Software History

Software Release Date: November 27, 2018

Document History

Document Version: 1.1
Document Date: March 2019

Legal Notice

Copyright © 2019 Bluefin Payment Systems LLC.

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

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

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

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

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

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

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

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

QuickSwipe® (Mobile POS) is a registered trademark of Bluefin Payment Systems LLC in the United States and/or other countries.
Table of Contents
Overview................................................................................................................... 6
    Contacting Support................................................................................................6
    Audience..............................................................................................................6
    Terminology .......................................................................................................7
Getting Started ........................................................................................................ 7
    Accessing P2PE Manager ....................................................................................7
    Dashboard ..........................................................................................................8
Receiving and Activating Your Device ......................................................................9
    Batch Receiving Devices ..................................................................................9
    Receiving Device with Special Serial Number Requirements ..............................11
Accessing Online Help Documentation ..................................................................12
    Downloading and Viewing PDF Files ................................................................12
    Downloading and Viewing Video Files ..............................................................12
Transactions ............................................................................................................13
    Creating the Chain of Custody Report ..............................................................13
    Creating a Client Transaction Summary Report .................................................14
    Creating the Inventory Summary Report ..........................................................15
    Exporting a Report ............................................................................................15
Administration .........................................................................................................16
    Managing Users ...............................................................................................16
    Adding a User ....................................................................................................16
    Updating a User ..............................................................................................17
    Resetting a User’s Password ...........................................................................17
    Managing Your Personal Settings ......................................................................18
    Resetting Your Password (Forgotten Password) ..............................................18
    Adding Locations ............................................................................................19
    Editing Locations ............................................................................................20
    Removing Locations ........................................................................................20
Device Management .................................................................................................20
    Device Activation Process Flow ........................................................................20
    Updating Devices .............................................................................................21
    Device State Definitions ...................................................................................22
    Viewing Device Details ....................................................................................22
    Chain of Custody .............................................................................................22
Device State History ........................................................................................................... 23
Lifecycle Report - Detailed Device History ......................................................................... 23
Return Merchandise Authorization Process ........................................................................... 24
Checking on Device Shipment and Tracking ........................................................................ 25
Checking Tracking Number ................................................................................................. 25
Checking Device Status ....................................................................................................... 25
Checking Order Status ......................................................................................................... 26
Transferring a Device between Custodians or Locations ...................................................... 26
  Transferring Multiple Device Locations ........................................................................... 27
Equipment .............................................................................................................................. 29
  Ordering Additional Equipment ......................................................................................... 29
  Deploying Equipment ......................................................................................................... 30
Opt Out of Bluefin Program .................................................................................................. 30
Device Inspections and Attestations .................................................................................. 31
  Inspecting a Device ............................................................................................................ 31
  Inspections Report: Viewing Details of Past Inspections .................................................. 31
  Device Attestations ............................................................................................................ 32
  Changing Device Attestation Date ...................................................................................... 34
    Batch Process: Change Device Attestation Date .......................................................... 34
  Viewing Future Scheduled Attestations ............................................................................. 35
Device Tampering Detection ................................................................................................. 36
Appendix:  User Roles ........................................................................................................... 37
  Client / Merchant Roles ...................................................................................................... 37
  Partner Roles ..................................................................................................................... 37
Appendix:  Receiving and Activating Your Device ................................................................. 38
  Step 1. Access the P2PE Manager Online ........................................................................ 38
  Step 2: Log Receipt of the Shipment ................................................................................ 39
  Step 3: Activate Your Device ............................................................................................ 41
  Reporting a Tampered Device .......................................................................................... 42
Appendix:  Partners ............................................................................................................... 43
  Client / Merchant Communications .................................................................................... 43
  Administration .................................................................................................................... 43
    Adding a Partner Record (Sub-Partner) .......................................................................... 44
    Adding a Client / Merchant ............................................................................................... 45
  Partner Device Types ......................................................................................................... 47
  Shared Devices .................................................................................................................... 47
Client Import ..................................................................................................... 48
Device Transfer .................................................................................................. 49
Reporting ............................................................................................................. 49
Partner Transaction Summary .............................................................................. 49
User Report ....................................................................................................... 50
Device Activity ................................................................................................... 50
Device Receipt ................................................................................................... 50
Daily Report....................................................................................................... 51
Overview

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

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

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

Contacting Support

**PHONE**: 800-675-6573 **Option 2 for Technical Support** and **Option 4 for Customer Service**

- **Monday – Friday**: 7:00 am – 6:00 pm Central
- **Saturday**: 8:00 am – 4:30 pm Central

**EMAIL**: service@bluefin.com

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

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 access to certain capabilities.

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

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

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

Key terms used throughout this guide are defined below:

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

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

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

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

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

![Diagram of P2PE ecosystem](image)

Getting Started

**Accessing P2PE Manager**

You will receive a **Welcome** email with your username.
Follow the instructions in the email:

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

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

- Number of devices by state (displayed in a List tile and a Bar Chart tile)
- Number of devices shipped by device type (displayed in a List tile and a Bar Chart tile)
- Number of Clients and Locations
- Attestations Due on Devices (device serial numbers displayed)

**Receiving and Activating Your Device**

For detailed information, refer to the Appendix: Receiving and Activating Your Device.

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

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

**Related Information:**

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

**Batch Receiving Devices**

With P2PE Manager, you can Batch Receive devices by scanning them into the system. Any scanner connected via USB/Serial or Ethernet will work with P2PEManager.
NOTE: Partners need to use the drop-down options at the top of the page and select a Partner and Client first.

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

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

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

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

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

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

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

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

   If you did not select Auto Activate device, then the Device State will display as Received. To continue, follow the actions in Step 3: Activate Your Device in the Appendix: Receiving and Activating Your Device.
Receiving Device with Special Serial Number Requirements

In special circumstances, P2PEManager 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.  

6. Wait for the green success message. The device will be marked as Received and the progress bar will be completed.
Accessing Online Help Documentation

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

### Downloading and Viewing PDF Files

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

![Appendix A IDtech SscuRED v1.1.pdf](image)

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](image)

**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

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

The Transaction Summary lists transactions including encryption and decryption status.

To create this report, do the following:

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

Related Information: See Exporting a Report below.

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:

   (Point of Interaction = POI)
2. Enter a date range, select a POI, custodian or location based on your preference.

3. Click Apply.

Related Information: See Exporting a Report below.

Creating a Client Transaction Summary Report

To create this report, do the following:

- Click the Reports tab.
- Click Client Transaction Summary in the left column.
- Enter the date range.
- (Partner users only: Select partner from the drop-down list.)
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 Summary Report Table]

   **Inventory By Type**
   
<table>
<thead>
<tr>
<th>Device Type</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecuRED</td>
<td>1</td>
</tr>
<tr>
<td>SREDKey</td>
<td>17</td>
</tr>
</tbody>
</table>

   **Inventory By Status**
   
<table>
<thead>
<tr>
<th>Device Status</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activated</td>
<td>12</td>
</tr>
<tr>
<td>Activating</td>
<td>5</td>
</tr>
<tr>
<td>Lost</td>
<td>1</td>
</tr>
</tbody>
</table>

Related Information: See **Exporting a Report** below.

Exporting a Report

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

To export data, do the following:

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

## Administration

**IMPORTANT:** This option is restricted to Client Administrators.

### Managing Users

Select the “Manage” tab and click “Users” in the left column. Then a list of users displays.

### Adding a User

- Select **Manage > Users** and then click **Create**.
• Enter the user’s information.

- Check the “Active” check box.
- Select a Role. Refer to Appendix: User Roles.
- Click “Send welcome email.”
- 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.

**Resetting a User’s Password**

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

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

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

## Managing Your Personal Settings

Your Personal Settings include:

- **Profile:** Update your name and email address
- **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 the left column based on your preference.

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

## Resetting Your Password (Forgotten Password)

If you **forget your password**, do the following:
1. From the login screen, enter your user name and then click **Forgot password**.

![Portal Login](image)

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).

**NOTE:** Client users can see all locations and can add/edit locations.

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:

- Select **Locations** in the left column.
- Click **Create**.
- Complete the information requested.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner</td>
<td>Required</td>
</tr>
<tr>
<td>Client</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Location Type</strong></td>
<td>Required. Select an option from the drop-down list.</td>
</tr>
<tr>
<td><strong>Location Name</strong></td>
<td>Required. Enter a name for the location to easily identify it. This name will be used in reports.</td>
</tr>
<tr>
<td><strong>Name of Business</strong></td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>Required. Street address, City, Postal code, Country, State Province</td>
</tr>
<tr>
<td><strong>Mail Address</strong></td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Contact Person</strong></td>
<td>Required. Enter: First Name, Last Name, Email, Phone</td>
</tr>
</tbody>
</table>

**NOTE:** The contact person does not have to be the device custodian.
• Check **Active** to enable the location.
• 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.

**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.

**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, and virtual.

![Device Management Table](device_table.png)

**Device Activation Process Flow**

The following diagram describes the device activation flow.
### Updating Devices

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

Refer to Changing Device Attestation Date for details.

Related Information: For instructions for activating a brand-new device, see Batch Receive.

Device State Definitions

NOTE: 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.)

<table>
<thead>
<tr>
<th>STATE</th>
<th>CAN PROCESS?</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damaged</td>
<td>NO</td>
<td>Unit is inoperable due to physical damage</td>
</tr>
<tr>
<td>Retired</td>
<td>NO</td>
<td>Merchant no longer wishes to use a device. If the merchant closes their Bluefin account, all devices will be marked as retired.</td>
</tr>
<tr>
<td>Destroyed</td>
<td></td>
<td>Unit is inoperable and cannot be recovered</td>
</tr>
<tr>
<td>Tampered</td>
<td>NO</td>
<td>If a merchant believes that a device was tampered with, they must put the device in this state. This state is automatically triggered when the system detects tampering. Marking a device as “tampered” will trigger a notification to a Bluefin employee who will assist in determining next steps.</td>
</tr>
<tr>
<td>Malfunctioning</td>
<td>NO</td>
<td>Unit is inoperable or inconsistently operable for unknown reasons</td>
</tr>
<tr>
<td>Lost</td>
<td>NO</td>
<td>Merchant does not know where device is</td>
</tr>
<tr>
<td>Quarantined</td>
<td></td>
<td>Unit was discovered to be malfunctioning or was tampered with prior to shipping.</td>
</tr>
<tr>
<td>Injected</td>
<td></td>
<td>Encryption key has been injected into the unit.</td>
</tr>
<tr>
<td>In Repair</td>
<td>NO</td>
<td>Device needs to be removed from service for repair</td>
</tr>
<tr>
<td>RMA</td>
<td>NO</td>
<td>A tamper bag and return label has been sent to merchant to retrieve device that is not working correctly</td>
</tr>
<tr>
<td>Unassigned</td>
<td></td>
<td>Unit is injected and held by a Key Injection Facility.</td>
</tr>
<tr>
<td>Stored</td>
<td>NO</td>
<td>Device is in possession of merchant and stored in a secure location, but not ready to begin processing cards</td>
</tr>
<tr>
<td>Activating</td>
<td>YES</td>
<td>Device is in hands of merchant and ready to begin processing cards</td>
</tr>
<tr>
<td>Activated</td>
<td>YES</td>
<td>Device is in hands of merchant and processing of cards has begun (state change from “activating” to “active” occurs automatically)</td>
</tr>
</tbody>
</table>

Viewing Device Details

Chain of Custody

From the Devices tab, click the edit icon (pencil) 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.

---

### Device State History

From the **Devices** tab, click the edit icon (pencil) 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.

---

### Lifecycle Report - Detailed Device History

From the **Devices** tab, click the edit icon (pencil) 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.
Return Merchandise Authorization Process

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

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

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

1) Select your “Partner Account” and choose “Client” if applicable.
2) Click on the “Pencil Icon” for the device.
3) Change “Device State” to RMA.

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

**NOTE:** When the device status is RMA, it will not process transactions.
Checking on Device Shipment and Tracking

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

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

Checking Tracking Number

1) Go to “Shipments” tab
2) 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

![Image of Shipments tab]

Checking Device Status

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

If there is no tracking number, do the following:

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

![Image of Equipment tab]

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

Checking Order Status

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

1. Navigate to the “Deploy Equipment” tab.
2. Look under the “Status” section.
   - INITIAL: Order was successfully submitted.
   - PENDING: Someone at key injection facility has been assigned the order and is working on it.
   - COMPLETED: Order has been shipped.

Transferring a Device between Custodians or Locations

IMPORTANT: These instructions only apply to active functioning devices. (If a device is retired, lost, or stolen, these steps do not apply.) Additionally, this option is restricted to Client Administrators and Client Custodians.
You can transfer a device to a different location if the device is moved. **Example:** A device is moved from the “Chicago Office” to the “San Francisco Office.”

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

To transfer a device, do the following:

1) Go to “Devices” tab.
2) Click the pencil icon to select the device you would like to transfer.
3) Click the “Chain Of Custody” tab.
4) Click “Create.”
5) Fill in fields and click “Save.”

**Transfer Method:**

a. Choose “Manual” if device is handed off or if there is simply someone else taking responsibility for the device
b. Choose “Shipment” if device is being mailed from one location or custodian to another, additional fields will be required

---

**Transferring Multiple Device Locations**

**NOTE:** This functionality is restricted to following user roles: Client Admins 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**.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SerialNumber</td>
<td>Location</td>
<td>DeviceType</td>
</tr>
<tr>
<td>2</td>
<td>123AD33377</td>
<td>Company Location 1</td>
<td>SREDKey</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

Ordering Additional Equipment

IMPORTANT: This option is restricted to Client Administrators and Client Procurement. When ordering equipment from this page, all Bluefin equipment is listed. Keep in mind that this equipment may or may not be compatible with your specific processing solution.

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

The process described below is for ordering additional equipment using the portal. You can also order additional equipment by contacting Bluefin Support.

Navigate to Equipment > Order Inventory and then click Create.

Complete the form and click Save

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Client</td>
<td>(Partners Users only: Select the Partner and Client from the drop-down lists.)</td>
</tr>
</tbody>
</table>
Deploying Equipment

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

**IMPORTANT:** “Deploying Equipment” refers only to placing an order to send equipment to your location(s).

To deploy equipment, navigate to Equipment > Deploy Equipment and then click Create. Complete the form (refer to the table in Ordering Additional Equipment) and click Save.

Opt Out of Bluefin Program

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

**NOTE:** Opt Out will not entirely cancel your Bluefin account. You will also need to contact Bluefin to notify us and for additional cancellation instructions (varies depending on account configuration and setup). Refer to Contacting Support.

1) Access the Opt Out tab
2) Check the acknowledgement check box and click “Opt Out”
Device Inspections and Attestations

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

Inspecting a Device

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

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

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

Inspections Report: Viewing Details of Past Inspections

PCI Compliance Regulations for Point-to-Point Encryption mandate that devices are inspected annually. Follow the instructions below to view reports of past inspections of the device.

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

Click the "Inspections" tab to see details of past inspections.

**NOTE:** User names display with a hyperlink, so you can see their contact information.
Related Information:  For instructions for conducting and logging an inspection, see Device Attestation.

Device Attestations

Shortly before a device needs to be inspected and attested to, you will receive an email notification. Additionally, a notification displays on the dashboard.

1) Click the Attestations tab.
2) Select Current Attestations in the left column.
3) Select the checkbox next to the device(s).

![Image of Current Attestations]

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

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

![Image of Create Attestation]
6) **Optional:** Based on your preference, you can upload a picture. Click **Choose File** and then navigate your network to select the image file.

**NOTE:** The following file types can be selected: .jpg, .jpeg, .png.

7) Click **Save** when you’re done.

---

**Changing Device Attestation Date**

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

1) Navigate to “Devices” tab. All devices will be listed.
2) Click the pencil icon next to the device you want to edit.
3) You can set the attestation period frequency by selecting from a list of options. Based on your selection, the system will prompt you to perform the attestation.

![Attestation Period Image](image)

4) **Optional.** Update the “Audit Next Date” based on your preference and click “Save.”

![Audit Next Date Image](image)

---

**Batch Process: Change Device Attestation Date**

You change the device attestation date for a group of devices (up to 500) from the **Future Attestation** list.
• Select the devices and then click **Attestation Batch Update**.  
**NOTE:** You can select up to 500 devices.

![Future Attestation](image)

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

![Attestation Next Date Batch Update](image)

• Click **Save** when you’re done.

**Viewing Future Scheduled Attestations**

1) Navigate to the Attestations tab  
2) On the left tab, click “Future Attestations”

![Future Attestation](image)
3) Review the “Audit Next Date” for the next date the device is scheduled to be audited.

**Device Tampering Detection**

Bluefin’s P2PE devices have three mechanisms to detect tampering, each outlined below. The one that is triggered will depend on which method of tampering 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 get it swapped out.
- If the device does not detect tampering at the time (which may be the case with external tampering), it will detect changes in the submitted data string and will go into “quarantine” mode within P2PE manager. The screen may look the same, but transaction processing ability will be deactivated. If this happens, please contact Bluefin.
- The device may suspect tampering by certain processing attempt patterns that are consistent with data thief testing. If these patterns are detected the device will go into “quarantine” mode 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

<table>
<thead>
<tr>
<th></th>
<th>Client Admin</th>
<th>Client Custodian</th>
<th>Client Procurement</th>
<th>Client User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Manage</td>
<td>Manage</td>
<td>Manage</td>
<td>View</td>
</tr>
<tr>
<td>Shipments</td>
<td>Manage</td>
<td>Manage</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>Attestations</td>
<td>Conduct</td>
<td>Conduct</td>
<td>Conduct</td>
<td>Conduct</td>
</tr>
<tr>
<td>Encrypted Transactions</td>
<td>View</td>
<td>(No Access)</td>
<td>(No Access)</td>
<td>View</td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Equipment</td>
<td>Yes</td>
<td>(No Access)</td>
<td>Yes</td>
<td>(No Access)</td>
</tr>
<tr>
<td>Users</td>
<td>Manage</td>
<td>(No Access)</td>
<td>(No Access)</td>
<td>(No Access)</td>
</tr>
<tr>
<td>Locations</td>
<td>Manage</td>
<td>(No Access)</td>
<td>(No Access)</td>
<td>(No Access)</td>
</tr>
<tr>
<td>Device Transfer</td>
<td>Manage</td>
<td>(No Access)</td>
<td>(No Access)</td>
<td>(No Access)</td>
</tr>
</tbody>
</table>

### Partner Roles

<table>
<thead>
<tr>
<th></th>
<th>Partner Supervisor</th>
<th>Partner Fulfillment</th>
<th>Partner User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>Manage</td>
<td>Manage</td>
<td>Manage</td>
</tr>
<tr>
<td>Shipments</td>
<td>Manage</td>
<td>Manage</td>
<td>(No Access)</td>
</tr>
<tr>
<td>Attestations</td>
<td>Conduct</td>
<td>Conduct</td>
<td>Conduct</td>
</tr>
<tr>
<td>Encrypted Transactions</td>
<td>View</td>
<td>View</td>
<td>View</td>
</tr>
<tr>
<td>Reports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Equipment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Users</td>
<td>Manage</td>
<td>(No Access)</td>
<td>Manage</td>
</tr>
<tr>
<td>Locations</td>
<td>Manage</td>
<td>(No Access)</td>
<td>Manage</td>
</tr>
<tr>
<td>Device Transfer</td>
<td>Manage</td>
<td>(No Access)</td>
<td>Manage</td>
</tr>
<tr>
<td>Partners</td>
<td>Manage</td>
<td>(No Access)</td>
<td>Manage</td>
</tr>
<tr>
<td>Clients</td>
<td>Manage</td>
<td>(No Access)</td>
<td>Manage</td>
</tr>
<tr>
<td>Import Clients</td>
<td>Yes</td>
<td>(No Access)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Appendix: Receiving and Activating Your Device

You will receive your device in the mail.

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

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

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

---

**Step 1. Access the Point-to-Point Encryption (P2PE) Manager Online**

To log into P2PE Manager, do the following:

1. Access the P2PE Manager from a browser: [P2PE Manager](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 from “no-reply@p2pemanager.com” and the **subject line** is: “Welcome to Bluefin’s P2PE Manager!”)
Step 2: Log Receipt of the Shipment

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

To log receipt of your shipment, do the following:

Optional: To Batch Receive the devices in a shipment, refer to Batch Receiving.

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.

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, 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.)
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.

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

**TIP:** To take advantage of this time saving option, you must select it before entering the device serial number and tamper label.

6. Click **Receive**. Notice that the **Device State** and **Received Date** fields are updated.
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.
3. Click the **Device State** drop-down arrow and then select **Activating**.

![Device State drop-down](image)

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 cards! Once you begin processing cards, your device will automatically change from **Activating** to **Active**.

### Reporting a Tampered Device

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

- The secure bag is **not** sealed closed
- The secure bag is damaged
- The “No Tear” sticker is broken or damaged

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

**Email:** service@bluefin.com  
**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 number 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.

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

Client / Merchant Communications

P2PE Manager automatically sends email communications to your clients for each of the scenarios outlined below. If you would like to customize the verbiage or recipients, please contact Bluefin.

Email communications automatically sent to clients in these scenarios:

- Device Attestation due
  **NOTE:** If there are multiple devices that need to be attested to in a single calendar day, there will be only one email that mentions the group of devices.
- Device Attestation complete
- Device firmware issue detected
- Device sends clear-text cardholder data
- Device sends corrupt data
- Device has been shipped
- Device state is changed
- Password reset
- User welcome email

Administration
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:

- Click Partners in the left column.
- Click Create.
- Enter the information requested for the required fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Partner</td>
<td>Select partner from the drop-down list when applicable. <strong>NOTE:</strong> You must select a Parent Partner when creating sub-partners.</td>
</tr>
<tr>
<td>Name</td>
<td>Required. Enter the partner’s name</td>
</tr>
<tr>
<td>Partner ID</td>
<td>Required. Enter the partner ID</td>
</tr>
<tr>
<td>Status</td>
<td>Required. Select the partner’s status</td>
</tr>
<tr>
<td>Verification Phrase</td>
<td>Optional.</td>
</tr>
<tr>
<td>CardConexID</td>
<td>Required. This is the 15-digit unique code in the CardConex URL for a partner / sub-partner. (This is a third-party system reference ID. If you do not have a code, enter any numeric data.) <strong>NOTE:</strong> This field is optional for sub-partners.</td>
</tr>
<tr>
<td>Allow Client(s) To Order Equipment</td>
<td>Optional. Select the option if applicable.</td>
</tr>
<tr>
<td>Contact Person</td>
<td>Required. Enter the <strong>First Name, Last Name, Email address, Phone</strong> and <strong>P2PE User Name</strong>. <strong>Best Practice:</strong> Use first initial and last name and email address for the user name. (Example: <a href="mailto:jdoe@yourcompany.com">jdoe@yourcompany.com</a>.) Select the <strong>Active</strong> checkbox to enable the contact person.</td>
</tr>
<tr>
<td>Location</td>
<td>Required. Select the <strong>Location Type</strong>.</td>
</tr>
<tr>
<td>Mail Address</td>
<td>Optional.</td>
</tr>
<tr>
<td>Remember Devices</td>
<td>Optional.</td>
</tr>
</tbody>
</table>
You can enable two-factor authentication. When it is enabled, it will affect all users who belong to the Client or Partner record.

You can send new users a welcome email. This option is selected by default.

Attestation Period

Optional.

• Click **Save** when you’re done.

**Adding a Client / Merchant**

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

• Click **Clients** in the left column.
• Click **Create**.
• Enter the information requested for the required fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Partner</td>
<td>Required. Select the partner from the list.</td>
</tr>
<tr>
<td>Name</td>
<td>Required. Enter the client’s/merchant’s name.</td>
</tr>
<tr>
<td>Active</td>
<td>Optional. Select the checkbox to enable the client.</td>
</tr>
<tr>
<td>CardConexID</td>
<td>Optional.</td>
</tr>
<tr>
<td>Mid</td>
<td>Optional.</td>
</tr>
</tbody>
</table>
| Contact Person     | Required. Enter the 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@yourcompany.com.)  
**NOTE:** The **Active** checkbox for the contact person is selected for you. |
| Location           | Select the **Location Type**.                                                |
| Mail Address       | Optional.                                                                    |
| Remember Devices   | Optional.  
• You can enable two-factor authentication. When it is enabled, it will affect all users.  
• You can send new users a welcome email. This option is selected by default. |
| Attestation Period | Optional.                                                                    |
• Click **Save** when you’re done.

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

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

![Partner Name Displayed](image)

### Editing a Client’s Contact Person

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

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

To update the contact person, do the following:

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**.

![Contact Person Editing](image)

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

![Partner Device Types](image)

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

Shared Devices

To see a summary of shared devices, do the following from the Manage tab:

- Select Shared Devices in the left column
- Select the Partner from the drop-down list.

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

You can create client records in a CSV file and batch upload them to P2PE Manager.

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.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectPartner</td>
<td>Required.</td>
</tr>
<tr>
<td>ClientName</td>
<td>Required.</td>
</tr>
<tr>
<td>ClientCardConexId</td>
<td>Optional.</td>
</tr>
<tr>
<td>LocationName</td>
<td>Required.</td>
</tr>
<tr>
<td>LocationType</td>
<td>Required. Options: BF Fulfillment location, Corporate Headquarters, Field Office, KIF, Manufacturer, Manufacturer long time storage, CSR Location, Merchant Long time storage location, Merchant Retail Location, Merchant short term storage &amp; distribution, Partner Location, Regional Office, Vendor Fulfillment Location</td>
</tr>
<tr>
<td>LocationNameofBusiness</td>
<td>Optional.</td>
</tr>
<tr>
<td>LocationCountry</td>
<td>Required.</td>
</tr>
<tr>
<td>LocationAddress1</td>
<td>Required.</td>
</tr>
<tr>
<td>LocationAddress2</td>
<td>Optional.</td>
</tr>
<tr>
<td>LocationCity</td>
<td>Required.</td>
</tr>
<tr>
<td>LocationState</td>
<td>Optional.</td>
</tr>
<tr>
<td>LocationPostalCode</td>
<td>Optional.</td>
</tr>
<tr>
<td>UserName</td>
<td>Required.</td>
</tr>
<tr>
<td>UserRole</td>
<td>Optional.</td>
</tr>
<tr>
<td>FirstName</td>
<td>Required.</td>
</tr>
<tr>
<td>LastName</td>
<td>Required.</td>
</tr>
<tr>
<td>Email</td>
<td>Required.</td>
</tr>
<tr>
<td>Phone</td>
<td>Required.</td>
</tr>
</tbody>
</table>

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

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

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

---

**Reporting**

**Partner Transaction Summary**

You can use the Partner Transaction Summary to audit your monthly invoice.
Select **Reports > Partner Transaction Summary.** The information displayed summarizes decryptions by partner / sub-partner according to the date range specified. Additionally, the type of decryption that was used also displays.

You can optionally select the checkbox **Search based on UTC** which converts the browser time (e.g. EST, PST) to Greenwich Mean Time (GMT) for the query.

### User Report

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

### Device Activity

Select **Reports > Device Activity.** The information displayed includes: serial number, device type (model), device location, status, date/time of first use, date/time of last use and device custodian.

### Device Receipt

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

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