

# Genius Smart P2PE™

## P2PE Instruction Manual

Public

Doc no: CO-PUB-0101

Version 1.6.1 – 17th April 2020

**CAYAN™**

The Payment Possibilities Company™



## Copyright notice

Copyright © 2020 Cayan LLC. All rights reserved.

No part of this publication may be reproduced, copied, manipulated, altered, or transmitted in any form or by any means, electronic or mechanical, including, without limitation, by photocopy, imaging, or recording, without the express prior written consent in each case of the copyright owner. The names, trademarks, logos, and service marks displayed in this publication will be protected by the owner to the fullest extent of the law, and any use without the express prior written permission of the trademark owner is strictly prohibited. The information contained in this publication is current when published; however, the publisher reserves the right to update and modify the specifications or other product information at any time without notice.



**Contents**

Copyright notice ..... 2

Contents ..... 3

1. P2PE Solution Information and Solution Provider Contact Details ..... 4

2. Approved POI Devices, Applications/Software, and the Merchant Inventory ..... 5

3. POI Device Installation Instructions ..... 9

4. POI Device Transit..... 31

5. POI Device Tamper Monitoring and Skimming Prevention ..... 32

6. Device Encryption Issues..... 44

7. POI Device Troubleshooting ..... 45

8. Additional Solution Provider Information ..... 48

9. Appendix: Checklist for Remote Key Injection..... 49

## 1. P2PE Solution Information and Solution Provider Contact Details

### 1.1 P2PE Solution Information

Solution name:	Genius Smart P2PE
Solution reference number per PCI SSC website:	2017.01037.001

### 1.2 Solution Provider Contact Information

Company name:	Cayan LLC
Company address:	1 Federal Street Second Floor Boston MA 02110
Company URL:	www.tsys.com
Contact name:	Contact Center Services
Contact phone number:	(1) (888) 249-3220
Contact e-mail address:	p2pe@cayan.com

#### P2PE and PCI DSS

Merchants using this P2PE Solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

## 2. Approved POI Devices, Applications/Software, and the Merchant Inventory

### 2.1 POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution.

**Note:** All POI device information can be verified by visiting:

[https://www.pcisecuritystandards.org/approved\\_companies\\_providers/approved\\_pin\\_transaction\\_security.php](https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php)

POI device vendor:	Verifone
POI device model name and number:	MX915: P132-40x-xx-xxx
Hardware version #(s):	3.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x
Firmware version #(s):	Vault: 1.x.x, 3.x.x, 4.x.x, 11.x.x, 12.x.x, AppM: 1.x.x; 3.x.x; 4.x.x; 5.x.x, 5A.x.x, 6.x.x, SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx, Vault: 13.x.x, AppM: 7.x.x, Vault: 17.x.x, AppM: 10.x.x, SRED: 7.x.x, OP: 7.x.x
PCI PTS Approval #(s):	4-10110

POI device vendor:	Verifone
POI device model name and number:	MX925: P132-50x-xx-xxx
Hardware version #(s):	3.x, Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x
Firmware version #(s):	Vault: 1.x.x, 3.x.x, 4.x.x, 11.x.x, 12.x.x, AppM: 1.x.x; 3.x.x; 4.x.x; 5.x.x, 5A.x.x, 6.x.x, SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx, Vault: 13.x.x, AppM: 7.x.x, Vault: 17.x.x, AppM: 10.x.x, SRED: 7.x.x, OP: 7.x.x
PCI PTS Approval #(s):	4-10110

POI device vendor:	Verifone
POI device model name and number:	MX915: P177-40x-xx-xxx
Hardware version #(s):	4.x
Firmware version #(s):	Vault: 12.x.x, AppM: 6.x.x, SRED: 4.x.x, OP: 7.x.x
PCI PTS Approval #(s):	4-10177

POI device vendor:	Verifone
POI device model name and number:	MX925: P177-50x-xx-xxx
Hardware version #(s):	4.x
Firmware version #(s):	Vault: 12.x.x, AppM: 6.x.x, SRED: 4.x.x, OP: 7.x.x
PCI PTS Approval #(s):	4-10177

POI device vendor:	BBPOS International Limited
POI device model name and number:	WSX2
Hardware version #(s):	WSX2XXX-XX-XXX (WSX2)
Firmware version #(s):	WSX1.002-08.x.xx.xx.xx.xx (WSX2)
PCI PTS Approval #(s):	4-10204

## 2.2 POI Software/application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution.

*Note that all applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.*

Application vendor, name and version #	POI device vendor	POI device model name(s) and number:	POI Device Hardware & Firmware Version #	Is application PCI listed? (Y/N)	Does application have access to clear-text account data (Y/N)
Cayan, Genius version 5.2.*.*	Verifone	MX915 P133-40x-xx-xxx MX925 P132-50x-xx-xxx	Hardware version: 3.x Vault: 14.x.x; AppM: 8.x.x; SRED: 7.x.x, Vault: 16.x.x; AppM: 10.x.x Vault: 1.x.x, 3.x.x, 4.x.x, 11.x.x, 12.x.x, AppM: 1.x.x; 3.x.x; 4.x.x; 5.x.x, 5A.x.x, 6.x.x, SRED: 1.x.x, 3.x.x; 4.x.x; 5.x.x, OP: 1.x.x, 3.x.x; 4.x.x; 7.x.x, SRED 5.x.x.xxx, Vault: 13.x.x, AppM: 7.x.x, Vault: 17.x.x, AppM: 10.x.x, SRED: 7.x.x, OP: 7.x.x	Y	Y
Cayan, Genius version 5.2.*.*	Verifone	MX915 P177-40x-xx-xxx MX925 P177-50x-xx-xxx	Hardware version: 4.x Vault: 12.x.x, AppM: 6.x.x, SRED: 4.x.x, OP: 7.x.x	Y	Y

## 2.3 POI Inventory & Monitoring

- All POI devices, must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted POI devices, must be reported to Cayan via the contact information in Section 1.2.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

You must maintain an inventory of all your P2PE devices, and include at least the following information about each device:

- Make and model
- Location
- Status
  - Awaiting deployment
  - Deployed
  - Not in use
  - Awaiting replacement
- Serial number



**Important:** You must use only PCI-approved P2PE devices to process transactions. If you process any transactions using devices that are not P2PE validated, you are no longer considered P2PE compliant.

**Sample Inventory Table**

Device vendor	Device model name(s) and number:	Device location	Device status	Serial number or other unique identifier



### 3. POI Device Installation Instructions

#### **Do not connect non-approved cardholder data capture devices.**

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in table 2.1 are allowed for cardholder data capture.

If a merchant's PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

- The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.
- Only P2PE approved capture mechanisms as designated on PCI's list of Validated P2PE Solutions and in the PIM can be used.

#### **Do not change or attempt to change device configurations or settings.**

**Changing or attempting to change device configurations or settings will invalidate the PCI-approved P2PE solution in its entirety.** Examples include, but are not limited to:

- Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device
- Attempting to alter security configurations or authentication controls
- Physically opening the device
- Attempting to install applications onto the device

## 3.1 Installation and connection instructions

### 3.1.1 Getting started

#### 3.1.1.1 Genius Countertop devices

To use Genius Smart P2PE, you can either purchase new devices from us or we can remotely inject keys into your existing devices. To use existing devices, they must be version 3.0 or version 4.0 of Verifone's hardware and be listed as PCI approved PTS devices.

##### *Existing devices*

To use existing devices:

- Complete "Appendix: Checklist for Remote Key Injection" on page 49 and send it to [P2PERequests@cayan.com](mailto:P2PERequests@cayan.com)
- After we remotely inject keys into your devices, complete "Verifying that the Genius device is ready" on page 13 to page 14 and "Testing a transaction" on page 15.
- All other sections of the PIM apply when you are using existing devices, except for section 5.3 on page 40 to page 43.

#### 3.1.1.2 Genius Handheld devices

To use Genius Smart P2PE, you must purchase Handheld devices from us.

## 3.1 Installation and connection instructions

### 3.1.2 New Genius Countertop devices

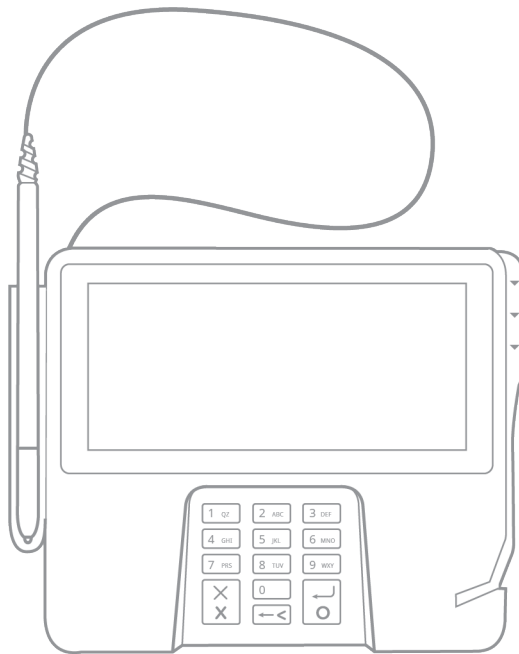
Before you install your Genius device, complete the following tasks:

- Locate your Merchantware credentials. We sent your credentials in an email that had a subject line with the words "Merchantware Credentials".
- Check that your Internet connection is functioning correctly, and that there is an available network port on your router or switch.

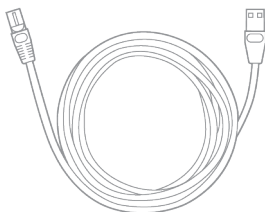
**Note:** A video tutorial is available at

<https://help.tsys.com/support/solutions/articles/33000233395-setting-up-your-genius-device-using-the-multiport-cable>

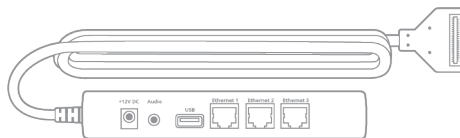
#### 3.1.2.1 Genius Countertop components



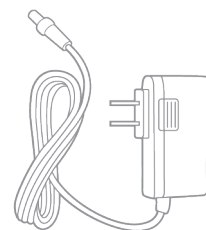
*Genius Countertop device*



*Ethernet cable*



*Multiport cable*

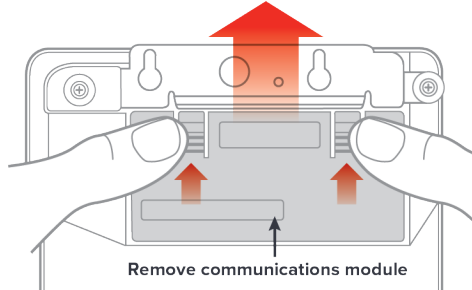


*AC adapter*

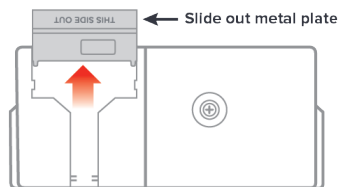
## 3.1 Installation and connection instructions

### 3.1.2.2 Connecting the communications module

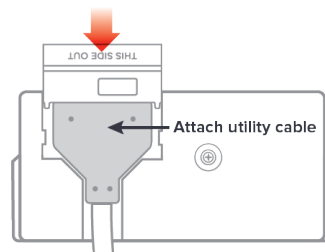
1. Turn the Genius device upside-down and place it on a flat, stable surface. Firmly press the flexible tabs and push up to remove the communications module.



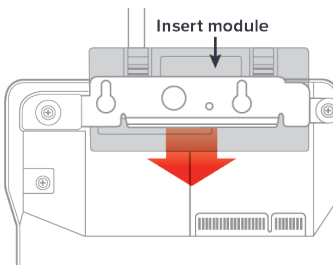
2. Hold the module securely in your hands and slide the metal plate out.



3. Attach the multiport cable connector as shown and slide out the metal plate back into place.



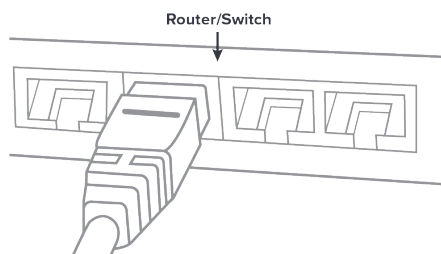
4. Insert the communications module into the Genius device.



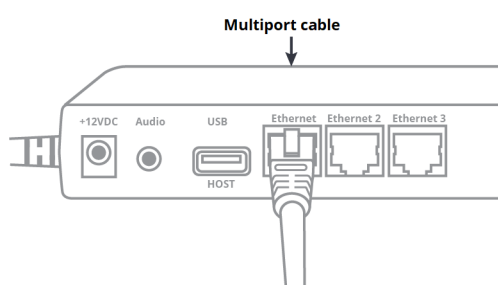
## 3.1 Installation and connection instructions

### 3.1.2.3 Connecting to the network

1. Connect one end of your Ethernet cable to an available port on your router or switch.

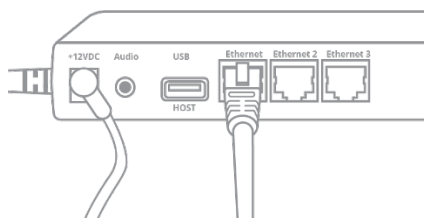


2. Connect the other end of the Ethernet cable to the Ethernet port on the multiport cable.



### 3.1.2.4 Powering the Genius Countertop device

1. Check that the communications module is firmly in place on the Genius device.
2. Connect the AC adapter to the +12V connection on the multiport cable and plug the adapter into a power socket.



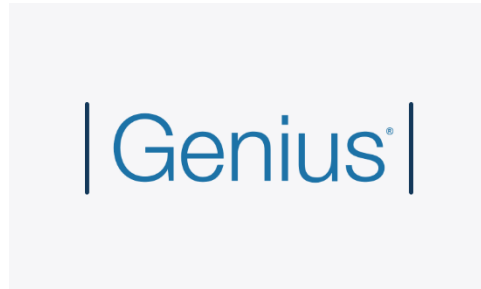
## 3.1 Installation and connection instructions

### 3.1.2.5 Verifying that the Genius Countertop device is ready to use



**Important:** We have configured the Genius Countertop device to receive an IP Address from a Dynamic Host Configuration Protocol (DHCP) server by default. If you need to configure a Static IP address, please see “Setting a static IP address” on page 15.

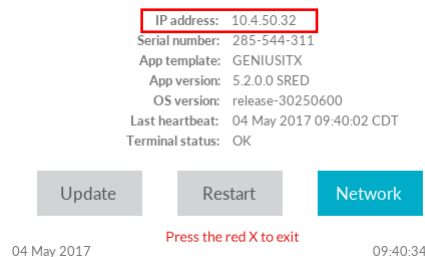
1. When Genius is displaying the splash screen, press **0** on the keypad three times.



2. Using the keypad type the password, then press **Enter** (green button). The default password is **9416557**.



3. Confirm that the **IP Address** field is populated. Take a note of the address for use with your POS.



## 3.1 Installation and connection instructions

- Confirm that Secure Reading and Exchange of Data (SRED) is enabled on your device by checking that the **App version** shows **SRED**.

IP address: 10.4.50.32  
 Serial number: 285-544-311  
 App template: GENIUSITX  
 App version: 5.2.0.1 **SRED**  
 OS version: release-30250600  
 Last heartbeat: 04 May 2017 09:40:02 CDT  
 Terminal status: OK

Update

Restart

Network

04 May 2017

Press the red X to exit

09:40:34



**Important:** If your device does not show **SRED**, do **NOT** use the device. Contact our Customer Support Team at **(1) (888) 249-3220**.

- Tap **Network**, then tap **Test**.

IP Mode: DHCP  
 IP Address: 10.4.50.211  
 Netmask: 255.255.254.0  
 Gateway: 10.4.50.1  
 DNS1: 10.4.20.10  
 DNS2: 10.4.20.20

Back

Configure

Test

Press the red X to exit

- Confirm that the **Gateway Connection Test** passed.

### GATEWAY CONNECTION TEST

Passed

Transport: Passed  
 Genius: Passed  
 SFTP: Passed

Test again

Done

Press the red X to exit

- Tap **Done**.
- On the keypad, press the **X** button to exit and return to the Splash screen.



**Note:** If the **Gateway connection test** fails, check your Internet connection or contact our Customer Support Team at **(1) (888) 249-3220**.

### 3.1.2.6 Configuring your POS

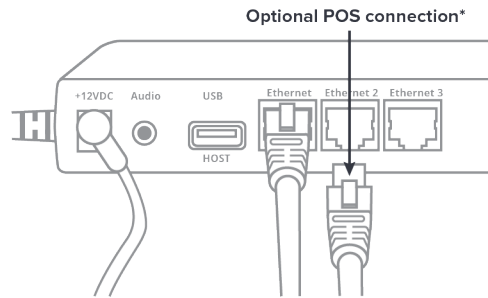
- Find your Merchantware credentials.
- Consult with your POS provider for help with configuring your POS system with the Genius Countertop device.

## 3.1 Installation and connection instructions

3. Configure your POS with the **IP Address** of your Genius Countertop device, your **Merchantware Name**, **SiteID**, and **Key**.



**Note:** If you do not have access to a free port on your router or switch, you can plug the Ethernet cable from your POS directly into one of the Ethernet ports on the Genius multiport cable.



### 3.1.2.7 Testing a transaction

We recommend that you run a test transaction on your POS to check that you have correctly configured it with your Genius Countertop device.

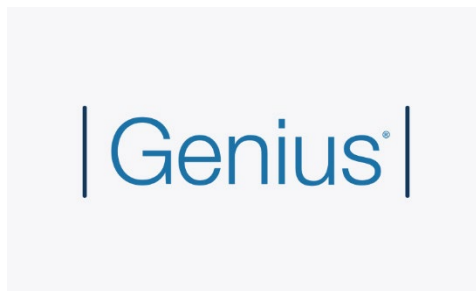
- If the test transaction transfers successfully to the Genius Countertop device, you do not need to configure anything else. Cancel the transaction on your POS and start processing live sales.
- If the test transaction is unsuccessful, call our Customer Support Team at **(1) (888) 249-3220**.

### 3.1.2.8 Setting a static IP address (optional)

This is an optional procedure that you should complete only if your network requires that you set a static IP address on your device.

You can set a static IP address on your Genius Countertop device using the **Admin** menu.

1. When Genius is displaying the splash screen, press **0** on the keypad three times.



2. Using the keypad type the password, then press **Enter** (green button). The default password is **9416557**.

## 3.1 Installation and connection instructions



### 3. Navigate to the Network Configuration menu:

- a. Tap **Network**.
- b. Tap **Configure**.
- c. Tap **Static**.

Select Static

IP Mode: ☒ Static ☐ DHCP

IP Address: 010.004.050.067

Netmask: 255.255.254.000

Gateway: 010.004.050.001

DNS1: 010.200.200.235

DNS2: 010.200.200.235

Cancel Save

### 4. To change any of the network settings:

- a. Tap the information field of the setting that you want to change. For example, to change the device's IP address, tap the **IP Address** field.

IP Mode: ☒ Static ☐ DHCP

IP Address: 010.004.050.067

Netmask: 255.255.254.000

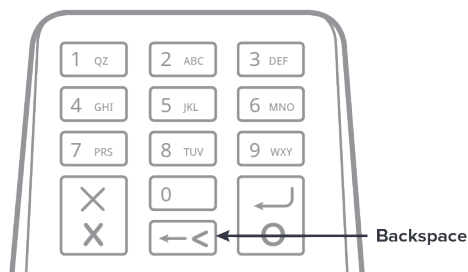
Gateway: 010.004.050.001

DNS1: 010.200.200.235

DNS2: 010.200.200.235

Cancel Save

- b. To remove the current information, press the **Backspace** key on the keypad.



- c. Using the keypad, type the static IP settings provided by your network administrator.



## 3.1 Installation and connection instructions

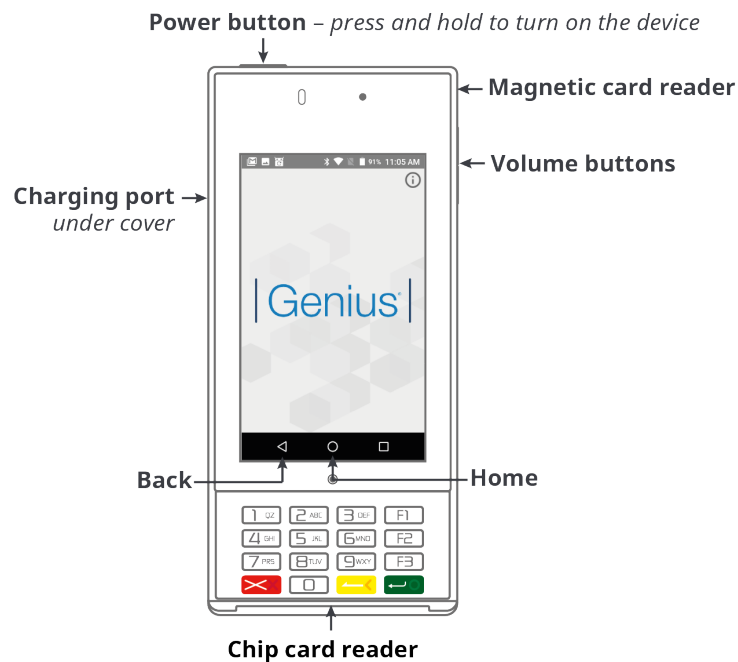
- d. To change the other network settings, repeat steps a to c.
5. Tap **Save**.
6. On the keypad, press the **X** button to exit and return to the splash screen.

### 3.1.3 Genius Handheld devices

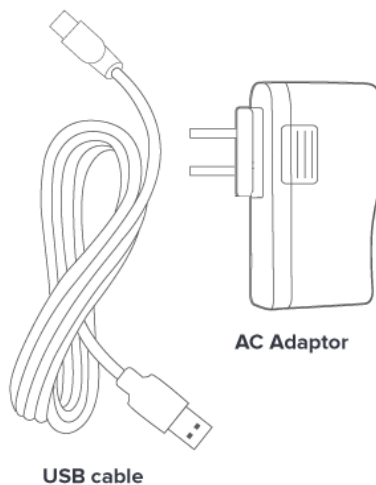
Before you use your Genius Handheld device, complete the following tasks:

- Locate your Merchantware credentials. We sent your credentials in an email that had a subject line with the words "Merchantware Credentials".
- Check that your wireless router is connected to the internet and is functioning correctly, and that you have your wireless network name and password ready.

#### 3.1.3.1 Genius Handheld components



**Genius Handheld device**

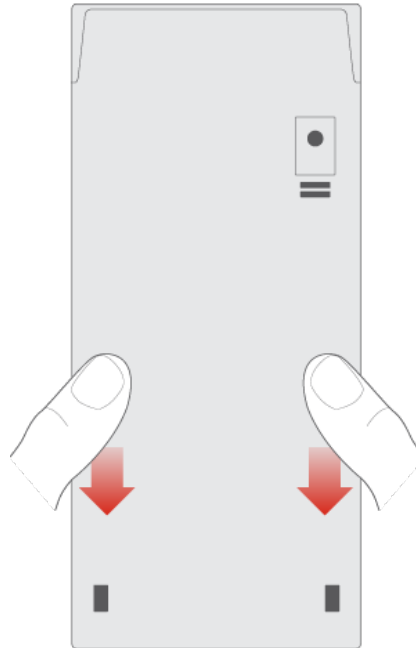


## 3.1 Installation and connection instructions

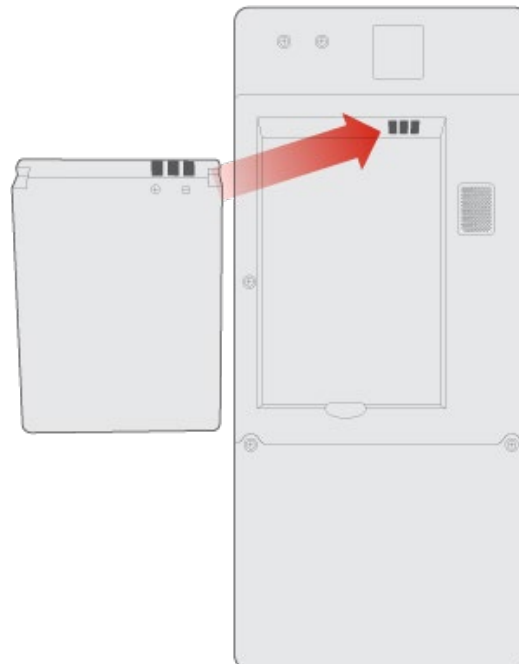
### 3.1.3.2 Fitting the battery

Before you use the battery in the device:

- Check that the surface of the battery is clean.
  - If the battery terminals are dirty, rub them with a clean, dry cloth.
1. Remove the rear battery cover by sliding it down until you hear a click, then lifting it off.

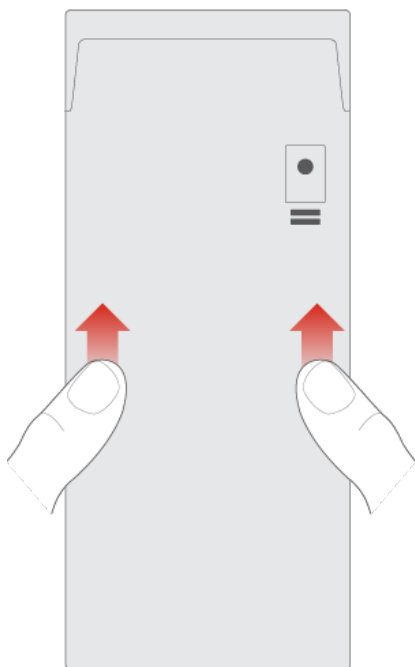


2. Insert the new battery by aligning the three gold contacts on the top of the battery with the contacts on the device. Press down on the battery until you hear a click.



## 3.1 Installation and connection instructions

3. Replace the rear battery cover and slide it up until you hear a click. Check that the cover is secure before charging and turning on the device.



### 3.1.3.3 Turning on the Genius Handheld device

- Press and hold the **Power** button to turn on the device.

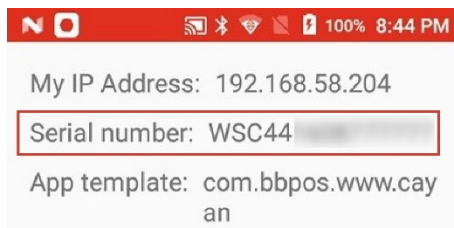
### 3.1.3.4 Checking the serial number and firmware version

1. Tap **O**, then open the Genius app.
2. Tap **i** to open the Admin screen.



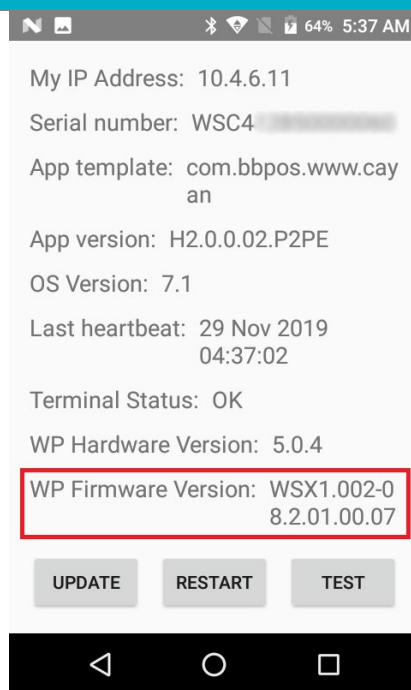
Tap to open the Admin screen


3. Confirm that the **Serial number** matches the serial number printed on the rear of the Genius Handheld device.



4. Confirm that the **WP Firmware Version** is **WSX1.002-08.x.xx.xx.xx**.

## 3.1 Installation and connection instructions



5. Tap  to return to the **Genius app** screen.





**Important:** If the serial number or WP Firmware version is not correct, **do not** use the Genius Handheld device and call our Customer Support Team at **(1) (888) 249-3220**.

## 3.1 Installation and connection instructions

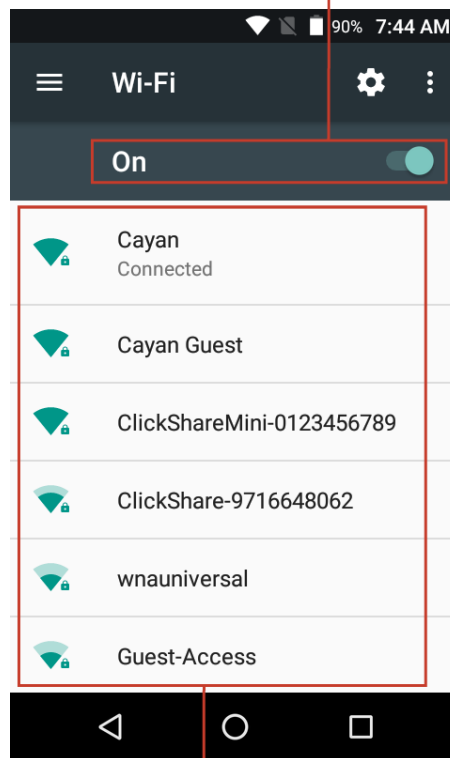
### 3.1.3.5 Connecting to the network



**Important:** We have configured the Genius Handheld device to receive an IP Address from a Dynamic Host Configuration Protocol (DHCP) server by default. If you need to configure a Static IP address, see "Setting a static IP address" on page 23.

1. On the **Home** screen, tap .
2. Tap **Settings** , then tap **Wi-Fi**.
3. Ensure **Wi-Fi** is turned on and select your wireless network.

Ensure Wi-Fi is on



Select your wireless network

4. Type your wireless network **password**, then tap **Connect**.



**Note:** If your wireless network requires a user name and password, enter your user name and swipe up to access the **Password** field.

## 3.1 Installation and connection instructions

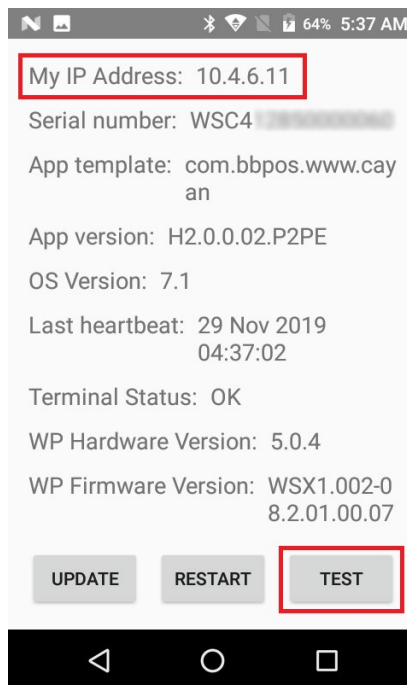
### 3.1.3.6 Verifying that the Genius Handheld device is ready

1. Tap **O**, then open the Genius app.
2. Tap **i** to open the Admin screen.

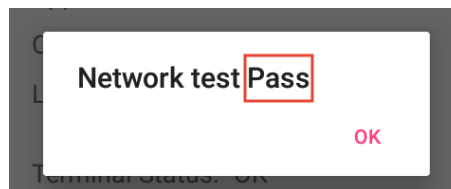


Tap to open the Admin screen

3. Confirm that the **IP address** field is populated. Take a note of the address for use with your POS system.
4. Tap **Test** to run the **Network** test.



5. **Confirm** that the **Network Test** says **Pass**, then tap **OK**.



6. Tap **<** to return to the **Genius app** screen.

## 3.1 Installation and connection instructions

### 3.1.3.7 Testing a transaction



**Important:** Keep the Genius app open when you are processing transactions.





We recommend that you run a test transaction on your POS to check that you have correctly configured it with the Genius Handheld device.

- If the test transaction transfers successfully to the Genius Handheld device, you do not need to configure anything else. Cancel the transaction on your POS and start processing live sales.
- If the test transaction is unsuccessful, please call our Customer Support Team at **(1) (888) 249-3220**.

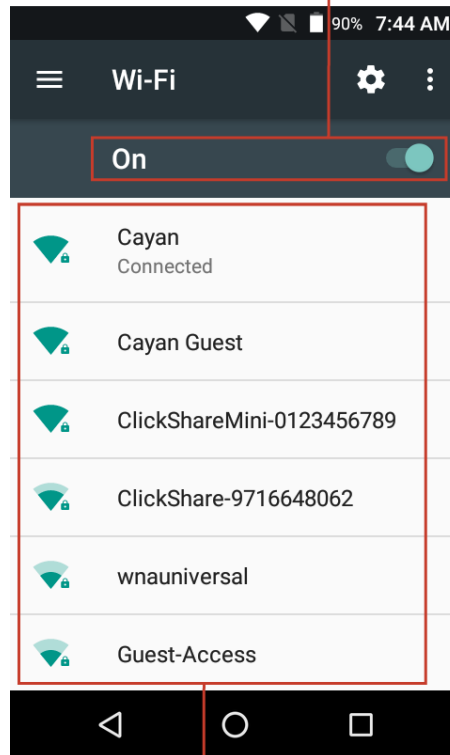
### 3.1.3.8 Setting a static IP address (optional)

Make sure you have your IP address, Network prefix length, Gateway, DNS1, and DNS2 from your network administrator for your Genius Handheld device to connect to your wireless network.

1. On the **Home** screen, tap .
2. Tap **Settings** , then **Wi-Fi**.
3. Ensure **Wi-Fi** is turned on, then press and hold your wireless network.

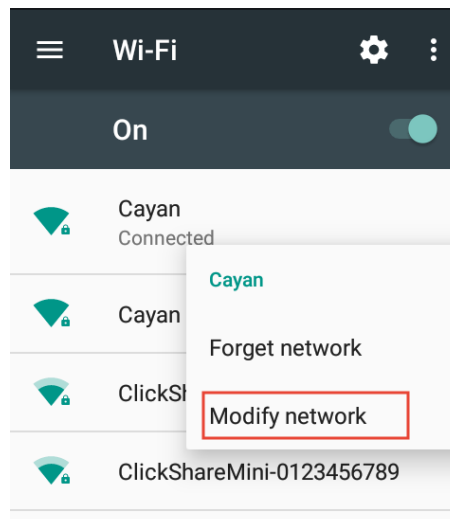
## 3.1 Installation and connection instructions

Ensure Wi-Fi is on



Select your wireless network

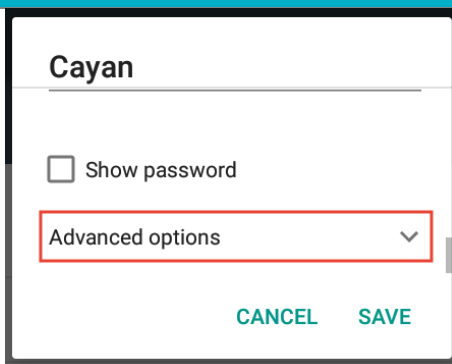
4. Tap **Modify network**.



5. From the **Advanced options** drop-down menu, change the IP settings to **Static**.



## 3.1 Installation and connection instructions



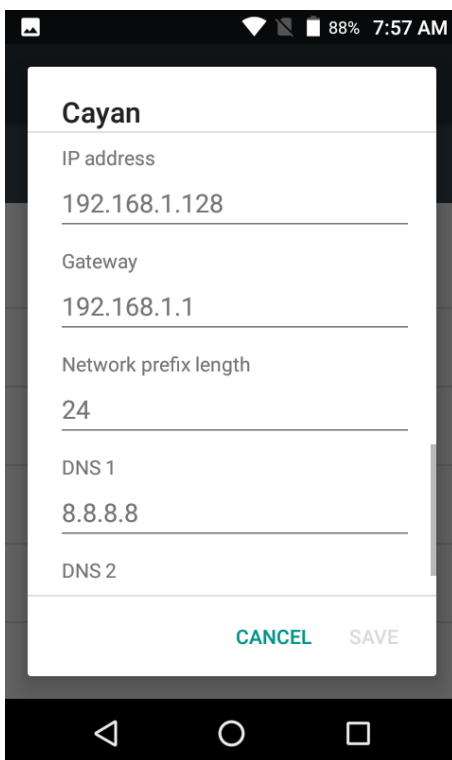
Cayan

☐ Show password

Advanced options ▼

CANCEL SAVE

6. Type your **IP address**, **Gateway**, **Network prefix length**, and **DNS** settings.



Cayan

IP address  
192.168.1.128

Gateway  
192.168.1.1

Network prefix length  
24

DNS 1  
8.8.8.8

DNS 2

CANCEL SAVE

7. Tap **Save**.

**Note:** Only PCI-approved POI devices listed in the PIM are allowed for use in the P2PE solution for account data capture.

### Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

## 3.2 Guidance for selecting appropriate locations for deployed devices

You must install your device in a secure location to reduce the risk of criminals targeting the device for skimming. We recommend that you consider the following when selecting installation locations:

- Control public access to the device, so that people have access only to the parts of the device that they need to complete a transaction. For example, PIN pad and card reader.
- Locate the device where authorized personnel can easily observe and monitor it, for example during daily checks by store or security staff.
- Locate the device in a secure environment that deters compromise attempts, including, but not limited to:
  - Visible security measures
  - Video surveillance
  - Adequate lighting
  - Access paths
- Physically secure the device so that criminals cannot easily remove it. For example, when using Genius Countertop devices, install them on the stand that we provide or when using Genius Handheld devices, store them in a lockable area when they are not in use.
- Enforce operational security processes to make sure that members of staff or security regularly inspect the device.

## 3.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

### 3.3.1 Genius Countertop devices

You must physically secure a deployed device to prevent unauthorized removal or substitution. For example, install the device securely on the stand that we provide.

This includes devices that you use for attended and unattended services, as applicable to the P2PE solution. For example, kiosks, pay-at-the-pump, etc.

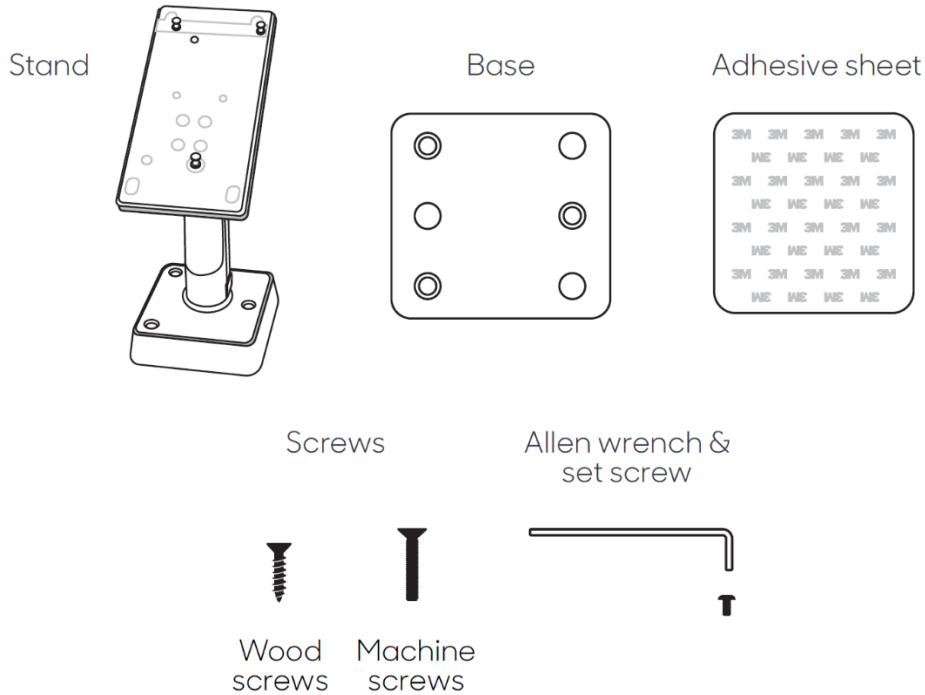
You must prevent unauthorized access to devices awaiting replacement while in your possession.



**Important:** If your device develops a fault, we arrange for you to return the device to us, and we ship a replacement device to you. We do not repair deployed devices; therefore, you should **NOT** grant access to any person that claims to be repair or support personnel.

## 3.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

### 3.3.1.2 Genius stand assembly parts



There are two options for setting up the stand:

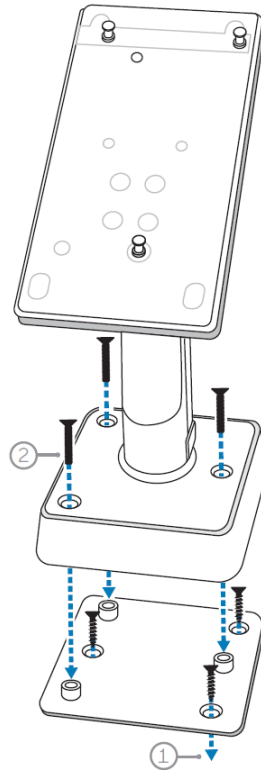
- Attached to the counter with screws
- Attached to the counter with adhesive label



**Note:** Attaching your stand to the counter with screws is the most secure solution.

## 3.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

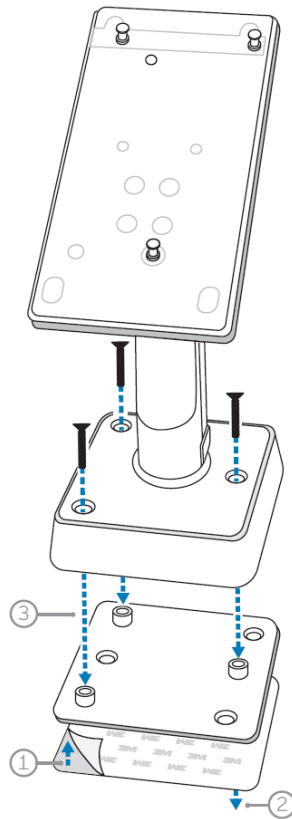
### 3.3.1.3 Attaching a stand to the counter with screws



1. Use the three self-tapping wood screws to secure the base to the counter.
2. Align the holes on the stand with the holes on the base and use the machine screws to attach the stand to the base.

## 3.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

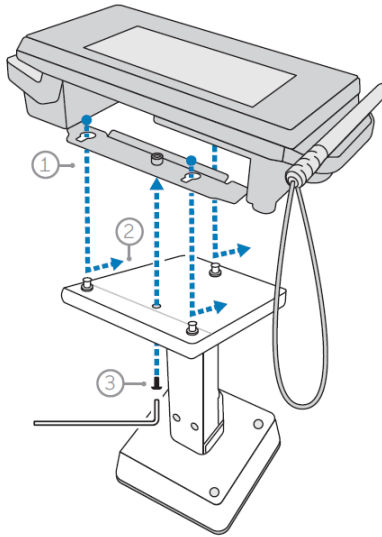
### 3.3.1.4 Attaching a stand to the counter with the adhesive sheet



1. Remove the backing from one side of the adhesive sheet and stick it to the bottom of the base.
2. Remove the backing from the other side of the adhesive sheet and secure the base to the counter.
3. Align the holes on the stand with the holes on the base and use the machine screws to attach the stand to the base.

## 3.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

### 3.3.1.5 Attaching your Genius device to the stand



1. Align the mounting holes on the bottom of the device with the pins on the stand.
2. Press the terminal firmly onto the stand and slide it down until you hear a click.
3. Use the Allen wrench to secure the terminal to the stand with the set screw.

### 3.3.1.6 Genius Handheld devices

You must ensure that when your Genius Handheld devices are in use, they are kept under the supervision of authorized employees. Whenever possible, your authorized employees should remain in possession of the device. If a cardholder needs to directly interact with the device, we recommend your authorized employees do the following:

- Remain with the cardholder during the interaction
- Keep the device in their sight
- Visually inspect the device after a cardholder interaction, they should ensure the cardholder has not:
  - Opened the device
  - Interfered with the card readers
  - Substituted the device for another

As Genius Handheld devices do not have any physical fasteners, you should have a lockable area where authorized employees store the devices when not in use. Authorized employees should sign out devices when they need them and sign in devices when returning them for storage. The lockable area should be in view of a camera system to ensure any unauthorized access to the devices is captured.

You should also enforce operational security processes to make sure that members of staff or security regularly inspect the device.

## 4. POI Device Transit

### 4.1 Instructions for securing POI devices intended for, and during, transit

Anytime you transport devices between locations, you must:

- Pack the devices in tamper-evident packaging before transit. For example, using tamper-evident bags, tamper seals, or security tape.
- Ship devices using a trusted, trackable courier or shipping company.
- Notify the company or site that you are shipping the devices to, including package tracking details and tamper-seal serial numbers.

### 4.2 Instructions for ensuring POI devices originate from, and are only shipped to, trusted sites/locations

Transport devices to and from trusted locations only. To help manage this process, you must:

- Maintain a list of trusted sites that you may accept devices from and send them to.
- Use only devices that you receive from trusted sites.

If you receive a device from an unknown or untrusted location:

- Do not use the device until you verify that the source is trusted.
- Contact us at **(1) (888) 249-3220** to verify that the device is authorized for use with your P2PE solution.

#### 4.2.1 Cayan's trusted locations

We ship devices from one of two secure facilities:

- POS Portal, 1627 Main Ave, Sacramento, CA 95838
- POS Portal, 1920 Watterson Trail # A, Louisville, KY 40299

## 5. POI Device Tamper Monitoring and Skimming Prevention

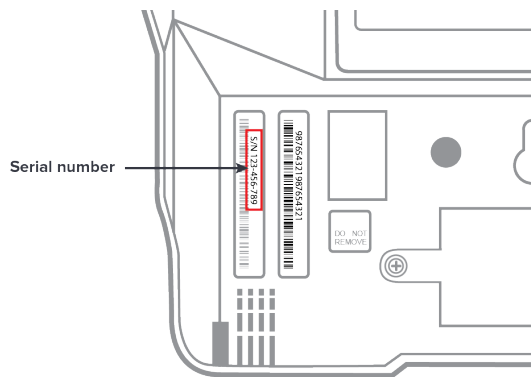
### 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

Additional guidance for skimming prevention on POI terminals can be found in the document entitled “Skimming Prevention: Best Practices for Merchants”, available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

#### 5.1.1 Before deploying a device

**Note:** When using devices that we have remotely injected with keys, skip to “After deploying a device” on page 35 to page 39. All other sections of the PIM apply when using existing devices, except for section 5.3 on page 40 to page 43.

- Keep your device in its tamper-evident bag and store it securely until immediately before deployment.
- Check that the serial number of the device matches the serial number printed on the packing slip.
- The serial number of the Genius device is located on the back of the device.



*Genius Countertop device*



*Genius Handheld device*

- The corresponding serial number is printed in the rightmost column of the packing slip.



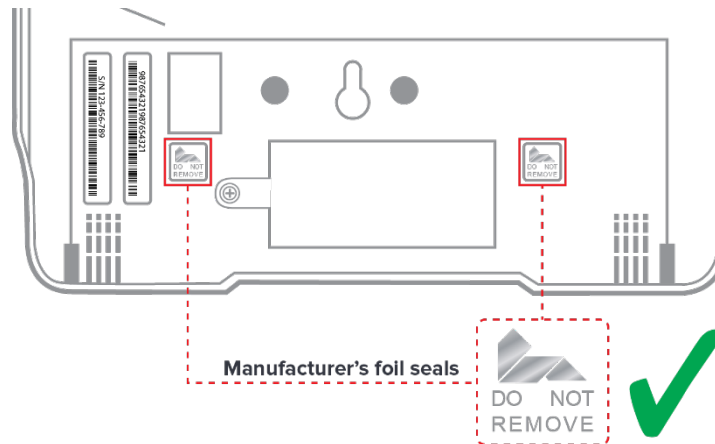
## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

Order No. **1234567**  
 Ordered On: 01/01/2017 10:00 AM  
 MID: 123456789  
 DBA: Cayan LLC

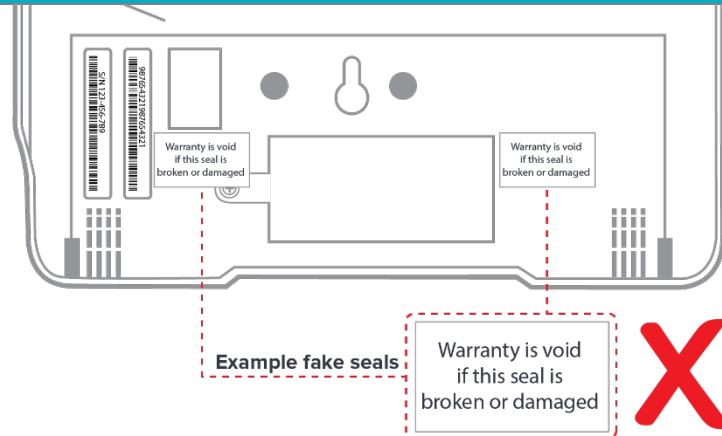
Ship Method: FedEx Ground Service

SHIP TO				
Company Name				
Contact Name				
Address 1				
Address 2				
Phone: 123456789				
	Quantity			
	Lot	Ordered	Shipped	
ew	Ea.	1	1	123-456-789 ← Serial number

- Record the device in your inventory.
- Inspect the device:
  - For Genius Countertop devices, inspect the device to make sure that the foil seals covering the screws are intact and have not been replaced with non-manufacturer seals.



## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity



**Note:** The Genius Countertop device has two foil seals covering two of the screws on the back of the device. Take note of what the seals look like and check them as part of your regular device inspections.

- For Genius Handheld devices, inspect the devices for any signs of attempts to open them. Check for puncture marks, prize marks, and damage to the screws that are under the battery cover.
- Weigh your device when you first receive it and check the weight of the device as part of your regular device inspections.
  - MX915 weight as specified by Verifone: 0.6 kg
  - MX925 weight as specified by Verifone: 0.9 kg
  - WS2 weight as specified by BBPOS International Ltd:
    - Excluding battery: 0.185 kg
    - Including battery: 0.235 kg
- Inspect the device before deployment to verify that the device has not been tampered with. If you notice anything suspicious, do not use the device, and immediately report your suspicions to our Customer Support Team at **(1) (888) 249-3220**.

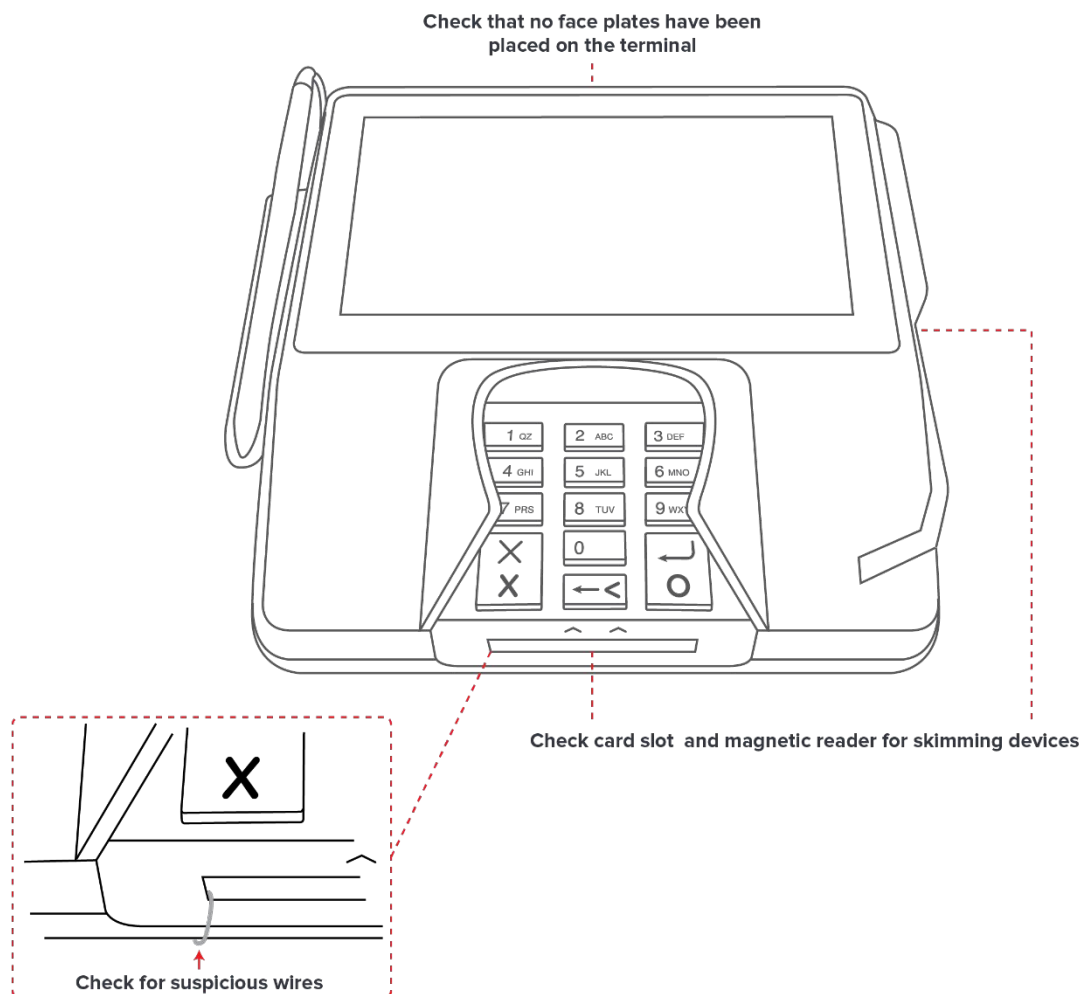
## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

### 5.1.2 After deploying a device

Check that the device meets the security standards described by the manufacturer. You can download the manufacturer's security standards from

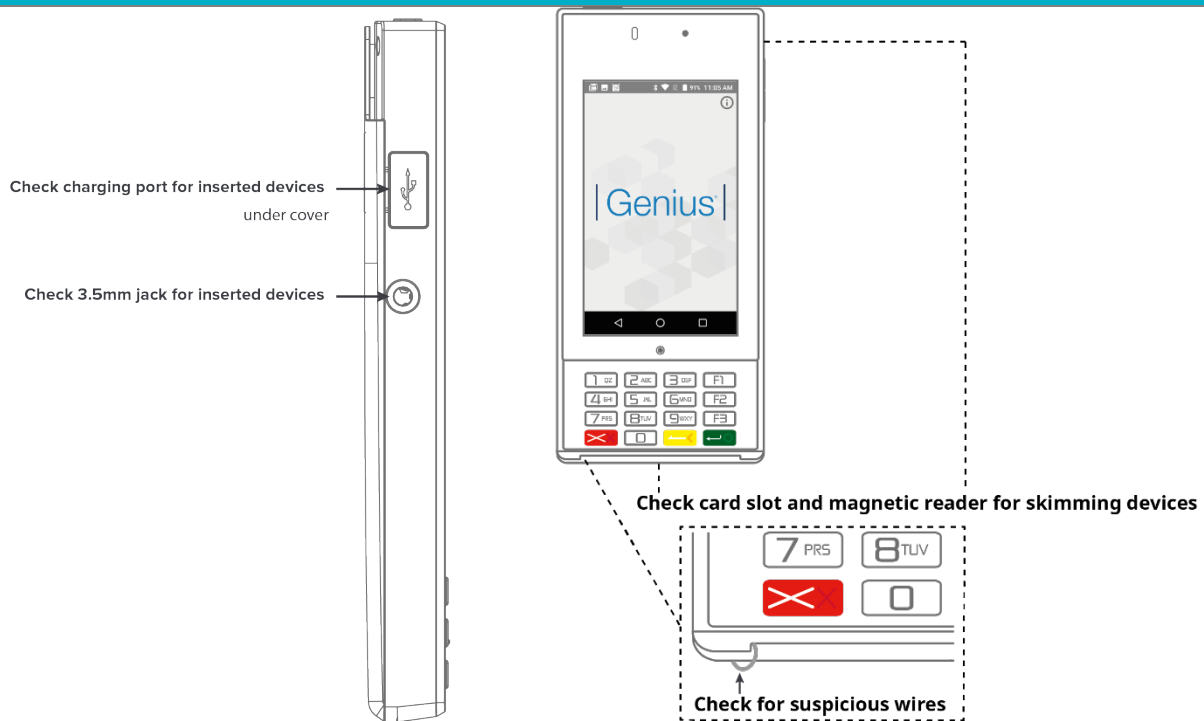
[https://www.pcisecuritystandards.org/assessors\\_and\\_solutions/pin\\_transaction\\_devices](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices)

- Inspect your device regularly for signs of tampering, including:
  - A change in weight
  - Missing or changed screws
  - Broken or changed tamper seals
  - Holes in the device
  - Additional wires or components, or other covering material that could be used to mask evidence of tampering
  - Serial number changes
  - Broken or differently colored casing
  - Additional faceplate or casing that may conceal a skimming device

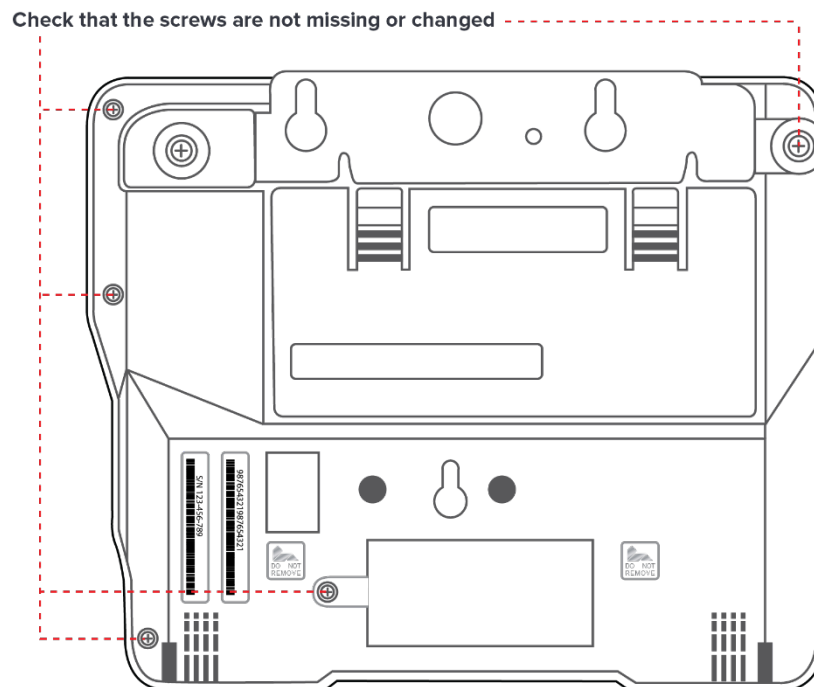


*Genius Countertop device*

## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity



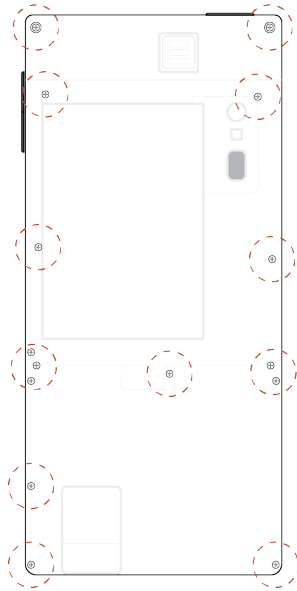
Genius Handheld device



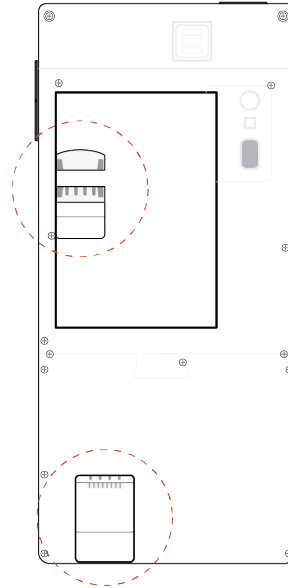
Genius Countertop device

## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

Remove the battery cover and check that the 15 screws are not missing or changed



Check that nothing is inserted in the card slots underneath the battery



Check that nothing is inserted in the two card slots underneath the battery cover

*Genius Handheld device*

Additional guidance for skimming prevention on POI terminals can be found in the document entitled "Skimming Prevention: Best Practices for Merchants", available at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)



**Note:** The required frequency of inspections depends on factors such as the location of the device and whether it is attended or unattended. For example, devices left in a public area with little supervision should be inspected more regularly than devices that are kept in secure areas or that are supervised.

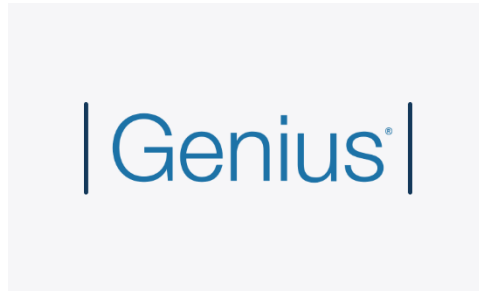
- If you cannot remove your device from its stand to weigh it, take alternative steps to monitor whether the device has been tampered with. For example, using tamper-seals or stickers to indicate if a device has been removed and replaced.
- Monitor devices in remote or unattended locations, for example, using video surveillance or other physical mechanisms to alert personnel of suspicious behavior.

## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

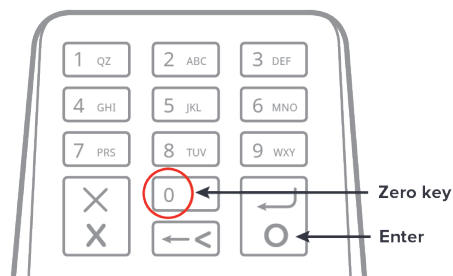
### 5.1.3 Genius Countertop devices fitted to stands

- If you cannot remove your device from its stand to check the printed serial number, you can check it in the **Admin** menu as follows:

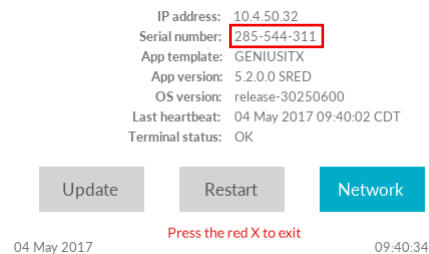
- When Genius is displaying the splash screen, press 0 on the keypad three times.



- Using the keypad type the password, then press **Enter** (green button). The default password is **9416557**.



- Check that the serial number matches the entry in your inventory.



## 5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

### 5.1.4 Reporting suspicious activity

If you detect suspicious activity:

- Do not use the device.
- Immediately contact our Customer Support Team at **(1) (888) 249-3220** and give a full description of the suspected activity.
- Follow the instructions of our Customer Support Team for returning the device.



**Important:** If your device develops a fault, we arrange for you to return the device to us, and we ship a replacement device to you. We do not repair deployed devices; therefore, you should **NOT** grant access to any person that claims to be repair or support personnel.

## 5.2 Instructions for responding to evidence of POI device tampering

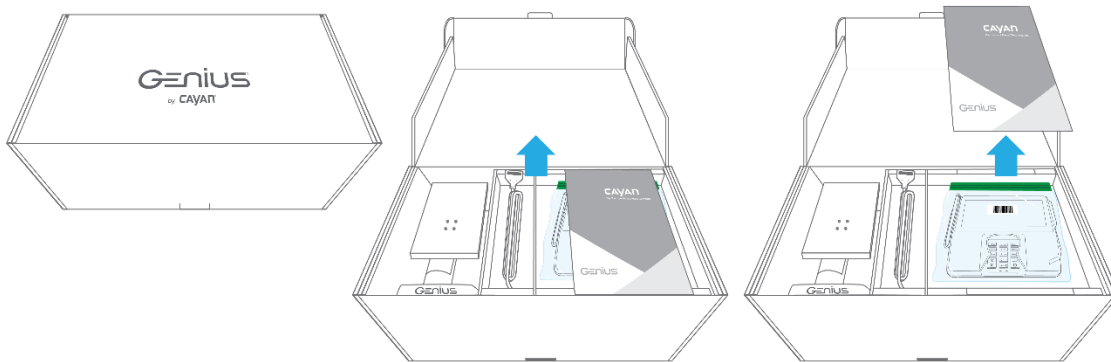
If you suspect that someone has tampered with your device:

- Do not use the device.
- Immediately contact our Customer Support Team at **(1) (888) 249-3220** and give a full description of the suspected tampering.
- Follow the instructions of our Customer Support Team for returning the device.

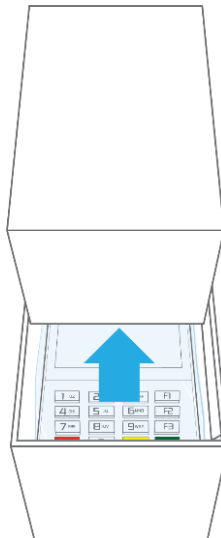
## 5.3 Instructions for confirming device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider

To confirm that your device was shipped from a trusted location, and was not tampered with during shipping, complete the following checks:

1. Check the shipping label to confirm that the device was shipped from one of the following two secure sites:
  - POS Portal, 1627 Main Ave, Sacramento, CA 95838
  - POS Portal, 1920 Watterson Trail # A, Louisville, KY 40299
2. Open the shipping box and remove the packing slip and the Genius box.
3. Open the Genius box.



*Genius Countertop packaging*

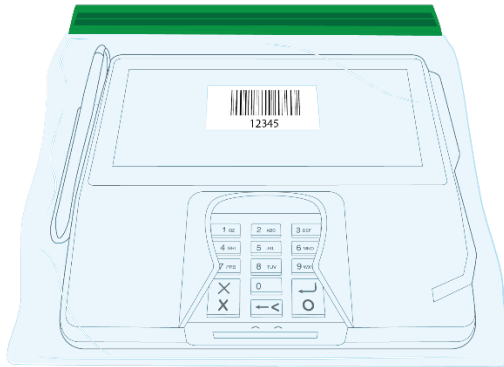


*Genius Handheld packaging*



## 5.3 Instructions for confirming device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider

4. Check that the Genius device is packed in a tamper-evident bag.

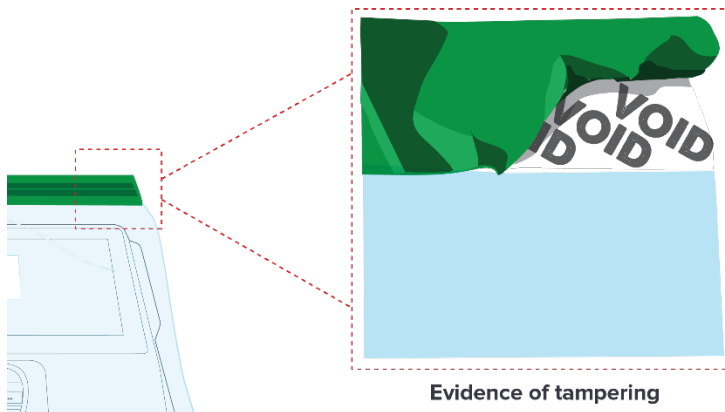


*Genius Countertop device*



*Genius Handheld device*

5. Confirm that the tamper-evident bag has no rips or evidence of tampering.
6. Check the tape that seals the top of the bag for evidence of tampering. If anyone has tried to remove the tape, the word "VOID" is displayed.



**Evidence of tampering**

7. Check that the serial number of the tamper-evident bag matches the serial number printed on the packing slip.
  - The serial number of the tamper-evident bag is located underneath the barcode on the front of the bag.



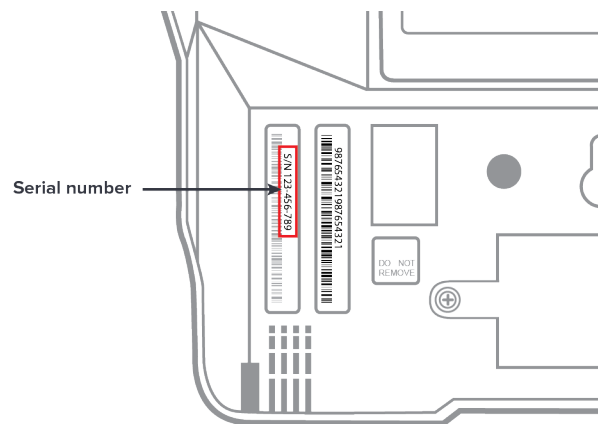
## 5.3 Instructions for confirming device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider

- The corresponding serial number is printed in the rightmost column of the packing slip, after the letters **TE**.

Name			
ime			
1456789			
Quantity			
Lot	Ordered	Shipped	
Ea.	1	1	123-456-789 (TE 12345)

Serial number

- Check that the serial number of the device matches the serial number printed on the packing slip.
  - The serial number of the Genius device is located on the back of the device.



Genius Countertop device



Genius Handheld device

## 5.3 Instructions for confirming device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider

- The corresponding serial number is printed in the rightmost column of the packing slip.

Order No. **1234567**  
 Ordered On: 01/01/2017 10:00 AM  
 MID: 123456789  
 DBA: Cayan LLC

Ship Method: FedEx Ground Service

SHIP TO				
Company Name				
Contact Name				
Address 1				
Address 2				
Phone: 123456789				
	Quantity			
	Lot	Ordered	Shipped	
ew	Ea.	1	1	123-456-789 ← Serial number

## 5.4 Guidance for granting third party personnel access to POI devices

We do not repair deployed devices at your premises; therefore, you should **NOT** grant access to any person that claims to be repair or support personnel.

## 6. Device Encryption Issues

### 6.1 Instructions for responding to POI device encryption failures

In the event of a device encryption failure you must immediately stop using the device. Do not re-enable the device until:

- You confirm that full P2PE-encryption functions are restored and re-enabled.

**Or**

- You provide us with written notification, signed by an executive officer of your business, formally requesting to stop P2PE encryption.
  - For more information about what information to include in the written notification, see Section 6.2.

### 6.2 Instructions for formally requesting of the P2PE solution provider that P2PE encryption of account data be stopped

To formally request that we stop the P2PE encryption of account data, call our Customer Support Team at **(1) (888) 249-3220**. Complete the form that the Customer Support Team send to you, and make sure that an executive officer of your business signs it, before returning it to us.

By completing and returning this form, you acknowledge that you accept responsibility for the following:

- The security impact to your account data and potential risks associated with processing transactions without P2PE protection.
- Implementing alternative controls to protect account data in lieu of the P2PE solution
- That you are no longer eligible for completing SAQ P2PE, associated with the use of PCI P2PE solutions.
- Informing your acquirer that you are no longer using the P2PE solution .
- That processing transactions without P2PE protection may affect your PCI DSS compliance validation and you should confirm with your acquirer or payment brand, as applicable, for all PCI payment brands affected.

## 7. POI Device Troubleshooting

### 7.1 Instructions for troubleshooting a POI device

#### 7.1.1 Genius Countertop devices

If your Genius Countertop device is not functioning correctly, complete the following tasks:

##### A) Run the Genius device connection test

1. When Genius is displaying the splash screen, press 0 on the keypad three times.
2. Using the keypad type the password, then press **Enter** (green button). The default password is **9416557**.
3. Tap **Network**, then tap **Test**.
4. Confirm that the **Gateway Connection Test** passed.

- If the tests all show **Passed**, continue to **Task E**.
- If any of the tests show **Failed**, take a note of the failed tests and continue to **Task B**.

##### B) Confirm that all necessary ports and hosts are open and available

1. Consult with your system administrator to confirm the that following ports are open:
    - 443:TLS
    - 7622:SFTP (via SSH)
  2. Confirm that the following hosts are available:
    - genius.merchantware.net
    - transport.merchantware.net
    - s01.merchantware.net
- If the device is still not functioning correctly, continue to **Task C**.

##### C) Restart the Genius device

Restart the Genius device by removing the AC power cord from the multiport cable for 30 seconds or more, then plug the cable back in.

- If the device is still not functioning correctly, continue to **Task D**.

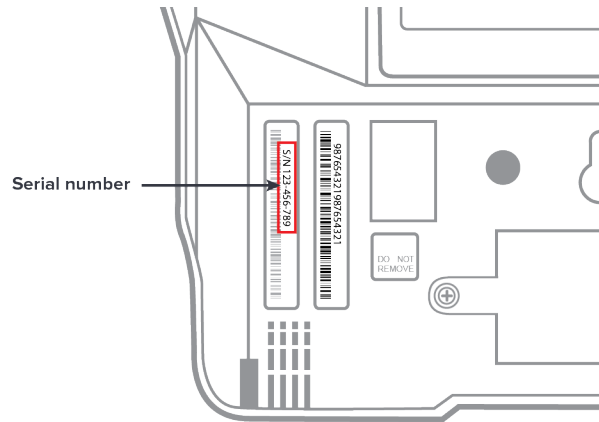
##### D) Check that the Genius device has received an IP address

1. When Genius is displaying the splash screen, press 0 on the keypad three times.
  2. Using the keypad type the password, then press **Enter** (green button). The default password is **9416557**.
  3. Confirm that the IP Address field is populated.
- If there is no IP address, follow the process for configuring a static IP address as described on page 15.
  - If the device has an IP address, and is still not functioning correctly, take note of the IP address and continue to **Task E**.

## 7.1 Instructions for troubleshooting a POI device

### E) Take a note of the device serial number

- Turn your Genius device upside-down and make a note of the serial number on the sticker.



- Continue to **Task F**.

### F) Contact the Customer Support Team

Contact our Customer Support Team by calling **(1) (888) 249-3220**. To help us with your support call, have the following information ready:

- Your business information so that we can identify your account.
- The connection test results from **Task A**.
- The device serial number as described in **Task E**.
- Your Merchantware credentials.

## 7.1 Instructions for troubleshooting a POI device

### 7.1.2 Genius Handheld devices

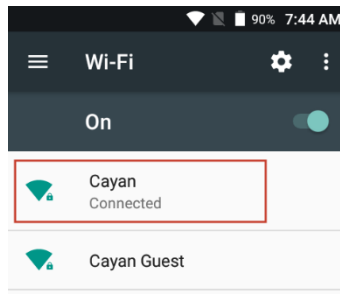
If your Genius Handheld device is not functioning correctly, complete the following tasks:

#### A) Check that the Genius Handheld device has received an IP address

1. Tap **O**, then open the Genius app.
2. Tap **i** to open the Admin screen.
3. Confirm that the **IP address** field is populated.
4. Tap **<** to return to the **Genius app** screen.

#### B) Check that the Genius Handheld device is connected to your network

1. On the **Home** screen, tap **⋮**.
2. Tap **Settings** **⚙️**, then **Wi-Fi**.
3. Ensure **Wi-Fi** is turned on and the Genius Handheld device is connected to the network.



4. Tap **<** to return to the **Genius app** screen.

#### C) Run the Genius Handheld device connection test

1. Tap **O**, then open the Genius app.
2. Tap **i** to open the Admin screen.
3. Tap **Test**, to run the **Network** test.
4. **Confirm** that the **Network Test** says **Pass**, then tap **OK**.
5. Tap **<** to return to the **Genius app** screen.
  - If the tests all show **Passed**, continue to **Task F**.
  - If any of the tests show **Failed**, take a note of the failed tests and continue to **Task D**.

#### D) Confirm that all necessary ports and hosts are open and available

3. Consult with your system administrator to confirm the that following ports are open:
  - 443:TLS
  - 7622:SFTP (via SSH)
4. Confirm that the following hosts are available:
  - genius.merchantware.net
  - transport.merchantware.net
  - s01.merchantware.net
- If the device is still not functioning correctly, continue to **Task E**.

## 7.1 Instructions for troubleshooting a POI device

### E) Restart the Genius Handheld device

Restart the Genius Handheld device:

1. Press and hold the Power button.
  2. Tap **Reboot**.
- If the device is still not functioning correctly, continue to **Task F**.

### F) Take note of the device serial number

- Turn your Genius device upside-down and make a note of the serial number on the sticker.



### G) Contact the Customer Support Team

Contact our Customer Support Team by calling **(1) (888) 249-3220**. To help us with your support call, please have the following information ready:

- Your business information so that we can identify your account.
- The connection test results from **Task C**.
- The device serial number as described in **Task F**.
- Your MerchantWARE credentials.

## 8. Additional Solution Provider Information



**Important:** We **cannot** share cardholder data with merchants who are using our P2PE solution, under any circumstances.

- For more useful help articles and troubleshooting information, visit <https://help.tsys.com>.



## 9. Appendix: Checklist for Remote Key Injection

We can remotely inject P2PE keys into your existing Genius Countertop devices. This process allows you to use our Genius Smart P2PE solution without purchasing new devices or sending your existing devices to us. Your devices must be either version three or version four of Verifone's hardware and be listed as a PCI approved PTS device.

Before we can remotely inject P2PE keys into your devices, you need to inspect them to ensure that no one has tampered with or fitted skimming devices to them.



**Important:** You must include all the devices that you want to use with our Genius Smart P2PE solution on this form.

**Sample Table of Devices for use with Genius Smart P2PE**

Device vendor	PCI ID	Device model name(s) and number:	Serial number (S/N)

## Attestation Checklist

Complete the following checklist to confirm the suitability of the devices that you want use with Genius Smart P2PE.

Check	For more information	Complete
Devices are versions listed in the PCI PTS approval	Visit <a href="https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices">https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices</a>	
Foil seals on the rear of the devices are intact	See "Before deploying a device" on page 32 to page 34.	
Devices are the correct weight	See "Before deploying a device" on page 32 to page 34.	
Devices do not have any holes or signs of attempted access to the internal components	-	
Devices do not have any additional wires or components, or other material that could be used to mask evidence of tampering.	See "After deploying a device" on page 35 to page 39.	
Devices do not have any broken or different colored casings	-	

## Attesting the suitability of your devices

By signing this attestation, I confirm the following:

- By completing this checklist, I confirm that I have visually and physically inspected each of the devices I have listed in the table of devices I want to use for Genius Smart P2PE.
- I have checked each of the devices I want to use with Genius Smart P2PE, and I have accurately recorded the results on this checklist.
- I understand that I must treat these devices like any other P2PE devices and that I must keep an up-to-date inventory.
- I understand that I will be held responsible should I use devices that are not suitable for use with Genius Smart P2PE and that any transactions I process using these devices will not be considered compliant with our P2PE solution.

**Merchant:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_



**CAYAN™**

The Payment Possibilities Company™