

Point-to-Point Encryption (P2PE) Manager

User Guide

Copyright © 2022 Bluefin Payment Systems LLC. All rights reserved. Privileged and Confidential.

Document Date: February 10, 2022

Legal Notice

Copyright © 2022 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.

 $\mathsf{Decryptx}$ (R) 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

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

Viewing Device Details	
Chain of Custody	30
Device State History	31
Lifecycle Report - Detailed Device History	
Return Merchandise Authorization Process	31
Checking on Device Shipment and Tracking	
Checking Tracking Number	
Checking Device Status	33
Checking Order Status	34
Transferring a Device between Custodians or Locations	
Transferring Multiple Device Locations	
Equipment	
Deploying Equipment	
Opt Out of Bluefin Program	
Device Inspections and Attestations	
Inspecting a Device	
Inspections Report: Viewing Details of Past Inspections	
Device Attestations	40
Changing Device Attestation Date	42
Batch Process: Change Device Attestation Date	43
Viewing Future Scheduled Attestations	44
Viewing Attestation History	44
Device Tampering Detection	
Appendix: User Roles	
Client / Merchant Roles	
Partner Roles	
Appendix: Receiving and Activating Your Device	4/
Overview	47
Step 1. Access the P2PE Manager Online	47 10
Step 2. Log Receipt of the Shipment	40 50
Penerting a Tampored Device	
Appendix: Partners	51 51
Client Merchant Communications	JZ 52
Customizing Email Templates	52 53
Adding Data Tokens	55 53
Deleting Email Templates	55 54
Administration	51 54
Editing Your Own Partner Record	
Adding a Partner Record (Sub-Partner)	55
Adding a Client / Merchant	<u>55</u> 57
Editing a Client's Contact Person	59
Client Import	60
Running Reports	62

Partner Summary	
Client Summary	63
Partner Transaction Summary	<u></u> 63
Billing Report	64
Managing Devices	<u></u> 64
Partner Device Types	<u></u> 64
Shared Devices	65
Device Transfer	<u></u> 65
Single Sign-On (SSO)	66
Benefits	66
Setup Process	<u></u> 66
Frequently Asked Questions	67
What is SAML?	67
Who establishes SAML / SSO in P2PE Manager?	67
What are the SSO setup requirements?	67
What will I receive from Bluefin to establish SSO?	67
What does the Identity Provider need to do?	67
How many Identity Providers are supported?	<u></u> 68
Information Identity Providers Need	68
Sample IDP Setup	<u></u> 68
IDP Configuration	68
IDP User Configuration	
Azure Setup Overview	72
Single Sign-On Request Form (Sample)	74

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 Over**view.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: <u>Appendix User Roles</u>.

Oftentimes the only difference between how clients/partners access information is in setting certain parameters. <u>Partners must populate the Partner and Client fields</u> 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 <u>not</u> 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

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.

Getting Started

Logging In

You will receive a system-generated **Welcome** email with your username.

2PE Manager is Bluefin's onl encryption devices. Please clic notification from Bluefin Dem	ine portal for managing chain of custody and activation status of your point-to-point of the link below to setup your password. Additionally, you will receive an email o's Client Service with implementation instructions for the POS system
USERNAME: username	
URL: https://staging-bluefin.p code=eyJhbGciOiJIUz11NilsInf NIcm5hbWUifQ.1Lt1WhVAnFi	2pemanager.com/forgot? \ScCl6lkpXVCJ9.eyJpYXQiOjE0NzQzOTc2NjAsImV4cCl6MTQ3NDM5ODI2MCwic3ViljoidX a2DExqwEkqFBom1FfTV0lUrBrxFmgEJU
If you did not expect this mail call 800-675-6573 as soon as	 or have any questions, do not reply to this email. Please email <u>service@bluefin.com</u> or possible.
Thank you!	
Bluefin Demo Merchant Suppo bluefin.com/merchant-suppor service@bluefin.com 100-675-6573 Option 2	ort t

Follow the instructions in the email:

- 1. Click the link in the email.
- Create a new password.
 NOTE: Passwords must contain one uppercase letter and one symbol character.
- 3. Click **Reset**.

	Reset password	
User Name *	usemame	
Password *		✓
Password confirm *		•
	Reset Close	

Dashboard

The Dashboard is the first screen you'll see after logging in. You can also navigate to it by clicking the **Dashboard** tab any time. The dashboard displays a summary of your devices and other useful information organized in "tiles."

Notifications Vou have an open device shipment Dismiss Continue Date From 10/17/2018 60:00:00	that needs to be checked in. When	you receive the device(s), please click here to begin	n)	Date To 10/17/2019 23 59 59		Арру
Summary Information C						
Devices		Shipped devices by type		Attestations Due on 2 Devices:	User Count	
Stored	0	PAX D210 :	7	Serial No.	8 (Total Users)	8 (Users 2018)
Activated	0	Augusta S :	1	30358	Jan:0 Feb:0	Mar: 0
Tampered :	1	Total :	8	30360	Apr:0 May:0 Jul:0 Aug:1	Jun : 0 Sep : 7
Malfunctioning	0				Oct : 0 Nov : 0	Dec:0
Rma	0					
Total :	1					
					2018 (8)	
Device Locations						

The information displayed is <u>dynamic</u> 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 <u>remove</u> it. To hide the banner, click **Continue**. To review <u>unread notifications</u>, click the red notifications icon in the top right corner to see a list.

System No	tifications
* Dismiss	Notification
0	Details about Notification 01 will display here.
0	Sample notification 02. Additional details will display here.

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.

Devi Viev	ce Locations					
	Device Location	ons	C	Expand)	13 devices
	United States		13 total d	evices		100.00%
	Devices added in	last ye	ar			
	Sep '18 : 3 Dec '18 : 0 Mar '19 : 0 Jun '19 : 0	Oct Jan Apr Jul '	'18 : 7 '19 : 0 '19 : 0 19 : 0	Nov ' Feb ' May ' Aug '	18 : 19 : (19 : 19 :	1 0 1 0

Menu Options At A Glance

Bluefin[®] Dashboard Manage Devices Shipments Attestations Transactions Reports Equipment Documentation Contact Support

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 <u>Appendix: User Roles</u> for details.

Tab	Description
Manage	Manage Users, Locations, Device Transfers and Sys- tem Notifications
	NOTE : Partners can additionally manage other func- tions. Refer to <u>Appendix: Partners</u> for details.
Devices	Displays a summary of all devices.
Shipments	Displays incoming shipments.
Attestations	Displays Current Attestations, History and Future Attestations.
Transactions	Displays a summary of transactions including encryp- tion and decryption status.
Reports	POI Chain of Custody, Client Summary, Client Trans- action Summary, Inventory Summary, User Report, Device Activity, Device Receipt, Daily Report and Decryption Totals.
	NOTE : Partners can run additional reports. Refer to <u>Appendix: Partners</u> for details.

Tab	Description
Equipment	Deploy equipment (order equipment and check device status.)
	NOTE : Partners can additionally create equipment requests. Refer to <u>Appendix: Partners</u> for details.
Opt Out	Retire all devices in your account so they cannot con- duct transactions.
	IMPORTANT : This option is restricted to Client Admin- istrators.
Documentation	Help files and videos. Refer to <u>Accessing Online Help</u> <u>Documentation</u> for details.
Customer Support	Submit a help request online and review help contact information.

Receiving and Activating Your Device

For detailed information, refer to the <u>Appendix: Receiving and Activating Your Device</u>.

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 <u>Accessing Online Documentation</u>.
- See <u>Batch Receiving Devices</u> for information about scanning multiple devices into P2PE Manager.
- See <u>Receiving Device with Special Serial Number Requirements</u> 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 dropdown list: All, In-transit, Received 1. From the **Shipments** tab, select a shipment and then click **Batch Receive**.

Bluefin*	nteed Manage Deckin Shipmens Alter							
Shipment details								
Devices can be received individually	y or using the batch receive option.							
Shipment		Devices						
Client:	SUNY Oswego	* Serial Number	Alternate Key	Device Name	Tamper Label	Device State	Received	Received
Tracking:	1234						Date	
Certier:	Carrier 3	06765/		testy	<< not received>>>	in Transit		Receive
Shipment Type:	KIF Shipment	Showing 1 to 1 of 5 entries						
Ship Date:	03/02/2022 6:19 AM	Batch Receive						
Date Received:								
Close								
* indicates required entry								

2. <u>Optional</u>: 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, <u>you must select it before scanning your devices</u>.

 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.)

Receiving device			
Scan or enter device serial nur proceed next device.	mber and tar	mper label if present. If d	evice is matched
Matching options			
Matching pattern *		Matching length *	
Full Match	•	5	*
Padding pattern *		Padding length *	Character *
None	*	10 🔻	0
Serial number * Serial number Tamper label			
Tamper label			
Auto Activate device			
Progress			

- 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**.

<u>If you did not select Auto Activate device</u>, then the **Device State** will display as **Received**. <u>To continue</u>, follow the actions in **Step 3: Activate Your Device** in the <u>Appendix: Receiving and Activating Your Device</u>.

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.

Scan or enter device serial number proceed next device.	er and tar	mper label if present. If d	levice is matched
Matching options			
Matching pattern *		Matching length *	
Partial Match From Start		5	
Padding pattern *		Padding length *	Character *
Pad on the left		1 *	0000000
Serial number (searching: 12345) * 123456789 Tamper label	+	-	0
Serial number (searching: 12345) * 123456789[Tamper label Tamper label	+		a
Serial number (searching: 12345) * 123456789[Tamper label Tamper label Auto Activate device	•		a
Serial number (searching: 12345)* 123456788 Tamper label Tamper label Auto Activate device Progress	•		Q
Serial number (searching: 12345)* 123456785 Tamper label Tamper label Auto Activate device Progress	+		0
Serial number (searching: 12345) * 123456769[Tamper label Tamper label Auto Activate device Progress	•		0

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.

Bluefin [®] Dashboard Manage Device	Shipments Attestations Transactions Reports Equipm	eret Documentation Contact Support	
Documentation			
User Guides	P2PE Instruction Manuals	Video Library	
Biuefin P2PE Manager Merchant and Client User Guide (1) pdf	Appendix A IDtech SecuRED v1.1 pdf downliaded on Aug 14, 2018 128-41 PM	Equipment Tab Overview.mp4 rot downloaded	
not downloaded Bluefin P2PE Manager Partner User Guide.pdf	Appendix B IDtech SREDkey v1.1.pdf X not downloaded	P2PE Device Attestation.mp4 downleaded on Jul 19, 2018 3 10 21 PM	
not downloaded	Appendix C Ingenico IPP 350 320 310 v1.1 pdf Appendix C Ingenico IPP 350 320 310 v1.1 pdf Appendix C Ingenico IPP 350 320 310 v1.1 pdf	P2PE Manager Client Setup mp4 rot downloaded	
	Appendix D Ingenico ISC 250 v2.dd pdf K not downloaded	P2PE Manager Client Training mp4 ret downloaded	

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:

Equipment Tab Overview.mp4

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

Transa	ctions															
A2Z Pa	rtner	•	a x	Blue Surf Resorts 👻	Select a locati	on in the list or sear	ch it by name, addres	• @ 1	Î Any	♥ 01/01/2	020 00:00:00	: 05	29/2020 23:59:59		Search based o	n UTC
Skip so	orting (fast per	formance)	✓ Apple	Click "Apply" bu	itton in order to	get transactions										
25	 ✓ entries 	s on page											Search:			CSV
* F	Partner	Direct Partner	Clie	ent Transacti Client ID	on MID	Serial Number	Alternate Key	Device Name	Message ID	Reference	Method	# Encrypted	# Decrypted	§ Succes	s Completed	Virtual
								No data av	ailable in table							
															Pre	vious 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. (<u>Partner users only</u>: 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. <u>Optional</u>. 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)

	Aanage Devices Shipments Attest	ations Transactions Rej	ports Equipment	Documentation	Contact Support					:
Report	POI Chain of Custody Rep	ort								
POI Chain of Custody	×Q									
Partner Summary										•
Client Summary										•
Partner Transaction Summary	Date From	03/02/2021 12:00:00				Date To	03/02/2022 12:00:00			
Client Transaction Summary	«AI POIs »									~
Inventory Summary	<< Al Custodians >>									~
User Report										
Device Activity										*)
Davice Receipt	Apply									
Daily Report										PDF CSV
Decryption Totals	Model Serial Number	Alternate Key 💡	Date of Event	Location	Address Cit	y State / Province	Postal Code Country	Custodian	Status	Custom Reference
Billing Report					No data	available in table				

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 >>			T
<< All Custodians >>			٣
<< All Locations >>			٣
Apply			

3. Click **Apply**.

Related Information: See Exporting a Report.

Creating a Client Transaction Summary Report

					sactions	Reports Equ														
Report	Client Tr	ransaction	Summar	у																
POI Chain of Custody	×Q					Date From					Date To					Search bat	ed on UTC		Apply	
Partner Summary	<< Select	Partner >>																	(Constant)	
Client Summary																	a. e.			10000
Partner Transaction Summary																Se	arch:		PDF	CSV
Client Transaction Summary	* Partner	Direct Partner	Client	Location	I MID	Total Messages	Total Decrypt	3DES / CBC	3DES /	BPS Good	RSA- 2048	AES-	3DES / CBC	3DES /	BPS	RSA-	AES-	Total Device	Refere	m ence
Inventory Summary								Good	Goog		Good	Good	Bad	Bad		Bad	Bad	validate		
User Report									,	Vo data availa	ble in table									
Device Activity	Showing 0 t	o 0 of 0 entries																		
Device Receipt																				
Daily Report																				
Decryption Totals																				

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	A Total
Activated	12
Activating	5

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 act-ive/inactive status.

User Reports								
<< Select Partner >> • Q X	<< Select Client >>							
User Report								
25 v entries on page						Search:		PDF CSV
🗸 User Name 🔅 Name	Email	Phone	Partner	Direct Partner	Client	Role	Path	Active?

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**.

🛛 Bluefin° 🗠				ansactions P	Reports												
Report	Device	Activity															
POI Chain of Custody																	
Client Transaction Summary	Device	Activity															
Inventory Summary	25	- entries o	n page											Search:		PDF	CSV
User Report	+ Serial N	a. 0.	Alternate Key	Model	0.00	Location	Partner	Status	I MID	Address	Country	First Use	Last Use	Custodian Name	Custom Re	ference	
Device Activity				Incenico	0		State			1234 S Memorial							
Device Receipt	6789			Desk 35	500 D	C - Test	University of New York	Stored		Dr, Tulsa, Oklahoma, 75116	US				DC REF		
Daily Report							State										
Decryption Totals	45612379	D		SHEDK	ey O	Jswego	New York	Activating		Houte 104,Oswego	US						
	45612378	9		SREDK	ey B	Bluefin Tulsa Office	State University of New York	Stored		4500 S. 129th East Avenue, Tulsa, Oklahoma, 74134	US						
	444444			LEGACY	y c	Oswego	State University of New York	Activating		Route 104,Oswego	US						

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.

Device Receipt Report					
- Q X	Select no. of days	Apply	Missed Device Filter		
Device Receipt	6-10 Days 11-15 Days 15-30 Days				
25 v entries on page	30+ Days			Search:	PDF CSV
▼ Partner Name	Device	Type(s)	Total Device Count	Missed Device Count	Date of Last Shipment

Daily Report

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

P2PE Manager User Guide

Daily Report						
A2Z Partner Q X Select Client >> Date From	05/28/2020 12:00:00	Date To	Search based on UTC Apply			
Daily Report						
25 v entries on page				:	Search:	PDF CSV
v Client Name	MID	Encrypted Decrypted	Success Date	♦ Virtual ♦ Seria Num	al Alternate Device Iber Key Name	Partner Direct Partner Name Name
		No data available in	able			
Showing 0 to 0 of 0 entries						Previous Next

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 <u>dynamic</u> 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.

<u>Partner users only</u>: 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:

Bluefin	Destitoard	Manage	Devkes	Shipments	Attestations	Transactions	Reports	Ecoloment	Documentation	Contact Su	pat								1	
Transactions							-													1
A22 Faither	• Q # D.#	Sur'Amoti +	Select a loc	nder in the lite o	maint hty care	1	â [leg w	012825313138	* #	RG812728 22 19819	Secenth besed	m MFC - Dig safeg (in	a partemante d	~ Ant In	* 'Apply Invitor	in order to get t	tens etilente		
26 2 entries on p	nge															3			C9V	4
* PROM	Direct Parts	a	Client	Tra	insuction Client I	D MD		Scrial Nurr	aber All	emate Key	Device Name	Meanage ID	Reference	Method	A Encrypted	# Decrypted	Success	Completed Date	0 Virtual	
									N:	data available	in later									
																		Phone	tes Naol	

- 1. Set the parameters at top of page based on your preference.
- Set the number of entries based on your preference.
 IMPORTANT: Only the information <u>displayed</u> 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 <u>restricted to Client Administrators</u>.

Manage	
Users	
Locations	
Device Transfer	
System Notifications	

Managing Users

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

User	5					
25	• entries on page Create				Search:	CSV
	▲ First Name	Last Name		Phone	User Name	Role
1	AaronC	Admin	p2pemanagerusername@gmail.com	+1 800-675-6573	AaronCAdmin	Client Admin
	ChrisC	Custodian	p2pemanagerusername@gmail.com	+1 800-675-6573	ChrisCCustodian	Client Custodian
1	Francis	Surfe	p2pemanagermerchantuser@gmail.com	+1 800-675-6573	Francis_BlueSurfResorts	Client Procurement
1	Niel	Surfe	p2pemanagermerchantuser@gmail.com	+1 800-675-6573	Niel_bluesurfresorts	Client Custodian
1	PatC	Procurement	p2pemanagerusername@gmail.com	+1 800-675-6573	PatCProcurement	Client Procurement
1	Suri	Surfe	p2pemanagerusername@gmail.com	+1 800-675-6573	Suri_BlueSurfResorts	Client Admin
1	UmaC	User	p2pemanagerusername@gmail.com	+1 800-675-6573	UmaCUser	Client User
1	Your	Name	youremail@example.com	+1 800-675-6573	youmame	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.

Manage	User details - << empty >> << empty >>		
Users	First Name *		
	First Name		
	Last Name *		
	Last Name		
	Email *		
	Email		
	Phone *		
	+1 - Phone		
	User Name *		
	User Name		
	☑ Active		
	Role *		
	<< Select Role >>		
	☑ Send welcome email		
	Save		
	* indicates required entry		

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

Active		
Role *		
<< Select	Role >>	
Send v	velcome email	
Course	Concel	
Save	Cancel	

- 4. Select a **Role**. Refer to <u>Appendix: User Roles</u>.
- 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 <u>deactivate</u> a user, <u>deselect</u> 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 Account Settings

Your Account Settings include:

- Profile: Update your name, email address or your default login landing page (**NOTE**: Landing Page options are based on your user role.)
- Security: Update your password and set up two-factor authentication
- Notifications: Enable and select notifications you wish to receive.

To access your account 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.

Account Settings
Profile
Security
Notifications

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

Managing Your Notifications

Depending on your user role, you can choose to receive some or all the following email notifications.

Notification	User Roles	Received When	Email Notification
Device does not encrypt properly	Partner Supervisor, Client Admin	A device is sending credit card data in the clear, corrupt data, or bad firmware.	Device sent cc data in the clear is now titled Device does not encrypt properly. Current device sent corrupt data or device sent bad firmware notifications will be received depending on the circumstance of the device.
Device State Change	Partner Supervisor, Partner Fulfillment, Partner User, Client Admin	The device state of any of their devices has been changed.	Existing Device State Change email notification will be received.
Device waiting to be received	Partner Supervisor, Partner Fulfillment, Partner User, Client Admin	A device is waiting to be received from shipments.	Device Shipment Overdue email notification is now titled Device waiting to be received, and is the email notification that will be received.
Device approaching End of Life	Partner Supervisor, Partner Fulfillment, Partner User, Client Admin, Client Custodian	A device is approaching it's PTS Version Expiration Date 1 month before the PTS Expiration Date.	New PTS Expiration Date email notification will be received.
Completed Attestations	Partner Supervisor, Partner Fulfillment, Client Admin, Client User, Client Custodian, Client Procurement	An attestation has been completed.	Existing Device Attestation Complete email notification will be received.
Upcoming Attestations	Partner Supervisor, Partner Fulfillment, Client Admin, Client User, Client Custodian, Client Procurement	Devices are ready to be attested 14 days prior to their audit date.	Existing Devices Ready for Attestations email notification will be received.
Past Due Attestations	Partner Supervisor, Partner Fulfillment, Client Admin, Client User, Client Custodian, Client Procurement	Devices are 24hrs past dues their required attestation date.	Existing Past Due Attestation email will be received.
Shipment Confirmation	Partner Supervisor, Partner Fulfillment, Partner User, Client Admin	Devices have been shipped out.	Existing Shipment Confirmation Email notification will be received.

IMPORTANT:

- Root Partners who choose to receive notifications will receive them for all their Partners and Clients.
- Sub-Partners who choose to receive notifications will receive them for all of their Clients.
- Clients who choose to receive notifications will receive them for their own devices.

To enable all or selective notifications, do the following:

- 1. Select the Notifications in your Account Settings
- 2. Click on the slide button under Notifications so that it turns blue
- 3. Check the box next to all or only the notifications you wish to receive

To disable all Notifications and save your notification selection, do the following:

- 1. Select the Notifications in your Account Settings
- 2. Click on the slide button so that it turns grey

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 *	User Name			
Password *	Password			
	Log In Forgot 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 <u>confidential</u>, then separate clients should be created so users in one location <u>cannot</u> see information about another location.

IMPORTANT: Decisions about adding a location or creating a separate client do <u>not</u> 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**.

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

2. Complete the information requested.

Field	Description
Mail Address	Optional
Contact Person	Required. Enter First Name, Last Name, Email, Phone
	NOTE : 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:

Devid	ces		No.							
A2Z	Partner - Q	X Blue Surf Resorts - <	< Any State >>	Apply Click	Apply" button in orde	r to get devices				
25	\checkmark entries on page						Se	earch:	×	Search CSV
	Serial Number	Alternate Key	Name	Device Type	Device State	Client Name	Location Name	Activation Date	o Mid o Vin	tual Notes
1	000030350		Registration	PAX \$300	Activating	Blue Surf Resorts	Blue Surf Resort: Florida		No	
1	000030351		Restaurant	PAX D210	Activating	Blue Surf Resorts	Blue Surf Resort: Florida		No	
1	000030352			PAX S500	In Transit	Blue Surf Resorts	Blue Surf Resort: North Carolina		No	
1	000030353			PAX S500	Injected	Blue Surf Resorts	KIF		No	
1	000030354			PAX S500	Stored	Blue Surf Resorts	Blue Surf Resort: North Carolina		No	
1	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.

<< Active States >>	~
<< Any State >>	
<< Active States >>	
<< 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
Name	Enter a short name that allow you to easily identify the device.
	Example : "Lisa's desk", "Register 10", or "front desk."
	TIP : Device names do not affect processing.
Device State	Select an option from the drop-down list.
	< Change Device State >> Damaged Retired Tampered Malfunctioning Lost RMA Stored Stored
Attestation Period	Select an option for device inspections. Refer to <u>Changing Device Attestation Date</u> for details.

Audit Next Date

Select a date for device inspections. Refer to <u>Changing</u> <u>Device Attestation Date</u> for details.

Related Information: For instructions for activating a brand-new device, see <u>Batch Receiv</u>-<u>ing Devices</u>.

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			
Activated (Automatic)	YES	Device is in hands of merchant and processing of cards has begun (state change from "activating" to "active" occurs automatically.)			
		NOTE : In <u>Branded versions of P2PE Manager</u> , if Allow External Device Activation Mode is enabled by the system administrator, then system users, partner super- visors and client administrators can change a device's state to Activated manually and via batch upload.			
Activating	YES	Device is in hands of merchant and ready to begin pro- cessing cards			
Damaged	NO	Unit is inoperable due to physical damage.			
Destroyed	NO	Unit is inoperable and cannot be recovered. NOTE : System admins and users only.			
DOA by KIF NO		Device needs to be removed from service for destruc- tion. NOTE : Key Injection Facility (KIF) use only.			
In Repair	NO	Device needs to be removed from service for repair.			
In Transit (Automatic)	NO	Device has been shipped to the merchant. NOTE: KIF use only.			
Injected	NO	Encryption key has been injected into the unit. NOTE: KIF use only.			
KIF Test	NO	Used by the KIF to do an end-to-end test prior to ship- ping. NOTE : KIF use only.			
Lost	NO	Merchant does not know where device is.			
Malfunctioning	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.				
PIN Pad	YES	Device is in the hands of the merchant and is available to be used when processing cards.				
		PIN Pad devices are <u>optional</u> external devices used in conjunction with an activated "host" payment processing device. This is a non-billable device state.				
		NOTE : System admins and System users only.				
Quarantined	NO	Unit was discovered to be malfunctioning or was				
(by KIF)		tampered with prior to shipping. (Unit was returned to KIF outside of the RMA process.)				
		NOTE : System admins and System users only.				
Retired	NO	Merchant no longer wishes to use a device. If the mer- chant closes their Bluefin account, all devices will be marked as retired.				
RMA	NO	Device needs to be returned to the KIF.				
Return Merchandise Authorization		NOTE : Use caution when selecting this state because it is <u>not</u> reversable.				
		KIF will send return instructions to the merchant to retrieve device that is not working correctly.				
		Related Information : "Return Merchandise Author- ization Process" on the next page				
Stored	NO	Device is in possession of merchant and stored in a secure location, but not ready to begin processing cards.				
Tampered	NO	If a merchant believes that a device was tampered with, they must put the device in this state. Contact your rela- tionship manager or Bluefin Support for next steps.				
Unassigned	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				
1	02/11/2016 2:20 PM	TE SPENCER	Manual	John Smith		Not Completed				

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
1000	09/06/2018 11:34 AM	Injected	
Suri 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 Custor	dy History Lifecycle ins	pections						
Serial 000030350 KIF AC	KIF 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	(Custody Status: Received)	KIF			
Change State	09/06/2018 11:34 AM	1000	Injected					
Change Custody	09/06/2018 11:34 AM		In Transit	Suri Surfe (Custody Status: Received)	Blue Surf Resort: Florida	Tracking #: 100 (FedEx) Shipped or: 09/05/18 04:00 Received or: 09/06/18 04:53 Received by: Suri Surfe		
Change State	09/06/2018 12:53 PM	Suri 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 <u>malfunctioning</u> or suspect it has been <u>tampered</u> with, contact your relationship manager or contact Bluefin Support. Based on their guidance, <u>if you are advised to return the device</u>, 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 <u>RMA</u>.

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

Device State *				
Current State: Stored	<< Change Device State >>			
Device Type *	<< Change Device State >> Damaged			
Ingenico iSC Touch 480	Retired Tampered Malfunctioning			
Client	Lost			
Disneyland	Activating			

IMPORTANT:

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



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

Checking on Device Shipment and Tracking

NOTE: You will <u>not</u> 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-com	ing Shipments				
All					~
25	✓ entries on page			Search:	
	Client	Carrier	Tracking	▼ Date Shipped	Date Received
۲	Blue Surf Resorts	FedEx	12345	11/28/2018 3:45 PM	
۲	Blue Surf Resorts	FedEx	1051029	10/29/2018 12:00 PM	
۲	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 <u>not</u> 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

.....

If the device is listed, that means that the order has been successfully placed.
 NOTE: If the device is <u>not</u> listed, and depending on how your order was placed, the device will display just before it is shipped.

Equ											
Ap	pply										
25	✓ entr	ies on page Crea	ate			Search:					
	Request	§ 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 <u>not</u> listed <u>and</u> the device was ordered more than five business days ago, please contact Bluefin.

Devices											
<< Any State	er Apy State >> v Apry Click * Spaply" button in order to get directors										
25 v entries on page				•				Search: Search CSV			
	Serial Number	Alternate Key	Name	Device Type	Device State	Client Name	Location Name	Activation Date	0 Mid	0 Virtual	Notes
1	000030350		Registration	PAX S300	Activating	Blue Surf Resorts	Blue Surf Resort: Florida			No	
1	000030351		Restaurant	PAX D210	Activating	Blue Surf Resorts	Blue Surf Resort: Florida			No	
1	000030354			PAX S500	Stored	Blue Surf Resorts	Blue Surf Resort: North Carolina			No	
1	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.
- 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. (<u>If a device is</u> retired, lost, or stolen, these steps do not apply.) Additionally, this option is restricted to <u>Client Administrators and Client Custodians</u>.

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 <u>Manual</u> if device is handed off or if someone else taking responsibility for the device.
b. Choose <u>Shipment</u> 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	*	0	Î
Transfer Method *			
Manual			*
Custodian *			
Select a user in the list or search him by name		•	Î
Complete Date			
06/14/2016			
Notes			
			10
	Save	Ca	incel

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 <u>under the same Partner and Client record</u>.

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)	li
Choose File No file chosen	
Options	
<< Select Partner >>	• Q X
<< Select Client >>	-
Upload Cancel Sam	mple CSV
* 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		A B	
1	SerialNumber	Location	DeviceType
2	123AD33377	Company Location 1	SREDKey
3			

To transfer devices to another location under the <u>same Partner and Client record</u>, 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 <u>not</u> successfully transferred, hover your house 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 <u>placing an order</u> to send additional equipment to your location(s). This option is restricted to <u>Partners and Client Administrators.</u>

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 <u>not</u> have access to the **Equipment** tab. (If you do <u>not</u> 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**.

Shboard Manage Devices	Shipments Atlestations	Transactions Reports	Equipment	Documentation Contact St	upport	@bluefin.com
Equipment Requests			4			
Bluefin • Q	Bluefin - or << Sel	ect KIF >> 🔻				
25 • entries on page Crea	te				Search:	
Request ID Status	¢ Client	Location	♦ KIF	Device Type	Submit Date	Processed Date
		No data availa	able in table			
Showing 0 to 0 of 0 entries						Previous Nex

2. Complete the Deployment request as noted below.

Field	Description
Partner	(<u>Partners Users only</u> : Select the Partner from the drop- down lists.)
Client	(<u>Partners Users only</u> : Select the Client from the drop- down lists.)
Location	Required.
	TIP : If sending to a new location, add the location <u>before</u> placing order. Refer to <u>Adding Locations</u> .
Contact	Required.
Device Type	Required.
	IMPORTANT : 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.
Quantity	Required.
Client Order #	Optional. Enter the Client Order # if applicable. It will be included in the Bluefin invoice.
Client PO #	Optional. Enter the Client PO# if applicable. It will be included in the Bluefin invoice.
Client RA #	Not applicable.
Bluefin Order #	Not Applicable. (These fields are automatically gen-
Bluefin PO #	erated.)
Bluefin RA #	
Submit Date	(These fields are automatically generated.)
Processed Date	
Notes	Required. Notes are submitted to the KIF for processing.

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

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 <u>not</u> apply to Partners.



* indicates required entry

Opting Out retires all devices in your account so they <u>cannot</u> 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 <u>not</u> 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 <u>Contacting Support</u>.

Device 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.

Viewing Completed Attestations

The Completed Attestations tab provides you with a record of all the devices that have been attested.

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

	Manage	Devices	Shipments	Attestations	Transaction	s Reports	Equipment	Documentation	Contact Support		
Attestations	Comple	eted Atte	stations								
Past Due Attestations Upcoming Attestations	×Q «	< Select Partner	» •	<< Select Client >	•		From	n 04/20/2020 23:59:5	9 🖨 то	04/20/2020 23:59:59	Acopty Acopty
Completed Attestations	25 ~	entries on p	age							Search:	
	0.4	Attestation N	ame	Serial Number	н	Alternate Ke	ry .	Complete Date	Conta	ct Notes	Photo
		Annual Audit 2	2017	100200300				03/17/2022 12:58 PM	Jerry N	Aller View	4
		Annual Audit 2	2017	100200300				03/17/2022 12:58 PM	Jerry N	Aller View	÷
		Annual Audit 2	2017	100200300				03/17/2022 12:58 PM	Jerry N	Aller View	÷
		Annual Audit 2	2017	100200300				03/17/2022 12:58 PM	Jerry N	Aller View	÷
	Showing	1 to 4 of 4 er	ntries								Previous 1 N

3. Review the **Complete Date** for attested devices.

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.

In	ventory devices			I
0.0	Serial Number	Alternate Key	Device State	🗸 Audit Next Date
A	n_SV_2		Assigned	09/20/2016 12:00 AM

1. Click the **Attestations** tab. Select **Upcoming Attestations** in the left column.



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

Devi	entries on page	ups of not more than 500 at a time.
	Serial Number	Alternate Key
✓	30359 ng 1 to 1 of 1 entries	

NOTE: To select <u>all</u> 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
30359
Showing 1 to 1 of 1 entries
Create Attestation

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

Create Attestation	
Name *	
Attestation Name	
Notes	
Photos	
I acknowledge that I have reaperformed the inspection in a is suspected.	Choose File No file chosen ad the PIM document associated with this device and accordance with the instructions. I attest that no tampering
	Save
* indicates required entry	

5. Optional: Based on your preference, you can upload <u>one</u> 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)

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

IMPORTANT: Attestations can also be performed in the Past Due Attestations tab by following Step 2 through Step 5.

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.

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



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

Audit Next Date				
09/29/2016				
Activation Date				
03/26/2015				
Firmware Version				
1.0				
Firmware Update Date				
03/26/2015				
Save				

Batch Process: Change Device Attestation Date

You can change the device attestation date for a group of devices (up to 500) from **Attest-ation > Upcoming Attestation**. You can use the Search feature to narrow the list and you canoptionally download a list of devices into a PDF or CSV file.

1. Select the device(s) you want to change and then click **Update**. **NOTE**: You can select up to 500 devices.

Up	coming Attestations					
×	Q State University of New York -	SUNY Oswego 👻				
2	5 v entries on page				Search:	PDF CSV
•	Serial Number	Alternate Key	* Audit Next Date	Device Attestation Period	0 Contact	Device State
	1234		09/20/2021 11:32 AM	1 months	Nisa Sharif	Stored
	456123789		09/20/2021 11:34 AM	1 months	Nisa Sharif	Stored
	09876		09/20/2021 12:36 PM	1 months	Nisa Sharif	Stored
	456123790		09/20/2021 1:23 PM	1 months	Nisa Sharif	Activating
Sho	wing 1 to 4 of 4 entries pdate Create Attestation					Previous 1 Next

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

Attestation Next Date Batch Update
Note: Using this will NOT create an Attestation. This will only set the device(s) Next Date and Period to the values chosen.
Number of affected device(s) is 1
Audit Next Date
03/03/2022 12:00
Attestation Period 0
Configuration based (Yearly)
Save

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

Viewing Upcoming Attestations

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

eno >> Devices with a Next Audit Date in the future. es on page				
eno >>> Devices with a Next Audit Date in the future.				
eno >>> Devices with a Next Audit Date in the future. es on page				
>> Devices with a Next Audit Date in the future.				
Devices with a Next Audit Date in the future.				
es on page				
		Se	earch:	PDF
Number	* Audit Next Date	Device Attestation Period	Contact	Oevice State
00300 100200300	03/17/2022 12:58 PM	Yearly	Jerry Miller	Activated
00300 100200300	03/17/2022 12:58 PM	Monthly	Jerry Miller	Activated
00300 100200300	03/17/2022 12:58 PM	Quarterly	Jerry Miller	Activated
00300 100200300	03/17/2022 12:58 PM	Yearly	Jerry Miller	Activated
	00300 10020300 00300 10020300 00300 10020300 00300 10020300	00300 100200300 03/17/2022 12:58 PM 00300 100200300 03/17/2022 12:58 PM	002300 100200300 03/17/2022 12:58 PM Yearly 00300 100200300 03/17/2022 12:58 PM Monthly 00300 100200300 03/17/2022 12:58 PM Quarterly 00300 100200300 03/17/2022 12:58 PM Quarterly 00300 100200300 03/17/2022 12:58 PM Yearly	002000 100200300 03/17/2022 12:58 PM Yearly Jerry Miller 00300 100200300 03/17/2022 12:58 PM Monthly Jerry Miller 00300 100200300 03/17/2022 12:58 PM Monthly Jerry Miller 00300 100200300 03/17/2022 12:58 PM Quarterly Jerry Miller 00300 100200300 03/17/2022 12:58 PM Yearly Jerry Miller

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

IMPORTANT: Upcoming Attestations table will only display attestations 14 days prior the Audit Next Date.

Viewing Past Due Attestations

- 1. Navigate to the Attestations tab
- 2. Click **Past Due Attestations** in the left column.

	Manage		Shipments	Attestations	Transactions		Documentation	Contact Support	13
Attestations	Past [Due Attesta	ations						
Past Due Attestations	YO	< Salart Partnar		Salart Cliant					
Upcoming Attestations	~~	C. Denote Paravar		CO Delete Calera 2					
Completed Attestations	25	- entries on pa	age					Search:	PDF CSV
		Serial Numb	per	Alt	ernate Key		Past Due Date	Contact	Device State
		100200300				03/1	17/2022 12:58 PM	Jerry Miller	Activated
		100200300				03/1	17/2022 12:58 PM	Jerry Miller	Activated
		100200300				03/1	17/2022 12:58 PM	Jerry Miller	Activated
		100200300				03/1	17/2022 12:58 PM	Jerry Miller	Activated
	Showin	g 1 to 4 of 4 en	tries						Previous 1 Ne

3. Review the **Past Due Date** that the device was scheduled to be audited.

<u>Optional</u>: You can use the Search feature to narrow the list and you can optionally download a list of devices into a PDF or CSV file.

Sending a Reminder to Complete Past Due

Copyright © 2022 Bluefin Payment Systems LLC. All rights reserved. Privileged and Confidential.

Attestations

IMPORTANT: Only Partner Supervisors and Partner Fulfilment user send a reminder to their Sub-Partners, Clients, and Sub-Partner's Clients to remind them to complete past due attestations. The contact person listed for that device will receive the email.

- 1. Navigate to the **Attestations** tab
- 2. Click **Past Due Attestations** in the left column.
- 3. Select the device(s) you want to send a reminder for and click **Send a Reminder NOTE**: You can select up to 500 devices.

	Ma	nage	De	evices	Shipme	ents Attestations
Attestations		Ρ	ast	Due	Attesta	tions
Past Due Attestations			×Q	State	University of	New York 👻 SUNY
Upcoming Attestations						
Completed Attestations			25	\sim	entries on	page
					\$ S	Serial Number
			2		09	9876
		(11	111111
		(12	234
		(45	6123790
		SI	nowin	g 1 to	4 of 4 entrie	es
			Comp	olete A	Attestation	Send a Reminder

Device Tampering Detection

Bluefin's P2PE devices have <u>three mechanisms to detect tampering</u>, 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.
- <u>If the device does *not* detect tampering at the time</u> (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 <u>suspect tampering by certain processing attempt patterns</u> 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 User Roles & Permissions	Client Admin	Client Custodian	Client Procurement	Client User	
Devices	Manage	Manage	Manage	View	
Shipments	Manage	Manage	View	View	
Attestations	Conduct	Conduct	Conduct	Conduct	
Encrypted Transactions	View	(No Access)	(No Access)	View	
Reports	Yes	Yes	Yes	(No Access)	
Equipment	Yes	(No Access)	Yes	(No Access)	
Users	Manage	(No Access)	(No Access)	(No Access)	
Locations	Manage	(No Access)	(No Access)	(No Access)	
Device Transfer	Manage	Manage	(No Access)	(No Access)	

Partner Roles

Partner User Roles & Permissions	Partner Supervisor	Partner Fulfilment	Partner User	
Devices	Manage	Manage	Manage	
Shipments	Manage	Manage	(No Access)	
Attestations	Conduct	Conduct	Conduct	
Encrypted Transactions	View	View	View	
Reports	Yes	Yes	Yes	
Equipment	Yes	Yes	Yes	
Users	Manage	(No Access)	Manage	
Locations	Manage	(No Access)	Manage	
Device Transfer	Manage	(No Access)	Manage	
Partners	Manage	(No Access)	Manage	
Clients	Manage	(No Access)	Manage	
Import Clients	Yes	(No Access)	Yes	

Appendix: Receiving and Activating Your Device

You will receive your device in the mail.



IMPORTANT: You must complete <u>each</u> of the steps below before you can use your device!

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

!! Do <u>not</u> 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: <u>P2PE Manager</u> (https://bluefin.p2pemanager.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 <u>from</u> "noreply@p2pemanager.com" and the <u>subject line</u> is: "Welcome to Bluefin's P2PE Manager!")

	Bluefin [®]
	Portal Login
User Name *	
Password *	
	Log In Forgot password
	* indicates required entry

Step 2: Log Receipt of the Shipment

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

Bluefin °	Dashboard	Manage	Devices	Shipments	Attestations	Tran

Notifications

. There is an open shipment in your account that requires acceptance. Please receive it at your earliest convenience.

To log receipt of your shipment, do the following:

Optional: To **Batch Receive** the devices in a shipment, refer to <u>Batch Receiving Devices</u>.

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.

Dashboard Manage Devices	Shipments	Inventory	Reports	Order Equipment	Deploy Equipment	Opt Out
In-coming Shipments	Shipment	6				
	All					
	25 💌 er	tries on page				
		Carrier			Tracking	
	۲	FedEx			5697 2562 2365	
	Showing 1 to 1	l of 1 entries				

3. 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, <u>open</u> the secure bag and <u>save the bag</u>. 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.)



Shipments	Attestations	Transactions	Reports	Equipment	Opt Out	Documentation	Contact Support			Disneyland
	David		,							
	A Ser	ial Number	0 A	lternate Key		Device Name	0 Tamper Label	Device State	© Received Date	Received
	1234	56					<< not received>>	In Transit		Receive
	1234	56*					<< not received>>	In Transit		Receive
	1234	56**					<< not received>>	In Transit		Receive
	Showi	ng 1 to 3 of 3 entri	es							
	Bato	h Receive								

4. 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
	303541015
Security Seal	Auto Activate device Receive Cancel

5. <u>Optional</u>: 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 <u>before</u> entering the device serial number and tamper label. 6. Click **Receive**. Notice that the **Device State** and **Received Date** fields are updated.

Devices				L	Ļ
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:

2.

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

Dashb	ooard Mana	ge Dev	vices Ship	oments Ir	nventory	Reports C	order Equipment	Deploy Equip
ick the	e Edit icon	() next to	the dev	vice yo	u want to a	activate.	
Dashbo	Manage	Devices	Shipments	Inventory	Reports	Order Equipmer	t Deploy Equipm	nent
Device	es							
25	 entries on page 							
	Serial Numb	er 🔺 🖊	lternate Key	Name	,	Device Typ	e 🍦 Device	State
	0135100005					SecuRED	Activated	1
1	11115823			SREDK	ΈY	SREDKey	Stored	_
1	11115824			SREDK	ΈY	SREDKey	Stored	

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



- 4. <u>Optional</u>: 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, Work-station.
- 5. 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 State will automatically change <u>from</u> Activating to Active.

Reporting a Tampered Device

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

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

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

Email: <u>service@bluefin.com</u>

Phone: 800-675-6573 Option 4

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

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

Appendix: Partners

IMPORTANT: Capabilities restricted to Partners are described here.

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
Welcome Email	When a new user is added to P2PE Man- ager, login credentials are sent in email along with a link to set up a password.	P2PE User
Password Reset / Forgotten Password	When a user forgets their password, an email is sent with a link to set up <u>new</u> pass-word	P2PE User
Shipment	An email is sent when a device is shipped.	Device Custodian
Shipment Overdue	An alert is sent to the Custodian when a device shipment is not received within 14 days of it's ship date.	Device Custodian
Device State Changes	Notification that the device's state has changed. Refer to <u>Device State</u> <u>Definitions</u> .	Device Custodian
Attestation Due	10 days <u>prior</u> to the device audit date a notification is sent. NOTE : 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
Attestation Late	If an attestation is missed, 10 days <u>after</u> the device audit date an alert is sent. NOTE : If <u>multiple</u> devices are late, then <u>one email</u> that summarizes all late devices will be sent.	Device Custodian
Attestation Complete	Confirmation of completed attestation.	Device Custodian
Action Needed	Notification that action is needed when the following issues are detected: Device firmware issue detected Device sends clear-text card- holder data	Device Custodian and P2PE User

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 <u>copy</u> of the template that can be customized as <u>all fields</u> in the template can be modified.

	Aanaga Devices Shipments				
Manage	Email Templates				
Users	<< Any Type >>				
Partners					
Clients	1000 v entries on page				1
Partner Device Types		* Title	Subject	Partner	
Locations		Completed Attestations [6]	Bluefin Custom Devices Attestation complete notification		G
Email Templates		Contact Support Request [4]	Bluefin support request		C•
Shared Devices		Deployment Request Submit to KIF [10]	Deployment Request Submit to KIF		0-
Class lossast		Device approaching PTS Expiration Date [18]	Device approaching PTS Expiration Date		C•
Gient import		Device Bad Firmware [13]	ACTION NEEDED: Bluefin device issue detected		G
Device Transfer		Device Deployment Request to Salesforce [9]	60654 P2PE DEPLOYMENT - {{clientName}}		C*
System Notifications		Device Order Request to Salesforce [8]	60654 P2PE Manager Device ORDER		C•

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.

Partner	
A2Z Partner	
Type *	
Attestation notification	
То *	
{{merchantEmail}}	
From *	
no-reply@p2pemanager.com	
subject ~	
ACTION NEEDED: Bluefin Devices re Data Tokens Please select the	Idy for Attestation
ACTION NEEDED: Bluefin Devices re Data Tokens Please select the Sody *	Idy for Attestation
ACTION NEEDED: Bluefin Devices re Data Tokens - Please select the Body * There are {(amount); device(s) ready f	Idy for Attestation
ACTION NEEDED: Bluefin Devices re Data Tokens - Please select the Body * There are ((amount)) device(s) ready f Location(s): (flocation)) Serial Number(s) (fullserial number): ((serial)	ady for Attestation
ACTION NEEDED: Bluefin Devices re Data Tokens - Please select the r Body * There are ((amount)) device(s) ready f Location(s): ((location)) Serial Number(s) (fullserial number): ((serial)) To complete the Attestation of your device)	ady for Attestation Jata token which you want to insert to the body - • r attestation inspection. ices, 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.
ACTION NEEDED: Bluefin Devices re Data Tokens - Please select the Body * There are {(amount)) device(s) ready f Location(s): {(location)} Serial Number(s) {fullserial number): {(serial)} To complete the Attestation of your devices Essentially, you are checking to make	ady for Attestation ady for Attestation Jata token which you want to insert to the body • or attestation inspection. ices, 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 reviews ure 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.
ACTION NEEDED: Bluefin Devices re Data Tokens - Please select the Body * There are ((amount)) device(s) ready fr Location(s): ((location)) Serial Number(s) (fullserial number): ((serial)) To complete the Attestation of your der Essentially, you are checking to make If you need more information, please co	ady for Attestation I atta token which you want to insert to the body adv for Attestation Inspection. I atta token which you want to insert to the body adv for Attestation inspection. I cose, 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 I ure 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. I teck the Documentation tab in the P2PE Manager.
ACTION NEEDED: Bluefin Devices re Data Tokens - Please select the Body * There are ((amount)) device(s) ready f Location(s): ((location)) Serial Number(s) (fullserial number): ((serial)) To complete the Attestation of your dev Essentially, you are checking to make If you need more information, please of If you did not expect this mail or have a	ady for Attestation

Deleting Email Templates

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

Administration

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

Editing Your Own Partner Record

To edit your partner record, go to **Manage > Partner**. You can edit the fields based on your preference. Refer to **Adding a Partner Record (Sub-Partner)** for a details about each field.

NOTE:

- For the optional section **API Security**, refer to the Developer's portal for more information.
- To tokenize data using ShieldConex refer to Tokenization Configuration at the bottom of the page. Select a Provider (ShieldConex), Authorization Type (Basic or HMAC) and <u>enter</u> the appropriate ShieldConex template reference number (from your ShieldConex Partner account).
- Once these settings are selected, they apply all of your sub-partners and clients.

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

Field	Description
	Location Type * Corporate Headquarters Struttiment location Corporate Headquarters Field Office KiF Manufacturer Manufacturer iong term storage Marchant CSR location Merchant retail location Merchant retail location Merchant short term storage location Merchant retail location Merchant short term storage & distribution Partner Location Regional Office Vendor fulfilment location Required. Enter: Location Name, Address, City, Country
Mail Address	Optional.
Customization	
- Remember Devices	Optional. Select an option from the drop-down list.
- Attestation Period	Optional. Select an option from the drop-down list.
- Contact Support Over ride?	IMPORTANT : This field is restricted to Partner Supervisors Only.
	Optional. Select the checkbox to customize the Contact Support email address that displays on the Contact tab for subpartners and clients.
	Enter the Support Email address when prompted.

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
Direct Partner	Required. Select the partner from the list.
Name	Required. Enter the client's/merchant's name.
Active	Optional. Select the checkbox to enable the client.
Mid	Optional.
Contact Person	Required. Enter the First Name, Last Name, Email address, Phone and User Name.
	Best Practice: Use first initial and last name and email address for the user name. (EXAMPLE : jdoe@yourcompany.com.)
	NOTE : The Active checkbox for the contact person is selected for you.
Location	Select the Location Type. Location Type * Corporate Headquarters For Millinem Iocation Fried Office KIF Manufacturer Iong term storage Merchant long term storage & distribution Merchant short term storage & distribution Merchant shor
Mail Address	Optional.
Remember Devices	Optional. Select an option from the drop-down list.
Force users to use two-factor authen- tication	Optional checkbox. You can enable two-factor authentication. When it is enabled, it will affect <u>all users</u> who belong to the Cli- ent <u>or</u> Partner record.
Send welcome email	You can send new users a welcome email. This option is selected by default.
Contact Support Over- ride?	Optional. Select the checkbox to customize the Contact Support email address that displays on the Contact tab for subpartners and clients.

Field	Description
Attestation Period	Optional. Select an option from the drop-down list.

4. 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 <u>Adding a User</u>.

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:

Bluefin Appreciates You	-	<< Any Status >>	۳
-------------------------	---	------------------	---

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: <u>Do not Edit the Contact Field</u>. Instead, click **Update Contact Person**.

To update the contact person, do the following:

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

Corporate Headquarters			
Location Name *			
Disneyland			
Name Of Business			
Name Of Business			
Address 1 *			
8200 Roberts Dr			
Address 2			
Address 2			
City *		Postal Code	
Atlanta		30324	
Country *		State Province	
United States	•	<< Select State/Province >>	
Mail Address			
Remember Devices 0			
Every time			
Force client users to use two-factor authentication			
Send welcome email			
Save Cancel			Update Contact Person De
* indicates required entry			

- 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

Import Client Data		
Csv file * (limit of 500 rows per file)		
Choose File No file chosen		
Upload Cancel		Sample CSV
FILE UPLOAD * indicates required entry	CONFIRMATION	RESULTS

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	
DirectPartner	Required.	
ClientName	Required.	
LocationName	Required.	
LocationType	Required.	
Location Type * << Select Location Type >> BF fulfillment location Corporate Headquarters Field Office KIF Manufacturer Manufacturer long term storage Merchant CSR location Merchant retail location Merchant short term storage & distribution Partner Location Regional Office Vendor fulfillment location	Options: BF Fulfillment location, Corporate Headquarters, Field Office, KIF, Manufacturer, Manufacturer long time storage, CSR Location, Me chant Long time storage location, Merchant Retail Location, Merchant short term storage & dis- tribution, Partner Location, Regional Office, Vendor Fulfillment Location	
LocationNameofBusiness	Optional.	
LocationCountry	Required.	
LocationAddress1	Required.	
LocationAddress2	Optional.	

Fields	Description
LocationCity	Required.
LocationState	Optional.
LocationPostalCode	Optional.
UserName	Required.
UserRole	Optional.
FirstName	Required.
LastName	Required.
Email	Required.
Phone	Required.

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

4. Click **Upload**.

Running Reports

Partners can run the same reports as clients and additional reports that are restricted to just partners. Oftentimes the only difference between how clients/partners run these reports is in setup parameters. <u>Partners must populate the Partner and Client fields</u> by selecting an option from a drop-down list.

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

Related Information: See Exporting a Report.

Partner Summary

This report summarizes the following information: Partner, Path, Total Clients, Total Locations, Active and Inactive Users, Active Devices and Other Devices.

Partner Summary								
			s	earch:			PDF	CSV
A Partner	† Path	♦ Total Clients	♦ Total Locations	♦ Active Users	♦ Inactive Users	♦ Active Devices	♦ Oth Dev	ier vices
A2Z Partner	A2Z Partner	1	3	16	0	0	20	
ABC SubPartner	A2Z Partner -> ABC SubPartner	2	1	3	0	0	0	
DEF Subpartner	A2Z Partner -> DEF Subpartner	0	0	0	0	0	0	
GHI SubPartner	A2Z Partner -> GHI SubPartner	0	0	1	0	0	0	
Showing 1 to 4 of 4	entries							

Select **Reports** > **Partner Summary** to generate this report.

<u>Optional</u>: Use the Search field to narrow the results. You can also download the report as a PDF or CSV.

Client Summary

This report summarizes the following information: Partner, Direct Partner, Path, Client, Location, Active Users, Inactive Users, Active Devices and Other Devices.

				Se	arch:			PDF	CSV
Partner	Direct Partner	† Path	Client	↓ Location	+ Active Users	♦ Inactive Users	Active Devices	¢ O	ther evices
A2Z Partner	A2Z Partner	A2Z Partner	Blue Surf Resorts	Blue Surf Resorts Corporate Headquarters	8	0	0	20	
A2Z Partner	ABC SubPartner	A2Z Partner -> ABC SubPartner	Blueridge Mountain Spas	Blueridge Mountain Spas Headquarters	1	0	0	0	
A2Z Partner	ABC SubPartner	A2Z Partner -> ABC SubPartner	Blueridge General Stores	Blueridge General Stores	2	0	0	0	

Select **Reports** > **Client Summary** to generate this report.

<u>Optional</u>: Use the Search field to narrow the results. You can also download the report as a PDF or CSV.

Partner Transaction Summary

Partner Tran	isaction Sum	nmary		-								-			_	
A2Z Partner		• Q	× Date	From			U	ate lo				_Search I	based on UT	c	Apply	
											S	earch:			PDF	CSV
A Partner	Direct Partner	Total Messages	o Total Decrypt	Good 3DES/CBC	Good 3DES/ECB	BPS Good	RSA- 2048 Good	AES- 128 Good	3DES/CBC Bad	3DES/ECB Bad	BPS Bad	RSA- 2048 Bad	AES- 128 Bad	Total Partner Validate	Tota Devi Valid	il ice date

To generate this report do the following:

- 1. Select **Reports > Partner Transaction Summary**.
- 2. In the header, select a **Partner** from the drop-down list.
- 3. In the header, specify a date range using the date pickers.
- 4. Optional. You can select the checkbox **Search based on UTC** which converts the browser time (e.g. EST, PST) to Greenwich Mean Time (GMT) for the query.
- 5. Click **Apply** when you're done.

Optional: Download the report as a PDF or CSV.

Billing Report

You can use the Billing Report to assist with client billing. This report summarizes all clients and includes BillingID, ActivityDate (start date based on date range specified) and DeviceCount (total of activated devices.)

MacCause Calanta - X Q Dat Free	te 12/17/2020 12:00:00 🖬 Date To	2/18/2020 12:00:00	
25 × entries on page		Search:	CSV
• BillingId	ActivityDate	DeviceCount	
BI - XYZ987	2020-12-17 17:56:31	40	
BI - ABC123	2020-12-17 17:56:31	20	

To generate this report do the following:

- 1. Select **Reports > Billing Report**.
- 2. In the header, select a **Partner** from the drop-down list.
- 3. In the header, specify a date range using the date pickers.
- 4. Click **Apply** when you're done.

Optional: Download the report as a CSV.

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.

Manage	Partner Device Types
Users	A2Z Partner 🗸 🔍 🗶
Partners	
Clients	Device Type
Partner Device Types	 Augusta S
Locations	Bluepad-50
Shared Devices	 ExaDigm N5
Client Import	✓ iDynamo
Device Transfer	Ingenico ICMP
	✓ Ingenico iSC Touch 480
	✓ Ingenico iSC250 Touch
	Ingenico iUC150B
	Ingenico iUP250LE

NOTE: If a device is <u>missing</u>, please contact Bluefin support or your relationship manager.

Shared Devices

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

To <u>display</u> 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 Locaction.

Device Transfer

IMPORTANT: Only System users and administrators can move devices <u>across</u> Partner or Client records.

To transfer devices <u>under the same Partner and Client record</u>, refer to <u>Transferring a Device</u> <u>between Custodians or Locations</u> 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 <u>one Identity Provider</u> and is implemented by System Users

Benefits

Single Sign-On (SSO) enables seamless integration between the system that partners / subpartners / 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.



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

usernames. **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 <u>one Identity Provider</u> 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 <u>after</u> receipt of the **Single Sign-On Request Form**.

- URLs (The names of the fields vary such as ACS, Audience or Consumer.)

- Consumer Validator: bluefin.p2pemanager.com/saml/callback/samlconfigkey
- Consumer Connection URL: bluefin.p2pemanager.com/saml/callback/samlconfigkey
- Logout URL: (Depending on the IDP this might or might not be needed)
 bluefin.p2pemanager.com/logout

EXAMPLE:

https://cert-bluefin.p2pemanager.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	
Issuer URL 3 https://app.onelogin.com/saml/metadata/e5cab9ee-9bbc-4a19-998e-9e967b82db	ß
Issuer URL 3 https://app.onelogin.com/saml/metadata/e5cab9ee-9bbc-4a19-998e-9e967b82db SAML 2.0 Endpoint (HTTP) 4	•
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-4a19-9	6
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-4a19-9 SLO Endpoint (HTTP)	6

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

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)	
user@bluefin.com	
E-mail (Attribute)	
user@bluefin.com	
First Name (Attribute)	
Mister	
Last Name (Attribute)	
User	
Member of (Attribute)	
PersonImmutableID	
p2pe_username	
muser	
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 <u>not</u> 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**.

	21.368-0116	ources, services, and docs (G+/)	and the second		CETAIAT CHECTORY
Home > Default Directory Overview					
Default Directory Over Acres Acres Directory	rview				Documentation of
,0 Search (Ctrl+/)	« Switch directory 🔋 Delete directory + Create a dire	ectory 📑 What's new 🛛 🗢 Got feedback?			
O Overview					
🛒 Getting started	Azure Active Directory can help you enable remote work for	your employees and partners. Learn more			×
X Diagnose and solve problems					
Manage	Overview				
🚨 Users	Default Directory			Find	
A Groups	bluefinqaoutlook.onmicrosoft.com	Your role Global administrator and 1 other roles More info		Users	~
Crganizational relationships	Tenant ID bb62d282-13d4-41b1-bf12-0e422fad2e5a 🔯	Azure AD Free		Search.	
& Roles and administrators	~				
Enterprise applications	Azure AD Connect				
Cevices	Status Not enabled				
App registrations	Last sync. Sync has never run				
(A) Identity Governance					
Application proxy					
🛔 Licenses					
Azure AD Connect	Sign-ins				
Custom domain names			-		
D Mobility (MDM and MAM)	,				
Password reset					
Company branding	1				
User settings	1				
III Properties	Mar 8	Mar 15	Mar 12	Mar 29	

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

Microsoft Azure		P Search resources, ser	nces, and docs (G+/)			E 8	0	2	Diuefin-qat	Boutlook.co
Home > Default Directory > Enterprise a	epplications All applications									
Enterprise applications Debut Directory - Autor Action Directory	All applications									
< Overview	+ New application III Colum	m								
O Deniew	Try out the new Enterprise Apps to	earch preview! Click to enable the previe	m. ~4							
X Diagnose and solve problems	Application Type Enterprise Applications	Applications status	Application visibility	Apply Reset						
Manage										
All applications	First 10 shown, to search all of your	applications, enter a display name or	the application 10.							
Application proxy	Name	Ho	mepage URL		Object ID		A	oplication 1	D	
@ User settings	Azute AD SAML Toolkt	htt	ps://www.microsoft.com/		c451df33-06f9-42a5-6d9a-c7febe370fea		8	11c3f34-8fa	7-4f93-b764-2022be2	:34ce5
Security		D								
Sconditional Access										
Activity										
Sign-ins										
ua Usage & insights (Preview)										
Audit logs										
Provisioning logs (Preview)										
Access reviews										
Admin consent requests (Previe										
Troubleshooting + Support										
🐨 Virtual assistant (Preview)										
A New support request										

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

Microsoft Azure	P Searchire	ources, services, and docs (5+))		000000	bluefin-qa@outloo
Home > Default Directory > Enterprin	e applications All applications > Azure AD SAML Toolkit Overview	1			
Azure AD SAML Toolki	t Overview				
Coenser Co	Properties Properties Aura 40 344, tusht Application 0 Applica	/ /			
Single sign-on Provisioning Self-service Security Conditional Access arministice	1. Assign users and groups Provide specific users and groups access to the upplications Assign users and groups	2. Set up single sign on Enable uses to sign into their application using their Asive AD ordentials Get stanted	Provision User Accounts Voull need to create user accounts in the application Latin more	4. Conditional Access Secure access to this application with a contomotable access policy. Create a policy	
Token encryption Activity Sign-ins Casepe & insights (Preview) Activity Activit	 S. Self service Enable users to request access to the application using their Asure AD ordentals: Get started 				
Access reviews Access reviews Traublishapting + Support	What's New Sign in charts have moved! The new insights view shows sign in info along with oth	er useful application data. View insights			

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.

onfiguration guide of for help integrating SA	ML test signon.	62	
asic SAML Configuration		0	
lentifier (Entity ID)	p2pe_username		
eply URL (Assertion Consumer Service URL)	https://bluefin.p2pemanager.com/saml/callback/ 66c23c64c22f1fb3691b806ff4a72e88		
ign on URL	Optional		
lelay State	Optional		
ogout Url	Optional		
Jser Attributes & Claims		0	2
ivenname	user.givenname		
urname	user.surname		
mailaddress	user.mail		
name	user.userprincipalname		
Inique User Identifier	user.userprincipalname		
AML Signing Certificate		0	
tatus	Active		
Thumbprint	0E75A56251387629C16121487B55388989B4B43B		
xpiration	4/3/2023, 2:12:05 PM		
Notification Email	bluefin-qa@outlook.com		
App Federation Metadata Url	https://login.microsoftonline.com/bb62d282-13		
Certificate (Base64)	Download		
Certificate (Raw)	Download		
ederation Metadata XML	Download		
		_	
et up SAML test signon			
ou'll need to configure the application to link	c with Azure AD.		
ogin URL	https://login.microsoftonline.com/bb62d282-13		
zure AD Identifier	https://sts.windows.net/bb62d282-13d4-41b1		

Single Sign-On Request Form (Sample)

Do the following:

- 1. Complete this form and submit to Bluefin. (<u>service@bluefin.com</u>)
- 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 <u>create a field</u> 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 <u>one</u> Identity Provider per partner.

Partner Name	Enter the partner / sub-partner name. This will enable SAML for partner users (Partner Supervisors, Partner Fulfillment and Partner User.)
SAML Config Name	Enter the name of this SAML configuration.
SAML End Point	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.
SAML Field Name	The field/variable that contains the P2PE Manager Username. This could be a custom parameter from the Identity Provider or an existing one that con- tains the P2PE Manager Username.
	NOTE : The IDP administrator will need to create this field in their single sign-on system to validate P2PE Manager usernames.
SAML Issuer	Enter the Issuer URL of the Identity Provider. This is the URL of the Part- ner's IDP user connection to the P2PE Manager.
Certificate file included	Enter the Certificate from the Identity Provider that signs the authentication request.
	NOTE : The entire content of the certificate must be entered. (URL links are not allowed.)
	TIP : 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.
Bluefin returned SAML Con- figuration KEY	Bluefin will return this form with this value when the setup has been completed.

2.) SUBMITTER INFORMATION			
Submitted By [Name of Person Submitting Change Request]			
Submitter's Company [Name of Submitter's Company]			
Pate Submitted [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.