



P2PE Device Managing Merchant Portal

Contents

- P2PE Manager overview 5**
 - Terminology 5
- Portal access 6**
 - URL..... 6
 - Logging In 6
 - Notification 7
 - Account Settings..... 8
 - Managing Your Personal Settings 8
 - Resetting Your Password (Forgotten Password) 9
- Client / Merchant Roles 9**
- Menu Options at a Glance 10**
- Dashboard 10**
- Manage Tab 12**
 - Users 12
 - Adding a User..... 12
 - Updating a User..... 14
 - Resetting a User’s Password 14
 - Locations..... 14
 - Adding Locations 14
 - Removing Locations..... 15
 - Editing Locations..... 15

Device Transfer	15
Transferring a Device between Custodians or Locations.....	15
Transferring Devices in bulk between Locations.....	16
System Notification	18
Shipments Tab	18
Shipments Tracking	18
Receiving and Activating Device	19
Device activation.....	19
Overview.....	19
Step 1. Access the P2PE Manager Online	19
Step 2: Log Receipt of the Shipment.....	20
Step 3: Activate Your Device.....	22
Batch Receiving Devices	24
Receiving Device with Special Serial Number Requirements	26
Reporting a Tampered Device	27
Devices Tab	28
Updating Devices	28
Device State Definitions	29
Return Merchandise Authorization Process.....	30
Viewing Device Details	31
Chain of Custody.....	31
History	32
Lifecycle	32
Inspections	33
Attestations.....	34
Past Due Attestations.....	34
Upcoming Attestations.....	36

Completed Attestations	37
Changing Device Attestation Date.....	38
Batch Process: Change Device Attestation Date	39
Reports	40
POI Chain of Custody Report.....	40
Client Transaction Summary Report.....	41
Inventory Summary.....	41
User Report.....	42
Device Activity	43
Device Receipt.....	43
Daily Report.....	44
Decryption Totals Report.....	44
Documentation.....	45
Downloading and Viewing PDF Files	45
Downloading and Viewing Video Files.....	45
Contact	46

P2PE Manager overview

P2PE Manager is a web-based management system provided in conjunction with Bluefin's P2PE solution. P2PE Manager assists merchants in chain of custody management required for PCI compliance

Bluefin P2PE Manager portal provides the below features at a high level.

- Checking in new devices
- Creating new users and locations
- Managing PCI P2PE chain of custody
- Changing state of device
- Conducting annual PCI device attestations
- Reporting capabilities

Terminology

Key terms used throughout this guide are defined below:

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

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

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

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

Portal access

URL

<https://bluefin.p2pmanager.com/login>

Logging In

Once you are added as a user in Bluefin P2PE manager, you will receive a system-generated **Welcome** email with your username.

If you have not received an email to register, please contact

PHONE: 866-290-5400 Option 5

EMAIL: customerservice@forte.net

P2PE Manager is Bluefin's online portal for managing chain of custody and activation status of your point-to-point encryption devices. Please click the link below to setup your password. Additionally, you will receive an email notification from Bluefin Demo's Client Service with implementation instructions for the POS system

USERNAME: username

URL: <https://staging-bluefin.p2pmanager.com/forgot?code=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOiJlbnR5c2NjAsImV4cCI6MTQ3NDM5ODI2MCwic3ViljoidXNlcm5hbWUifQ.1Lt1WhVAnFla2DExqwEkqFBom1FftV0IUrBrxFmgEJU>

If you did not expect this mail or have any questions, do not reply to this email. Please email service@bluefin.com or call 800-675-6573 as soon as possible.

Thank you!

Bluefin Demo Merchant Support

bluefin.com/merchant-support

service@bluefin.com

800-675-6573 Option 2

Follow the instructions in the email:

1. Click the link in the email.
2. Create a new password.
3. Click **Reset**.

Reset password

User Name *

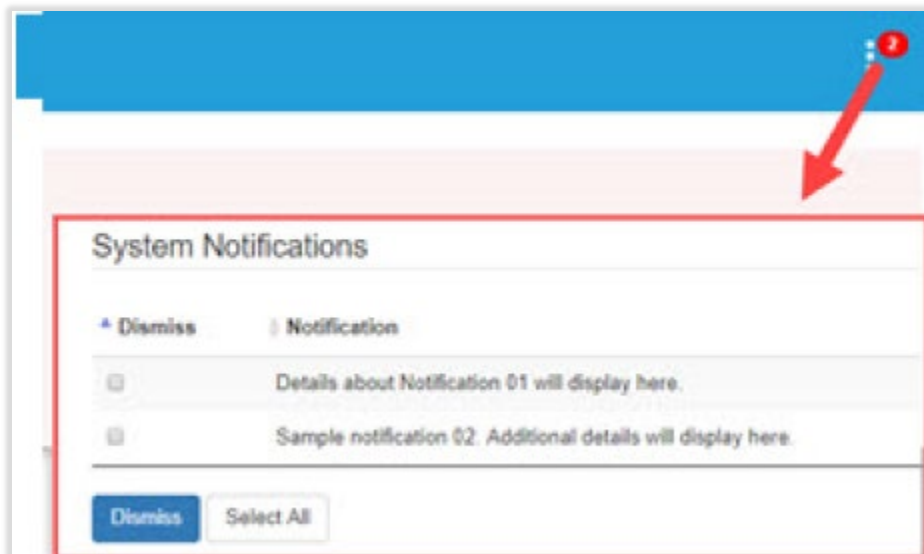
Password * ✓

Password confirm * ✓

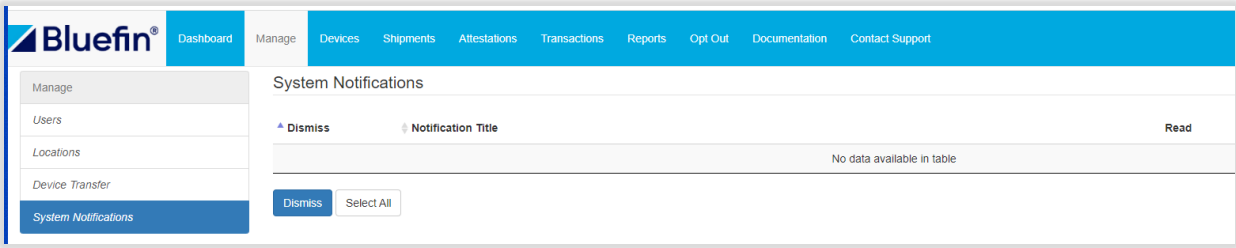
Notification

The Notifications banner displays alerts from the administrator when published.

- Click the red **notifications icon** in the top right corner, to review and see a list of unread notifications.
- Click **Dismiss** to remove it.
- Click **Continue**, to hide the notification banner.



You may also navigate to notifications, from **Manage > System Notifications**, to read or dismiss a notification



Account Settings

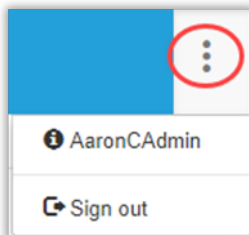
Managing Your Personal Settings

Your Personal Settings include:

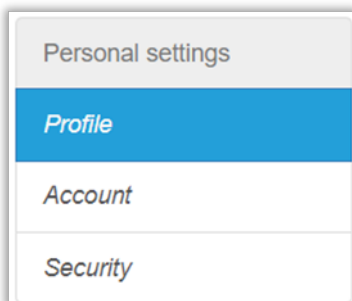
- Profile: Update your name, email address or your default login landing page (**NOTE:** Landing Page options are based on your user role.)
- Account: Update your password
- Security: Set up two-factor authentication

To access your personal settings, do the following:

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



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



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

Resetting Your Password (Forgotten Password)

If you forget your password, do the following:

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

Portal Login

User Name *

Password *

2. Follow the prompts to reset your password.

Client / Merchant Roles

	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	Yes
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	(No Access)	(No Access)	(No Access)

Menu Options at a Glance

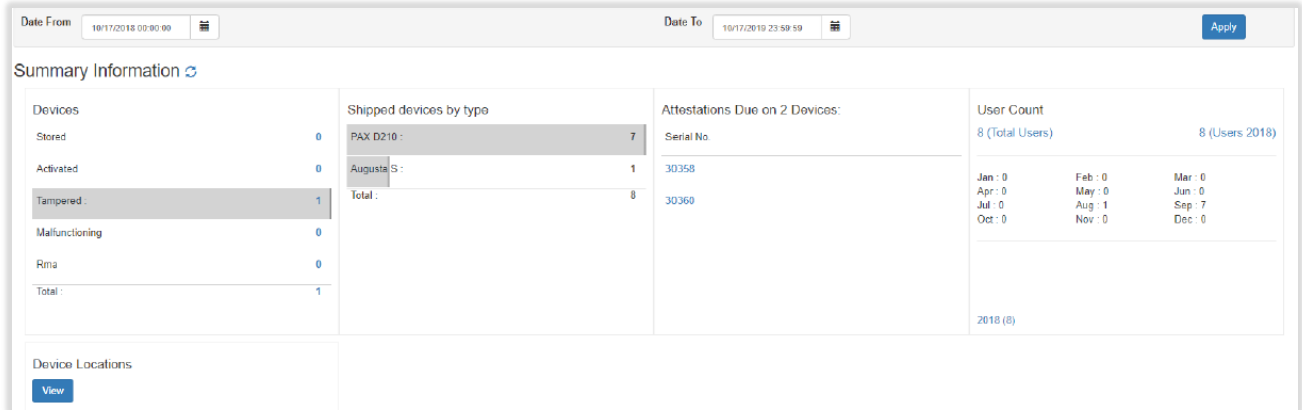


The tabs at the top of the screen, provides access to different menu options, depending on your level of access mentioned in [Client/Merchant Roles](#) table

Tab	Description
Dashboard	The dashboard displays a summary of your devices and other useful information organized in "tiles."
Manage	Provides ability to Manage Users, Locations and Device Transfers and System Notification
Devices	Displays a summary of all devices.
Shipments	Displays incoming shipments.
Attestations	Displays Current Attestations, History and Future Attestations.
Reports	POI Chain of Custody, Client Transaction Summary, Inventory Summary, User Report, Device Activity, Device Receipt, Daily Report and Decryption Totals.
Documentation	Provides documentation such as User Guides, Instruction Manuals and Video Library
Customer Support	Submit a help request online and review help contact information.

Dashboard

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

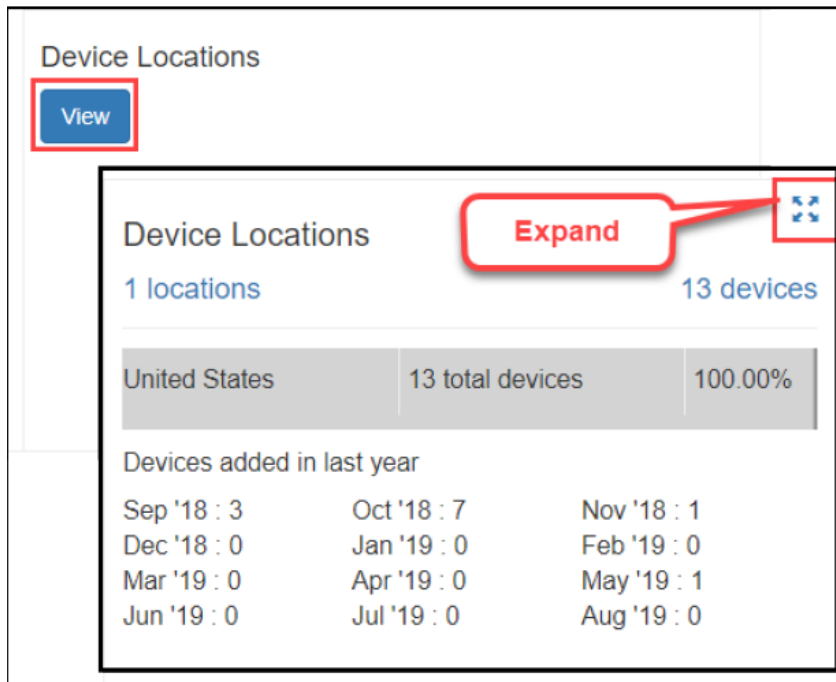


The information displayed is dynamic based on the date range specified and includes the following information:

Note: Based on the user role the dashboard information changes

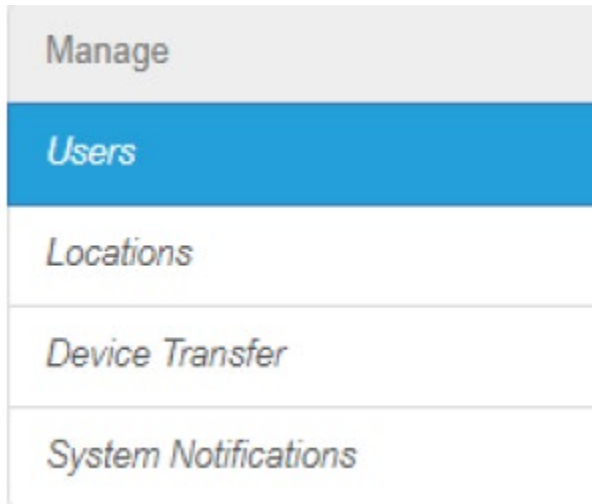
- Number of Devices by State
- Number of Shipped devices by Device Type
- Number of Devices due for Attestation
- Number of P2PE Manager Users in your account monthly - User Count
- Number of Devices by Location (active devices by country)

NOTE: When there's a lot of data to summarize in any "tile", You may click on **View** button to populate the data under the tile or click on **Expand** icon to enlarge a tile.



Manage Tab

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



Users

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

The screenshot shows the 'Users' page with a table of users. At the top, there is a search bar and a 'CSV' button. The table has columns for First Name, Last Name, Email, Phone, User Name, and Role. Each row has a pencil icon for editing.

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

Use the column names at the top to sort the list.

Adding a User

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

Manage

Users


User details - << empty >> << empty >>

First Name *

Last Name *

Email *

Phone *

 +1 Phone

User Name *

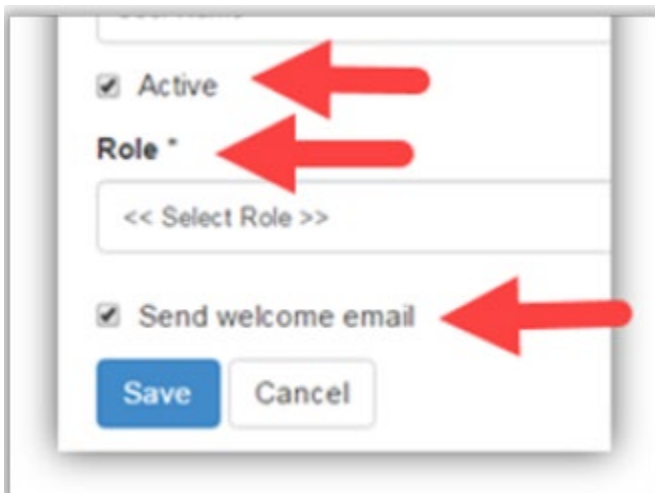
Active

Role *

Send welcome email

* indicates required entry

3. Check the **Active** check box



Active

Role *

Send welcome email

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

Updating a User

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

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

Resetting a User's Password

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

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

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

Locations

Adding Locations

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

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

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

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

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

Field	Description
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, Country, State Province
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 Transfer

Transferring a Device between Custodians or Locations

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

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

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

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

1. Click **Edit** (pencil icon) next to the device you would like to transfer.
2. Click the **Chain of Custody** tab and then click **Create**.
3. Complete fields and click **Save**. Transfer Method:
 - a. Choose Manual if device is handed off or if someone else taking responsibility for the device.
 - b. Choose Shipment if device is being mailed from one location or custodian to another. Complete additional fields when prompted

The screenshot shows a web form titled "Chain Of Custody - 321654". It contains several input fields: "Location *" with a dropdown menu and search icons; "Transfer Method *" with a dropdown menu showing "Manual" and a green checkmark; "Custodian *" with a dropdown menu and search icon; "Complete Date" with a date picker showing "06/14/2016"; and "Notes" with a text area. At the bottom right, there are "Save" and "Cancel" buttons.

Transferring Devices in bulk between Locations

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

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

Prerequisite:

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

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

	A	B	C
1	SerialNumber	Location	DeviceType
2	123AD33377	Company Location 1	SREDKey
3			

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

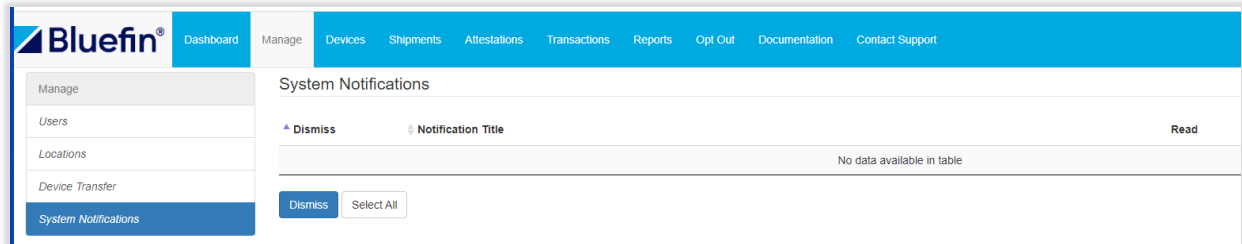
1. Select **Device Transfer** in the left column.
2. Click **Choose File** and navigate to your CSV file.
3. Click **Upload** when you're done.

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

System Notification

The **System Notification** displays notifications from the administrator when published.

From **Manage > System Notifications** you can read or dismiss a notification



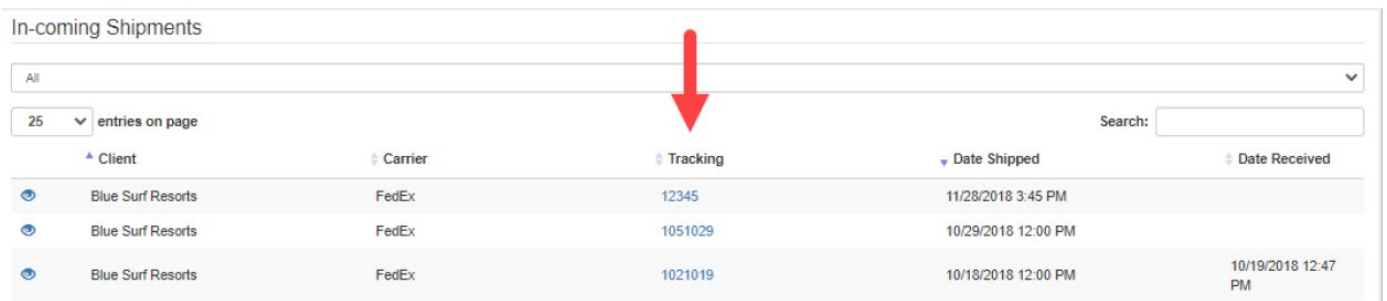
Shipments Tab

Shipments Tracking

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


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

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



In-coming Shipments				
All				
25 entries on page				
Client	Carrier	Tracking	Date Shipped	Date Received
Blue Surf Resorts	FedEx	12345	11/28/2018 3:45 PM	
Blue Surf Resorts	FedEx	1051029	10/29/2018 12:00 PM	
Blue Surf Resorts	FedEx	1021019	10/18/2018 12:00 PM	10/19/2018 12:47 PM

Receiving and Activating Device

 **Video Tutorial:** For video tutorial on **Device Activation**

1. Go to Documentation Tab
2. Download **P2PE Manager Device Activation v3.0.mp4** from **Video Library** section

Device activation

You will receive your device in the mail.



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

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

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

Overview

Step 1. Access the Point-to-Point Encryption (P2PE) Manager Online.
(<https://bluefin.p2pmanager.com/login>)

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

Step 3. Activate Your Device.

Step 1. Access the P2PE Manager Online

To log into P2PE Manager, do the following:

1. Access the P2PE Manager from a browser: [P2PE Manager](https://bluefin.p2pmanager.com/login)
(<https://bluefin.p2pmanager.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 will be sent from "noreply@p2pmanager.com" with the subject line: "Welcome to Bluefin's P2PE Manager!")



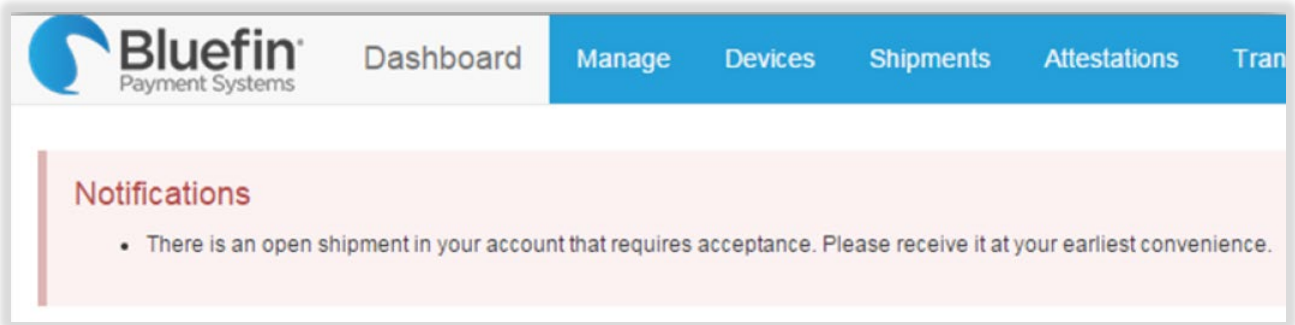
Portal Login

User Name *

Password *

Step 2: Log Receipt of the Shipment

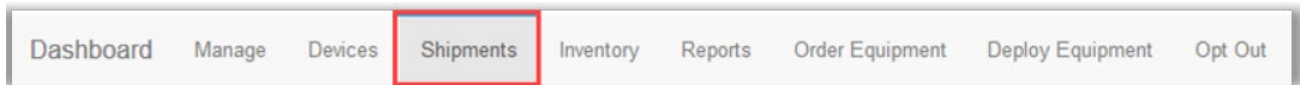
From your dashboard / home screen, you'll see a notification about an open shipment:



To log receipt of your shipment, do the following:

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

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



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

Dashboard Manage Devices **Shipments** Inventory Reports Order Equipment Deploy Equipment Opt Out

In-coming Shipments

Shipments

All

25 entries on page

Carrier	Tracking
FedEx	5697 2562 2365

Showing 1 to 1 of 1 entries

- Match the serial number on the back of your device with the serial number displayed online and then click **Receive** to open **Receiving Device** pop up box.

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



Shipments **Attestations** Transactions Reports Equipment Opt Out Documentation Contact Support Disneyland

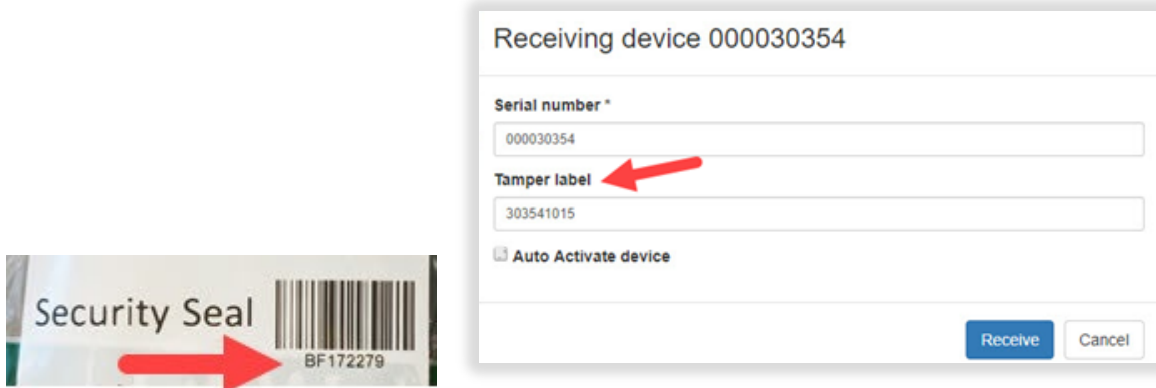
Devices

Serial Number	Alternate Key	Device Name	Tamper Label	Device State	Received Date	Received
123456			<< not received >>	In Transit		Receive
123456*			<< not received >>	In Transit		Receive
123456**			<< not received >>	In Transit		Receive

Showing 1 to 3 of 3 entries

Batch Receive

4. Optional: On the **Receiving Device** pop up, click **Auto Activate device** only if you are ready to activate and start using the device.
NOTE: To take advantage of this time saving option, you must select it before entering the device serial number and tamper label.
5. From the secure packing around your device, locate the **security seal number**, enter it into the **Tamper label** field and click **Receive** on the **Receiving Device** pop up.



NOTE:

- Perform the steps 3, 4 and 5 for each device you receive.
 - The serial number is populated for you based on the device you selected in #3 above.
6. Once received, notice that the **Device State** and **Received Date** fields are updated.


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:




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

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

Dashboard Manage **Devices** Shipments Inventory Reports Order Equipment Deploy Equipment

Devices

25 entries on page

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

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

Name

SREDKEY

Device State *

Current State: Stored

Device Type *

SREDKey

Audit Next Date

05/18/2017

<< Change Device State >>

<< Change Device State >>

Damaged

Retired

Tampered

Malfunctioning

Lost

In Repair

RMA

Activating

4. Optional: If you have multiple devices, you might want to enter a **Name**, so they can be easily identified without the serial number. **EXAMPLE:** Lane 1, Workstation.

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 will automatically change from Activating to Active.

Batch Receiving Devices

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

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

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

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

The screenshot shows the Bluefin P2PE Manager interface. The top navigation bar includes 'Dashboard', 'Manage', 'Devices', 'Shipments', 'Alterations', 'Transactions', 'Reports', 'Opt Out', 'Documentation', and 'Contact Support'. The 'Shipments' tab is active. Below the navigation bar, the 'Shipment details' section is visible. It contains a message: 'Devices can be received individually or using the batch receive option.' The shipment details are as follows:

Shipment		Devices						
Client:	Blue Surf Resorts	* Serial Number	Alternate Key	Device Name	Tamper Label	Device State	Received Date	Received
Tracking:	1041019	30360			<< not received >>	In Transit		Receive
Carrier:	FedEx	Showing 1 to 1 of 1 entries						
Shipment Type:	KF Shipment	<input type="button" value="Batch Receive"/>						
Ship Date:	10/18/2018 12:00 PM							
Date Received:								

A red arrow points to the 'Batch Receive' button in the 'Devices' section.

The 'Receiving device' dialog box is shown. It contains the following sections:

- Receiving device:** A yellow box with the text: 'Scan or enter device serial number and tamper label if present. If device is matched proceed next device.'
- Matching options:** A section with four dropdown menus: 'Matching pattern *' (Full Match), 'Matching length *' (5), 'Padding pattern *' (None), 'Padding length *' (10), and 'Character *' (0).
- Serial number *:** A text input field with the placeholder 'Serial number'.
- Tamper label:** A text input field with the placeholder 'Tamper label'.
- Auto Activate device:** A checkbox that is currently checked.
- Progress:** A progress bar.
- Close:** A button at the bottom right.

2. Optional: Click **Auto Activate device** only if you are ready to activate and start using the device now.

TIP: To take advantage of this time saving option, you must select it before scanning your devices.

3. Scan the **Serial Number**. The whole serial number will be displayed.

NOTE: For Ingenico devices, P2PEManager will automatically find a match based on the input from the Key Injection Facility (KIF.)

4. Scan the **security seal number**. (This number might also be called the tamper seal.) Wait for the green success message.

5. If you selected **Auto Activate device**, you're done! The **Device State** will display as **Activating**.


If you did not select Auto Activate device, then the **Device State** will display as **Received**. To continue, follow the below actions to activate device

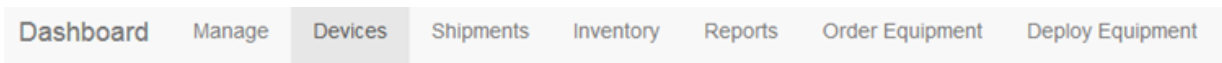
Activate Your Device

To activate your device, do the following:

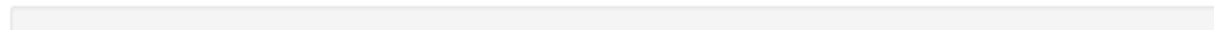
1. Click the **Devices** tab. Here you'll see all your devices.



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



Devices



25  entries on page

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

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

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

4. Optional: If you have multiple devices, you might want to enter a **Name**, so they can be easily identified without the serial number. **EXAMPLE:** Lane 1, Workstation.

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 will automatically change from Activating to Active.

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.

The screenshot shows a web interface titled "Receiving device". At the top, there is a yellow instruction box: "Scan or enter device serial number and tamper label if present. If device is matched proceed next device." Below this is the "Matching options" section, which includes:

- Matching pattern ***: A dropdown menu set to "Partial Match From Start".
- Matching length ***: A dropdown menu set to "5".
- Padding pattern ***: A dropdown menu set to "Pad on the left".
- Padding length ***: A dropdown menu set to "1".
- Character ***: A text input field containing "000000".

 Below the matching options is a "Serial number (searching: 12345) *" field with a red arrow pointing to it, containing the text "123456789". There is also a "Tamper label" field, an "Auto Activate device" checkbox, and a "Progress" bar. A "Close" button is located at the bottom right of the interface.

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


Reporting a Tampered Device

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

- The secure bag is not sealed closed.
 - The secure bag is damaged.
 - The "No Tear" sticker is broken or damaged.
1. Upon receipt of your device, if you suspect it has been tampered with, please contact support immediately by **Email:** customerservice@forte.net or **Phone:** 866-290-5400 Option 5
 2. Complete the steps in [Device Activation](#) above with the following changes:
 - a. Complete Steps 1 and 2 as written.
 - b. In Step 3 Click the **Device State** drop-down arrow and then select **Tampered**.
 - c. Click **Save**.

Devices Tab

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

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

Devices

A2Z Partner 🔍 Blue Surf Resorts << Any State >> Apply Click "Apply" button in order to get devices

25 entries on page Search: Search CSV


Serial Number	Alternate Key	Name	Device Type	Device State	Client Name	Location Name	Activation Date	Mid	Virtual	Notes
000030350		Registration	PAX S300	Activating	Blue Surf Resorts	Blue Surf Resort: Florida			No	
000030351		Restaurant	PAX D210	Activating	Blue Surf Resorts	Blue Surf Resort: Florida			No	
000030352			PAX S500	In Transit	Blue Surf Resorts	Blue Surf Resort: North Carolina			No	
000030353			PAX S500	Injected	Blue Surf Resorts	KIF			No	
000030354			PAX S500	Stored	Blue Surf Resorts	Blue Surf Resort: North Carolina			No	
000030355			PAX S500	Injected	Blue Surf Resorts	KIF			No	

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



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.  See Device State Definitions below for additional details.
Attestation Period	Select an option for device inspections. Refer to Changing Device Attestation Date for details.
Audit Next Date	Select a date for device inspections. Refer to Changing Device Attestation Date for details.

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.

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 supervisors 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 processing cards

Damaged	NO	Unit is inoperable due to physical damage.
In Repair	NO	Device needs to be removed from service for repair.
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.
Retired	NO	Merchant no longer wishes to use a device. If the merchant closes their Bluefin account, all devices will be marked as retired.
RMA Return Merchandise Authorization	NO	Device needs to be returned to the KIF. 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 Authorization 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 relationship manager or Bluefin Support for next steps.

Return Merchandise Authorization Process

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

If you discover that your device is malfunctioning or suspect it has been tampered with, please contact support immediately by **Email:** customerservice@forte.net or **Phone:** 866-290-5400 Option 5

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

1. Click **Edit** (pencil icon) next to the device.
2. Change **Device State** to RMA.

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 >>
Ingenico iSC Touch 480	Damaged
	Retired
	Tampered
	Malfunctioning
	Lost
	RMA
	Activating
Client	
Disneyland	

IMPORTANT:


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

EXAMPLE:

Devices

DPX18 Partner Test << Select Client >> or << Select KIF >> << Any State >>

25 entries on page

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

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


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: Usernames under column Created By and Custodian display with a hyperlink, so you can see their contact information by clicking on hyperlink.

Details Chain Of Custody History Lifecycle					
Create Return		PDF CSV			
▼ Create Date	Created By	↕ Transfer Method	Custodian	↕ Complete Date	↕ Status
 03/23/2021 1:01 AM	Tho [redacted] britt	Initial	BFI [redacted] KIF		Not Completed

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: Usernames Under column User display with a hyperlink, so you can see their contact information by clicking on hyperlink

Details Chain Of Custody History Lifecycle			
Return		PDF CSV	
User	▲ Date	Device State	Notes
Tho [redacted] britt	03/23/2021 1:01 AM	Injected	
Tho [redacted] britt	03/23/2021 1:01 AM	Stored	
Tho [redacted] britt	03/24/2021 10:22 PM	Activating	

Lifecycle

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: Usernames under the column Created By and Custodian display with a hyperlink, so you can see their contact information by clicking on hyperlink.

Serial: 18[REDACTED]23 KIF: BFKIF Device Type: V400c, V400c Plus

Return

PDF

CSV

Action	Date	Created By	Device State	Custodian	Location	Shipment	Notes
Change Custody	03/23/2021 1:01 AM	Thomas Tuohitt	Injected	BFKIF (Custody Status: Not Completed)	BFKIF		
Change State	03/23/2021 1:01 AM	Thomas Tuohitt	Previous State: Injected				
Change State	03/23/2021 1:01 AM	Thomas Tuohitt	Previous State: Stored				
Change State	03/24/2021 10:22 PM	Thomas Tuohitt	Previous State: Activating				
Current State	02/17/2022 11:40 AM		Activated				

Inspections

PCI Compliance Regulations for Point-to-Point Encryption mandate that devices are inspected annually. It requires that merchants using a P2PE solution inspect their devices for tampering at least once per year. As per the PCI council, a device inspection should accomplish the following:

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

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

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

NOTE: Username under column Contact displayed with a hyperlink, so you can see their contact information.

Device details - 123456789

Details Chain Of Custody History Lifecycle Inspections

Return CSV PDF

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

Bluefin Payment Systems © 2016

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

Attestations

Shortly before a device needs to be inspected and attested to, you will receive an email notification. (The email includes device serial number and location.) Additionally, a notification is displayed the dashboard. To inspect the device, follow the instructions on [Inspections](#) under the Device Tab

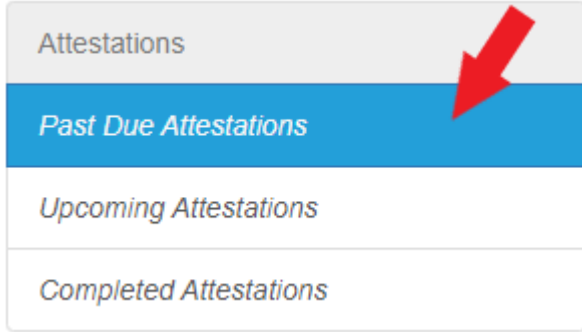
Inventory devices

Serial Number	Alternate Key	Device State	Audit Next Date
An_SV_2		Assigned	09/20/2016 12:00 AM

Past Due Attestations

It shows devices list that are past due date for device attestation date

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



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

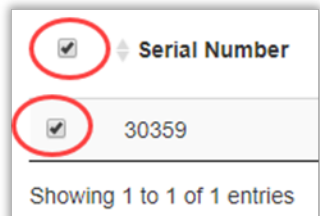
Past Due Attestations

25 entries on page Search: PDF CSV

<input type="checkbox"/>	Serial Number	Alternate Key	PastDueDate	Contact	Device State
<input type="checkbox"/>	100200300		08/18/2021 4:08 PM	Jaclyn Kelly	Activating
<input type="checkbox"/>	100200301		08/18/2021 4:08 PM	Jaclyn Kelly	Activating
<input type="checkbox"/>	231231231		07/23/2021 12:27 PM	Jaclyn Kelly	Activating

Previous Next

Complete Attestation Send a Reminder



Complete Attestation

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

Send a Remainder : functionality need to be updated

Create Attestation

Name *
annual 2016 ✓

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

Photos
An_SV_2 No file chosen

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

* indicates required entry

- Optional: Based on your preference, you can upload one image. Click **Choose File** and then navigate your network to select the image file.

NOTE: The following file types can be selected: .jpg, .jpeg, .png. (Maximum file size = 25 MB)

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

Upcoming Attestations

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

Bluefin® Dashboard Devices Shipments **Attestations** Reports Documentation Contact Support

Attestations
Past Due Attestations
Upcoming Attestations
Completed Attestations

Upcoming Attestations

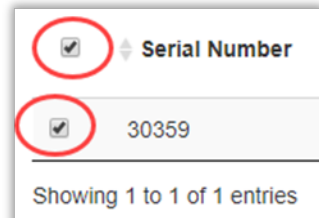
25 entries on page Search:

<input type="checkbox"/>	Serial Number	Alternate Key	Audit Next Date	Device Attestation Period	Contact	Device State
No data available in table						

Showing 0 to 0 of 0 entries

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

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



Complete Attestation

2. Click **Complete Attestation**.
3. Inspect the device(s), provide the information requested and select the agreement checkbox.

Create Attestation

Name *
annual 2016 ✓

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

Photos
An_SV_2 Choose File No file chosen

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

Save Cancel

* indicates required entry

4. Optional: Based on your preference, you can upload one image. Click **Choose File** and then navigate your network to select the image file.

NOTE: The following file types can be selected: .jpg, .jpeg, .png. (Maximum file size = 25 MB)

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

Completed Attestations

1. Navigate to the **Attestations** tab
2. Click **Completed Attestations** in the left column.
3. Enter a date range, select a POI, custodian or location based on your preference
4. The list of devices for the selected date range and filters are displayed
5. The information displayed includes:

Device serial number, Attestation Name, Completed Date, who performed attestation, Notes.

Completed Attestations

From 03/04/2021 00:00:00 To 03/04/2022 23:59:59 Apply

25 entries on page Search: PDF CSV

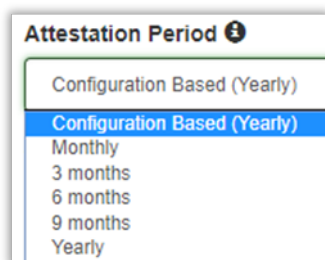
Serial Number	Alternate Key	Attestation Name	Completed Date	Performed by	Notes	Photo
000030356		2021 Q1	01/22/2021 03:49:51 PM	AaronC Admin	View	-
WPC202829001696		2021 Attestation	06/04/2021 10:02:07 AM	Jack Kelly	View	-
000030354		October 2021	09/14/2021 10:51:03 AM	Jack Kelly	View	-

6. Click on **PDF** or **CSV** to download the report in required format.

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. The attestation date can be modified from the Device tab. To change or set the device attestation date, you must:

1. Navigate to 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 attestation period frequency by selecting an option from the "Attestation Period" drop-down. Note: *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 done.

A modal form with the following fields and buttons:

- Audit Next Date:** Input field containing '09/29/2016' with a calendar icon to the right.
- Activation Date:** Input field containing '03/26/2015' with a calendar icon to the right.
- Firmware Version:** Input field containing '1.0'.
- Firmware Update Date:** Input field containing '03/26/2015' with a calendar icon to the right.
- Buttons:** A blue 'Save' button and a white 'Cancel' button with a grey border.

Batch Process: Change Device Attestation Date

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

1. Select the devices and then click **Update**. **NOTE:** You can select up to 500 devices.

A screenshot of a web interface showing a list of devices. At the top, there is a checkbox labeled 'Show only devices which have next attestation in the future' which is checked. Below this is a dropdown menu set to '25' with the text 'entries on page'. The list has two columns: 'Serial Number' and 'Alternate Key'. There are four rows of data, each with a checkbox in the first column:

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

Below the list, it says 'Showing 1 to 4 of 4 entries'. At the bottom of the list area is a blue button labeled 'Attestation Batch Update'.

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

Attestation Next Date Batch Update

Number of affected device(s) is 2

Audit Next Date

01/05/2019 12:00

Attestation Period ⓘ

Configuration based (Yearly)

Save Cancel

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

Reports

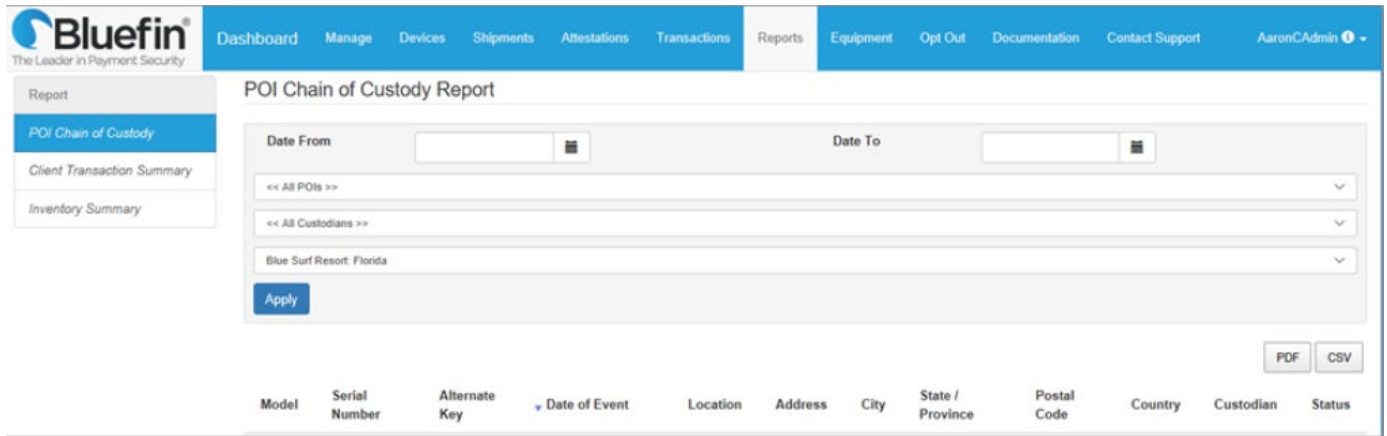
P2PE Manager Merchant allows you to generate multiple reports based on your requirement. The reports available are:

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

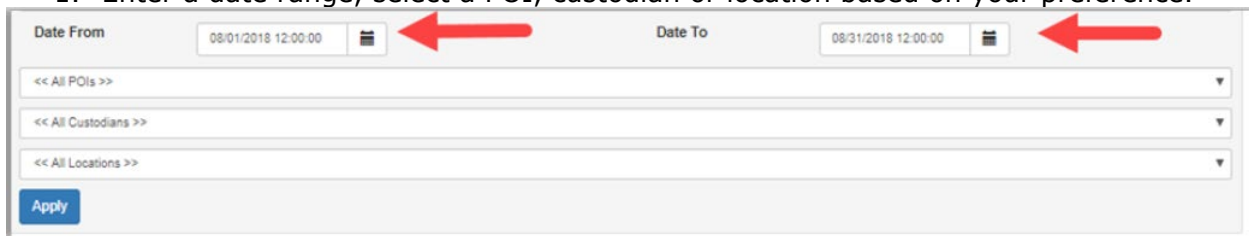
POI Chain of Custody Report

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

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

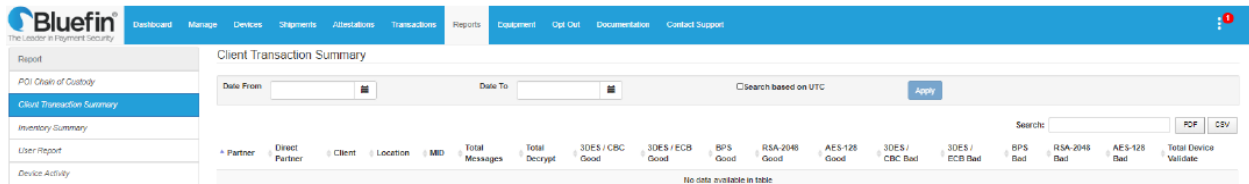


1. Enter a date range, select a POI, custodian or location based on your preference.



2. Click **Apply**.
3. The list of devices for the selected date range and filters are displayed.
4. Click on **PDF** or **CSV** to download the report in required format.

Client Transaction Summary Report



To create the Client Transaction Summary report, do the following:

1. Click the **Reports > Client Transaction Summary**
2. Enter the date range.
3. Click **Apply**. The report will display.
4. Click on **PDF** or **CSV** to download the report in required format.

Inventory Summary

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.

- The report shows your inventory by device type (total number per device type) and by status (total number of devices by status)
- Click on **PDF** or **CSV** to download the report in required format.

Inventory By Type

Device Type	Total
SecuRED	1
SREDKey	17

Showing 1 to 2 of 2 entries

Inventory By Status

Device Status	Total
Activated	12
Activating	5
Lost	1

User Report

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

Click on **PDF** or **CSV** to download the report in required format

User Report

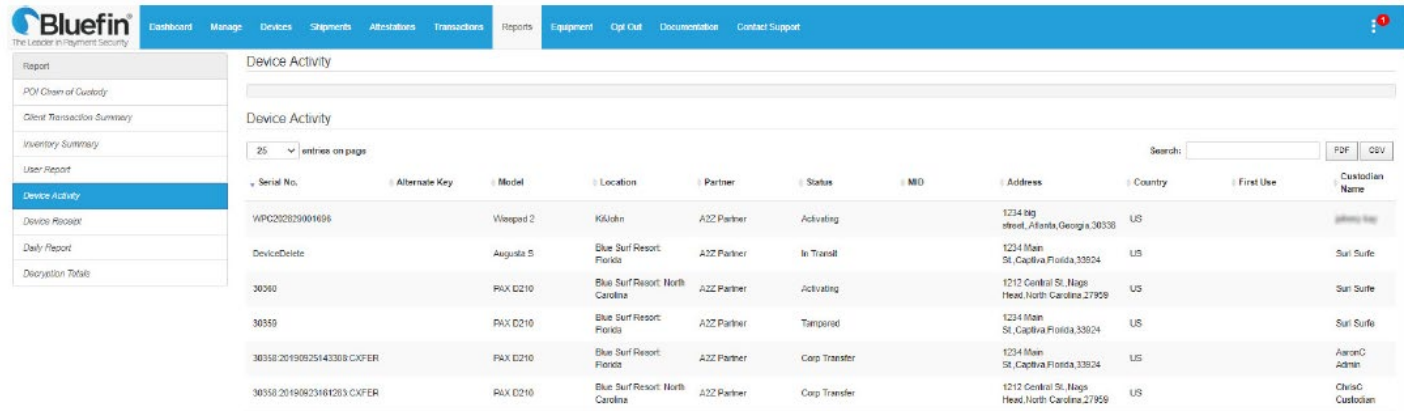
25 entries on page Search: PDF CSV

User Name	Name	Email	Phone	Partner	Direct Partner	Client	Role	Path	Activ
-----------	------	-------	-------	---------	----------------	--------	------	------	-------

Device Activity

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

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



Serial No.	Alternate Key	Model	Location	Partner	Status	MID	Address	Country	First Use	Custodian Name
WP6232829001496		Wipeed 2	KiUshn	A22 Partner	Activating		1234 big street, Atlanta, Georgia, 30338	US		Admin
DeviceDelete		Augusta 5	Blue Surf Resort, Florida	A22 Partner	In Transit		1234 Main St, Capiva Florida, 33024	US		Sun Suite
30360		PAX D210	Blue Surf Resort, North Carolina	A22 Partner	Activating		1212 Central St, Nags Head, North Carolina, 27959	US		Sun Suite
30359		PAX D210	Blue Surf Resort, Florida	A22 Partner	Tampered		1234 Main St, Capiva Florida, 33024	US		Sun Suite
30358.20190925143308.CXFER		PAX D210	Blue Surf Resort, Florida	A22 Partner	Corp Transfer		1234 Main St, Capiva Florida, 33024	US		AaronC Admin
30358.20190923161263.CXFER		PAX D210	Blue Surf Resort, North Carolina	A22 Partner	Corp Transfer		1212 Central St, Nags Head, North Carolina, 27959	US		ChrisC Custodian

NOTE: You can display All devices and then export the list for inventory purposes. Click on **PDF** or **CSV** to download the report in required format

Device Receipt

The Device Activity Report displays Partner name, Client name, Device types, Total Device Count, Missed Device Count, date of Last shipments.

To create this report,

1. click **Reports>Device Receipt** to know about shipments.
2. Select Number of days from drop down list
3. click **Apply**.
4. Click on **PDF** or **CSV** to download the report in required format

Device Receipt Report

30+ Days

Device Receipt

25 entries on page Search:

Partner Name	Client Name	Device Type(s)	Total Device Count	Missed Device Count	Date of Last Shipment
A2Z Partner	Blue Surf Resorts	A60,A77,A80,A920,A920Pro,Augusta S,Bluepad-50,D210,iUC 285,S300,S500,SREDKey,SREDkey 2,V400c, V400c Plus,VP6300,Wisepad 2	54	0	01/14/2020 9:15 AM

Showing 1 to 1 of 1 entries

Previous **1** Next

Daily Report

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

Daily Report

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

Daily Report

25 entries on page Search:

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

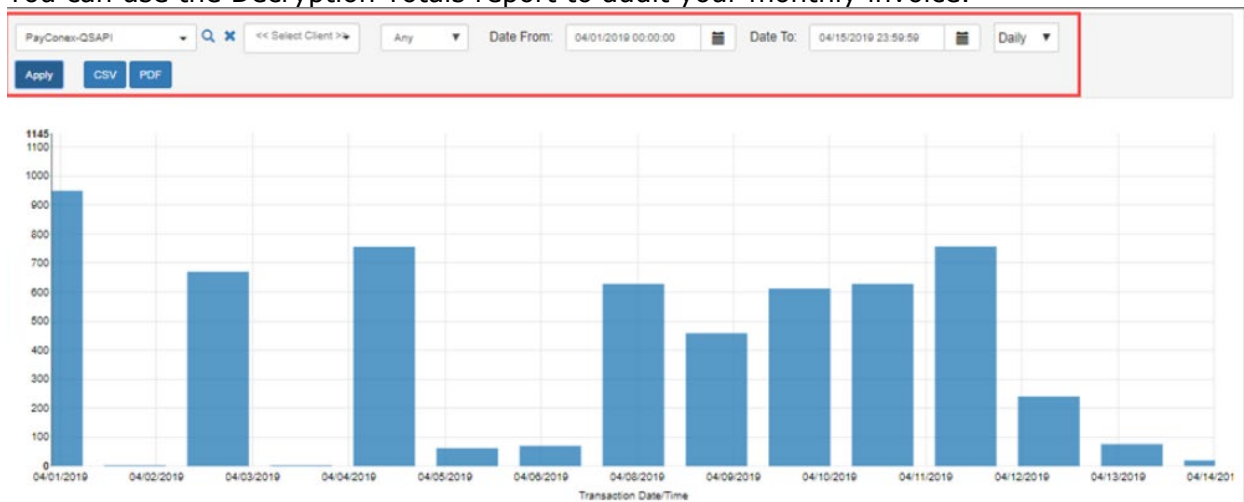
Showing 0 to 0 of 0 entries

Previous Next

Click on **PDF** or **CSV** to download the report in required format

Decryption Totals Report

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



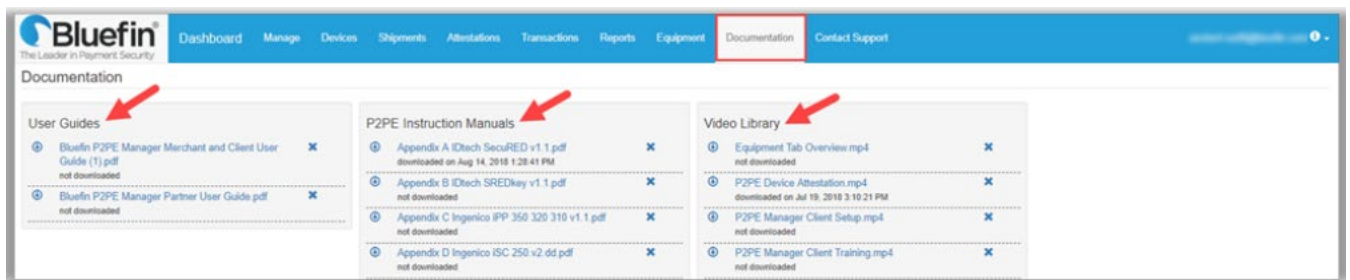
Select **Reports > Decryption Totals**. The information displayed summarizes decryption totals in a bar chart. You can filter by type of decryption and specify a date range. This information is dynamic and based on the parameters set at the top of the page.

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

Click on **PDF** or **CSV** to download the report in required format

Documentation

The **Documentation** tab provides access to User Guides, Instruction Manuals and Video Library.



Downloading and Viewing PDF Files

To download the a .pdf 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 (.mp4 file), click the download icon to the left of the file name:



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

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

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

Contact

For assistance on device integration, reach out to our Integration Team at

EMAIL EquipmentQuestions@forte.net

PHONE: 866-290-5400

Option 5 for Technical Support

Option 4 for Equipment Service