunctioning or was tampered with prior to shipping. (Unit was returned to KIF outside of the RMA process.)  <b>NOTE:</b> System admins and System users only.
<b>Retired</b>	NO	Merchant no longer wishes to use a device. If the merchant closes their Bluefin account, all devices will be marked as retired.
<b>RMA</b> <b>Return Merchandise Authorization</b>	NO	Device needs to be returned to the KIF.  <b>NOTE:</b> Use caution when selecting this state because it is <u>not</u> reversible.  KIF will send return instructions to the merchant to retrieve device that is not working correctly.  <b>Related Information:</b> "Return Merchandise Authorization Process" on the next page
<b>Stored</b>	NO	Device is in possession of merchant and stored in a secure location, but not ready to begin processing cards.
<b>Tampered</b>	NO	If a merchant believes that a device was tampered with, they must put the device in this state. Contact your relationship manager or Bluefin Support for next steps.
<b>Unassigned</b>	NO	Unit is injected and held by KIF.

## Viewing Device Details

### Chain of Custody

From the **Devices** tab, click **Edit** (pencil icon ) next to the device you want to review.

Click the **chain of custody** tab. It will display all custodians who were responsible for the device.

**NOTE:** User names display with a hyperlink, so you can see their contact information.

Details

Chain Of Custody

History

Lifecycle

Inspections

Create

Return

	Create Date	Created By	Transfer Method	Custodian	Complete Date	Status
	02/11/2016 2:20 PM	TE SPENCER	Manual	John Smith		Not Completed
	02/11/2016 11:36 AM	TE SPENCER	Initial	David Harris	02/11/2016	Received

## Device State History

From the **Devices** tab, click **Edit** (pencil icon ) next to the device you want to review.

Click the **History** tab. The device will be listed along with dates when the status changed.

**NOTE:** User names display with a hyperlink, so you can see their contact information.

Details	Chain Of Custody	History	Lifecycle	Inspections
---------	------------------	---------	-----------	-------------

Return				PDF	CSV
User	* Date	Device State	Notes		
	09/06/2018 11:34 AM	Injected			
Surf Surfe	09/06/2018 12:53 PM	In Transit			
Francis Surfe	09/06/2018 1:06 PM	Stored			

## Lifecycle Report - Detailed Device History

From the **Devices** tab, click **Edit** (pencil icon) next to the device you want to review.

Click the **Lifecycle** tab. The device will be listed along with dates when the device status changed as well as the location and custodian.

**NOTE:** User names display with a hyperlink, so you can see their contact information.

Details	Chain Of Custody	History	Lifecycle	Inspections
---------	------------------	---------	-----------	-------------

Serial: 000030350	KIF: ACKIF	Device Type: PAX S300
-------------------	------------	-----------------------

Return							PDF	CSV
Action	* Date	Created By	Device State	Custodian	Location	Shipment	Notes	
Change Custody	08/30/2018 3:58 PM		Injected		KIF			
Change State	09/06/2018 11:34 AM		Injected					
Change Custody	09/06/2018 11:34 AM		In Transit	Surf Surfe (Custody Status: Received)	Blue Surf Resort Florida	Tracking #: 100 (FedEx) Shipped on: 09/05/18 04:00 Received on: 09/06/18 04:53 Received by: Surf Surfe		
Change State	09/06/2018 12:53 PM	Surf Surfe	In Transit					
Change State	09/06/2018 1:06 PM	Francis Surfe	Stored					
Change Custody	09/06/2018 1:53 PM	Francis Surfe		Francis Surfe (Custody Status: Received)	Blue Surf Resort Florida		Device received and I will take custody of it.	
Current State	05/28/2020 3:58 PM	AaronC Admin	Activating	Francis Surfe (Custody Status: Received)	Blue Surf Resort Florida			

## Return Merchandise Authorization Process

**IMPORTANT:** The Return Merchandise Authorization (RMA) is an irreversible step!

If you discover that your device is malfunctioning or suspect it has been tampered with, contact your relationship manager or contact Bluefin Support.

Based on their guidance, if you are advised to return the device, do the following from the **Devices** tab:

1. Select your **Partner Account** and choose **Client** if applicable.
2. Click **Edit** (pencil icon) next to the device.

3. Change **Device State** to RMA.

**NOTE:** A device can only be moved to RMA after it's been received.

### IMPORTANT:

- When the device status is **RMA**, it will not process transactions.
- The device serial number will automatically be appended to include the date.

### EXAMPLE:

#### Devices

Serial Number	Alternate Key	Name	Device Type	Device State
111111111111:20200605194919:RMA	999999999999:20200605194919:RMA	Augusta S		RMA

Showing 1 to 1 of 1 entries (filtered from 5 total entries)

## Checking on Device Shipment and Tracking

**NOTE:** You will not see the device in P2PE Manager until the KIF injects the device and uploads it to P2PE Manager.

Below are instructions for viewing device status before and after it's shipped.

### Checking Tracking Number

Access the **Shipments** tab. If your device has been shipped, it will be listed along with the tracking number which you can use at the carrier's website to track the shipment.



In-coming Shipments

All

25 entries on page

Search:

Client	Carrier	Tracking	Date Shipped	Date Received
Blue Surf Resorts	FedEx	12345	11/28/2018 3:45 PM	
Blue Surf Resorts	FedEx	1051029	10/29/2018 12:00 PM	
Blue Surf Resorts	FedEx	1021019	10/18/2018 12:00 PM	10/19/2018 12:47 PM

## Checking Device Status

**NOTE:** Depending on how your organization was setup, you may or may not have access to the **Equipment** tab. (If you do not have access to the Equipment tab, check your email for updates or contact Bluefin Support.)

If there is no tracking number, do the following:

1. Select the **Equipment** tab
2. If the device is listed, that means that the order has been successfully placed.  
**NOTE:** If the device is not listed, and depending on how your order was placed, the device will display just before it is shipped.

### Equipment Requests

Apply

25 entries on page

Create

Search:

Request ID	Status	Client	Location	KIF	Device Type	Submit Date	Processed Date
245	Pending	Blue Surf Resorts	Blue Surf Resorts Corporate Headquarters		PAX A920		

3. Select the **Devices** tab.
4. Locate the device. If the **Device State = Injected**, the key has been injected and it will ship shortly.  
**NOTE:** If the device is not listed and the device was ordered more than five business days ago, please contact Bluefin.

### Devices

<< Any State >> Apply Click "Apply" button in order to get devices

25 entries on page

Search:

Serial Number	Alternate Key	Name	Device Type	Device State	Client Name	Location Name	Activation Date	Mid	Virtual	Notes
000030350		Registration	PAX S300	Activating	Blue Surf Resorts	Blue Surf Resort, Florida			No	
000030351		Restaurant	PAX D210	Activating	Blue Surf Resorts	Blue Surf Resort, Florida			No	
000030354			PAX S500	Stored	Blue Surf Resorts	Blue Surf Resort, North Carolina			No	
000030356			PAX A80	Activating	Blue Surf Resorts	Blue Surf Resort, North Carolina			No	

## Checking Order Status

**NOTE:** If the device is not listed, that doesn't mean that your order was not successfully placed. Depending on how your order was placed, it may not show up here.

1. Select the **Equipment** tab.
2. Refer to the **Status** section.

INITIAL: Order was successfully submitted.

PENDING: Someone at key injection facility has been assigned the order and is working on it.

COMPLETED: Order has been shipped.

## Transferring a Device between Custodians or Locations

**IMPORTANT:** These instructions only apply to active functioning devices. (If a device is retired, lost, or stolen, these steps do not apply.) Additionally, this option is restricted to Client Administrators and Client Custodians.

You can transfer a device to a different location if the device is moved. **EXAMPLE:** A device is moved from the "Chicago Office" to the "San Francisco Office."

You can also transfer a device's custodian from one person to another. **EXAMPLE:** A custodian changes job roles within the organization and is no longer overseeing device compliance. Or, the custodian is no longer employed by the organization.

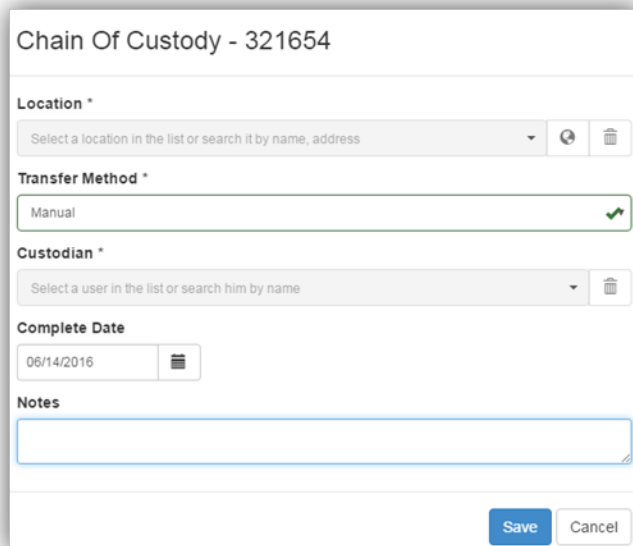
To transfer a device, do the following from the **Devices** tab:

1. Click **Edit** (pencil icon) next to the device you would like to transfer.
2. Click the **Chain Of Custody** tab and then click **Create**.
3. Complete fields and click **Save**.

Transfer Method:

- a. Choose Manual if device is handed off or if someone else taking responsibility for the device.

- b. Choose Shipment if device is being mailed from one location or custodian to another. Complete additional fields when prompted.



Chain Of Custody - 321654

**Location \***  
Select a location in the list or search it by name, address

**Transfer Method \***  
Manual

**Custodian \***  
Select a user in the list or search him by name

**Complete Date**  
06/14/2016

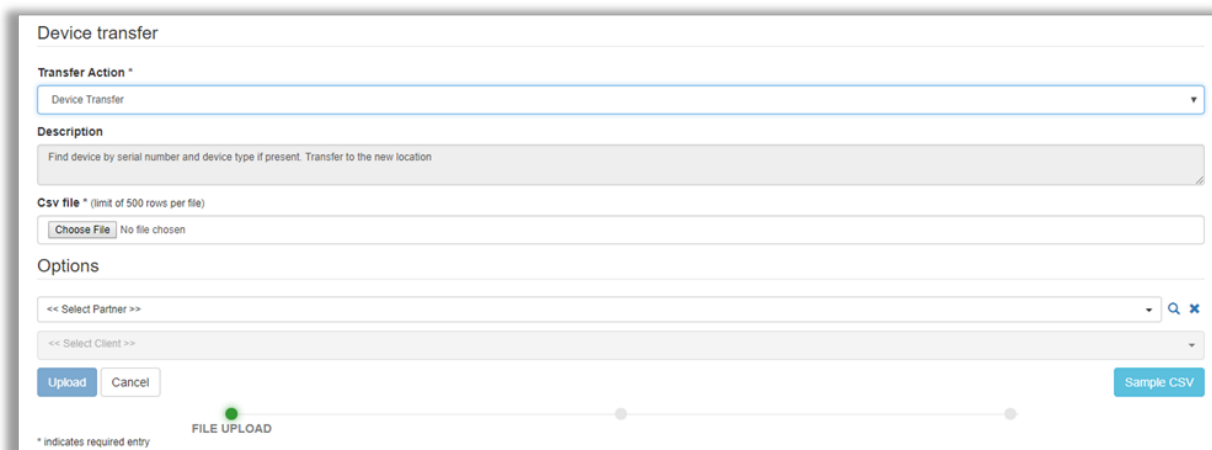
**Notes**

Save Cancel

## Transferring Multiple Device Locations

**IMPORTANT:** This functionality is restricted to following user roles: Client Administrators and all Partner roles.

You can use **Device Transfer** to move devices in bulk from one Location record to another Location under the same Partner and Client record.



Device transfer

**Transfer Action \***  
Device Transfer

**Description**  
Find device by serial number and device type if present. Transfer to the new location

**Csv file \*** (limit of 500 rows per file)  
Choose File No file chosen

**Options**  
<< Select Partner >>  
<< Select Client >>

Upload Cancel Sample CSV

FILE UPLOAD

\* indicates required entry

### Prerequisite:

Create a CSV file with the following column headings: **Serial Number, Location and Device Type**.

**TIP:** From **Manage > Device Transfer** you can download a Sample CSV.

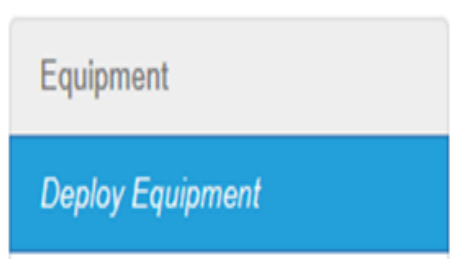
	A	B	C
1	<b>SerialNumber</b>	<b>Location</b>	<b>DeviceType</b>
2	123AD33377	Company Location 1	SREDKey
3			

To transfer devices to another location under the same Partner and Client record, do the following from the **Manage** tab:

1. Select **Device Transfer** in the left column.
2. Required. Click **Choose File** and navigate to your CSV file.
3. (Partners Users only: Select the **Partner** and **Client** from the drop-down lists.)
4. Click **Upload** when you're done.

**NOTE:** If devices were not successfully transferred, hover your mouse over the **Warning** sign for an error description.

## Equipment



During the account setup process, you will order equipment directly with your sales representative.

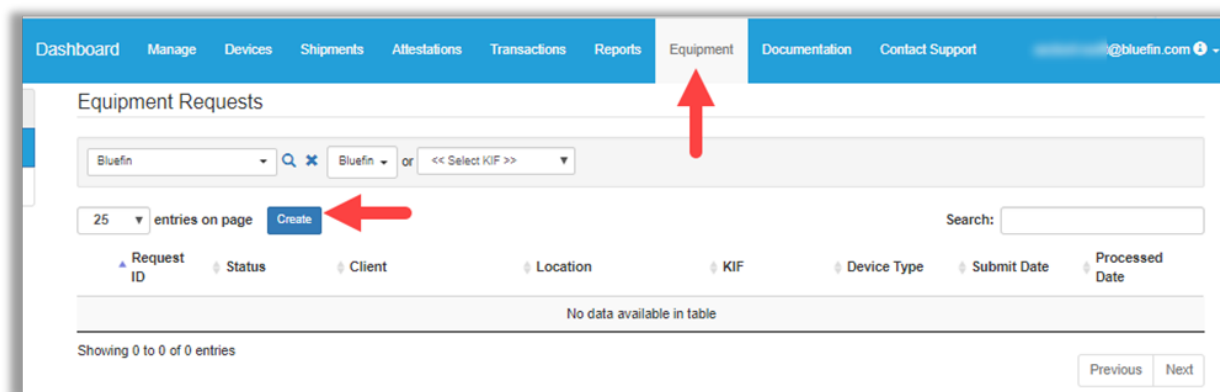
## Deploying Equipment

**IMPORTANT:** "Deploying Equipment" refers only to placing an order to send additional equipment to your location(s). This option is restricted to Partners, Client Administrators and Client Procurement.

All device orders must be tracked in P2PE Manager to properly track chain of custody.

Depending on how your organization was setup, you may or may not have access to the **Equipment** tab. (If you do not have access to the Equipment tab, check your email for updates or contact Bluefin Support.)

1. Navigate to **Equipment > Deploy Equipment** and then click **Create**.



2. Complete the Deployment request as noted below.

Field	Description
<b>Partner</b>	(Partners Users only: Select the Partner from the drop-down lists.)
<b>Client</b>	(Partners Users only: Select the Client from the drop-down lists.)
<b>Location</b>	Required. <b>TIP:</b> If sending to a new location, add the location <u>before</u> placing order. Refer to <a href="#">Adding Locations</a> .
<b>Contact</b>	Required.
<b>Device Type</b>	Required. <b>IMPORTANT:</b> All Bluefin equipment is listed as an option but keep in mind that this equipment may or may <u>not</u> be compatible with your specific processing solution.
<b>Quantity</b>	Required.
<b>Client Order #</b>	Optional. Enter the Client Order # if applicable. It will be included in the Bluefin invoice.
<b>Client PO #</b>	Optional. Enter the Client PO# if applicable. It will be included in the Bluefin invoice.
<b>Client RA #</b>	Not applicable.
<b>Bluefin Order #</b>	Not Applicable. (These fields are automatically generated.)
<b>Bluefin PO #</b>	
<b>Bluefin RA #</b>	
<b>Submit Date</b>	(These fields are automatically generated.)
<b>Processed Date</b>	
<b>Notes</b>	Required. Notes are submitted to the KIF for processing.

Field	Description
	<p><b>IMPORTANT:</b> Use the <b>Notes</b> field to document special data packages, specific configuration requests (RBA #) or debit keys, and so forth, that must be injected into the device.</p> <p><b>EXAMPLE:</b> RBA 22; Chase - PIN/Debit key</p>

3. Click **Save** to save your work and finish later. Click **Submit** when you're ready to submit the order for processing.

## Opt Out of Bluefin Program

**IMPORTANT:** This option is restricted to Client Administrators and does not apply to Partners.

Bluefin®  
The Leader in Payment Security

Dashboard Manage Devices Shipments Attestations Transactions Reports Equipment Opt Out Documentation Contact Support

Opt Out - Blue Surf Resorts

☐ I acknowledge I have read associated opt out documentation, and I'm authorized to agree to the terms of this opt out agreement.

Opt Out Cancel

\* indicates required entry

**Opting Out** retires all devices in your account so they cannot conduct transactions.

1. Access the **Opt Out** tab.
2. **Check** the acknowledgement check box and click **Opt Out**. An email alert is automatically sent to Bluefin Services.

**NOTE:** **Opt Out** will not entirely cancel your Bluefin account. To cancel, you will also need to contact Bluefin to notify us and receive additional cancellation instructions (varies depending on account configuration and setup). Refer to [Contacting Support](#).

# Device Inspections and Attestations

PCI Compliance requires that merchants using a P2PE solution inspect their devices for tampering at least once per year. P2PE Manager makes these inspections easy to complete.

## Inspecting a Device

Download the P2PE Instruction Manual (PIM) from the **Documentation** tab to see device-specific inspection instructions.

Per the PCI council, a device inspection should accomplish the following:

- Determine that device has not been stolen
- Determine that device has not been tampered with
- Determine that device has not been removed and replaced with a counterfeit device

## Inspections Report: Viewing Details of Past Inspections



PCI Compliance Regulations for Point-to-Point Encryption mandate that devices are inspected annually.

Follow the instructions below to view reports of past inspections of the device.

1. From the **Devices** tab, click **Edit** (pencil icon) next to the device you want to review.
2. Click the **Inspections** tab to see details of past inspections.

**NOTE:** User names display with a hyperlink, so you can see their contact inform-

ation.

Device details - 123456789						
Details	Chain Of Custody	History	Lifecycle	Inspections		
Return				CSV	PDF	
Attestation Name	Serial Number	Complete Date	Photo	Contact	Notes	
Inspection	123456789	05/31/2016 6:49 AM		*Client Admin	Device casing, interfaces, and connections inspected. S/N verified.	
20APR16	81152346	04/20/2016 8:28 PM		Tim Tester	Test Device Inspection	
wefe	AN_SV_1	04/20/2016 8:33 PM	-	Tim Tester	werwerqer	

Bluefin Payment Systems © 2016

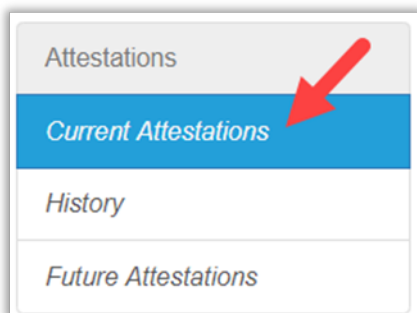
**Related Information:** For instructions to conduct and log an inspection, see **Device Attestations** below.

## Device Attestations

Shortly before a device needs to be inspected and attested to, you will receive an email notification. (The email includes device serial number and location.) Additionally, a notification displays on the dashboard.

Inventory devices			
Serial Number	Alternate Key	Device State	Audit Next Date
AN_SV_2		Assigned	09/20/2016 12:00 AM

1. Click the **Attestations** tab.
2. Select **CurrentAttestations** in the left column.





3. Select the **checkbox** next to the device(s).

Current Attestations

Device attestation should be performed in groups of not more than 500 at a time.

25 entries on page

<input type="checkbox"/>	Serial Number	Alternate Key
<input checked="" type="checkbox"/>	30359	

Showing 1 to 1 of 1 entries

Create Attestation

**NOTE:** To select all devices, click the check box above the list of devices. You can select up to 500 devices and perform attestations on the selection as a group.

☒ Serial Number

<input checked="" type="checkbox"/>	30359	
-------------------------------------	-------	--

Showing 1 to 1 of 1 entries

Create Attestation

4. Click **Create Attestation**.
5. Inspect the device(s), provide the information requested and select the agreement checkbox.

Create Attestation

Name \*

annual 2016

Notes

I have thoroughly inspected the device and determined that it has indeed not been tampered with.

Photos

An\_SV\_2 Choose File No file chosen

☒ I acknowledge I have read associated attestation document, and I'm liable the terms of the attestation agreement.

Save Cancel

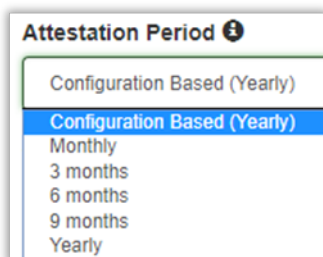
\* indicates required entry

- Optional: Based on your preference, you can upload one image. Click **Choose File** and then navigate your network to select the image file.  
**NOTE:** The following file types can be selected: .jpg, .jpeg, .png. (Maximum file size = 25 MB)
- Click **Save** when you're done.

## Changing Device Attestation Date

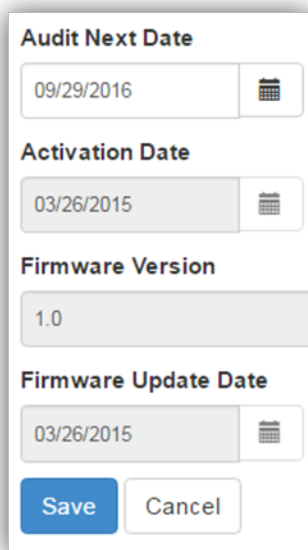
PCI standards indicate a device should be inspected at least once per year, but some merchants choose to inspect devices more often. Other merchants do inspections once per year but will adjust initial inspection dates to make sure that inspections of all devices are done on the same day.

- Select the **Devices** tab. All devices will be listed.
- Click **Edit** (pencil icon) next to the device you want to edit.
- You can set the attestation period frequency by selecting from a list of options. Based on your selection, the system will prompt you to perform the attestation.



A dropdown menu titled "Attestation Period" with a help icon. The menu is open, showing a list of options: "Configuration Based (Yearly)" (highlighted in blue), "Monthly", "3 months", "6 months", "9 months", and "Yearly".

- Optional. Update the **Audit Next Date** based on your preference and click **Save** when you're done.



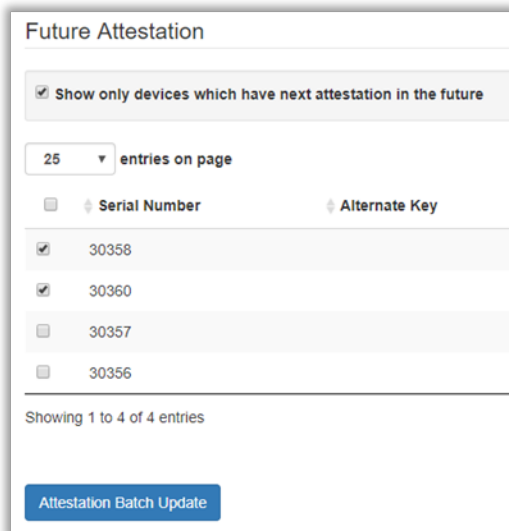
A form titled "Audit Next Date" with four sections: "Audit Next Date" (09/29/2016), "Activation Date" (03/26/2015), "Firmware Version" (1.0), and "Firmware Update Date" (03/26/2015). Each date field has a calendar icon. At the bottom are "Save" and "Cancel" buttons.

## Batch Process: Change Device Attestation Date

You can change the device attestation date for a group of devices (up to 500) from the **Future Attestation** list.

1. Select the devices and then click **Attestation Batch Update**.

**NOTE:** You can select up to 500 devices.



Future Attestation

☒ Show only devices which have next attestation in the future

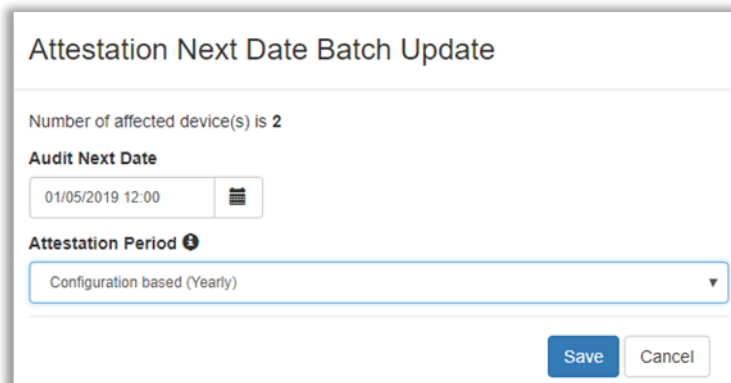
25 entries on page

<input type="checkbox"/>	Serial Number	Alternate Key
<input checked="" type="checkbox"/>	30358	
<input checked="" type="checkbox"/>	30360	
<input type="checkbox"/>	30357	
<input type="checkbox"/>	30356	

Showing 1 to 4 of 4 entries

Attestation Batch Update

2. Update the information as appropriate for **Audit Next Date** and **Attestation Period**.



Attestation Next Date Batch Update

Number of affected device(s) is 2

**Audit Next Date**

01/05/2019 12:00

**Attestation Period**

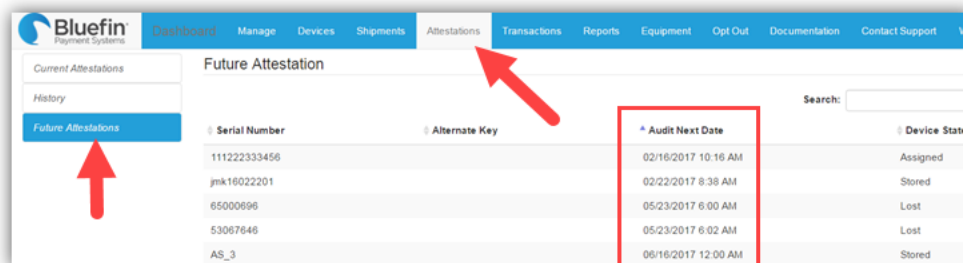
Configuration based (Yearly)

Save Cancel

3. Click **Save** when you're done.

## Viewing Future Scheduled Attestations

1. Navigate to the **Attestations** tab
2. Click **Future Attestations** in the left column.



Serial Number	Alternate Key	Audit Next Date	Device State
11122333456		02/16/2017 10:16 AM	Assigned
jmk16022201		02/22/2017 8:38 AM	Stored
65000696		05/23/2017 6:00 AM	Lost
53067646		05/23/2017 6:02 AM	Lost
AS_3		06/16/2017 12:00 AM	Stored

3. Review the **Audit Next Date** for the next date the device is scheduled to be audited.

## Device Tampering Detection

Bluefin's P2PE devices have three mechanisms to detect tampering, each outlined below. The one that is triggered depends on the method of tampering that was utilized by the attempted data thief. For security reasons, the activities that trigger each of these mechanisms are omitted.

- If the device detects tampering at the time that it is tampered with, it will lose transaction processing ability and display **tamper** on the screen. If this happens there is no way to remotely reactivate the device and you will need to coordinate with Bluefin to replace it.
- If the device does **not** detect tampering at the time (which may be the case with external tampering), it will detect changes in the submitted data string and display **quarantine** within P2PE manager. The screen may look the same, but transaction processing ability will be deactivated. If this happens, please contact Bluefin.
- The device may suspect tampering by certain processing attempt patterns that are consistent with data thief testing. If these patterns are detected the device will display **quarantine** within P2PE manager. The screen may look the same, but transaction processing ability will be deactivated. If this happens, please contact Bluefin.

## Appendix: User Roles

### Client / Merchant Roles

	Client Admin	Client Custodian	Client Procurement	Client User
<b>Devices</b>	Manage	Manage	Manage	View
<b>Shipments</b>	Manage	Manage	View	View
<b>Attestations</b>	Conduct	Conduct	Conduct	Conduct
<b>Encrypted Transactions</b>	View	(No Access)	(No Access)	View
<b>Reports</b>	Yes	Yes	Yes	Yes
<b>Equipment</b>	Yes	(No Access)	Yes	(No Access)
<b>Users</b>	Manage	(No Access)	(No Access)	(No Access)
<b>Locations</b>	Manage	(No Access)	(No Access)	(No Access)
<b>Device Transfer</b>	Manage	(No Access)	(No Access)	(No Access)

### Partner Roles

	Partner Supervisor	Partner Fulfillment	Partner User
<b>Devices</b>	Manage	Manage	Manage
<b>Shipments</b>	Manage	Manage	(No Access)
<b>Attestations</b>	Conduct	Conduct	Conduct
<b>Encrypted Transactions</b>	View	View	View
<b>Reports</b>	Yes	Yes	Yes
<b>Equipment</b>	Yes	Yes	Yes
<b>Users</b>	Manage	(No Access)	Manage
<b>Locations</b>	Manage	(No Access)	Manage
<b>Device Transfer</b>	Manage	(No Access)	Manage
<b>Partners</b>	Manage	(No Access)	Manage
<b>Clients</b>	Manage	(No Access)	Manage
<b>Import Clients</b>	Yes	(No Access)	Yes

## Appendix: Receiving and Activating Your Device

You will receive your device in the mail.



**IMPORTANT:** You must complete each of the steps below before you can use your device!

**Inspect** your device and verify that the secure bag is sealed closed and tamper free. If the device has been tampered with, follow the steps for ***Tampered Device*** below.

!! Do not open the secure bag on your device until you are ready to perform the following steps.

### Overview

**Step 1.** Access the Point-to-Point Encryption (P2PE) Manager Online. (<https://bluefin.p2pe-manager.com/login>)

**Step 2.** Log Receipt of the Shipment (serial number and associated security seal number) in the P2PE Manager online.

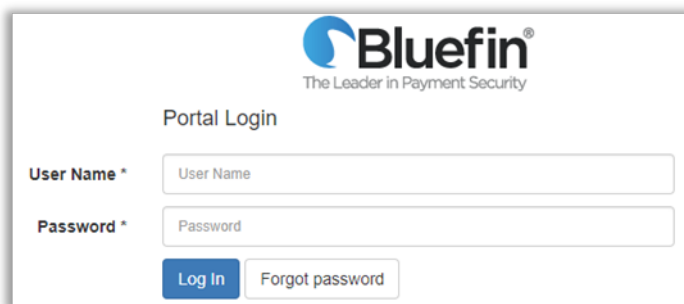
**Step 3.** Activate Your Device.

### Step 1. Access the P2PE Manager Online

To log into P2PE Manager, do the following:

1. Access the P2PE Manager from a browser: [P2PE Manager](https://bluefin.p2pe-manager.com/login) (<https://bluefin.p2pe-manager.com/login>)
2. Enter your login credentials. Customize your password if you haven't already done so.

**TIP:** Refer to your email for system credentials. (The email was sent from "no-reply@p2pemanager.com" and the subject line is: "Welcome to Bluefin's P2PE Manager!")



**Bluefin®**  
The Leader in Payment Security

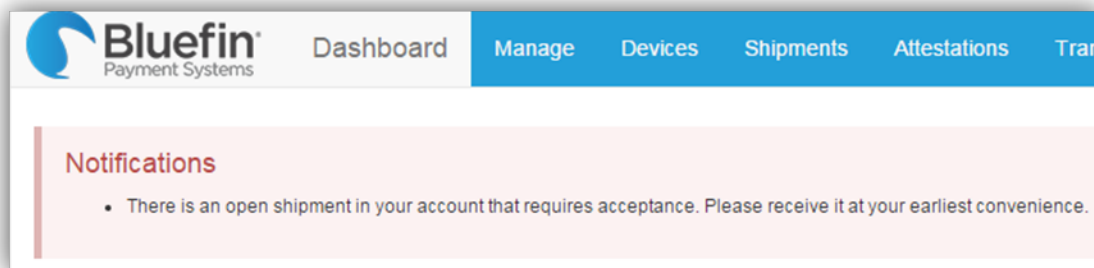
Portal Login

User Name \*

Password \*

## Step 2: Log Receipt of the Shipment

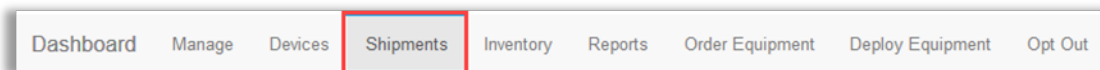
From your dashboard / home screen, you'll see a notification that there is an open shipment:




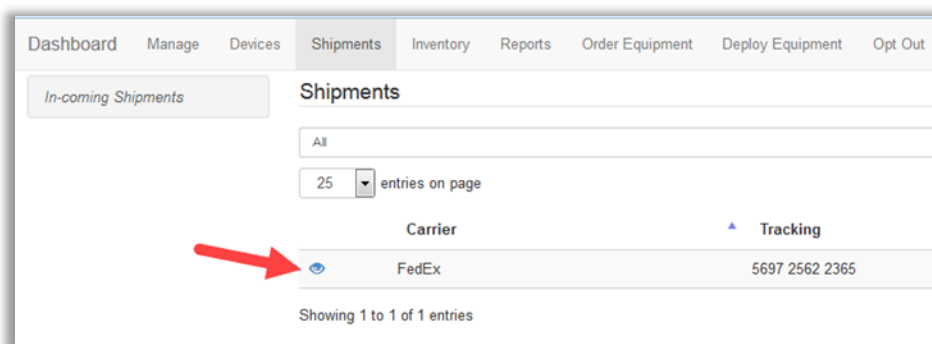
To log receipt of your shipment, do the following:

Optional: To **Batch Receive** the devices in a shipment, refer to [Batch Receiving Devices](#).

1. Click the **Shipments** tab. Here you'll see all shipments sent to you from Bluefin.

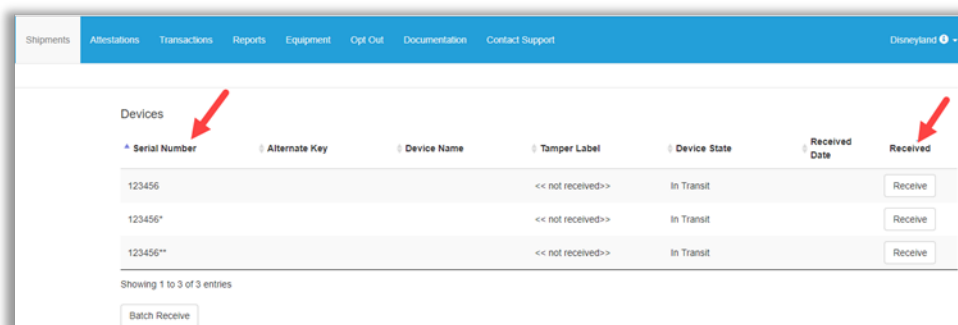


2. To document that you received the shipment, click the **View** icon (  ) next to the appropriate item.



- Match the serial number on the back of your device with the serial number displayed online and then click **Receive**. Perform steps 3 & 4 for each device you receive.

**IMPORTANT:** To read the serial number, open the secure bag and save the bag. Remember, the secure bag should be sealed closed and tamper free. (For your own reference, take a picture of the security seal with your smart phone.)



- From the secure packing around your device, locate the **security seal number** and enter it into the **Tamper label** field. Then click **Receive**.  
**NOTE:** The serial number is populated for you based on the device you selected in #3 above.



Receiving device 000030354

Serial number \*

000030354

Tamper label

303541015

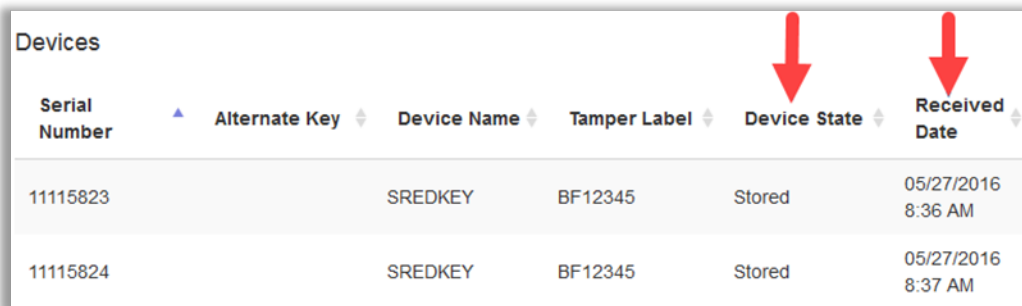
☒ Auto Activate device

Receive Cancel

- Optional: Click **Auto Activate device** only if you are ready to activate and start using the device now.  
**TIP:** To take advantage of this time saving option, you must select it before entering the device serial number and tamper label.



- Click **Receive**. Notice that the **Device State** and **Received Date** fields are updated.



The screenshot shows a table titled "Devices" with columns: Serial Number, Alternate Key, Device Name, Tamper Label, Device State, and Received Date. Two red arrows point to the "Device State" and "Received Date" columns. The table contains two rows of data.

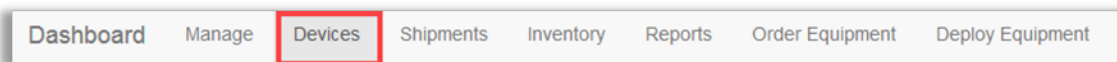
Serial Number	Alternate Key	Device Name	Tamper Label	Device State	Received Date
11115823		SREDKEY	BF12345	Stored	05/27/2016 8:36 AM
11115824		SREDKEY	BF12345	Stored	05/27/2016 8:37 AM


## Step 3: Activate Your Device

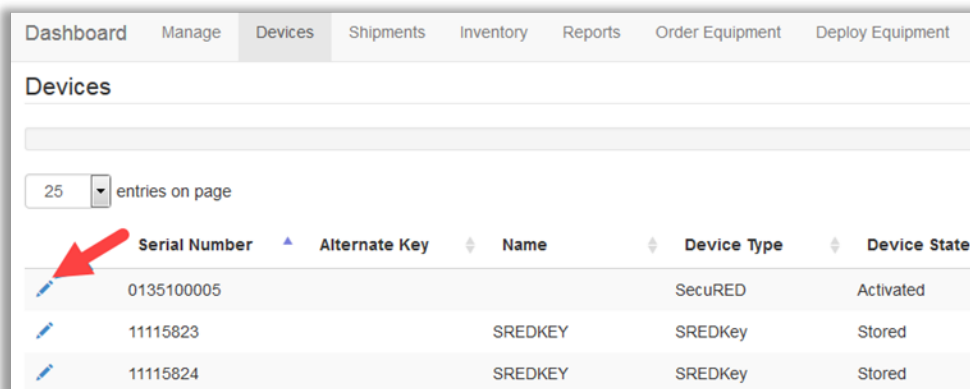
**NOTE:** If you selected **Auto Activate device**, you can skip this step.

To activate your device, do the following:

- Click the **Devices** tab. Here you'll see all your devices.



- Click the **Edit** icon (  ) next to the device you want to activate.



The screenshot shows the "Devices" tab selected in the navigation bar. Below the tabs is a "Devices" section with a search bar and a dropdown menu set to "25 entries on page". The table below has columns: Serial Number, Alternate Key, Name, Device Type, and Device State. A red arrow points to the edit icon (pencil) next to the first row.

Serial Number	Alternate Key	Name	Device Type	Device State
0135100005			SecuRED	Activated
11115823		SREDKEY	SREDKey	Stored
11115824		SREDKEY	SREDKey	Stored

- Click the **Device State** drop-down arrow and then select **Activating**.

<b>Name</b>	
SREDKEY	
<b>Device State *</b>	<div>Current State: Stored</div> <div>&lt;&lt; Change Device State &gt;&gt;</div>
<b>Device Type *</b>	<div>&lt;&lt; Change Device State &gt;&gt;</div> <div>Damaged</div> <div>Retired</div> <div>Tampered</div> <div>Malfunctioning</div> <div>Lost</div> <div>In Repair</div> <div>RMA</div> <div>Activating</div>
<b>Audit Next Date</b>	05/18/2017

- Optional: If you have multiple devices, you might want to enter a **Name**, so they can be easily identified without the serial number. **EXAMPLE**: Lane 1, Workstation.
- Click **Save** when you're done.

**NOTE:** After completing these steps, your device is now functional, and you can begin processing transactions! Once you begin processing cards, your device will automatically change from Activating to Active.

## Reporting a Tampered Device

Evidence of tampering might include one or more of the following:

- The secure bag is not sealed closed.
- The secure bag is damaged.
- The "No Tear" sticker is broken or damaged.

Upon receipt of your device, if you suspect it has been tampered with, please contact support immediately by email or phone:

**Email:** [service@bluefin.com](mailto:service@bluefin.com)

**Phone:** 800-675-6573 Option 4

Complete the steps in **Activating Your Device** above with the following changes:

- Complete Steps 1 and 2 as written.
- In Step 3, complete number 1 & 2 as written.
- Click the **Device State** drop-down arrow and then select **Tampered**.
- Click **Save** when you're done.

## Appendix: Partners

**IMPORTANT:** Capabilities restricted to Partners are described here.

Oftentimes the only difference between how clients/partners access information is in setting certain parameters. Partners must populate the Partner and Client fields by selecting an option from a drop-down list.

### Client Merchant Communications


P2PE Manager automatically sends email notifications to your clients for each of the scenarios outlined below.

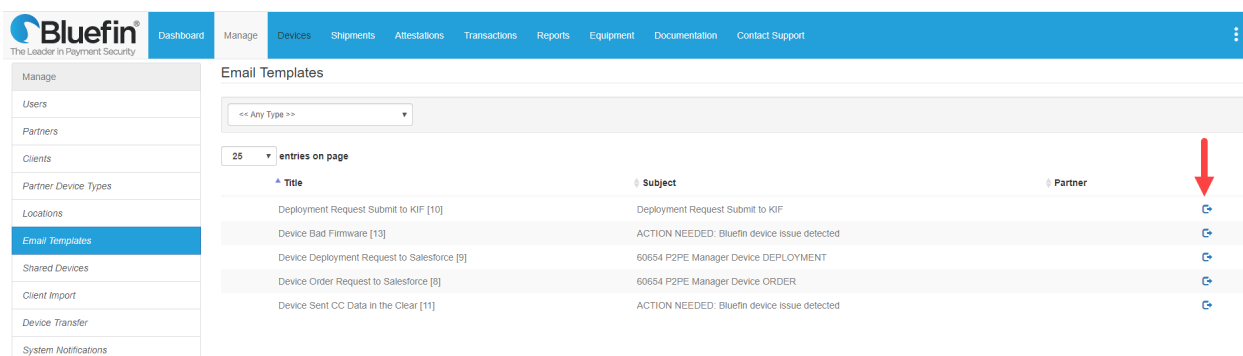
Email Notification	Explanation & Frequency	Sent To
<b>Welcome Email</b>	When a new user is added to P2PE Manager, login credentials are sent in email along with a link to set up a password.	P2PE User
<b>Password Reset / Forgotten Password</b>	When a user forgets their password, an email is sent with a link to set up <u>new</u> password	P2PE User
<b>Shipment</b>	An email is sent when a device is shipped.	Device Custodian
<b>Shipment Overdue</b>	An alert is sent to the Custodian when a device shipment is not received within 14 days of it's ship date.	Device Custodian
<b>Device State Changes</b>	Notification that the device's state has changed. Refer to <a href="#">Device State Definitions</a> .	Device Custodian
<b>Attestation Due</b>	10 days <u>prior</u> to the device audit date a notification is sent. <b>NOTE:</b> If <u>multiple</u> devices are due on the same day, then <u>one email</u> that summarizes all devices will be sent. Device serial number and location are included.	Device Custodian
<b>Attestation Late</b>	If an attestation is missed, 10 days <u>after</u> the device audit date an alert is sent. <b>NOTE:</b> If <u>multiple</u> devices are late, then <u>one email</u> that summarizes all late devices will be sent.	Device Custodian
<b>Attestation Complete</b>	Confirmation of completed attestation.	Device Custodian
<b>Action Needed</b>	Notification that action is needed when the following issues are detected: <ul style="list-style-type: none"> <li>• Device firmware issue detected</li> <li>• Device sends clear-text card-holder data</li> </ul>	Device Custodian and P2PE User

Email Notification	Explanation & Frequency	Sent To
	<ul style="list-style-type: none"> <li>Device sends corrupt data</li> </ul>	

## Customizing Email Templates

Partners and Sub-Partners can modify email templates as needed. From **Manage > Email**

**Templates** click override  next to the template of your choice. This creates a copy of the template that can be customized as all fields in the template can be modified.



## Adding Data Tokens

You can include **Data Tokens** - these are data parameters that will populate with data from within your system. To include a data token, place your cursor in the **Body** field precisely where you want to add a token. Then, make a selection from the **Data Tokens** drop-down list.

**NOTE:** The data tokens that display in the list are dynamic and depend on the email template selected.

Email template details - ACTION NEEDED: Bluefin Devices ready for Attestation

**Partner**  
A2Z Partner

**Type \***  
Attestation notification

**To \***  
{{merchantEmail}}

**From \***  
no-reply@p2pemanager.com

**Subject \***  
ACTION NEEDED: Bluefin Devices ready for Attestation

**Data Tokens** -- Please select the data token which you want to insert to the body -- ▾

**Body \***

There are {{amount}} device(s) ready for attestation inspection.

Location(s): {{location}}

Serial Number(s) (fullserial number):  
{{serial}}

To complete the Attestation of your devices, you will need to log on to P2PE Manager. <https://bluefin.p2pemanager.com/> There is a tab at the top of our dashboard labeled "Attestations", and it will list the devices that need to be reviewed.

Essentially, you are checking to make sure the devices have not been tampered with; that they are not damaged, and that they are in the same physical condition and location you expect them to be.

If you need more information, please check the Documentation tab in the P2PE Manager.

If you did not expect this mail or have any questions, do not reply to this email. Please email [service@bluefin.com](mailto:service@bluefin.com).

Thank you!

## Deleting Email Templates

Partners and Sub-Partners can delete the email templates that are created by overriding core templates.

## Administration

Manage
<i>Users</i>
<i>Partners</i>
<i>Clients</i>
<i>Partner Device Types</i>
<i>Locations</i>
<i>Email Templates</i>
<i>Shared Devices</i>
<i>Client Import</i>
<i>Device Transfer</i>
<i>System Notifications</i>

## Adding a Partner Record (Sub-Partner)

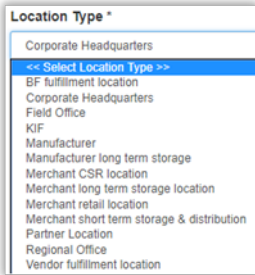
A sub-partner is another organization that resells devices and services. For example, a Bluefin partner that is a payment gateway provider might need to setup a sub-partner record for one of their resellers. This would enable the reseller to set up merchants (or “clients” as they are called in P2PE Manager).

To set up a sub-partner under your partner record, do the following from the **Manage** tab:

1. Click **Partners** in the left column.
2. Click **Create**.

3. Enter the information requested for the required fields.

Field	Description
<b>Parent Partner</b>	Select partner from the drop-down list when applicable. <b>NOTE:</b> You must select a Parent Partner when creating sub-partners.
<b>Name</b>	Required. Enter the partner's name
<b>Status</b>	Required. Select the partner's status
<b>Verification Phrase</b>	Optional.
<b>Allow Client(s) To Order Equipment</b>	Optional. Select the option if you want to allow your individual merchants or locations to order their own devices. <b>NOTE:</b> Do <u>not</u> select this option if you want to control who can order devices.
<b>Inherit Primary Contact from Parent Partner</b>	Optional. Select the option if you want the primary contact from the parent partner to automatically be the contact for the sub-partner.
<b>Contact Person</b>	Required. Enter: <b>First Name, Last Name, Email address, Phone</b> and <b>P2PE User Name</b> .  <b>Best Practice:</b> Use first initial and last name and email address for the user name. ( <b>EXAMPLE:</b> jdoe@yourcompany.com.)  <b>NOTE:</b> This information is automatically used <u>to create a Partner Supervisor user</u> .  Select the <b>Active</b> checkbox to enable the contact person.
<b>- Force users to use two-factor authentication</b>	Optional checkbox.  You can enable two-factor authentication. When it is enabled, it will affect <u>all users</u> who belong to the Client or Partner record.
<b>- Send welcome email</b>	You can send new users a welcome email. This option is selected by default.
<b>Location</b>	Required. Select the <b>Location Type</b> .

Field	Description
	 <p>Required. Enter: <b>Location Name, Address, City, Country.</b></p>
<b>Mail Address</b>	Optional.
<b>Customization</b>	
- <b>Remember Devices</b>	Optional. Select an option from the drop-down list.
- <b>Attestation Period</b>	Optional. Select an option from the drop-down list.
- <b>Contact Support Override?</b>	<p><b>IMPORTANT:</b> This field is restricted to Partner Supervisors Only.</p> <p>Optional. Select the checkbox to customize the Contact Support email address that displays on the Contact tab for subpartners and clients.</p> <p>Enter the Support Email address when prompted.</p>

4. Click **Save** when you're done.

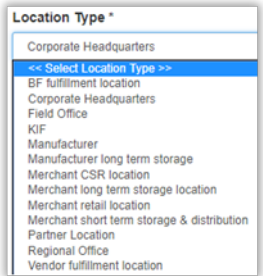
## Adding a Client / Merchant

To add Clients (Merchants) do the following from the **Manage** tab:

1. Click **Clients** in the left column.
2. Click **Create**.



3. Enter the information requested for the required fields.

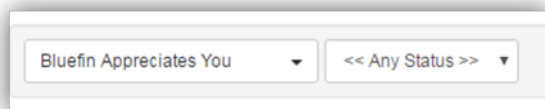
Field	Description
<b>Direct Partner</b>	Required. Select the partner from the list.
<b>Name</b>	Required. Enter the client's/merchant's name.
<b>Active</b>	Optional. Select the checkbox to enable the client.
<b>Mid</b>	Optional.
<b>Contact Person</b>	<p>Required. Enter the <b>First Name, Last Name, Email address, Phone and User Name.</b></p> <p><b>Best Practice:</b> Use first initial and last name and email address for the user name. (<b>EXAMPLE:</b> jdoe@yourcompany.com.)</p> <p><b>NOTE:</b> The <b>Active</b> checkbox for the contact person is selected for you.</p>
<b>Location</b>	<p>Select the <b>Location Type</b>.</p>  <p>Required. Enter the <b>Location Name, Address, City, Country.</b></p>
<b>Mail Address</b>	Optional.
<b>Remember Devices</b>	Optional. Select an option from the drop-down list.
<b>Force users to use two-factor authentication</b>	<p>Optional checkbox.</p> <p>You can enable two-factor authentication. When it is enabled, it will affect <u>all users</u> who belong to the Client <u>or</u> Partner record.</p>
<b>Send welcome email</b>	You can send new users a welcome email. This option is selected by default.
<b>Contact Support Override?</b>	<p>Optional. Select the checkbox to customize the Contact Support email address that displays on the Contact tab for subpartners and clients.</p> <p>(Enter the Support Email address when prompted.)</p>

Field	Description
<b>Attestation Period</b>	Optional. Select an option from the drop-down list.

- Click **Save** when you're done.

**NOTE:** At the time a client record is created, a client admin user is also created. To add additional users, refer to [Adding a User](#).

**TIP:** To display the client/merchant after you enter it, make sure your partner name is displayed at the top of the page as shown here:



A screenshot of a form with two dropdown menus. The first dropdown menu is labeled 'Bluefin Appreciates You' and the second dropdown menu is labeled '<< Any Status >>'. Both dropdown menus have a downward arrow on the right side.

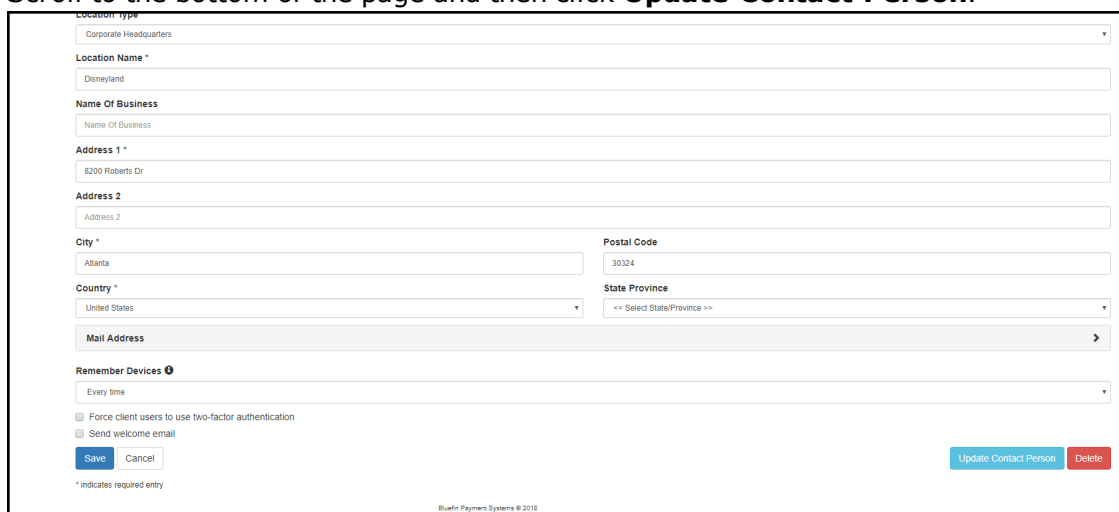
## Editing a Client's Contact Person

If the primary contact for a client location needs to be changed, you can preserve the chain of custody in P2PE Manager and update the contact person.

**IMPORTANT:** Do not Edit the Contact Field. Instead, click **Update Contact Person**.

To update the contact person, do the following:

- Select **Manage > Clients**.
- Select the **Partner** from the drop-down list.
- Select the appropriate Client from the list. (Click the edit icon.)
- Scroll to the bottom of the page and then click **Update Contact Person**.



A screenshot of the 'Update Contact Person' form in P2PE Manager. The form contains the following fields and sections:

- Location Type:** A dropdown menu with 'Corporate Headquarters' selected.
- Location Name \*:** A text input field with 'Disneyland' entered.
- Name Of Business:** A text input field with 'Name Of Business' entered.
- Address 1 \*:** A text input field with '8200 Roberts Dr' entered.
- Address 2:** A text input field with 'Address 2' entered.
- City \*:** A text input field with 'Atlanta' entered.
- Postal Code:** A text input field with '30324' entered.
- Country \*:** A dropdown menu with 'United States' selected.
- State Province:** A dropdown menu with '<< Select State/Province >>' selected.
- Mail Address:** A text input field with a right arrow icon.
- Remember Devices:** A section with a dropdown menu set to 'Every time' and two checkboxes: 'Force client users to use two-factor authentication' and 'Send welcome email'.
- Buttons:** 'Save', 'Cancel', 'Update Contact Person', and 'Delete'.
- Footnote:** '\* indicates required entry'.
- Footer:** 'Bluefin Payment Systems © 2018'.

5. Select the new contact person from the drop-down list.  
**TIP:** If the new contact person is not listed, you must create their user record first.
6. Click **Update** when you're done.

## Client Import

You can create client records in a CSV file and batch upload them.

**Best Practice:** Download and use the **Sample CSV** to create client records.

To import clients via batch, do the following from the **Manage** tab:

1. Select **Client Import** in the left column.
2. Download the **Sample CSV** and build your file.

Fields	Description
<b>DirectPartner</b>	Required.
<b>ClientName</b>	Required.
<b>LocationName</b>	Required.
<b>LocationType</b> <div> <b>Location Type *</b>            &lt;&lt; Select Location Type &gt;&gt;            &lt;&lt; Select Location Type &gt;&gt;            BF fulfillment location            Corporate Headquarters            Field Office            KIF            Manufacturer            Manufacturer long term storage            Merchant CSR location            Merchant long term storage location            Merchant retail location            Merchant short term storage &amp; distribution            Partner Location            Regional Office            Vendor fulfillment location         </div>	Required.  Options: BF Fulfillment location, Corporate Headquarters, Field Office, KIF, Manufacturer, Manufacturer long time storage, CSR Location, Merchant Long time storage location, Merchant Retail Location, Merchant short term storage & distribution, Partner Location, Regional Office, Vendor Fulfillment Location
<b>LocationNameofBusiness</b>	Optional.
<b>LocationCountry</b>	Required.
<b>LocationAddress1</b>	Required.
<b>LocationAddress2</b>	Optional.

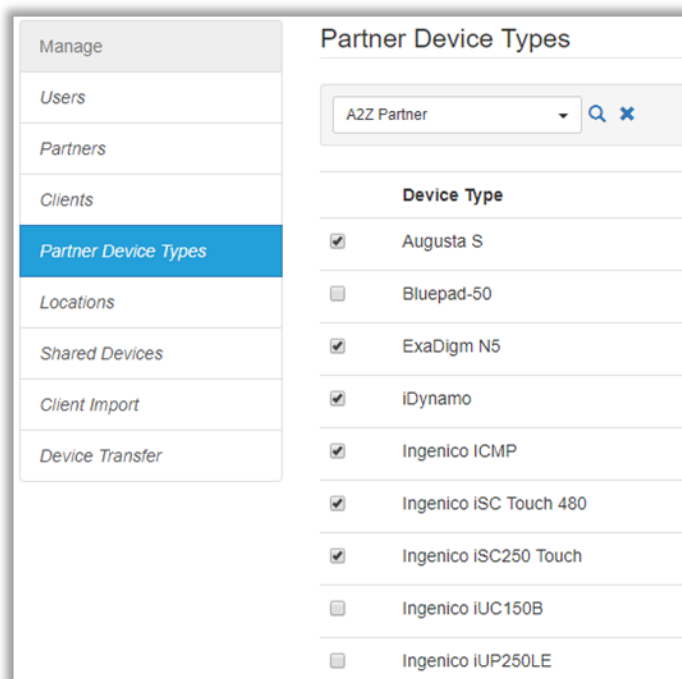
Fields	Description
<b>LocationCity</b>	Required.
<b>LocationState</b>	Optional.
<b>LocationPostalCode</b>	Optional.
<b>UserName</b>	Required.
<b>UserRole</b>	Optional.
<b>FirstName</b>	Required.
<b>LastName</b>	Required.
<b>Email</b>	Required.
<b>Phone</b>	Required.

3. Required. Click **Choose File** and navigate to the file you want to upload.
4. Click **Upload**.

## Managing Devices

### Partner Device Types

To view devices that are attributed to your organization, select **Manage > Partner Device Types**. Next, select the partner or sub-partner from the drop-down list. The devices will be displayed.



**NOTE:** If a device is missing, please contact Bluefin support or your relationship manager.

## Shared Devices

Shared Devices			
<div> <div>ABC SubPartner</div> <div>Q X</div> </div>			
<div> <div>25</div> <div>entries on page</div> <div>Search:</div> </div>			
Serial Number	Device Owner Partner	Device Owner Client	Device Location
30360	A2Z Partner	Blue Surf Resorts	Blue Surf Resort: North Carolina

To display a summary of shared devices including the partner owner and the partner with whom the device is shared, do the following from the **Manage** tab:

1. Select **Shared Devices** in the left column
2. Select the **Partner** from the drop-down list. For this partner, a list of their shared devices displays. For each device, you can track the Device Owner Partner, Device Owner Client, and Device Location.

## Device Transfer

**IMPORTANT:** Only System users and administrators can move devices across Partner or Client records.

To transfer devices under the same Partner and Client record, refer to [Transferring a Device between Custodians or Locations](#) for detailed steps.

## Single Sign-On (SSO)

Please contact your Bluefin Relationship Manager if you are interested in configuring Security Assertion Markup Language (SAML) which enables single sign-on. Single Sign-On (SSO) can be configured for partners, sub-partners and clients.

**IMPORTANT:** This feature is designed to support one Identity Provider and is implemented by System Users

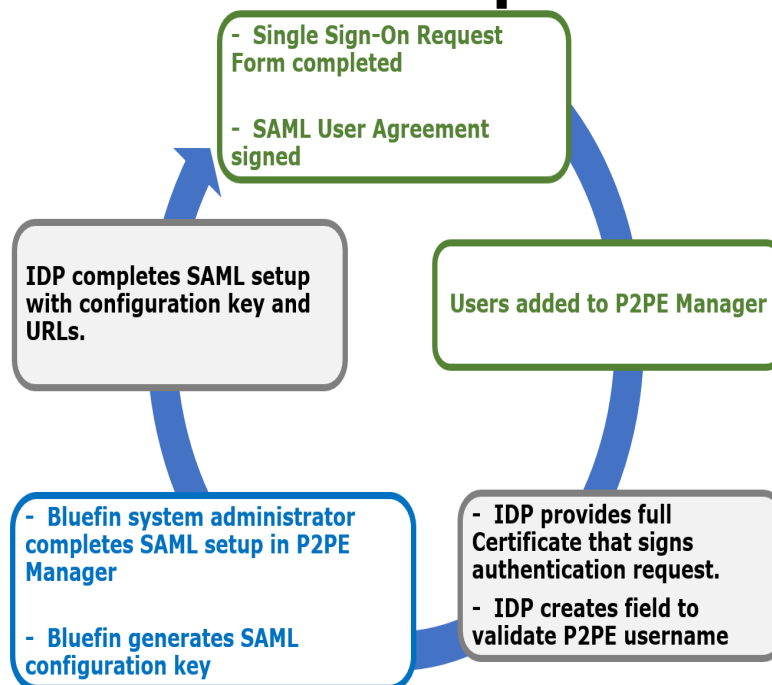
## Benefits

Single Sign-On (SSO) enables seamless integration between the system that partners / sub-partners / clients use in their environment and P2PE Manager. When users log into their own systems successfully, those credentials are recognized by P2PE Manager. This allows users to access P2PE Manager without having to enter login credentials unique to P2PE Manager.

## Setup Process

The following is an overview of the setup process.

## SAML / SSO Setup Process



1. Complete the **Single Sign-On Request Form** (see below for sample form) and the **SAML User Agreement**. Involve your Identity Provider to gather the requested information and to create a field in the SSO system to validate P2PE Manager user-names. **NOTE:** the Identity Provider will need to provide the entire X-509 Certificate.
2. Add users to P2PE Manager as usual. (Refer to [Managing Users.htm](#) for details.)
3. After Bluefin receives the requested information, our system administrators configure SAML in P2PE Manager. Then, the Single Sign-On Request form will be returned with the SAML Configuration key. (See below for a Sample IDP Setup and for information that Identity Providers need.)

## Frequently Asked Questions

### What is SAML?

Security Assertion Markup Language is an open standard for exchanging authentication and authorization data between parties. Security Assertion Markup Language (SAML) enables single sign-on. Single Sign-On (SSO) can be configured for partners, sub-partners and clients.

## Who establishes SAML / SSO in P2PE Manager?

Bluefin P2PE Manager system users configure SAML in P2PE Manager.

## What are the SSO setup requirements?

1. Complete the Single Sign-On Request form. (See below for a sample of the form and contact your Bluefin Relationship Manager to set up SSO.)
2. Sign the SAML User Agreement. (Contact your Bluefin Relationship Manager to set up SSO.)
3. Add users to P2PE Manager as usual. (Refer to [Managing Users.htm](#) for details.)
4. Involve your Identity Provider to create a field to validate P2PE Manager usernames.

## What will I receive from Bluefin to establish SSO?

After receiving the required information, Bluefin will configure P2PE Manager and return the Single Sign-On form along with the SAML Configuration key. **IMPORTANT:** This key must be shared with the Identity Provider.

## What does the Identity Provider need to do?

Identity Providers need to do the following:

- Provide the information requested in the Single Sign-On Request form. (See below for a sample of the form.)
- Create a field in the SSO system to validate P2PE Manager usernames.
- Configure system settings to enable the connection to P2PE Manager using the SAML configuration key from Bluefin.

## How many Identity Providers are supported?

This function is designed to support one Identity Provider per partner.

## Information Identity Providers Need

The following information is required by Identity Providers to facilitate SAML configuration. This information should be shared with your Identity Provider's administrator so that your single sign-on system can be updated.

- **Usernames.** (List of active P2PE Manager users.)
- **SAML Configuration Key** - This key is generated during the setup process after receipt of the **Single Sign-On Request Form**.
- **URLs** (The names of the fields vary such as ACS, Audience or Consumer.)

- Consumer Validator: `bluefin.p2pmanager.com/saml/callback/samlconfigkey`
- Consumer Connection URL: `bluefin.p2pmanager.com/saml/callback/samlconfigkey`
- Logout URL: (Depending on the IDP this might or might not be needed)  
`bluefin.p2pmanager.com/logout`

**EXAMPLE:**

`https://cert-bluefin.p2pmanager.com/saml/callback/8d34e9b997087646912c13a02c5ae726`

## Sample IDP Setup

### IDP Configuration

The following illustrates an IDP Configuration screen that's used and controlled by the Merchant. In this example, we're using screenshots from OneLogin.

**Enable SAML2.0**

Sign on method  
SAML2.0

X.509 Certificate **1**  
Standard Strength Certificate (2048-bit)  
[Change](#) [View Details](#)

SAML Signature Algorithm **2**  
SHA-1

Issuer URL **3**  
`https://app.onelogin.com/saml/metadata/e5cab9ee-9bbc-4a19-998e-9e967b82db`

SAML 2.0 Endpoint (HTTP) **4**  
`https://bluefin-payment-systems-dev.onelogin.com/trust/saml2/http-post/sso/e5cab9ee-9bbc-4a19-998e-9e967b82db`

SLO Endpoint (HTTP)  
`https://bluefin-payment-systems-dev.onelogin.com/trust/saml2/http-redirect/slo/1096952`



Field	Description
<b>1. X. 509 Certificate</b>	<p><b>IMPORTANT:</b> The value generated here needs to be communicated to Bluefin to setup the SSO connection.</p> <p>In this example, the actual certificate generated is inside the "View Details" link.</p>
<b>2. SAML Signature Algorithm</b>	<p>This setting contains the hash algorithm specified by the Partner based on their security level needs.</p> <p>Bluefin does <u>not</u> need this value.</p>
<b>3. Issuer URL</b>	<p><b>IMPORTANT:</b> The value here needs to be communicated to Bluefin to setup the SSO connection (SAML Issuer)</p> <p>This URL should be the <u>source URL</u> for all IDP users. (The URL from which all users originate from.)</p>
<b>4. SAML Endpoint URL</b>	<p><b>IMPORTANT:</b> The value here needs to be communicated to Bluefin to setup the SSO connection (SAML End Point)</p> <p>This URL should be the end point of the IDP being used.</p>

## IDP User Configuration

The following illustrates configuring a User inside an IDP. In this example, we're again using screenshots from OneLogin.

Email (SAML NameID)



E-mail (Attribute)

First Name (Attribute)

Last Name (Attribute)

Member of (Attribute)

PersonImmutableID

p2pe\_username

[Reset login](#) ( What's this? )

Basic demographic information about each user needs to be completed by the merchant in their IDP.

**NOTE:** The user login is the only field relevant to configuring SAML/SSO. In the example shown, the **p2pe\_username** parameter was added specifically for the SAML/SSO configuration to P2PE Manager.

**IMPORTANT:** This field name (p2pe\_username) needs to be communicated to Bluefin to setup the SSO connection (SAML Field Name) Bluefin does not need the value of this entry ("muser" in the example shown), but the value must match a User in the P2PE Manager who has access to this specific Partner/Client.

For reference, the following image illustrates the various IDP user fields including a field specifically added for the P2PE Manager SAML/SSO configuration. The IDP administrator should be familiar with this type of screen.

Credentials are

☒ Configured by admin

☐ Configured by admins and shared by all users

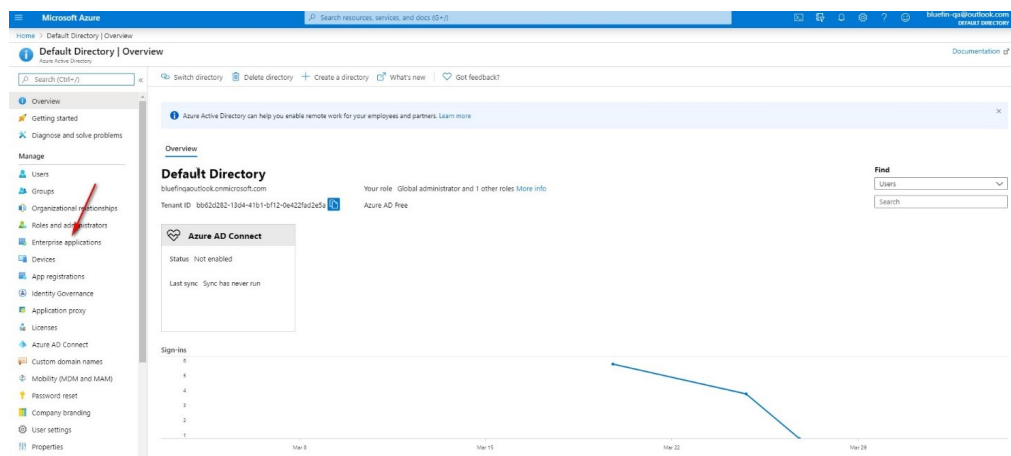
SAML Test Connector (IdP w/ attr w/ sign response) Field	Value	
E-mail (Attribute)	Email	
Email (SAML NameID)	Email	
First Name (Attribute)	First Name	
Last Name (Attribute)	Last Name	
Member of (Attribute)	MemberOf	
PersonImmutableID	- No default -	
p2pe_username	- No default -	custom parameter

## Azure Setup Overview

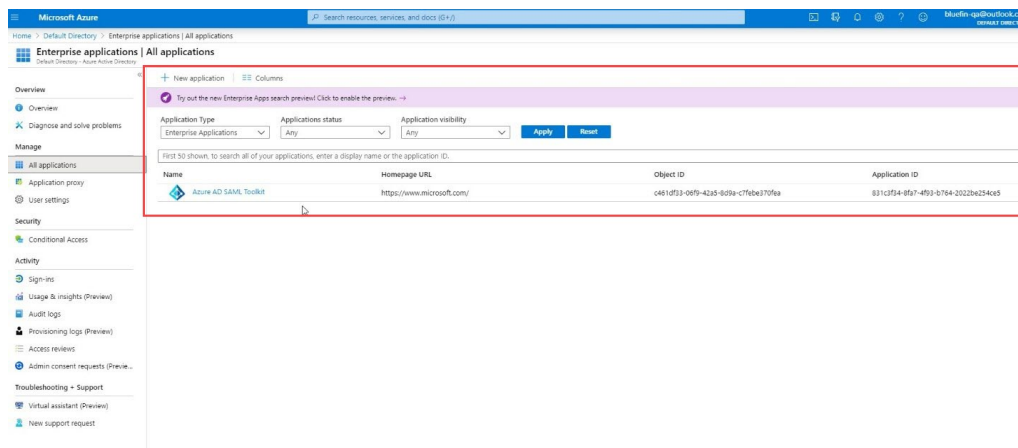
The following information is an overview of how to prepare Azure

To set up **Azure Active Directory** portal access do the following:

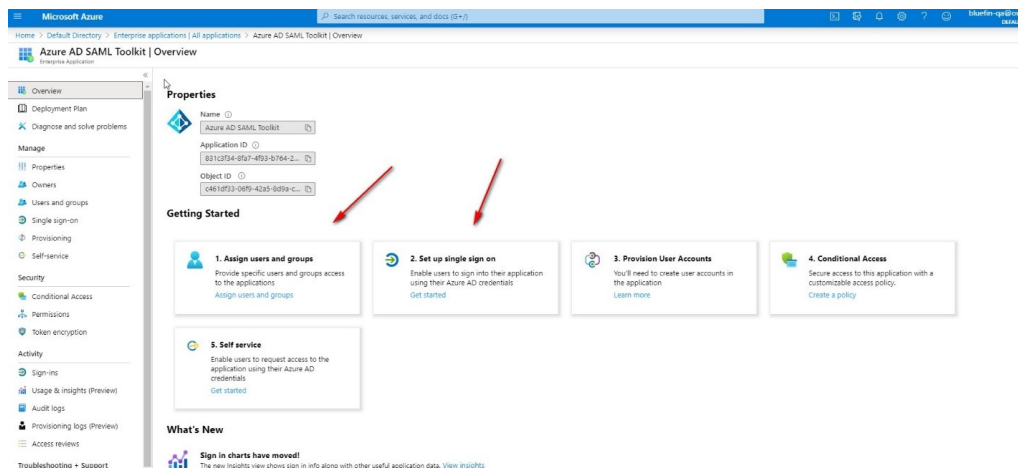
1. Log in to your Azure portal as usual and navigate to the **Azure Active Directory**.
2. In the left panel, select **Enterprise Applications**.



3. Create a new application or use an existing one.



4. Follow the instructions shown to assign users to the application and Set up Single Sign-On. **IMPORTANT:** The image below is for illustration purposes only. The steps you see will vary depending on the application you're using.



5. From the SSO page, enter your information into the **Set up SAML test signon** section to populate your information in P2PE Manager. **IMPORTANT:** This section might have a different name depending on the application you're using, but it should contain the same information.

[Upload metadata file](#)
[Change single sign-on mode](#)
[Test this application](#)
[Got feedback?](#)

Read the [configuration guide](#) for help integrating SAML test signon.

- ### Basic SAML Configuration

Identifier (Entity ID)	p2pe_username
Reply URL (Assertion Consumer Service URL)	https://bluefin.p2pemanager.com/saml/callback/66c23c64c22f1b3691b806f4a72e88
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- ### User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- ### SAML Signing Certificate

Status	Active
Thumbprint	0E75A56251387629C16121487B5538898984B438
Expiration	4/3/2023, 2:12:05 PM
Notification Email	bluefin-ga@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/bb62d282-13...
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>
- ### Set up SAML test signon

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/bb62d282-13...
Azure AD Identifier	https://sts.windows.net/bb62d282-13d4-41b1-...
Logout URL	https://login.microsoftonline.com/common/wsf...

[View step-by-step instructions](#)

## Single Sign-On Request Form (Sample)

Do the following:

1. Complete this form and submit to Bluefin. ([service@bluefin.com](mailto:service@bluefin.com))
2. Users need to be added to P2PE Manager as usual and be marked as **Active** users.
3. Your Identity Provider (IDP) administrator will need to create a field to validate the P2PE Manager username.
4. You will need to provide us with the full Certificate from the IDP that signs the authentication request.
5. Bluefin will return this SSO Request Form to the IDP Administrator along with the SAML configuration KEY.
6. The IDP Administrator will need to update their single sign-on software with the SAML configuration key and the proper URLs.

**NOTE:** After SSO is fully implemented by Bluefin and your IDP, users will access the P2PE Manager from the following URL: <https://bluefin.p2pemanager.com/saml/samlconfigkey>

## 1.) REQUEST GENERAL INFORMATION

**IMPORTANT: Single Sign-On is designed to support one Identity Provider per partner.**

<b>Partner Name</b>	Enter the partner / sub-partner name. This will enable SAML for partner users (Partner Supervisors, Partner Fulfillment and Partner User.)
<b>SAML Config Name</b>	Enter the name of this SAML configuration.
<b>SAML End Point</b>	Enter the URL of the Identity Provider for the SAML authentication request. (This is the URL of the Partner's instance of their IDP.) Typically called SAML Endpoint, SSO Endpoint, or IDP Login URL.
<b>SAML Field Name</b>	<p>The field/variable that contains the P2PE Manager Username. This could be a custom parameter from the Identity Provider or an existing one that contains the P2PE Manager Username.</p> <p><b>NOTE:</b> The IDP administrator will need to create this field in their single sign-on system to validate P2PE Manager usernames.</p>
<b>SAML Issuer</b>	Enter the Issuer URL of the Identity Provider. This is the URL of the Partner's IDP user connection to the P2PE Manager.
<b>Certificate file included</b>	<p>Enter the Certificate from the Identity Provider that signs the authentication request.</p> <p><b>NOTE:</b> The entire content of the certificate must be entered. (URL links are not allowed.)</p> <p><b>TIP:</b> This is commonly called the X-509 certificate that the Partner's IDP will generate for secure authentication to the P2PE Manager. You might need to download the certificate as Base 64 and then open it as a text file.</p>
<b>Bluefin returned SAML Configuration KEY</b>	Bluefin will return this form with this value when the setup has been completed.

## 2.) SUBMITTER INFORMATION

<b>Submitted By</b>	[Name of Person Submitting Change Request]
<b>Submitter's Company</b>	[Name of Submitter's Company]
<b>Date Submitted</b>	[mm/dd/yyyy]

Requests are completed 48 hours from receipt of complete and accurate forms. Changes are completed during business hours. Monday through Friday, 8:30 a.m. to 5:30 p.m. CST. Requests may require scheduling and may take longer than 48 hours to complete.

Partners and Resellers are responsible for Tier 1 application and IDP support.