Point-to-Point Encryption (P2PE) Manager

User Guide

Document Date: February 10, 2022

Legal Notice

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

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

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

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

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

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

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

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

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

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

Table of Contents

Overview

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

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

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

Audience

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

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

Related Information: Appendix User Roles.

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

Capabilities restricted to Partners are described in Appendix: Partners.

Terminology

Key terms used throughout this guide are defined below:

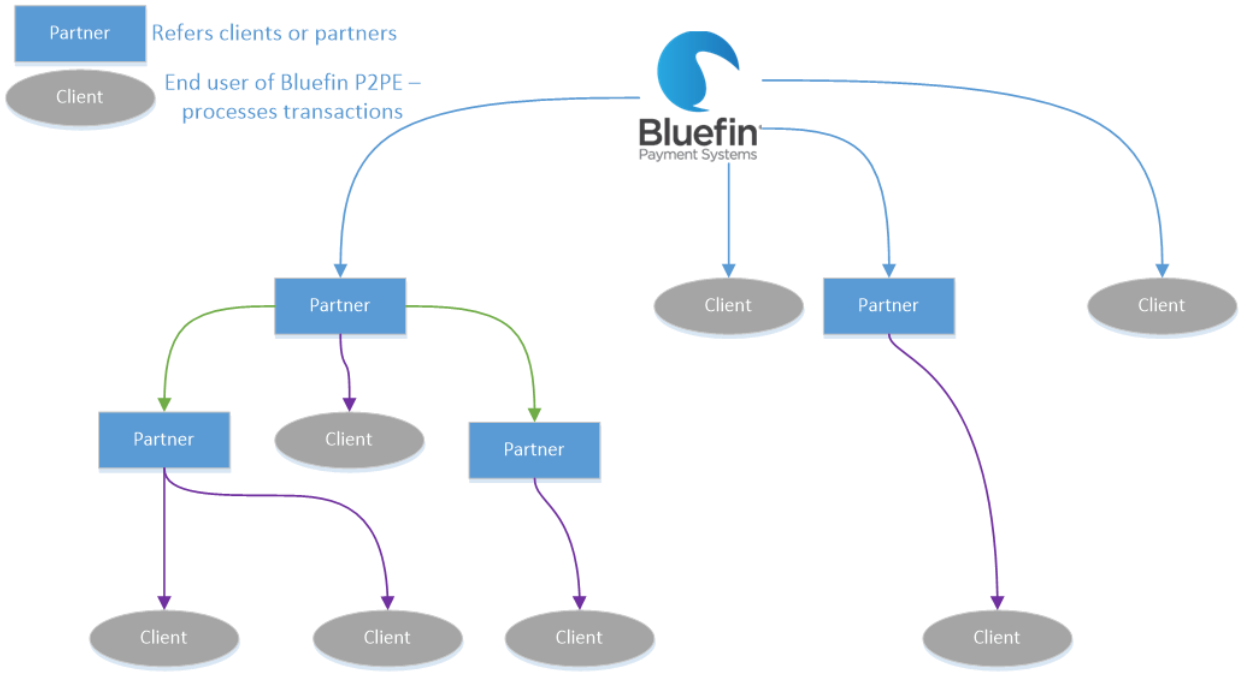
A **partner** is an entity that resells devices and services to merchants.

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

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

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

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



Contacting Support

PHONE: 800-675-6573

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

Option 2 for Technical Support

Option 4 for Customer Service

EMAIL: service@bluefin.com

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

Response Times

VOICEMAIL: Call back within four hours during business hours.

EMAIL: Response within 24 hours.

Subscribe to System Updates

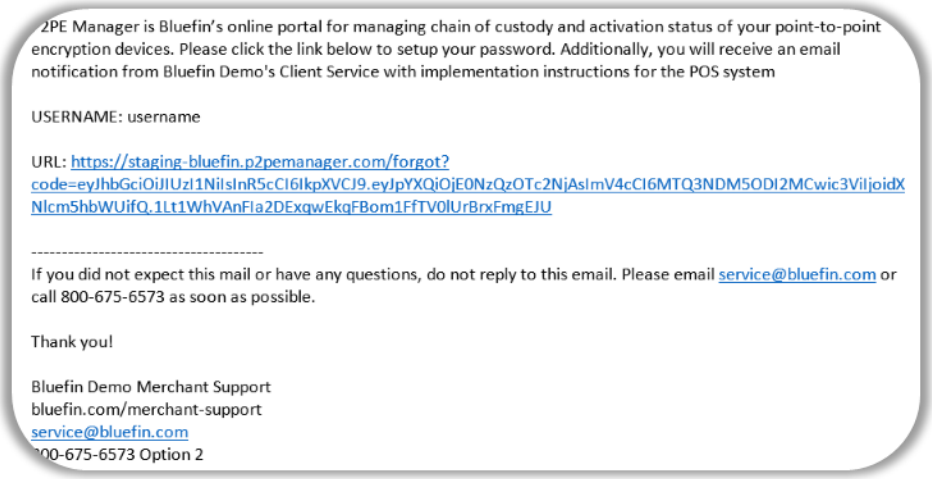
You can subscribe and get automated email notifications whenever Bluefin Payment Systems creates, updates or resolves an incident.

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

Getting Started

Logging In

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



2PE Manager is Bluefin's 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.p2pemanager.com/forgot?code=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQiOjE0NzQzOTc2NjAsImV4cCI6MTQ3NDM5ODI2MCwic3ViIjoidXNlcm5hbWUifQ.1Lt1WhVAnFla2DExqwEkqFBom1FfTV0lUrBrxFmgEJU

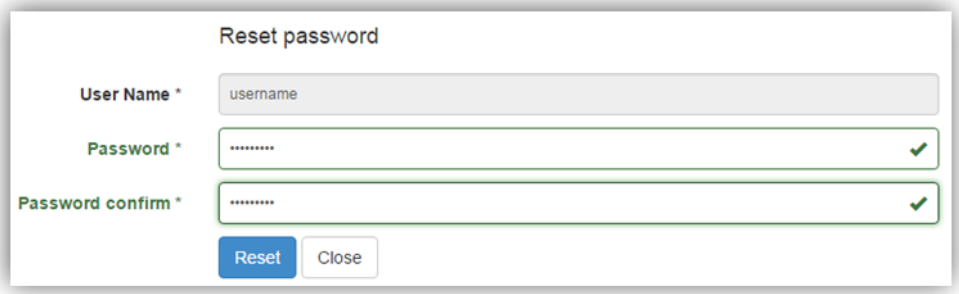
If you did not expect this mail or have any questions, do not reply to this email. Please email service@bluefin.com or call 800-675-6573 as soon as possible.

Thank you!

Bluefin Demo Merchant Support
bluefin.com/merchant-support
service@bluefin.com
800-675-6573 Option 2

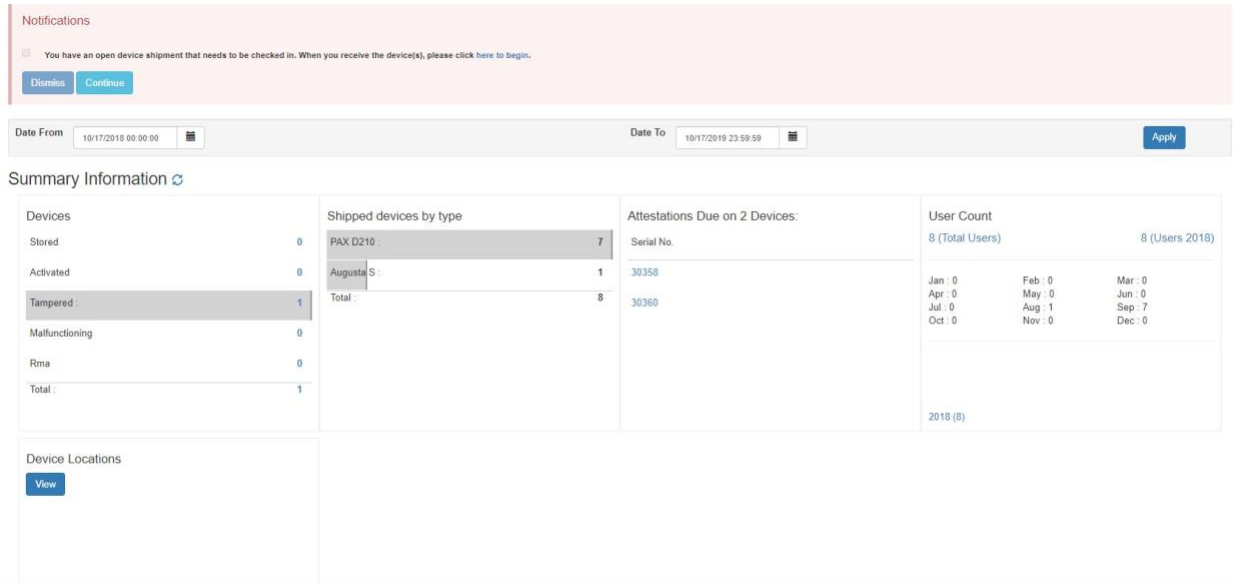
Follow the instructions in the email:

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



Dashboard

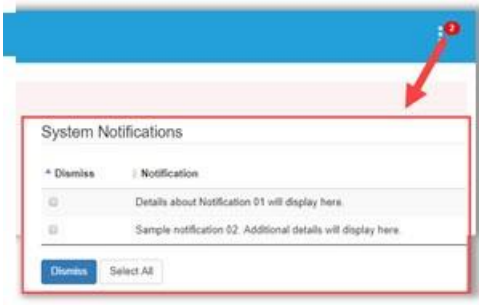
The Dashboard is the first screen you'll see after logging in. You can also navigate to it by clicking the **Dashboard** tab any time. The dashboard displays a summary of your devices and other useful information organized in "tiles."



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

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

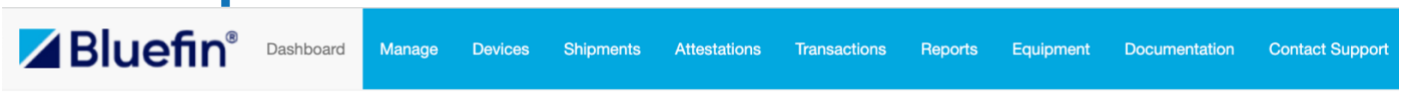
The Notifications banner displays as needed when alerts from the administrator are published. After reading a notification, you can select it and then click **Dismiss** to remove it. To hide the banner, click **Continue**. To review unread notifications, click the red notifications icon in the top right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



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

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

Menu Options At A Glance



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

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

Tab	Description
Manage	Manage Users, Locations, Device Transfers and System Notifications **NOTE**: Partners can additionally manage other functions. Refer to Appendix: Partners for details.
Devices	Displays a summary of all devices.
Shipments	Displays incoming shipments.
Attestations	Displays Current Attestations, History and Future Attestations.
Transactions	Displays a summary of transactions including encryption and decryption status.
Reports	POI Chain of Custody, Client Summary, Client Transaction Summary, Inventory Summary, User Report, Device Activity, Device Receipt, Daily Report and Decryption Totals. **NOTE**: Partners can run additional reports. Refer to Appendix: Partners for details.

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

Receiving and Activating Your Device

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

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

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

Related Information:

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

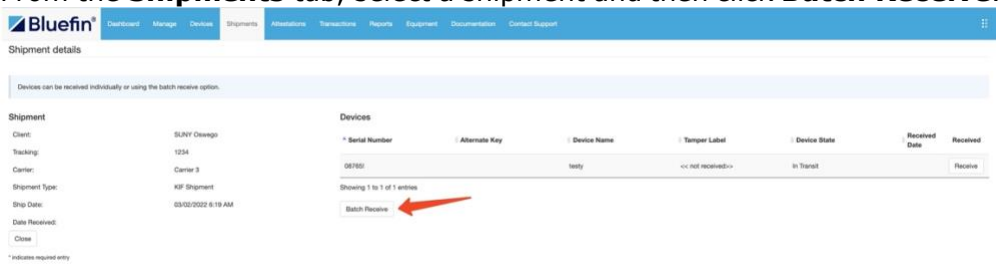
Batch Receiving Devices

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

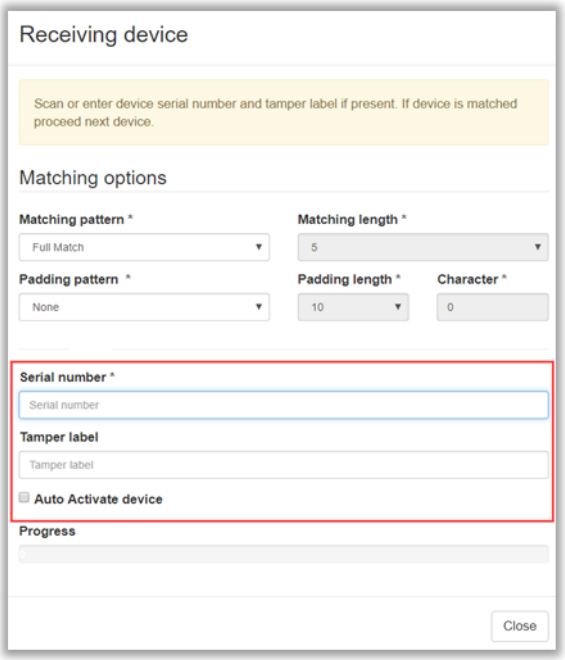
NOTE: Partners need to use the drop-down options at the top of the page and select a **Partner** and **Client** first.

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

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



2. Optional: Click **Auto Activate device** only if you are ready to activate and start using the device now.
   TIP: To take advantage of this time saving option, you must select it before scanning your devices.
3. Scan the **Serial Number**. The whole serial number will be displayed.
   NOTE: For Ingenico devices, P2PEManager will automatically find a match based on the input from the Key Injection Facility (KIF.)

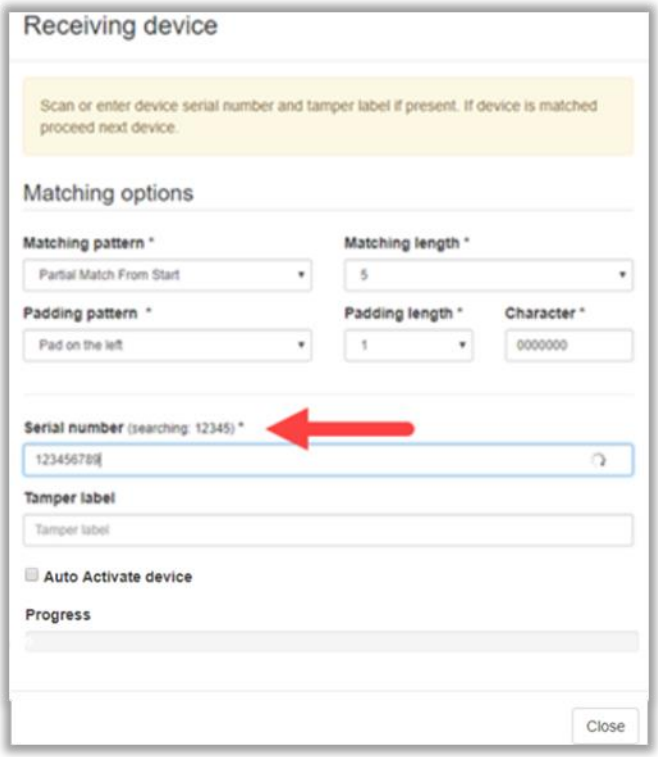


4. Scan the **security seal number**. (This number might also be called the tamper seal.) Wait for the green success message.
5. If you selected **Auto Activate device**, you're done! The **Device State** will display as **Activating**.
   If you did not select Auto Activate device, then the **Device State** will display as **Received**. To continue, follow the actions in **Step 3: Activate Your Device** in the Appendix: Receiving and Activating Your Device.

Receiving Device with Special Serial Number Requirements

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

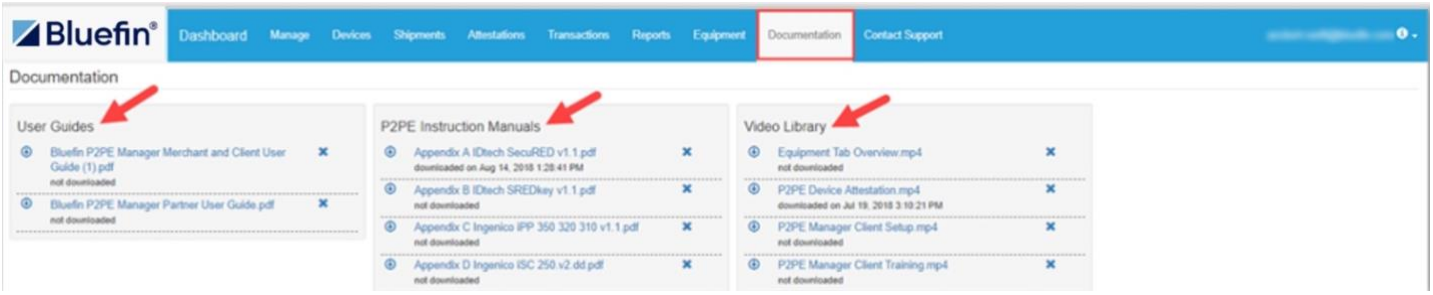
1. From the **Shipments** tab, select a shipment and then click **Batch Receive**.
2. Enter the serial number. (manual entry or scanner)
3. Select **Matching Pattern** based on your solution requirements.
    a. Full Match
    b. Partial Match from Start: Configure the Matching Length by counting from the beginning of the serial number.
    c. Partial Match from End: Configure the Matching Length by counting from the End of the serial number
4. Select a **Padding Pattern** based on your solution requirements.
    a. Pad on the Left: Configure the extra character length in the "Padding Length" and then enter in the values in the "Character" field.
    b. Pad on the Right: Configure the extra character length in the "Padding Length" and then enter in the values in the "Character" field.
5. Review the **Matching options** that display based on your configurations.



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

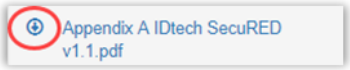
Accessing Online Help Documentation

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



Downloading and Viewing PDF Files

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

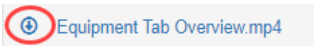


Depending on your browser, the file will automatically download to your local drive, or you will be prompted to **Open/Save** the file.

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

Downloading and Viewing Video Files

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

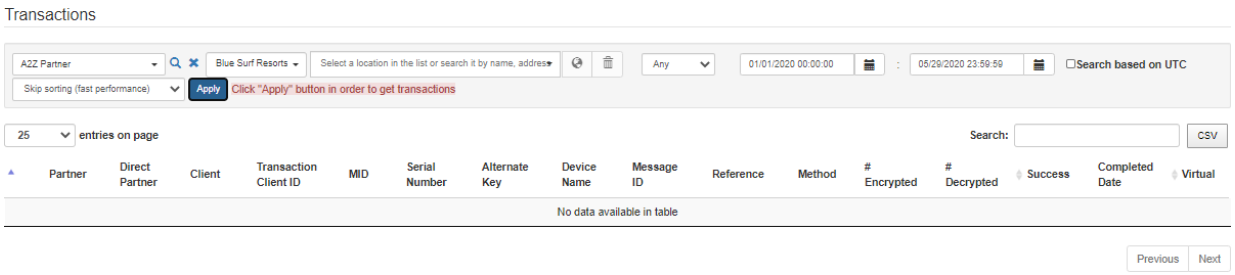


NOTE: Video file types are: .mp4 or .wav.

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

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

Transactions



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

The Transaction Summary lists transactions including encryption and decryption status.

To create this report, do the following:

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

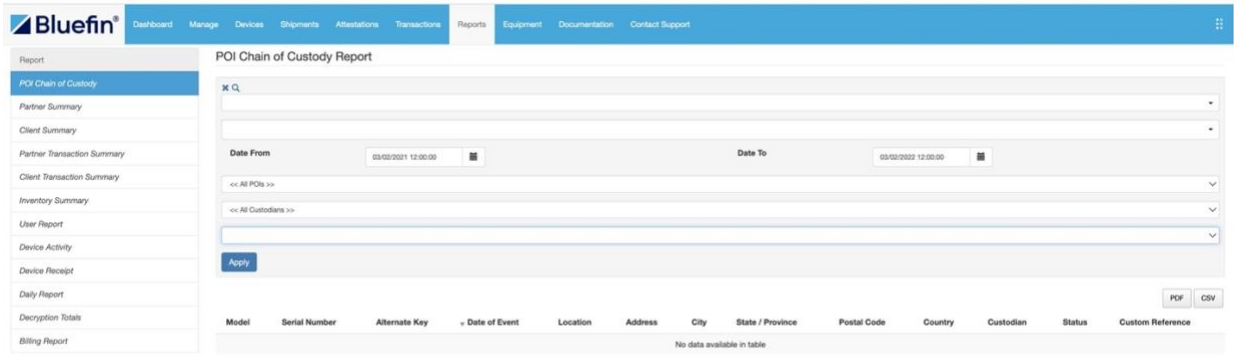
Related Information: See Exporting a Report.

Reporting

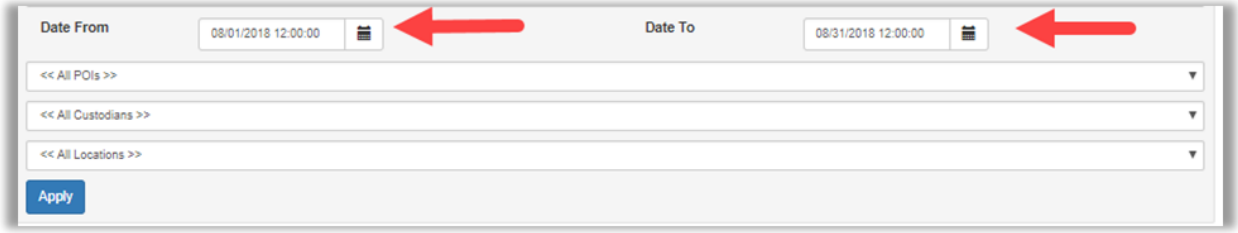
Creating the Chain of Custody Report

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

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



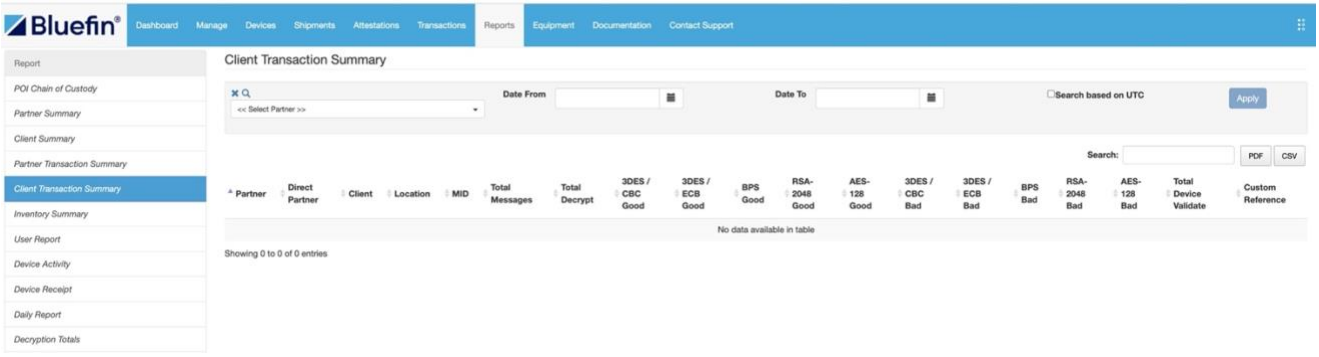
2. Enter a date range, select a POI, custodian or location based on your preference.



3. Click **Apply**.

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

Creating a Client Transaction Summary Report



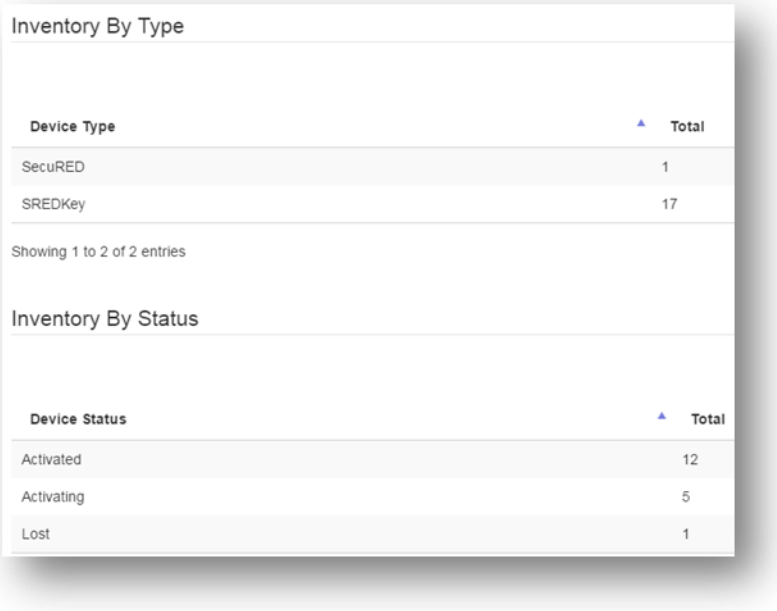
To create this report, do the following:

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

Creating the Inventory Summary Report

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

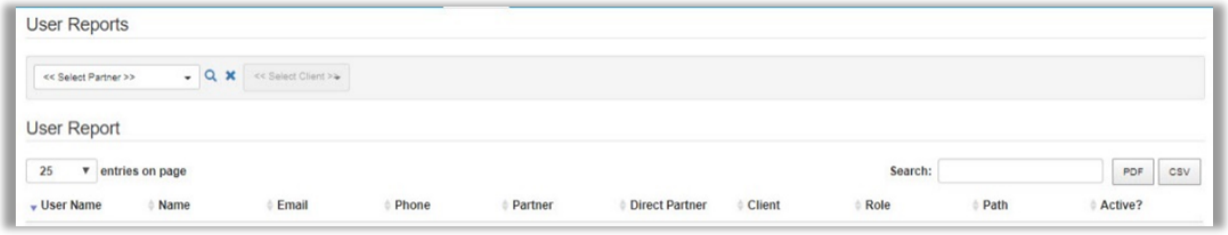
1. Click the **Reports** tab.
2. Click **Inventory Summary** in the left menu.
3. (Partner users only: Select partner and client from the drop-down lists.)
4. The report shows your inventory by device type (total number per device type) and by status (total number of devices by status):



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

User Report

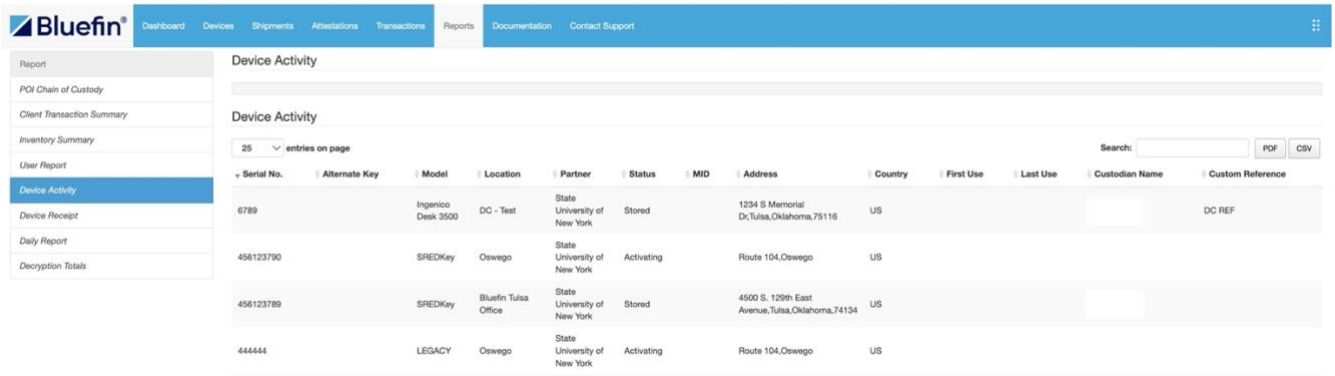
Select **Reports > User Report** to track user activity. The information displayed includes: user contact info, partner and client relationship, individual role, path and the user's active/inactive status.



Device Activity Report

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

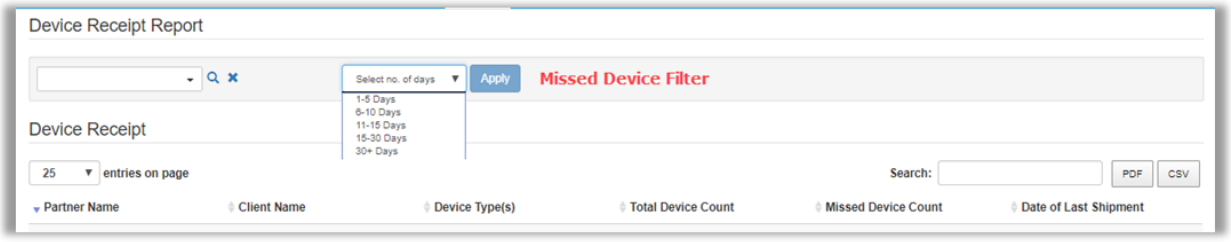
To create this report, click **Reports > Device Activity**.



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

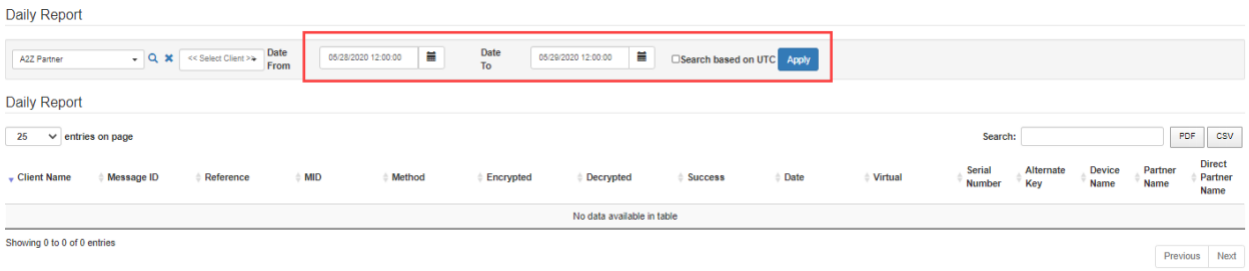
Device Receipt

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



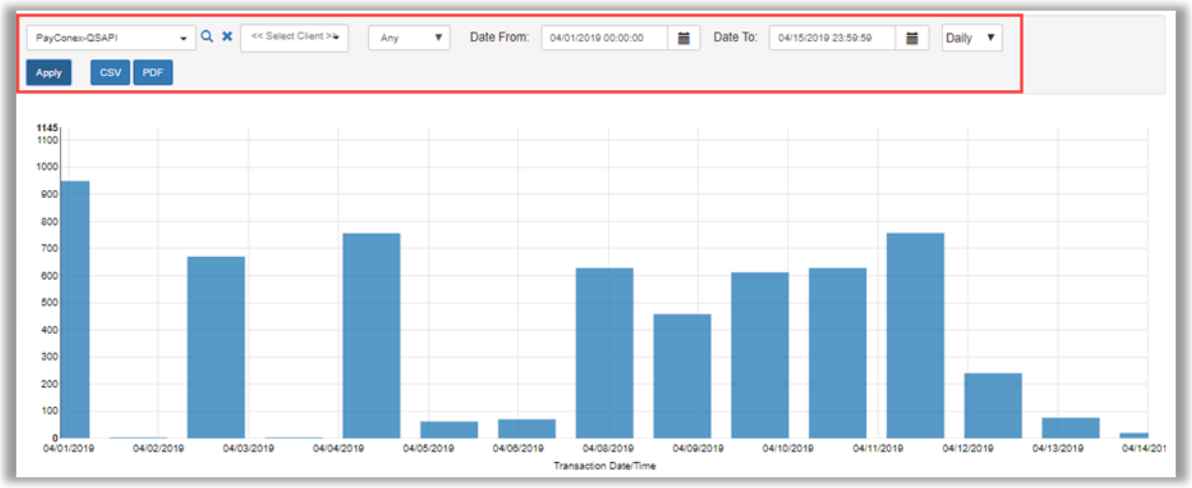
Daily Report

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



Decryption Totals

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

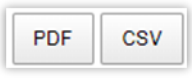


Select **Reports > Decryption Totals**. The information displayed summarizes decryption totals in a bar chart. You can filter by type of decryption and specify a date range. This information is dynamic and based on the parameters set at the top of the page.

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

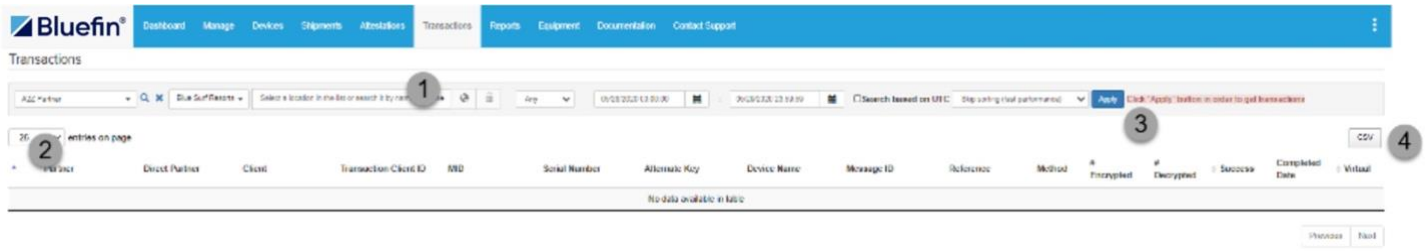
Partner users only: Options display at the top to select partner / sub-partner and client.

Exporting a Report



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

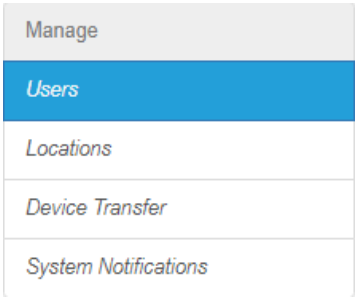
To export data, do the following:



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

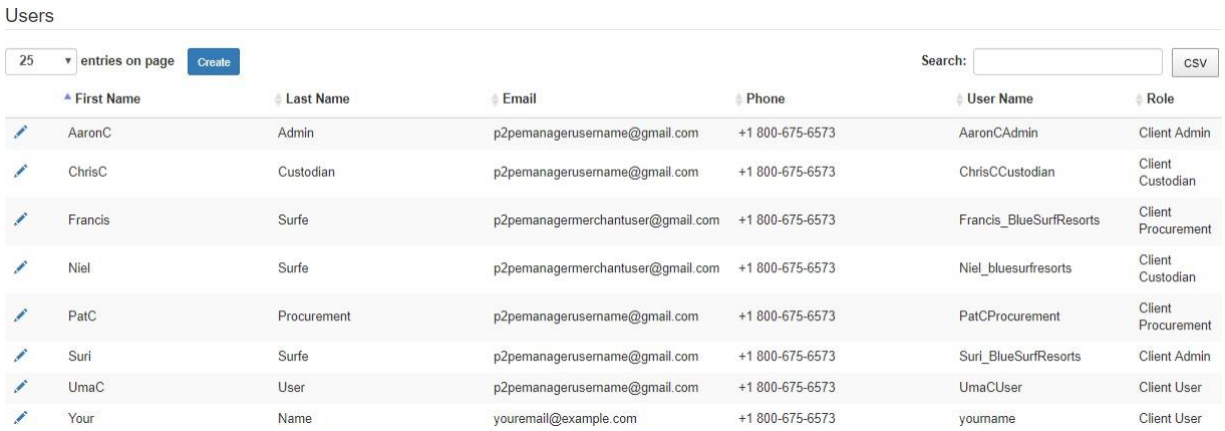
Administration

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



Managing Users

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

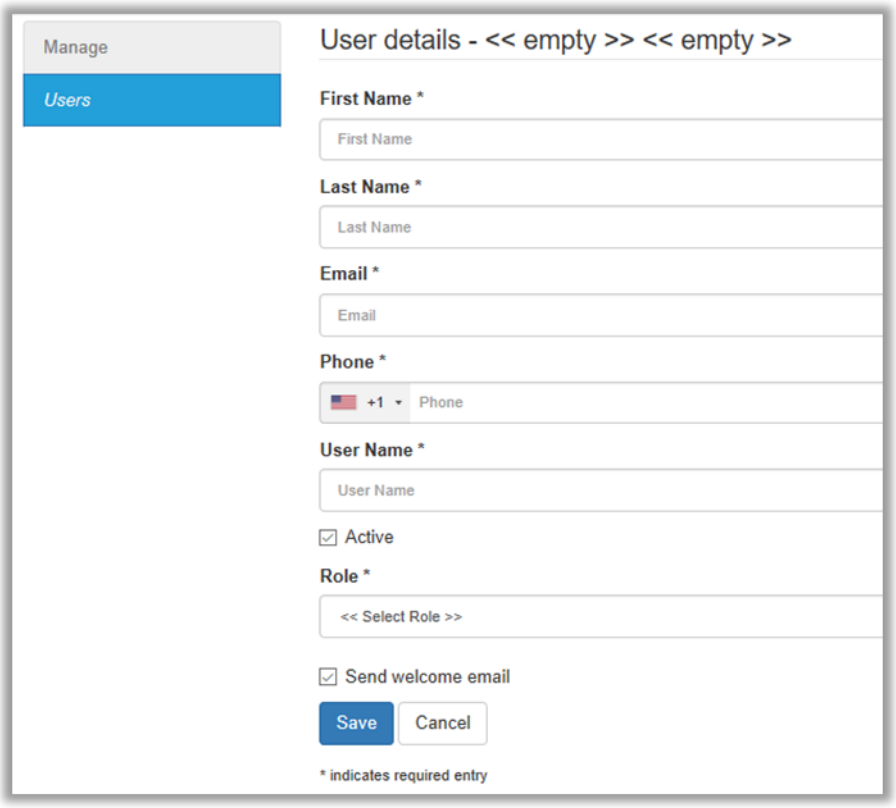


First Name	Last Name	Email	Phone	User Name	Role
AaronC	Admin	p2pemanagerusername@gmail.com	+1 800-675-6573	AaronCAdmin	Client Admin
ChrisC	Custodian	p2pemanagerusername@gmail.com	+1 800-675-6573	ChrisCCustodian	Client Custodian
Francis	Surfe	p2pemanagermerchantuser@gmail.com	+1 800-675-6573	Francis_BlueSurfResorts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

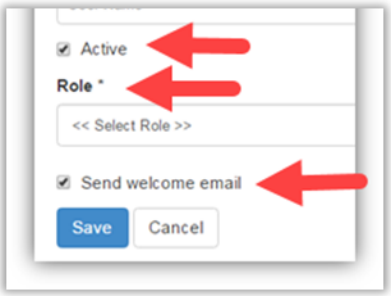
Use the filters at the top to sort the list by partner, client, and status.

Adding a User

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



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



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

Updating a User

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

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

Resetting a User's Password

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

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

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

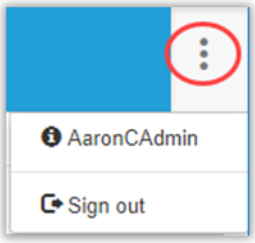
Managing Your Account Settings

Your Account Settings include:

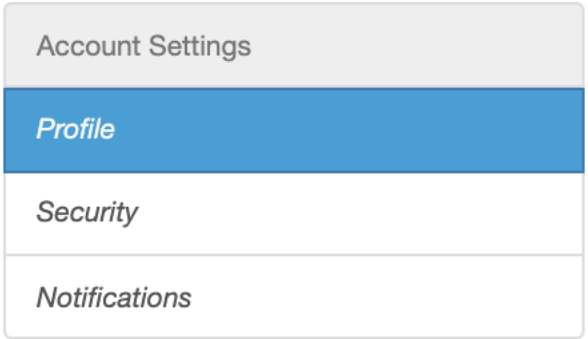
- Profile: Update your name, email address or your default login landing page (**NOTE**: Landing Page options are based on your user role.)
- Security: Update your password and set up two-factor authentication
- Notifications: Enable and select notifications you wish to receive.

To access your account settings, do the following:

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



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



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

Managing Your Notifications

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

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

IMPORTANT:

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

To enable all or selective notifications, do the following:

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

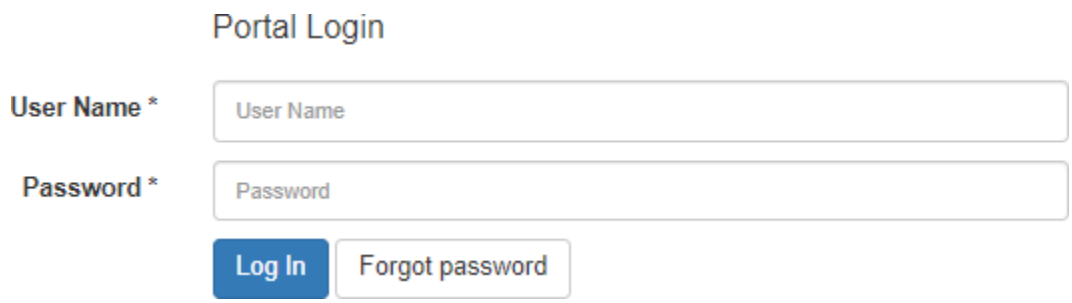
To disable all Notifications and save your notification selection, do the following:

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

Resetting Your Password (Forgotten Password)

If you forget your password, do the following:

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



2. Follow the prompts to reset your password.

Adding Locations

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

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

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

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

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

Field	Description
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

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

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

Removing Locations

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

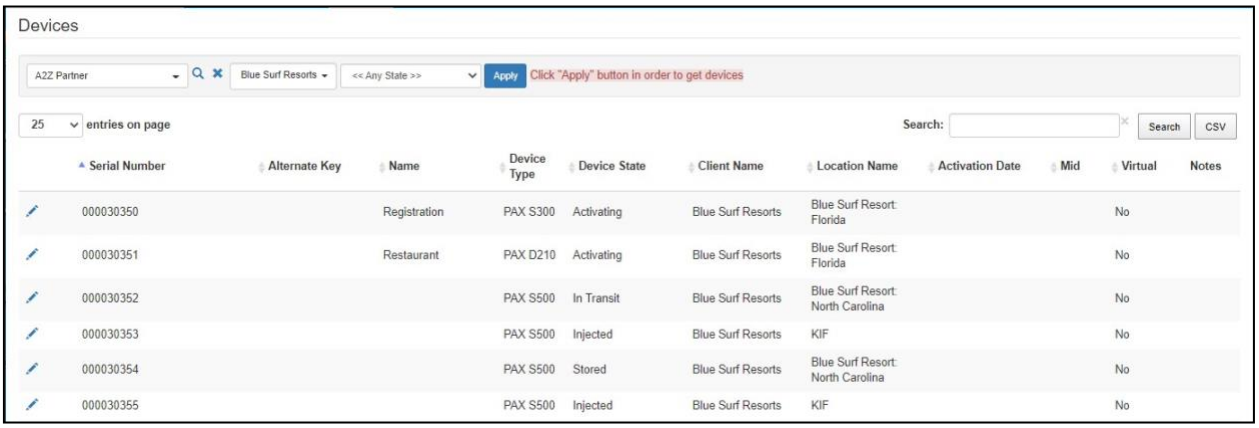
Editing Locations

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

Device Management

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

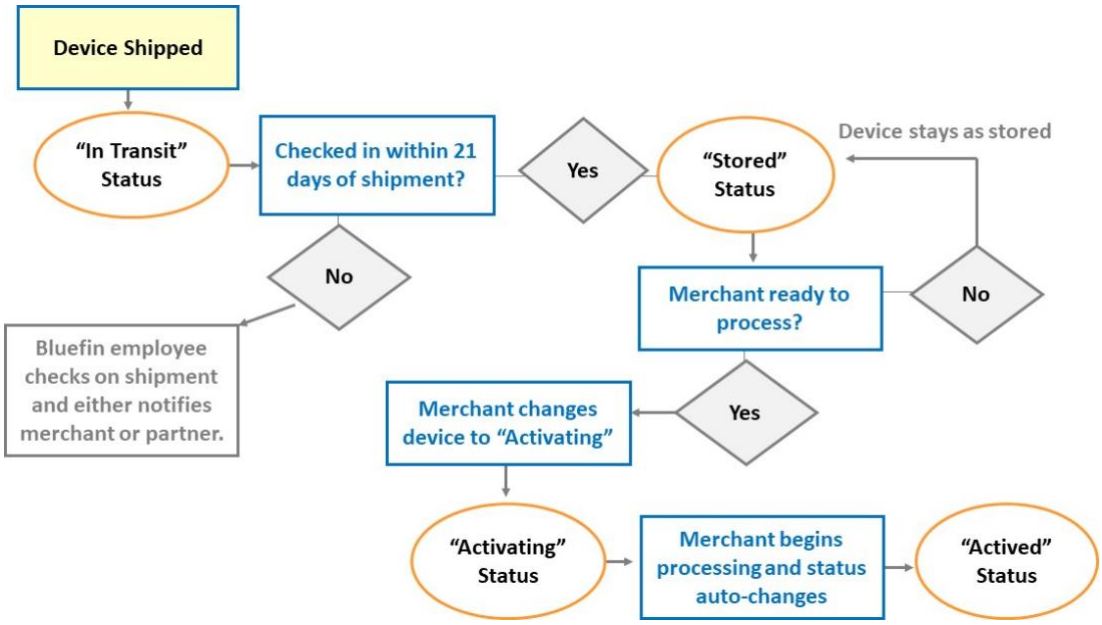
NOTE: Shared devices display with a "sharing" icon:



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

Device Activation Process Flow

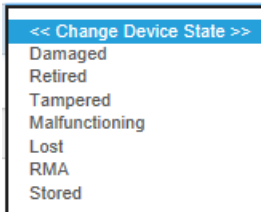
The following diagram describes the device activation flow.



Updating Devices

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

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

Field	Description
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.

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

Device State Definitions

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

STATE	CAN PROCESS?	DEFINITION
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 Branded versions of P2PE Manager, 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.
Destroyed	NO	Unit is inoperable and cannot be recovered. **NOTE**: System admins and users only.
DOA by KIF	NO	Device needs to be removed from service for destruction. **NOTE**: Key Injection Facility (KIF) use only.
In Repair	NO	Device needs to be removed from service for repair.
In Transit **(Automatic)**	NO	Device has been shipped to the merchant. **NOTE:** KIF use only.
Injected	NO	Encryption key has been injected into the unit. **NOTE:** KIF use only.
KIF Test	NO	Used by the KIF to do an end-to-end test prior to shipping. **NOTE**: KIF use only.
Lost	NO	Merchant does not know where device is.
Malfunctioning	NO	Unit is inoperable or inconsistently operable for unknown reasons. The state is automatically triggered when the system

		detects 10 consecutive decryption failures. Additionally, an email alert is sent to the device custodian so they can address this issue with Bluefin or their service provider.
PIN Pad	YES	Device is in the hands of the merchant and is available to be used when processing cards. PIN Pad devices are optional external devices used in conjunction with an activated "host" payment processing device. This is a non-billable device state. **NOTE**: System admins and System users only.
Quarantined **(by KIF)**	NO	Unit was discovered to be malfunctioning or was tampered with prior to shipping. (Unit was returned to KIF outside of the RMA process.) **NOTE**: System admins and System users only.
Retired	NO	Merchant no longer wishes to use a device. If the 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 not 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.
Unassigned	NO	Unit is injected and held by KIF.

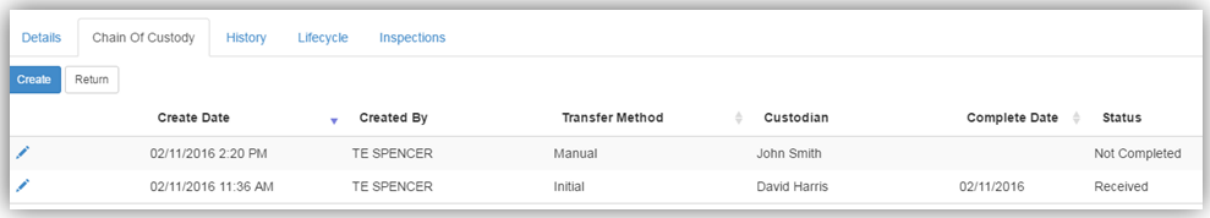
Viewing Device Details

Chain of Custody

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

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

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



Device State History

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

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

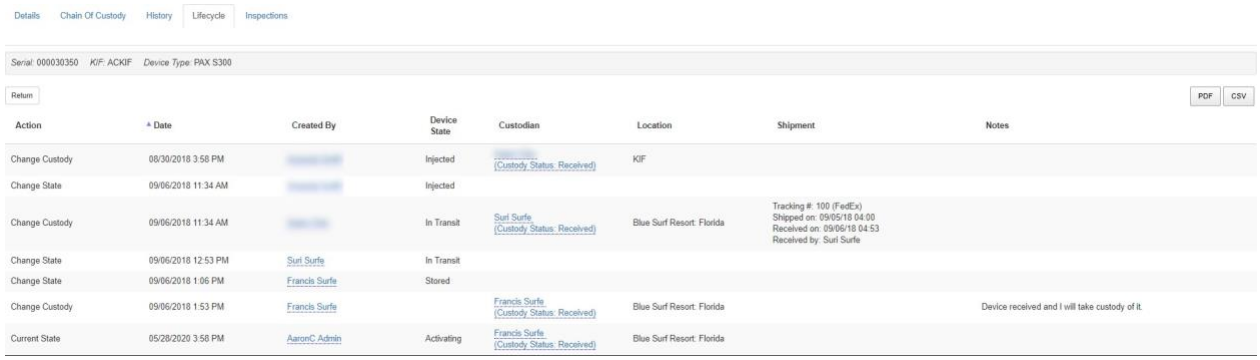
NOTE: User names display with a hyperlink, so you can see their contact information.

Lifecycle Report - Detailed Device History

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

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

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



Return Merchandise Authorization Process

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

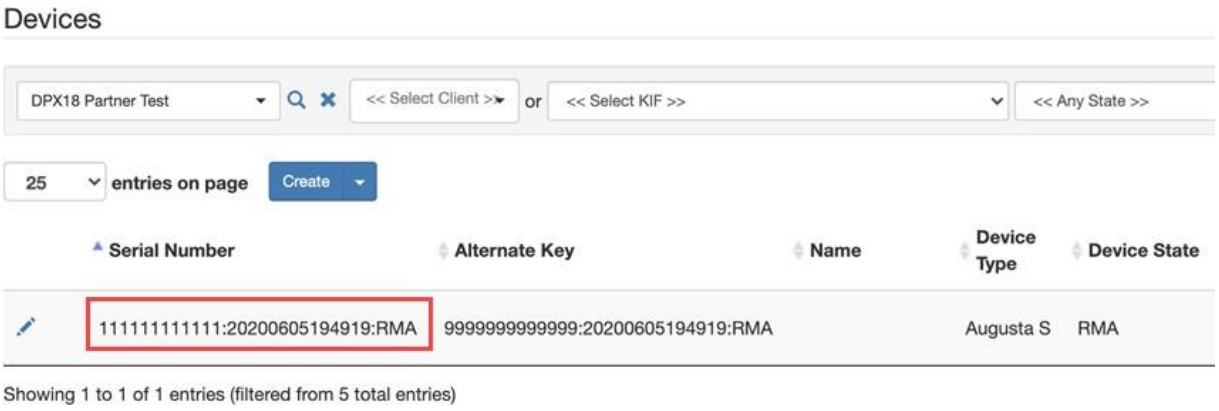
If you discover that your device is malfunctioning or suspect it has been tampered with, contact your relationship manager or contact Bluefin Support.

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

1. Select your **Partner Accoun**t and choose **Client** if applicable.
2. Click **Edit** (pencil icon) next to the device.
3. Change **Device State** to RMA.
   NOTE: A device can only be moved to RMA after it's been received.

IMPORTANT:

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



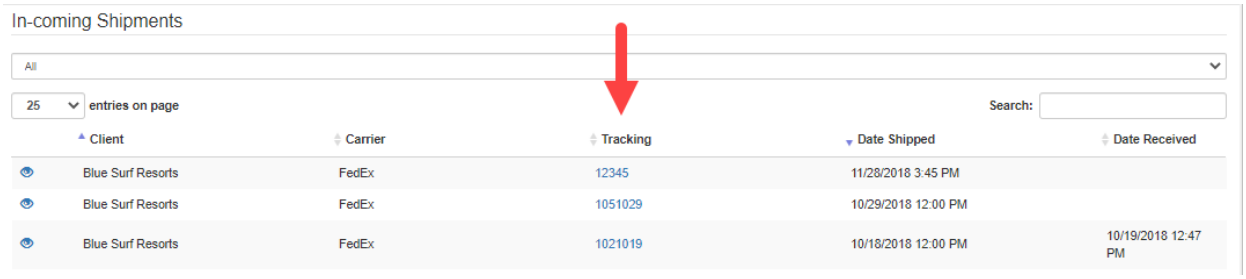
Checking on Device Shipment and Tracking

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

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

Checking Tracking Number

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

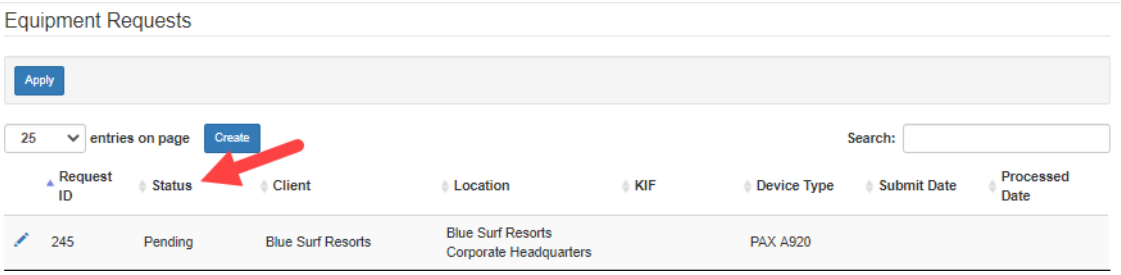


Checking Device Status

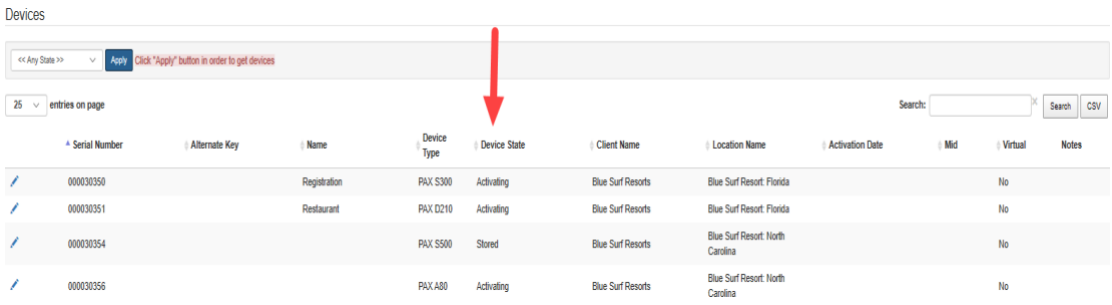
NOTE: Depending on how your organization was setup, you may or may not have access to the **Equipment** tab. (If you do not have access to the Equipment tab, check your email for updates or contact Bluefin Support.)

If there is no tracking number, do the following:

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



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 mean that your order was not successfully placed. Depending on how your order was placed, it may not show up here.

1. Select the **Equipment** tab.
2. Refer to the **Status** section.
   INITIAL: Order was successfully submitted.
   PENDING: Someone at key injection facility has been assigned the order and is working on it.
   COMPLETED: Order has been shipped.

Transferring a Device between Custodians or Locations

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

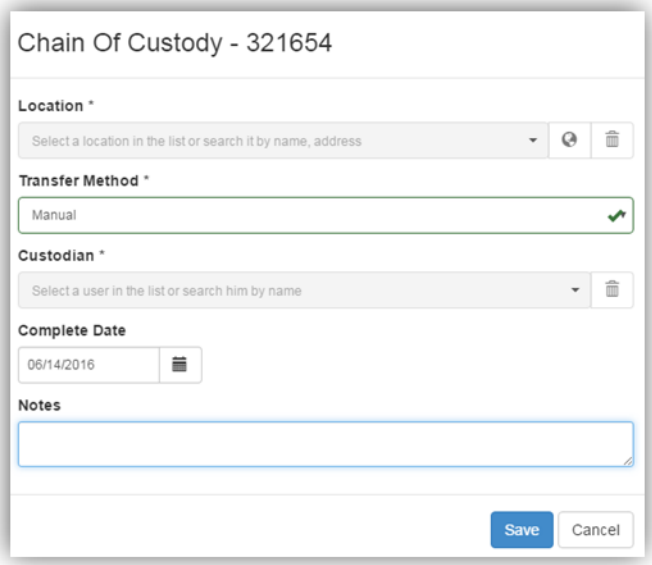
You can transfer a device to a different location if the device is moved. **EXAMPLE**: A device is moved from the "Chicago Office" to the "San Francisco Office."

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

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

1. Click **Edit** (pencil icon) next to the device you would like to transfer.
2. Click the **Chain Of Custody** tab and then click **Create**.
3. Complete fields and click **Save**.
   Transfer Method:
   a. Choose Manual if device is handed off or if someone else taking responsibility for the device.

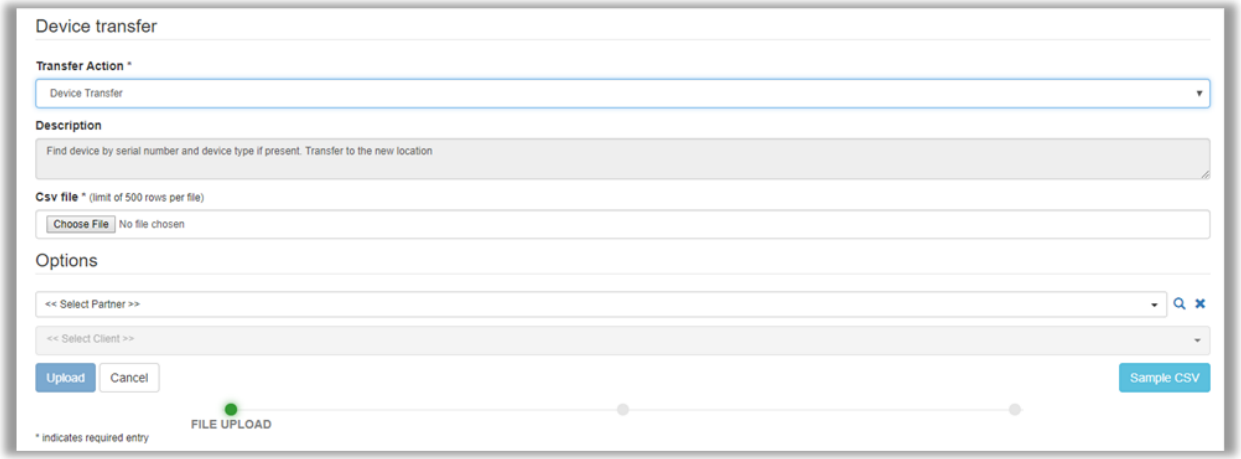
b. Choose Shipment if device is being mailed from one location or custodian to another. Complete additional fields when prompted.



Transferring Multiple Device Locations

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

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



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. 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.

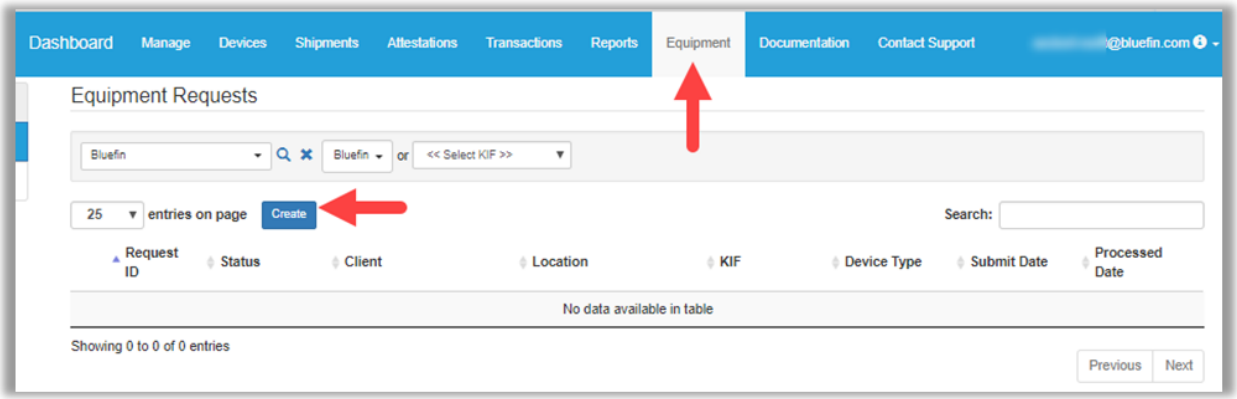
Deploying Equipment

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

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

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

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



2. Complete the Deployment request as noted below.

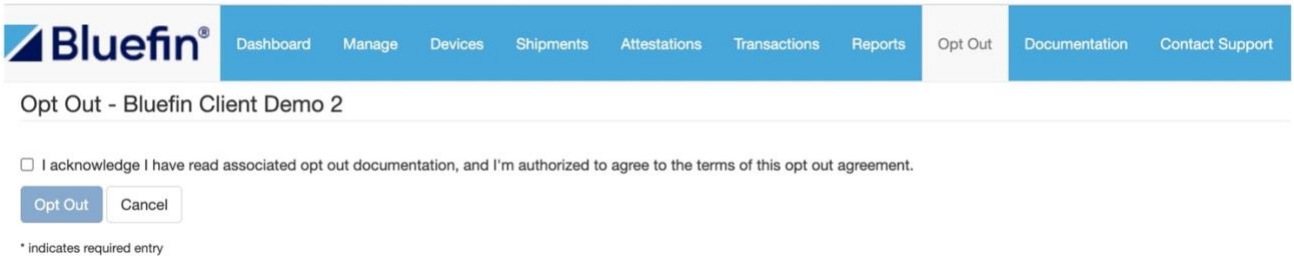
Field	Description
Partner	(Partners Users only: Select the Partner from the drop-down lists.)
Client	(Partners Users only: Select the Client from the drop-down lists.)
Location	Required. **TIP**: If sending to a new location, add the location before placing order. Refer to Adding Locations.
Contact	Required.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

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

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

Opt Out of Bluefin Program

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



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

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

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

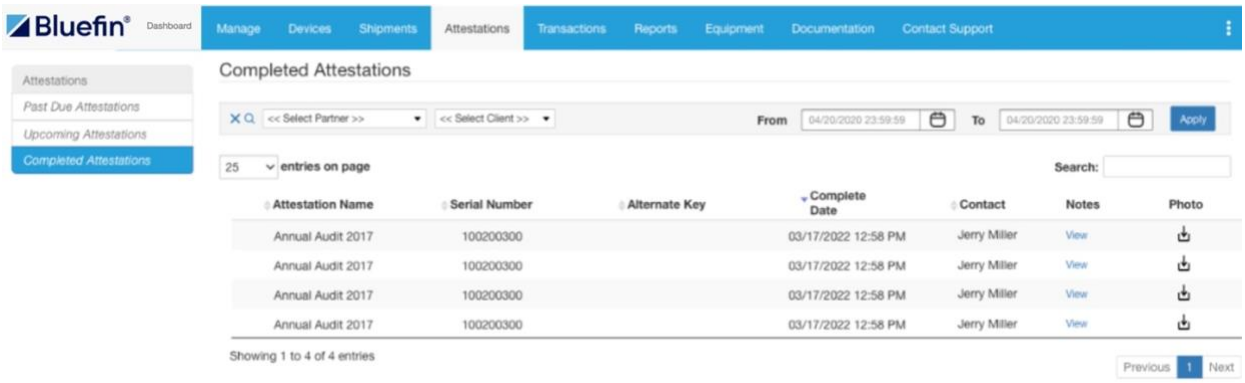
Device Attestations

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

Viewing Completed Attestations

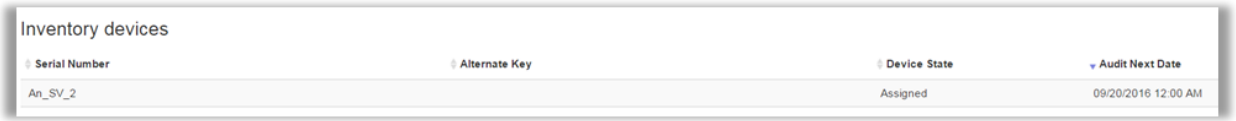
The Completed Attestations tab provides you with a record of all the devices that have been attested.

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



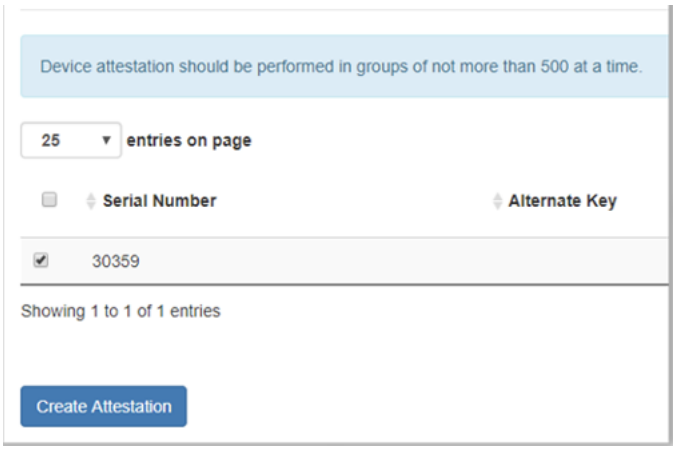
3. Review the **Complete Date** for attested devices.

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



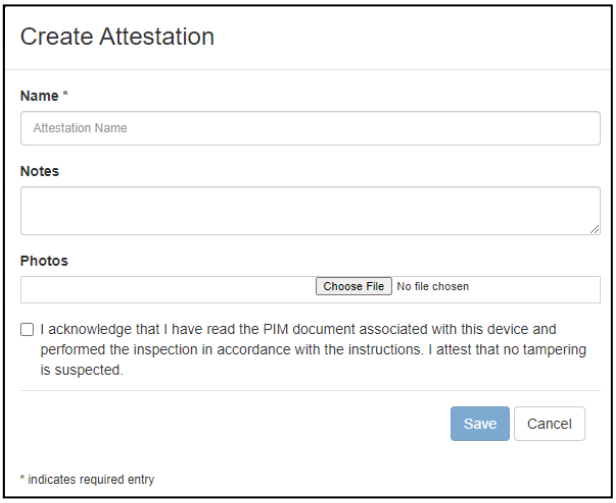
1. Click the **Attestations** tab. Select **Upcoming Attestations** in the left column.

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



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

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



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

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

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

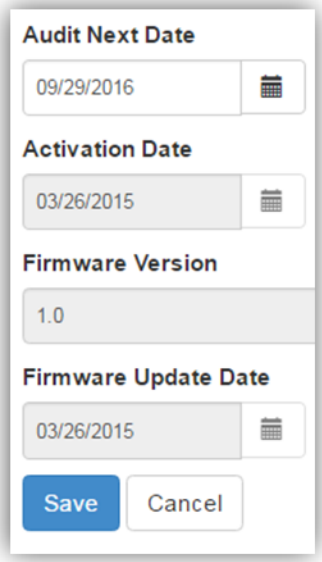
IMPORTANT: Attestations can also be performed in the Past Due Attestations tab by following Step 2 through Step 5.

Changing Device Attestation Date

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

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

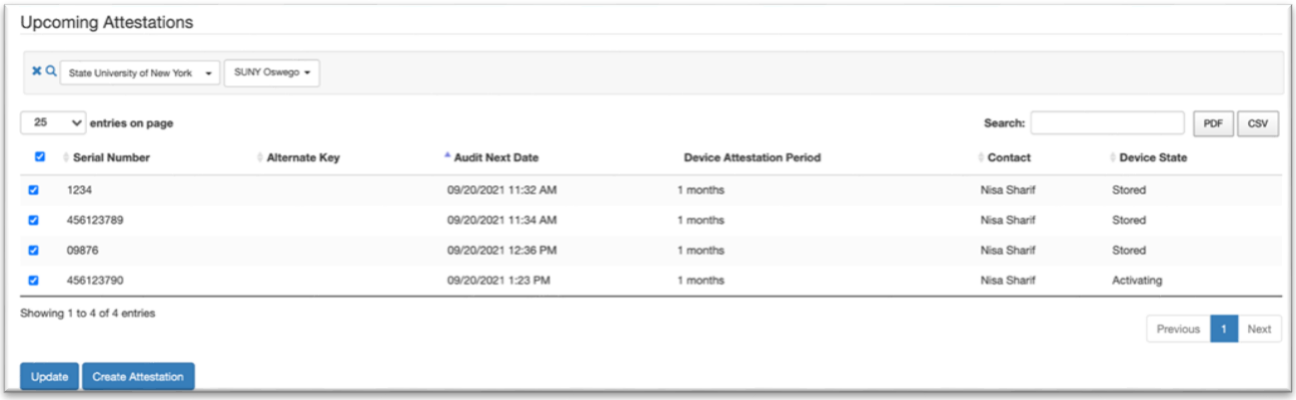
4. Optional. Update the **Audit Next Date** based on your preference and click **Save** when you're done.



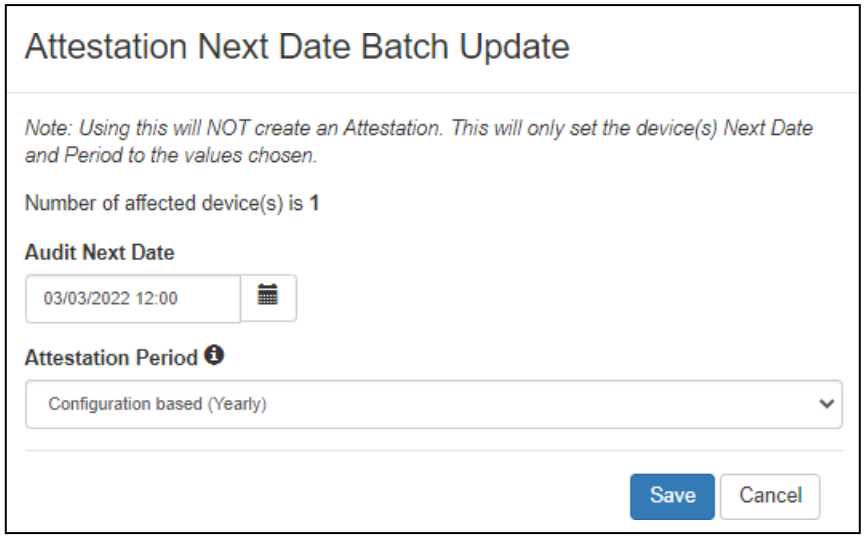
Batch Process: Change Device Attestation Date

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

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



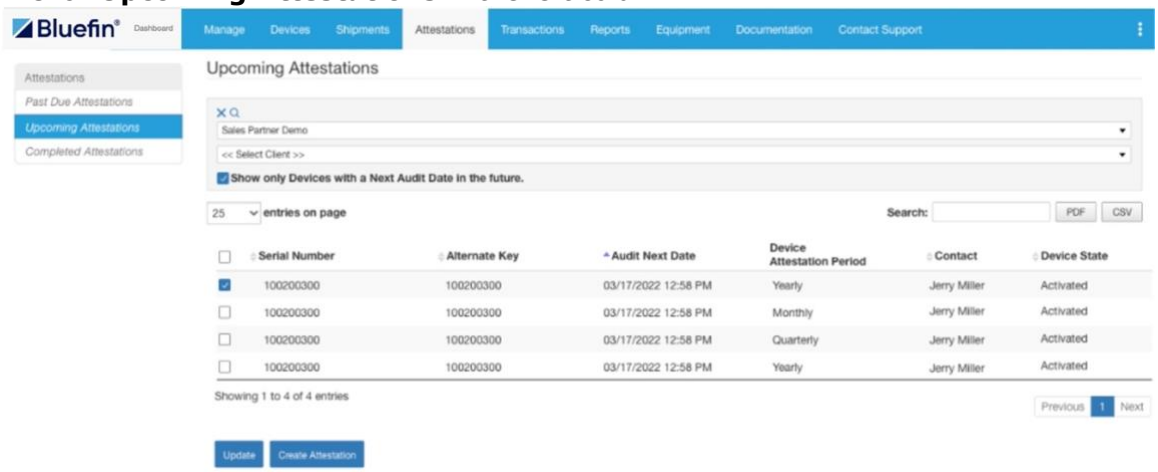
2. Update the information as appropriate for **Audit Next Date** and **Attestation Period**.



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

Viewing Upcoming Attestations

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

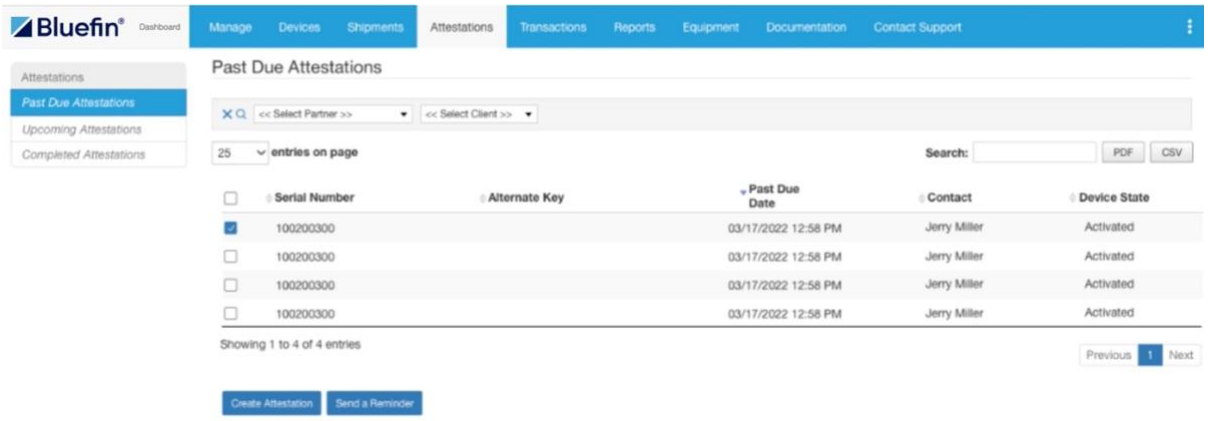


3. Review the **Audit Next Date** for the next date the device is scheduled to be audited.

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

Viewing Past Due Attestations

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



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

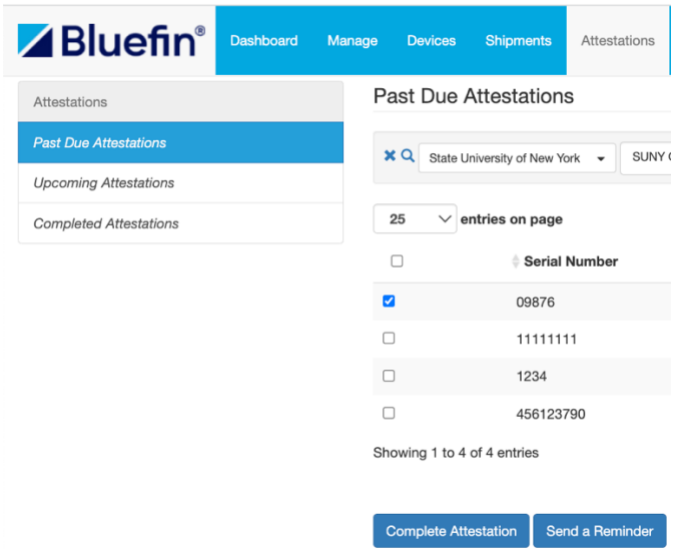
Optional: You can use the Search feature to narrow the list and you can optionally download a list of devices into a PDF or CSV file.

Sending a Reminder to Complete Past Due

Attestations

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

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



Device Tampering Detection

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

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

Appendix: User Roles

Client / Merchant Roles

Client User Roles & Permissions	Client Admin	Client Custodian	Client Procurement	Client User
Devices	Manage	Manage	Manage	View
Shipments	Manage	Manage	View	View
Attestations	Conduct	Conduct	Conduct	Conduct
Encrypted Transactions	View	(No Access)	(No Access)	View
Reports	Yes	Yes	Yes	(No Access)
Equipment	Yes	(No Access)	Yes	(No Access)
Users	Manage	(No Access)	(No Access)	(No Access)
Locations	Manage	(No Access)	(No Access)	(No Access)
Device Transfer	Manage	Manage	(No Access)	(No Access)

Partner Roles

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

Appendix: Receiving and Activating Your Device

You will receive your device in the mail.

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

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

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

Overview

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

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

Step 3. Activate Your Device.

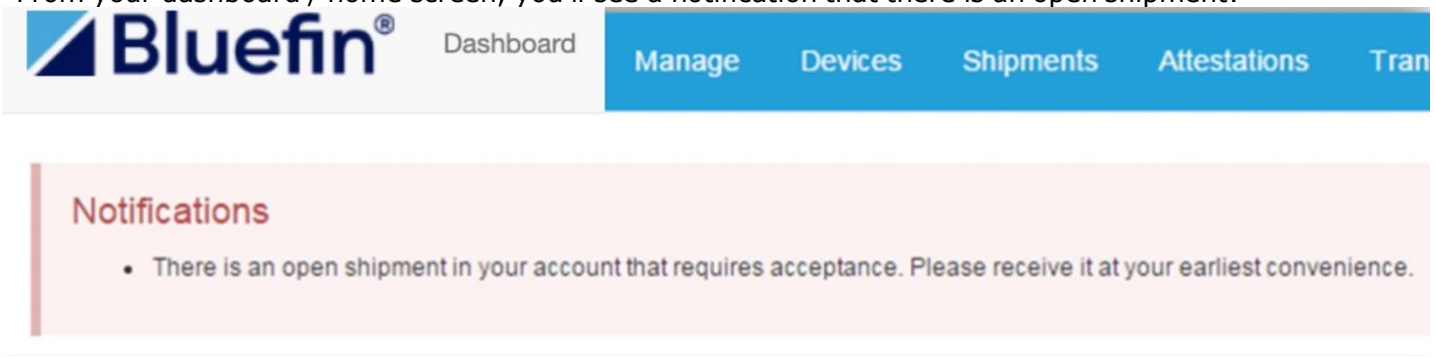
Step 1. Access the P2PE Manager Online

To log into P2PE Manager, do the following:

1. Access the P2PE Manager from a browser: P2PE Manager (https://bluefin.p2pe-manager.com/login)
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

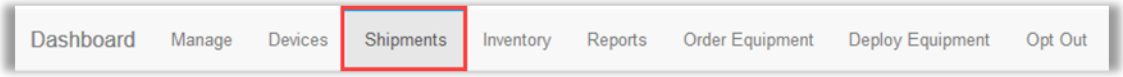
From your dashboard / home screen, you'll see a notification that there is an open shipment:



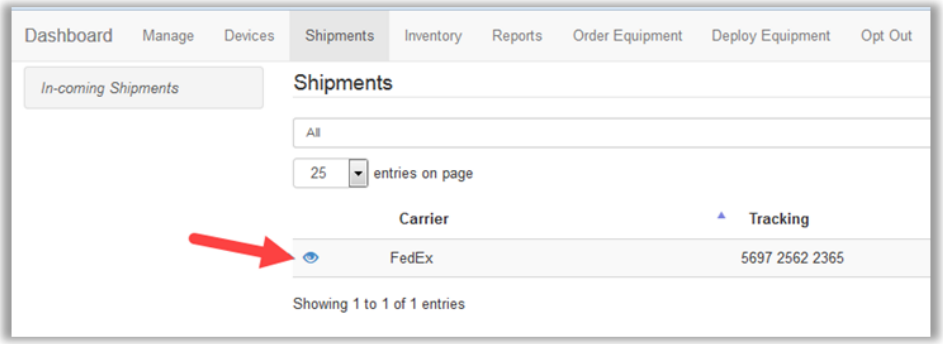
To log receipt of your shipment, do the following:

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

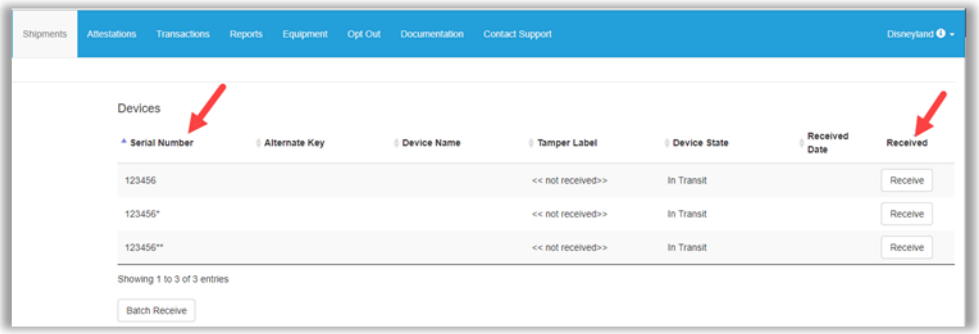
1. Click the **Shipments** tab. Here you'll see all shipments sent to you from Bluefin.



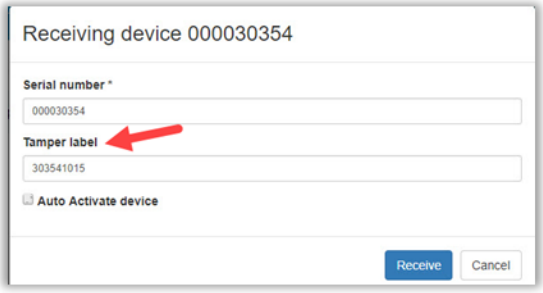
2. To document that you received the shipment, click the **View** icon ( ) next to the appropriate item.



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.)

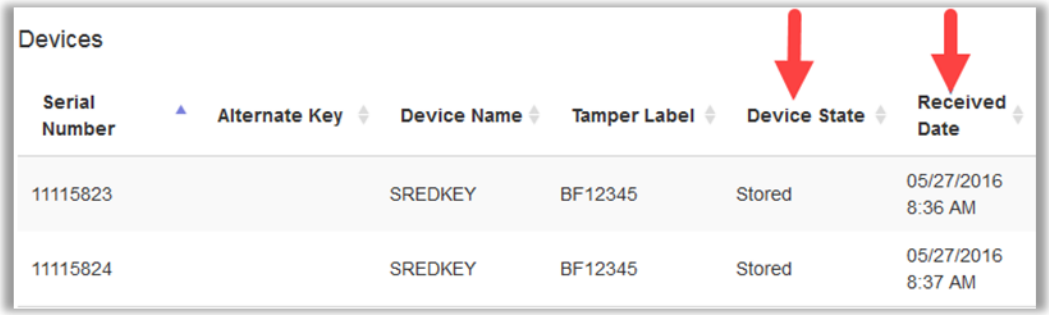


4. From the secure packing around your device, locate the **security seal number** and enter it into the **Tamper label** field. Then click **Receive**.
   NOTE: The serial number is populated for you based on the device you selected in #3 above.



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.

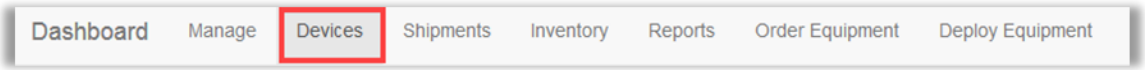


Step 3: Activate Your Device

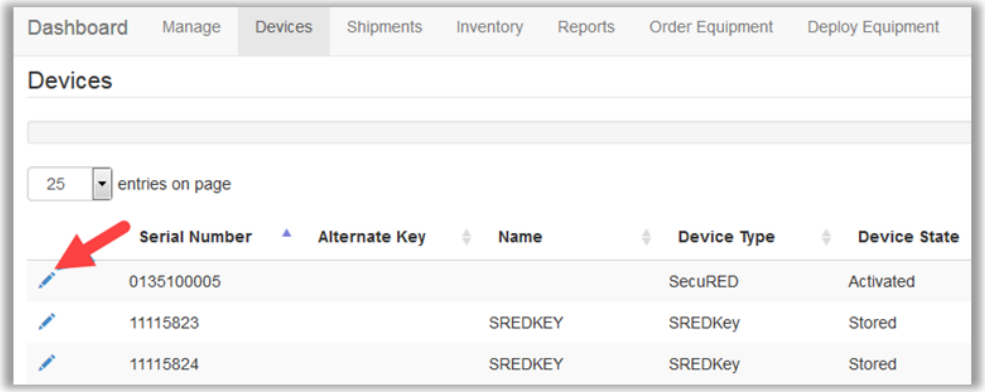
NOTE: If you selected **Auto Activate device**, you can skip this step.

To activate your device, do the following:

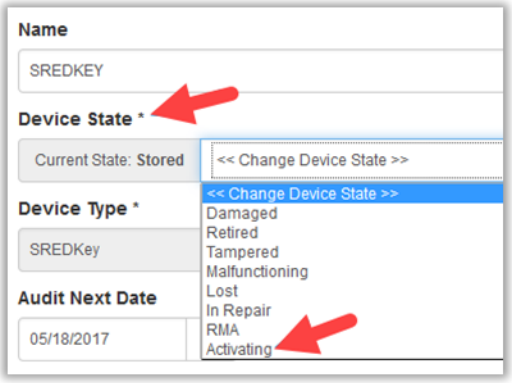
1. Click the **Devices** tab. Here you'll see all your devices.



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**.



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, Work-station.
5. Click **Save** when you're done.

NOTE: After completing these steps, your device is now functional, and you can begin processing transactions! Once you begin processing cards, your Device State will automatically change 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 actions 1 & 2 as written.
3. Click the **Device State** drop-down arrow and then select **Tampered**.
4. Click **Save** when you're done.

Appendix: Partners

IMPORTANT: Capabilities restricted to Partners are described here.

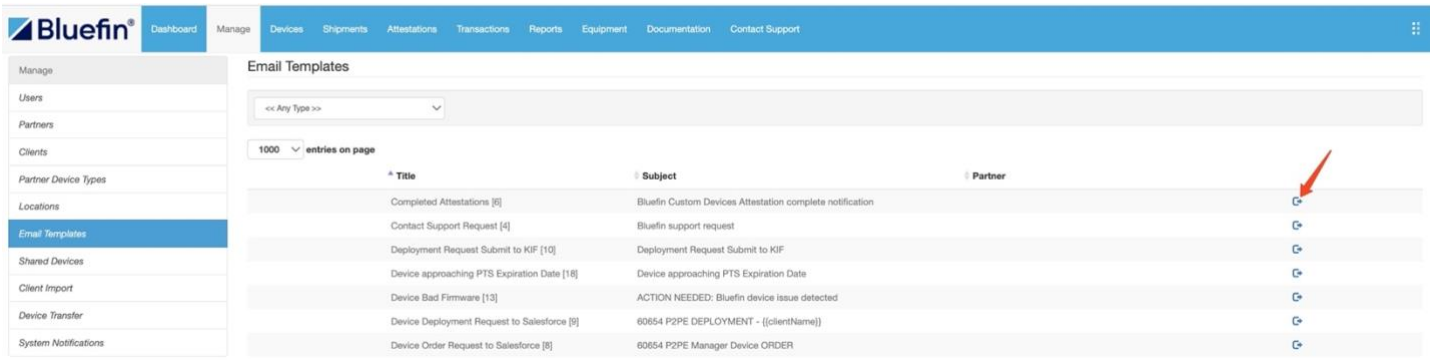
Client Merchant Communications

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

Email Notification	Explanation & Frequency	Sent To
Welcome Email	When a new user is added to P2PE Manager, login credentials are sent in email along with a link to set up a password.	P2PE User
Password Reset / Forgotten Password	When a user forgets their password, an email is sent with a link to set up new password	P2PE User
Shipment	An email is sent when a device is shipped.	Device Custodian
Shipment Overdue	An alert is sent to the Custodian when a device shipment is not received within 14 days of it's ship date.	Device Custodian
Device State Changes	Notification that the device's state has changed. Refer to Device State Definitions.	Device Custodian
Attestation Due	10 days prior to the device audit date a notification is sent. **NOTE**: If multiple devices are due on the same day, then one email that summarizes all devices will be sent. Device serial number and location are included.	Device Custodian
Attestation Late	If an attestation is missed, 10 days after the device audit date an alert is sent. **NOTE**: If multiple devices are late, then one email that summarizes all late devices will be sent.	Device Custodian
Attestation Complete	Confirmation of completed attestation.	Device Custodian
Action Needed	Notification that action is needed when the following issues are detected: • Device firmware issue detected • Device sends clear-text cardholder data • Device sends corrupt data	Device Custodian and P2PE User

Customizing Email Templates

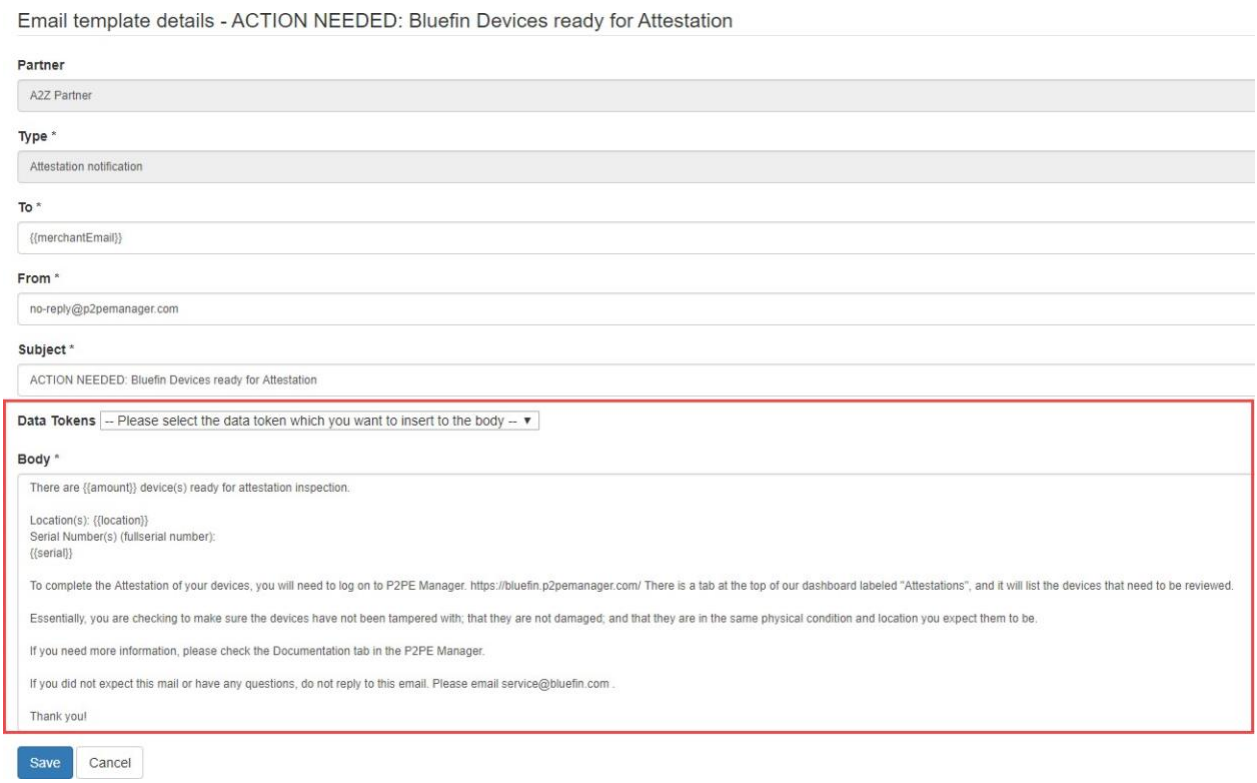
Partners and Sub-Partners can modify email templates as needed. From **Manage > Email Templates** click override next to the template of your choice. This creates a copy of the template that can be customized as all fields in the template can be modified.



Adding Data Tokens

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

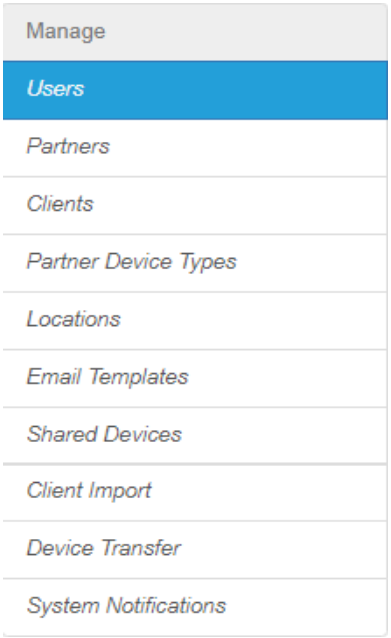
NOTE: The data tokens that display in the list are dynamic and depend on the email template selected.



Deleting Email Templates

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

Administration



Editing Your Own Partner Record

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

NOTE:

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

Adding a Partner Record (Sub-Partner)

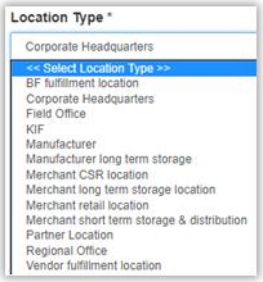
A sub-partner is another organization that resells devices and services. For example, a Bluefin partner that is a payment gateway provider might need to setup a sub-partner record for one of their resellers. This would enable the reseller to set up merchants (or "clients" as they are called in P2PE Manager).

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

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

3. Enter the information requested for the required fields.

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

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

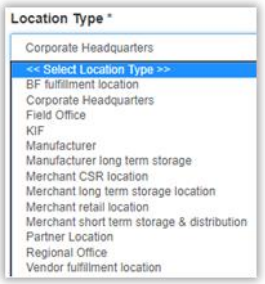
4. Click **Save** when you're done.

Adding a Client / Merchant

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

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

3. Enter the information requested for the required fields.

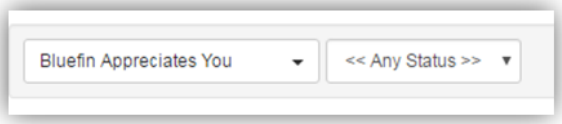
Field	Description
Direct Partner	Required. Select the partner from the list.
Name	Required. Enter the client's/merchant's name.
Active	Optional. Select the checkbox to enable the client.
Mid	Optional.
Contact Person	Required. Enter the **First Name, Last Name, Email address, Phone and User Name**. ***Best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

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

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

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



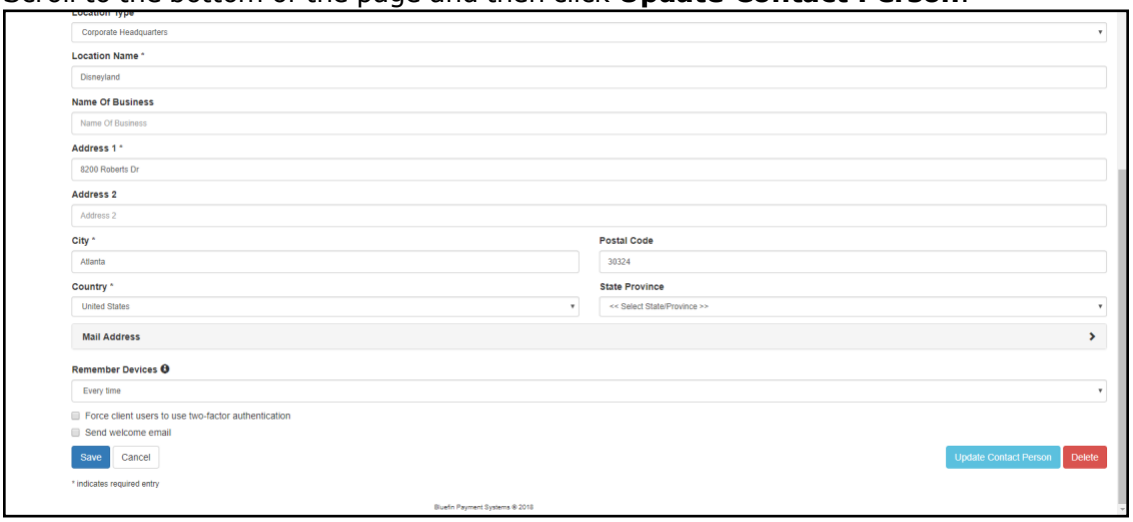
Editing a Client's Contact Person

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**.

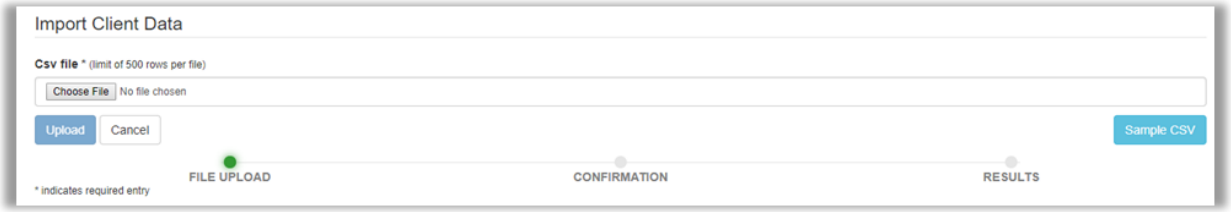
To update the contact person, do the following:

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**.



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

Client Import

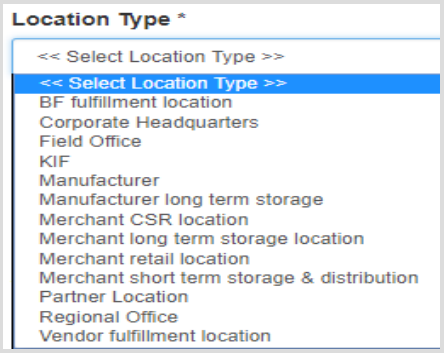


You can create client records in a CSV file and batch upload them.

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

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

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

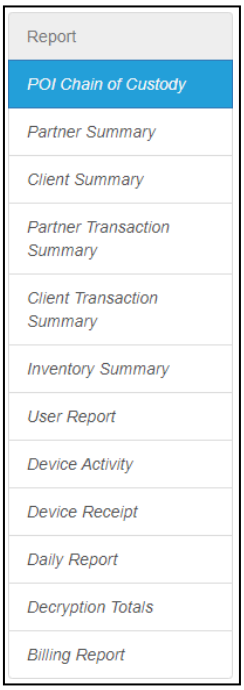
Fields	Description
DirectPartner	Required.
ClientName	Required.
LocationName	Required.
LocationType 	Required. Options: BF Fulfillment location, Corporate Headquarters, Field Office, KIF, Manufacturer, Manufacturer long time storage, CSR Location, Merchant Long time storage location, Merchant Retail Location, Merchant short term storage & distribution, Partner Location, Regional Office, Vendor Fulfillment Location
LocationNameofBusiness	Optional.
LocationCountry	Required.
LocationAddress1	Required.
LocationAddress2	Optional.

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

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

Running Reports

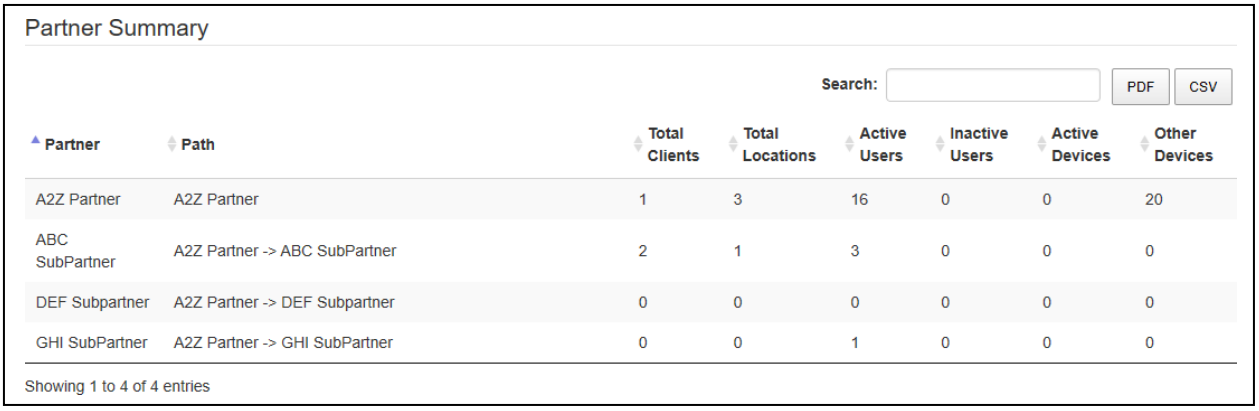
Partners can run the same reports as clients and additional reports that are restricted to just partners. Oftentimes the only difference between how clients/partners run these reports is in setup parameters. Partners must populate the Partner and Client fields by selecting an option from a drop-down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



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

Partner Summary

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



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

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

Client Summary

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


Client Summary

Search: PDF CSV

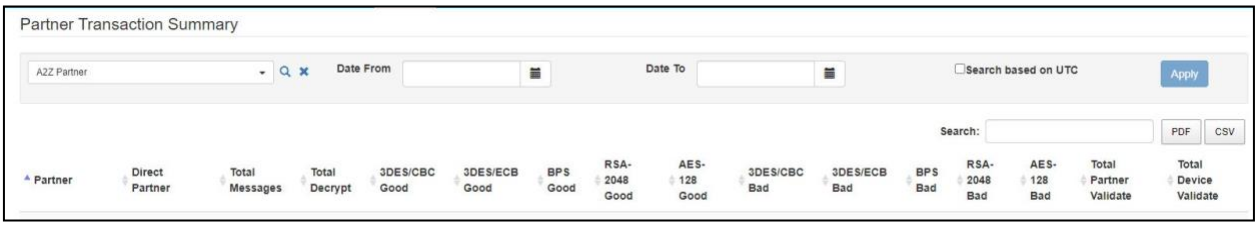
Partner	Direct Partner	Path	Client	Location	Active Users	Inactive Users	Active Devices	Other Devices
A2Z Partner	A2Z Partner	A2Z Partner	Blue Surf Resorts	Blue Surf Resorts Corporate Headquarters	8	0	0	20
A2Z Partner	ABC SubPartner	A2Z Partner -> ABC SubPartner	Blueridge Mountain Spas	Blueridge Mountain Spas Headquarters	1	0	0	0
A2Z Partner	ABC SubPartner	A2Z Partner -> ABC SubPartner	Blueridge General Stores	Blueridge General Stores	2	0	0	0

Showing 1 to 3 of 3 entries

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

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

Partner Transaction Summary



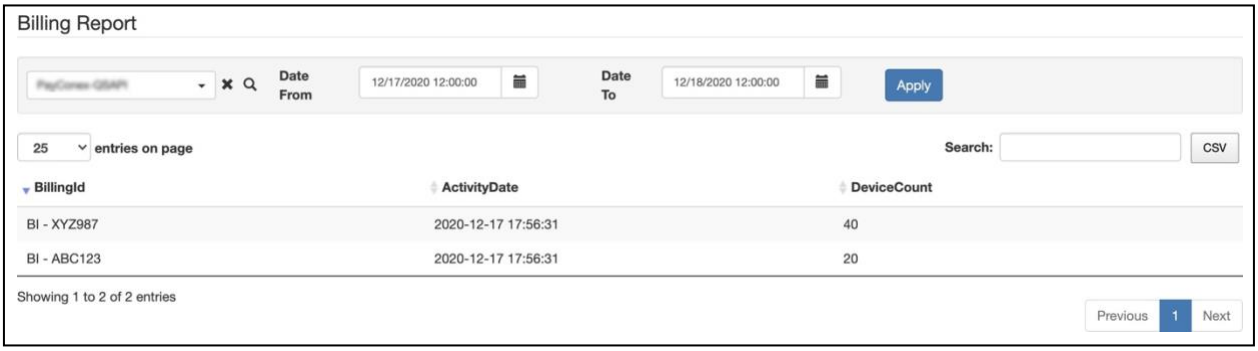
To generate this report do the following:

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

Optional: Download the report as a PDF or CSV.

Billing Report

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



To generate this report do the following:

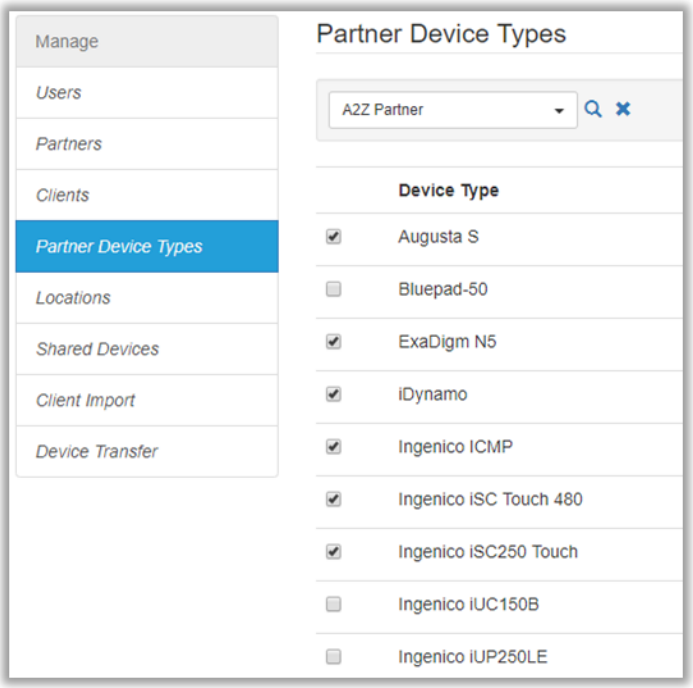
1. Select **Reports** > **Billing Report**.
2. In the header, select a **Partner** from the drop-down list.
3. In the header, specify a date range using the date pickers.
4. Click **Apply** when you're done.

Optional: Download the report as a CSV.

Managing Devices

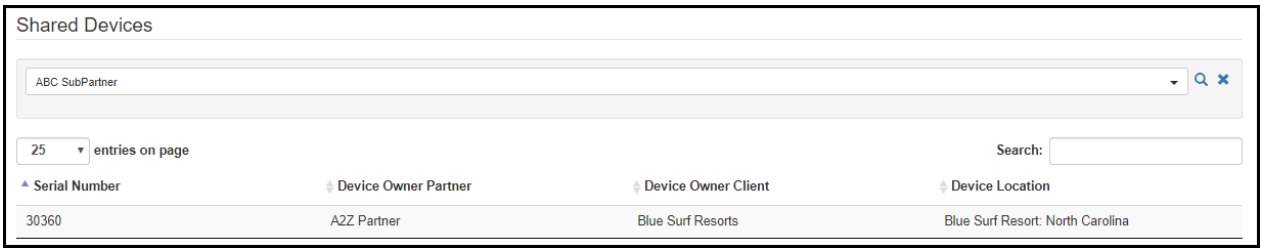
Partner Device Types

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



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

Shared Devices



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

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

Device Transfer

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

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

Single Sign-On (SSO)

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

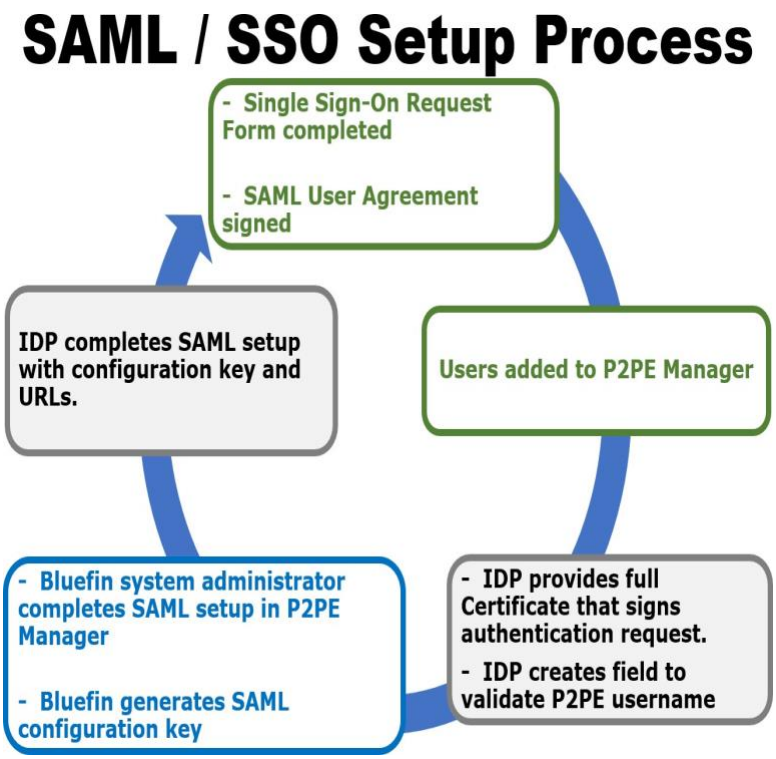
IMPORTANT: This feature is designed to support one Identity Provider and is implemented by System Users

Benefits

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

Setup Process

The following is an overview of the setup process.



1. Complete the ***Single Sign-On Request Form*** (see below for sample form) and the ***SAML User Agreement***. Involve your Identity Provider to gather the requested information and to create a field in the SSO system to validate P2PE Manager

usernames. **NOTE**: the Identity Provider will need to provide the entire X-509 Certificate.

2. Add users to P2PE Manager as usual. (Refer to Managing Users.htm for details.)
3. After Bluefin receives the requested information, our system administrators configure SAML in P2PE Manager. Then, the Single Sign-On Request form will be returned with the SAML Configuration key. (See below for a Sample IDP Setup and for information that Identity Providers need.)

Frequently Asked Questions

What is SAML?

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

Who establishes SAML / SSO in P2PE Manager?

Bluefin P2PE Manager system users configure SAML in P2PE Manager.

What are the SSO setup requirements?

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

What will I receive from Bluefin to establish SSO?

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

What does the Identity Provider need to do?

Identity Providers need to do the following:

- Provide the information requested in the Single Sign-On Request form. (See below for a sample of the form.)
- Create a field in the SSO system to validate P2PE Manager usernames.

- Configure system settings to enable the connection to P2PE Manager using the SAML configuration key from Bluefin.

How many Identity Providers are supported?

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

Information Identity Providers Need

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

- **Usernames**. (List of active P2PE Manager users.)

- **SAML Configuration Key** - This key is generated during the setup process after receipt of the ***Single Sign-On Request Form***.

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

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

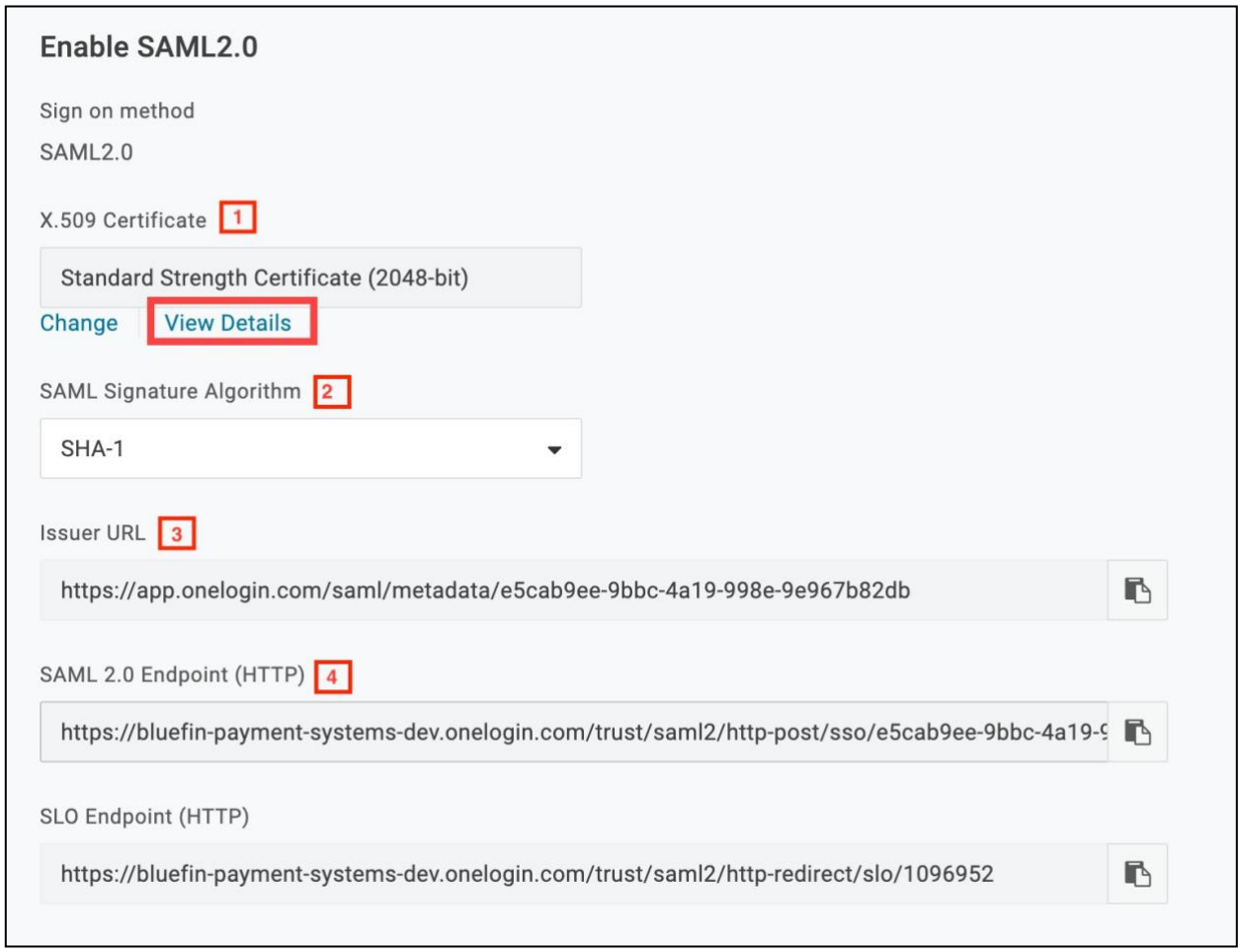
EXAMPLE:

```
https://cert-bluefin.p2pemanager.com/saml/callback/8d34e9b997087646912c13a02c5ae726
```

Sample IDP Setup

IDP Configuration

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

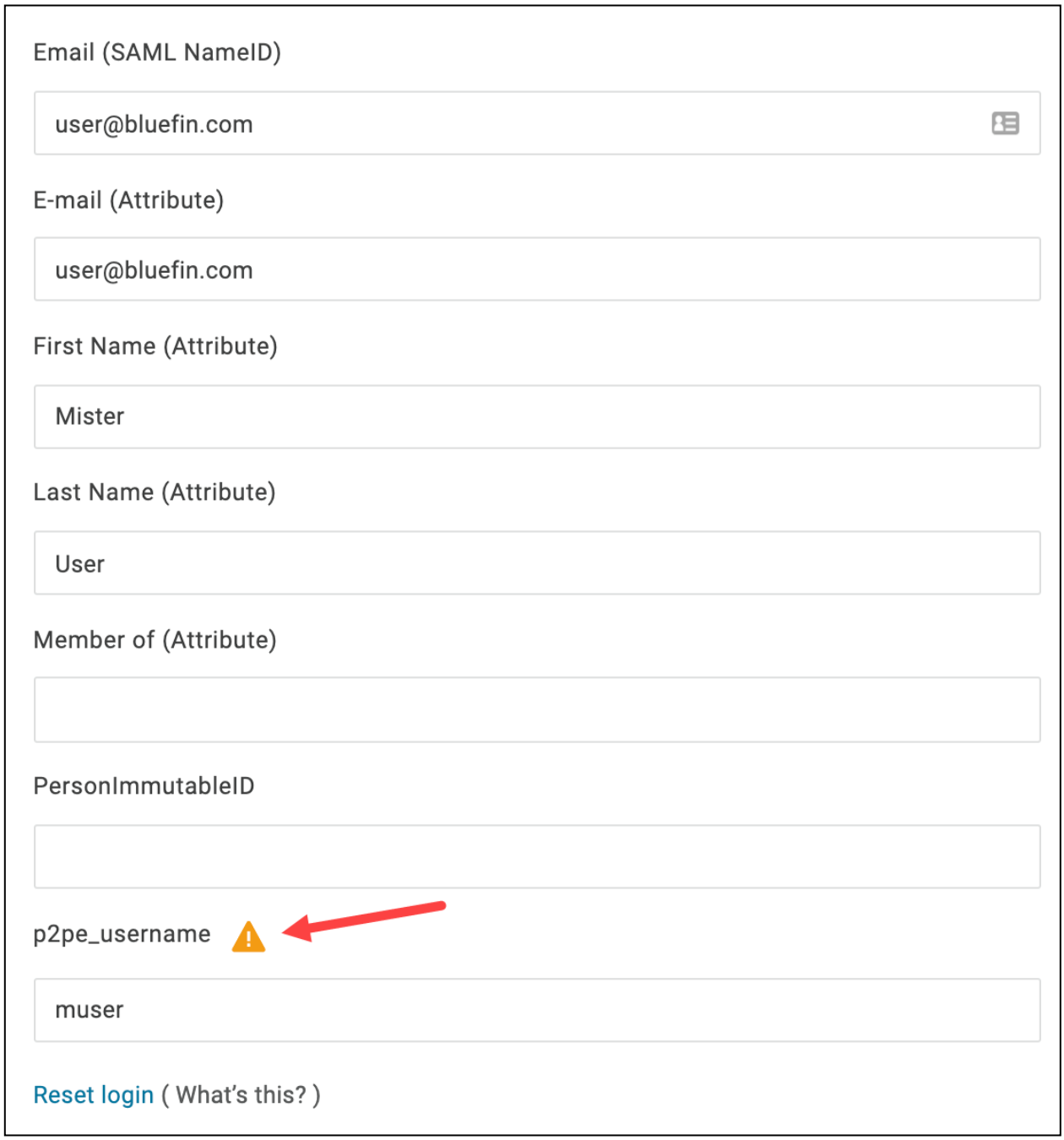


Field	Description
1. X. 509 Certificate	**IMPORTANT**: The value generated here needs to be communicated to Bluefin to setup the SSO connection. In this example, the actual certificate generated is inside the "View Details" link.
2. SAML Signature Algorithm	This setting contains the hash algorithm specified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

Field	Description
4. SAML Endpoint URL	**IMPORTANT**: The value here needs to be communicated to Bluefin to setup the SSO connection (SAML End Point) This URL should be the end point of the IDP being used.

IDP User Configuration

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



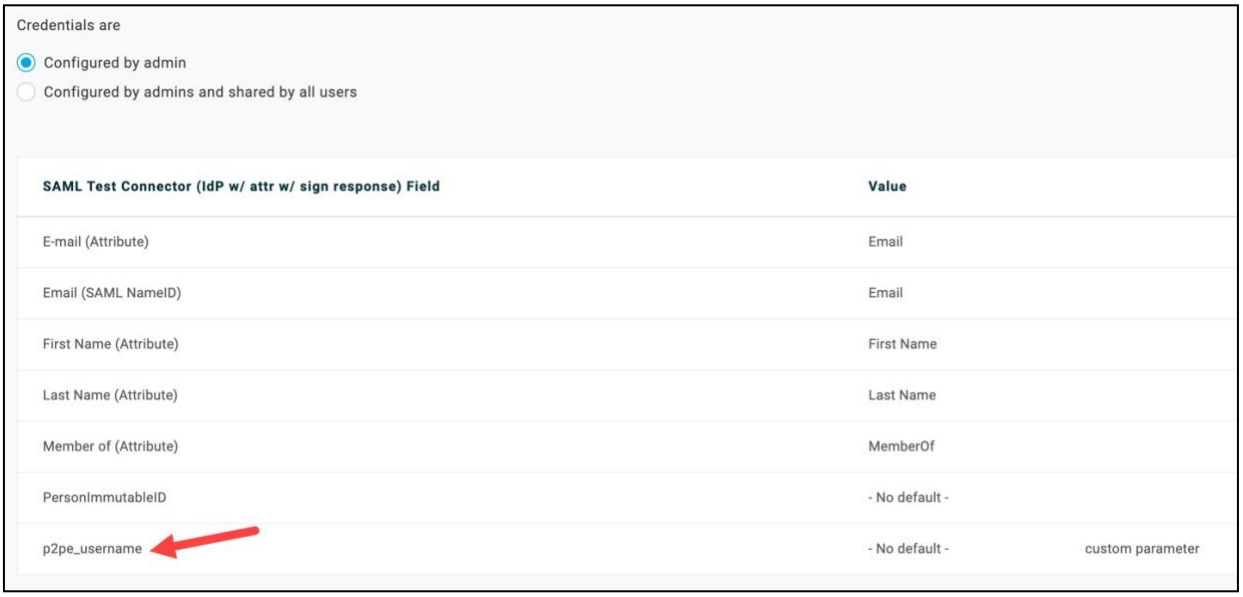
Basic demographic information about each user needs to be completed by the merchant in their IDP.

NOTE: The user login is the only field relevant to configuring SAML/SSO. In the example shown, the **p2pe_username** parameter was added specifically for the SAML/SSO configuration to P2PE Manager.

IMPORTANT: This field name (p2pe_username) needs to be communicated to Bluefin to setup the SSO connection (SAML Field Name) Bluefin does not need the value of this entry

("muser" in the example shown), but the value must match a User in the P2PE Manager who has access to this specific Partner/Client.

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

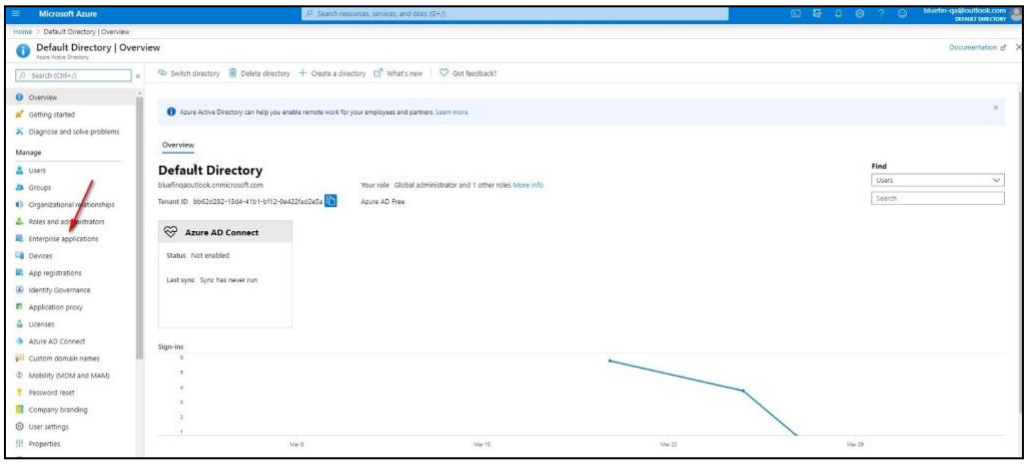


Azure Setup Overview

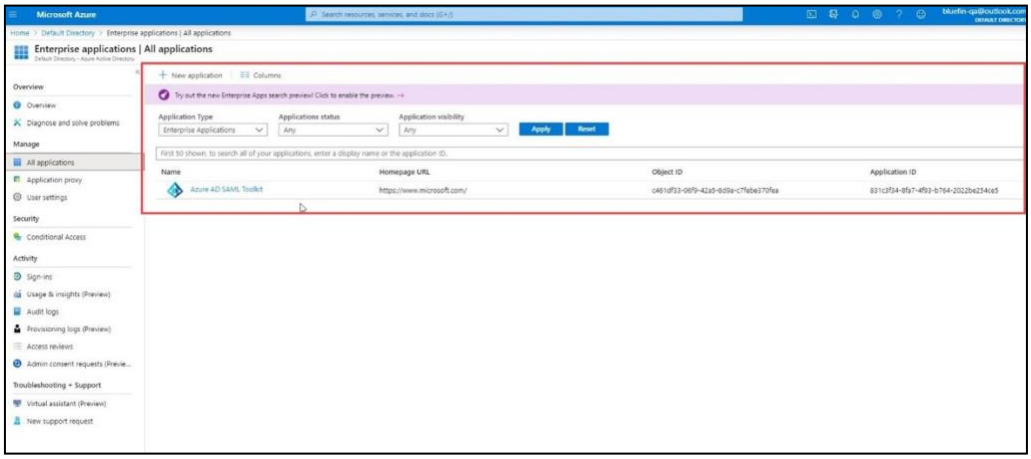
The following information is an overview of how to prepare Azure

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

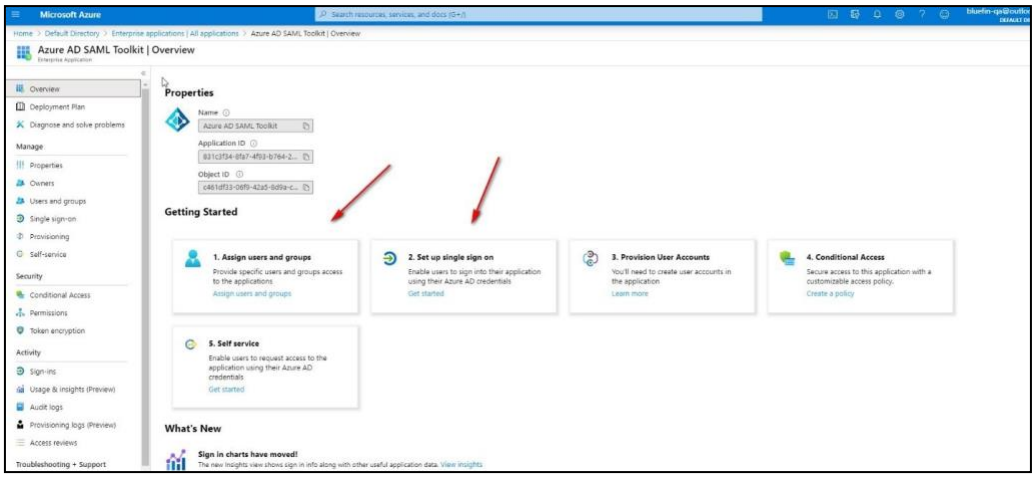
1. Log in to your Azure portal as usual and navigate to the **Azure Active Directory**.
2. In the left panel, select **Enterprise Applications**.



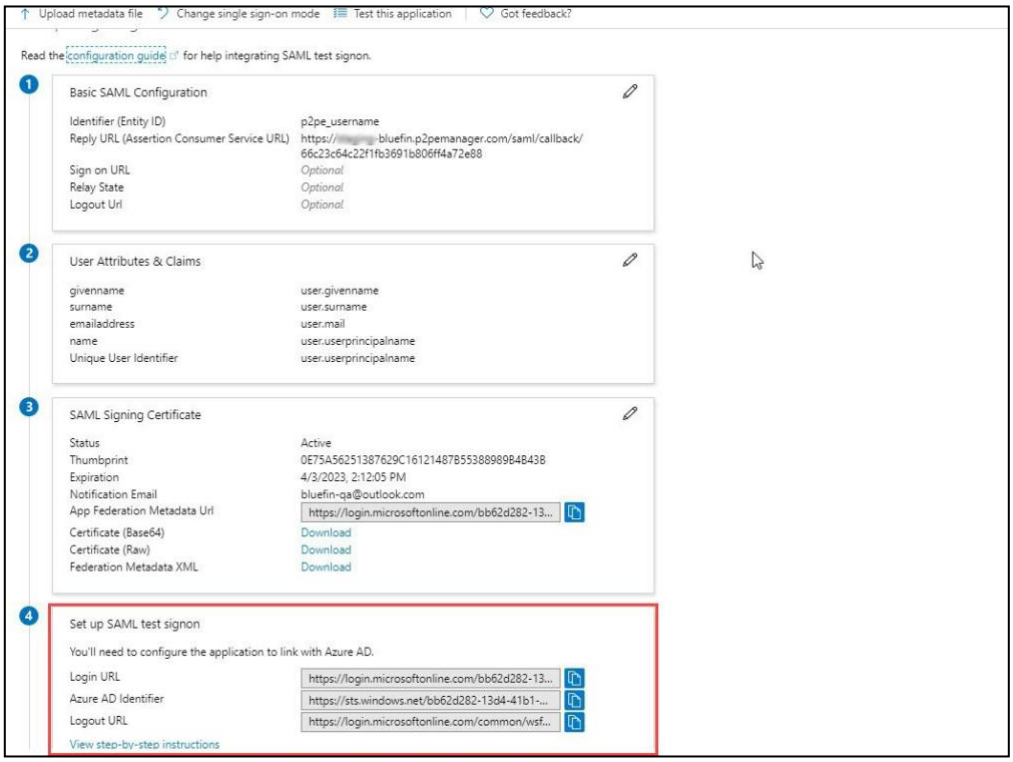
3. Create a new application or use an existing one.



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



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



Single Sign-On Request Form (Sample)

Do the following:

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

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

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

2.) SUBMITTER INFORMATION	
Submitted By	[Name of Person Submitting Change Request]
Submitter's Company	[Name of Submitter's Company]
Date Submitted	[mm/dd/yyyy]

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

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