cardconnect®
A First Data Company

P2PE Instruction Manual (PIM)

v2.9 June 2019

Revision History

Version	Date	Contributors
1.0	Oct 2014	Rush Taggart
1.1	Nov 2014	Andy Liaskos
1.2	Dec 2014	Justin Shipe
1.3	Jan 2016	Rush Taggart
2.0	Aug 2016	Justin Shipe
2.1	Jan 2017	Dave Gouger, Justin Shipe, Andy Liaskos
2.2	Mar 2017	Dave Gouger, Justin Shipe, Andy Liaskos
2.3	Jun 2017	Justin Shipe
2.4	Dec 2017	Justin Shipe
2.5	Apr 2018	Chris Kemmerer
2.6	May 2018	Chris Kemmerer
2.7	June 2018	Chris Kemmerer
2.8	March 2019	Chris Kemmerer, Christopher Edmundowicz
2.9	June 2019	Ken Groninger

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	CardSecure P2PE
Solution reference number per PCI SSC website:	2017-00113.004

1.2 Solution Provider Contact Information	
Company name:	CardConnect, LLC
Company address:	1000 Continental Drive, Suite 300, King of Prussia PA 19406
Company URL:	www.cardconnect.com
Contact name:	CardPointe Support
Contact phone number:	877-828-0720 > option 1 > option 1
Contact e-mail address:	cardpointesupport@cardconnect.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

POI device vendor:	IDTECH
POI device model name and number:	SecurRED
Hardware version #(s):	IDSR-33x1xxxxx
Firmware version #(s):	SRED: 1.07, 1.08, 2.00
PCI PTS Approval #(s):	4-10144 (PTS v3.x)

POI device vendor:	IDTECH
POI device model name and number:	Spectrum Pro
Hardware version #(s):	106, 108
Firmware version #(s):	1.00, 1.01
PCI PTS Approval #(s):	4-10217 (PTS v4.x)

POI device vendor:	IDTECH
POI device model name and number:	SREDKey
Hardware version #(s):	IDSK-53XXXXXXX
Firmware version #(s):	SRED: 1.01
PCI PTS Approval #(s):	4-10156 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	Desk/3500
Hardware version #(s):	DES35BA (CTLS)
Firmware version #(s):	820547v01.xx
PCI PTS Approval #(s):	4-20283 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	Desk/5000
Hardware version #(s):	DES50BA (CTLS)
Firmware version #(s):	820547v01.xx
PCI PTS Approval #(s):	4-20281 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iCMP
Hardware version #(s):	ICMxxx-01Txxxxx, ICMxxx-11Txxxxx, ICMxxx-21Txxxxx, ICMxxx-31Txxxxx
Firmware version #(s):	820305V01.xx, 820365V02.xx, SRED (CTLS): 820528V02.xx, 820539V01.xx
PCI PTS Approval #(s):	4-20235 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iCT220, iCT250
Hardware version #(s):	iCT2xx-11Txxxxx
Firmware version #(s):	820305V02.xx, 820375V01.xx, 820365 V02.xx, SRED (Non CTLS): 820528V02.x
PCI PTS Approval #(s):	4-20196 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iPP310, iPP320, iPP350
Hardware version #(s):	iPP3xx-11Txxxxx
Firmware version #(s):	SRED (CTLS): 820365 V02.xx, 820305V02.xx, 820528V02.xx, SRED (Non CTLS): 820375V01.xx, 820554v01.xx
PCI PTS Approval #(s):	4-20184 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iPP315
Hardware version #(s):	iPP3xx-31Txxxxx
Firmware version #(s):	820305 V11.xx, 820180 V01.xx
PCI PTS Approval #(s):	4-10217 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iPP320, iPP350, iPP310, iPP315
Hardware version #(s):	iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx
Firmware version #(s):	820305V11.xx, 820073V01.xx, 820528V02.xx
PCI PTS Approval #(s):	4-30176 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iSC Touch 250
Hardware version #(s):	iSC2xx-21Txxxxx, iSC2xx-31Txxxxx
Firmware version #(s):	820518 V02.xx, SRED (CTLS): 820528V02.xx
PCI PTS Approval #(s):	4-30135 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iSC Touch 250
Hardware version #(s):	iSC2xx-21Txxxxx, iSC2xx-31Txxxxx
Firmware version #(s):	820518 V12.xx, SRED (CTLS): 820528V02.xx
PCI PTS Approval #(s):	4-30132 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iSC Touch 480
Hardware version #(s):	ISC4xx-01Txxxxx (no CTLS), ISC4xx-11Txxxxx (CTLS)
Firmware version #(s):	820518 V11.xx, 820518 V12.xx, SRED (CTLS): 820528V02.xx
PCI PTS Approval #(s):	4-30125 (PTS v4.x)

POI device vendor:	Ingenico
POI device model name and number:	iSMP
Hardware version #(s):	iMP3xx-01Txxxxx, iMP3x0-01Txxxxx (already approved hardware version), iMP3x2-01Txxxxx (new hardware version)
Firmware version #(s):	820305V01.xx, 820365V02.xx, SRED (Non CTLS) : 820528V02.xx
PCI PTS Approval #(s):	4-20183 (PTS v3.x)

POI device vendor:	Ingenico
POI device model name and number:	iSMP4
Hardware version #(s):	IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless), IMP6xx-02Txxxxx, (without contactless), IMP6xx-12Txxxxx(with contactless)
Firmware version #(s):	820305v11.xx
PCI PTS Approval #(s):	4-30220 (PTS v4.x)

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)
Bolt v1.6.x	Ingenico	iPP310, iPP320, iPP350 (PTS v3.x)	**Hardware Version:** iPP3xx-11Txxxxx **Firmware Version:** SRED (CTLS): 820365 V02.xx, 820305V02.xx, 820528V02.xx, SRED (Non CTLS): 820375V01.xx, 820554v01.xx	Yes	Yes
		iPP320, iPP350, iPP310, iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx **Firmware Version:** 820305V11.xx, 820073V01.xx, 820528V02.xx	Yes	Yes

		iSC Touch 250 (PTS v3.x)	**Hardware Version:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx **Firmware Version:** 820518 V02.xx, SRED (CTLS): 820528V02.xx	Yes	Yes
		iSC Touch 250 (PTS v4.x)	**Hardware Version:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx **Firmware Version:** 820518 V12.xx, SRED (CTLS): 820528V02.xx	Yes	Yes
		iSMP4 (PTS v4.x)	**Hardware Version:** IMP6xx-01Txxxxx (without contactless), IMP6xx-11Txxxxx (with contactless), IMP6xx-02Txxxxx, (without contactless), IMP6xx-12Txxxxx(with contactless) **Firmware Version:** 820305v11.xx	Yes	Yes
CardConnect PANpad v5.3.x	Ingenico	iPP310, iPP320, iPP350 (PTS v3.x)	**Hardware Version:** iPP3xx-11Txxxxx **Firmware Version:** 820305V02.xx 820528V02.xx	Yes	Yes

		iPP320, iPP350, iPP310, iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-21Txxxxx, iPP3xx-31Txxxxx, iPP3xx-41Txxxxx, iPP3xx-51Txxxxx **Firmware Version:** 820305V11.xx 820073V01.xx 820528V02.xx	Yes	Yes
		iSC Touch 250 (PTS v3.x)	**Hardware Version:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx **Firmware Version:** 820518V02.xx 820528V02.xx	Yes	Yes
		iSC Touch 250 (PTS v4.x)	**Hardware Version:** iSC2xx-21Txxxxx, iSC2xx-31Txxxxx **Firmware Version:** 820518V12.xx 820528V02.xx	Yes	Yes
CardConnect PANpad v5.2.x	Ingenico	iCT220, iCT250	**Hardware Version:** iCT2xx-11Txxxxx **Firmware Versions:** 820305V02.xx, 820375V01.xx, 820365V02.xx, SRED (Non CTLS): 820528V02.x	Yes	Yes

		iPP310, iPP320, iPP350	**Hardware Version:** iPP3xx-11Txxxxx **Firmware Versions:** 820305V01.xx, 820365V02.xx, SRED (Non CTLS): 820157V01.xx	Yes	Yes
CardPointe TRA v2.2.x	Ingenico	Desk 3500 (PTS v4.x)	**Hardware Version:** DES35BA (CTLS) **Firmware Version:** 820547v01.xx, 820376v01.xx, 820549v01.xx (SRED), 820549v01.xx, 820556v01.xx, 820565v01.xx (SRED)	Yes	Yes
		Desk 5000 (PTS v4.x)	**Hardware Version:** DES50BA (CTLS) **Firmware Version:** 820547v01.xx; 820376v01.xx, 820549V01.xx (SRED OnGuard FPE), 820555v01.xx (SRED AWL), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)	Yes	Yes

		iCT220, iCT250 (PTS v3.x)	**Hardware Version:** iCT2xx-11Txxxxx **Firmware Versions:** 820305V02.xx, 820375V01.xx, 820365V02.xx, SRED (Non CTLS): 820528V02.x	Yes	Yes
		iPP315 (PTS v4.x)	**Hardware Version:** iPP3xx-31Txxxxx **Firmware Version:** 820305 V11.xx, 820180 V01.xx	Yes	Yes
		iPP320 (PTS v3.x)	**Hardware Version:** IPP3xx-11Txxxxx **Firmware Version:** SRED (CTLS): 820365V02.xx, 820305V02.xx, 820528V02.xx, SRED (Non CTLS): 820375V01. xx, 820554v01.xx	Yes	Yes
CardPointe TRA v1.2.x	Ingenico	iCT220, iCT250	**Hardware Version:** iCT2xx-11Txxxxx **Firmware Versions:** 820305V02.xx, 820375V01.xx, 820365V02.xx, SRED (Non CTLS): 820528V02.x	Yes	Yes

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).
- The intent of the device inventory is to ensure that a merchant can locate a device based on its serial number.
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted POI devices, must be reported to CardConnect via the contact information in Section 1.2 above.
- The sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Secure Inventory Control

Merchants are responsible for maintaining inventory and monitoring inventory of all terminals in your charge. This includes terminals that are in use, devices that are waiting to be used and devices that are in the process of being repaired. A missing or unaccounted for device could indicate that a terminal has been intercepted by an unauthorized party.

The CardConnect Terminal Management System provides reports of all devices shipped to a location. This must match the devices in use at that location.

Annual Audit of Terminal Inventory

Merchants are responsible for maintaining inventory and monitoring inventory of all devices processing cardholder data. This includes terminals that are in use, devices that are waiting to be used and devices that are in the process of being repaired. For this reason, CardConnect recommends any terminal not in active use or in the installation process be securely stored on premises, or returned to CardConnect. The CardConnect TMS will record returned terminals and remove them from merchant responsibility. CardConnect grants program managers' access to the Terminal Management System to review device inventory information.

At least once a year, a full inventory of all terminals (POI devices) must be conducted to ensure that all devices are accounted for and match the serial numbers documented in your inventory. All merchants should be familiar with their terminal models, including security markings, screws, and tamper seals so that inspections are effective at detecting tampered or compromised devices.

If a discrepancy is found during the annual inventory, the following steps must be taken:

1. Isolate the missing device or devices.
2. Determine the last known location of the device and if possible the last known use.
3. Determine the serial number/type of device.
4. Verify what state the device was in (deployed, spare/backup, undergoing repair).
5. Contact CardPointe Support with all the information collected about the missing device. Contact information and points of contact are found in Appendix A of this document.
6. Work with CardConnect to verify if cardholder data has been compromised.
7. If you determine that cardholder data has been compromised, follow the steps outlined by Visa at: http://www.visaeurope.com/en/businesses retailers/payment security/downloads resources.aspx

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

Installation

Your CardConnect device is shipped to you pre-programmed and ready to use. There is no need for you to perform any update or download once you receive your device. Perform the following upon receiving the device:

1. Unpack the device from the box.
2. Connect the included cabling.
3. Connect the USB, Ethernet or Serial cable to your network, and then plugin the power supply to a wall outlet to power up your device.

   Your device will now go through boot cycle to power up.

For PANpad devices, once your device completes booting up it should display 'Panpad No Connection'.

For Bolt devices, it will read "Bolted".

If your device displays another message, or if you are unable to process a transaction, contact the CardPointe Support team at 877-828-0720 > option 1 > option 1 for immediate support.

After initial installation, it is considered best practice to disconnect and securely store your devices when unattended.

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

It is important that your devices are placed in secure and well-lit locations that are not left unattended for extended periods of time. Devices that are not in use should be stored in a secured location.

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

We recommended physically securing POI devices with security tethers to prevent the terminal(s) from being compromised. Devices should be placed in a location that allows customers to use them in a manner that obscures their PIN entry from other customers. In addition, it is best practice to block ports on the device to prevent tampering.

4. POI Device Transit

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

Terminals must be secured before and during transportation. When developing your transportation procedure, be sure to cover the following areas:

- Package the device in such a way that is tamper-evident. Use tamper tape on boxes. Track the device number and shipping details together.
- Verify the packages have not been tampered before shipment. Inspect the tape to ensure no seals are broken or cracked. If the package shows signs of tampering, do not ship it. Review your access log for information on the last person to access the area and contact CardPointe Support for further instructions.

Terminal shipments must use only secure courier services that provide tracking services.

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

As a P2PE merchant, you are responsible for maintaining all information regarding the chain of custody of your P2PE terminals. The intent of this control is to clearly identify which devices are in your possession, the device status, and location. If a terminal is not correctly encrypting card data, you, the merchant, must be able to locate a device in your possession using a Hardware Serial Number (HSN).

Devices are shipped from select trusted sources of CardConnect. When receiving device shipments, ensure that the shipper address matches one of the following:

- **CardConnect**
  1000 Continental Dr
  Ste 300
  King of Prussia PA 19406
- **TASQ Technology**
  1169 Canton Rd
  Marietta, GA 30066
- **Ingenico Inc.**
  6190 Shiloh Crossing
  Suite-C
  Alpharetta, GA, 30005
- **ID Tech**
  10721 Walker Street
  Cypress, CA 90630

Transporting Devices

Terminals must be secured before and during transportation. Ensure that you do the following:

- **Establish Trusted Locations**
  Establish a list of trusted locations for which you are storing or deploying devices.
- **Use Tamper Evident Packaging**
  Use tamper tape on boxes, and sign/initial over the edge of the tape.
- **Track Device and Shipment Details**
  Track the device quantity, make, model, serial numbers, and shipping details together.
- **Inspect Packages Before Shipping**
  Verify the packages have not been tampered before shipment. Inspect the tape to ensure no seals are broken or cracked. If the package shows signs of tampering, do not ship it. Review your access log for information on the last person to access the area and contact Customer Support for further instructions.
- **Secure Shipping Services**
  Terminal shipments must use only secured courier services such as FedEx and UPS.

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 titled *Skimming Prevention: Best Practices for Merchants,* available at www.pcisecuritystandards.org.

Step 1

Inspect the terminal daily and make sure that there are no unusual scratches or marks on it that were not present the previous day.

- If using a base or stand, ensure that the base is firmly mounted to the counter top and that the terminal is firmly attached to the base.
- Ensure that there are no unusual marks or scratches on the terminal.
- Ensure that the card reader is clean and an undamaged and that nothing is protruding from the opening. Verify that a card fits tightly in the opening.
- Ensure that no case or cover has been placed over the device.

Step 2

Inspect all wires and cables to ensure that they are securely connected.

- Verify that the terminal cable is securely attached to the device and there is nothing in-between it and the device.
- Verify that the connecting USB, Serial, or Ethernet cable is securely plugged in.
- Verify that no device is placed between the terminal and the USB, Serial, or Ethernet cable.
- Verify that all wires and cables are in good condition with no tears or ripping.

Following these steps will help maintain the integrity of your credit card terminals. If you feel that your terminal has been tampered with in any way, stop processing credit cards and immediately call CardConnect's Cardpointe Support team at 877-828-0720 > option 1 > option 1.

5.2 Instructions for responding to evidence of POI device tampering

In the event devices show physical signs of tampering, stop using the device immediately. Contact CardPointe Support with the following information:

- The date and time when you initially noticed the tampering
- The suspected the cause of the tampering (i.e. missing screws, holes or additional seals in the device, the device weights too much, etc.)
- Last status of the device in your asset inventory
- Date of last inspection

Your CardConnect contact will assist you in gathering information, troubleshooting, and responding to the incident. Any other suspicious activity of POI devices should be reported to CardPointe Support for investigation and resolution.

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

You can confirm that your original terminal device is in place by comparing:

- Make and Model
- Serial number
- General description
- Security seals, labels, hidden markings, etc. You may dab a dot of nail polish inconspicuously on one corner, for instance.
- Number and type of physical connections to device (ONE)
- Date of last inspection

You must maintain a log of these security checks for each device and provide it to your PCI auditor for inspection. A handwritten notebook is sufficient. It should be kept in a secure location.

You may also email cardpointesupport@cardconnect.com with the device serial number, inspection result, and optionally a photograph. CardConnect will maintain this record.

Should you detect any indication of tampering with the device please contact CardPointe Support as soon as possible for assistance. If you suspect any transactions were processed on a tampered device, please inform the CardPointe Support team.

To verify secure communications, follow the instructions in section 3.1 of this document.

5.4 Instructions for identifying third-party device support personnel

At no time will CardConnect send a technician to perform on-site terminal repair. All staff at merchant locations must be trained to check the personal identification and credentials of any person that claims to be a terminal repair technician. Before allowing any person physical access to a payment terminal for troubleshooting or maintenance purposes, contact CardPointe Support using the information provided in section 8.

6. Device Encryption Issues

6.1 Instructions for responding to POI device encryption failures
In the case of an encryption failure, users should identify all POI devices that have encryption or tokenization errors. Merchant should notify the CardConnect support team with details of the devices and error received. CardConnect will facilitate any troubleshooting necessary to prove whether it is an encryption error and if that is the case, CardConnect will coordinate replacement of the device(s).

6.2 Instructions for formally requesting of the P2PE solution provider that P2PE encryption of account data be stopped
A request to the P2PE Solution Provider, CardConnect, to stop encryption of account data would require the merchant to stop the use of the P2PE solution and return all devices to CardConnect. Such a request can be made to the CardConnect Support Team, cardpointesupport@cardconnect.com.

7. POI Device Troubleshooting

7.1 Instructions for troubleshooting a POI device
The CardConnect terminal management and fulfilment partners cannot facilitate any on-site terminal repairs. Troubleshooting takes place only between the merchant and CardConnect. When a POI device presents an issue that requires troubleshooting, the merchant should contact CardConnect. CardConnect will triage the issue and attempt to provide resolution. CardConnect will contact their fulfilment partners for troubleshooting and/or replacement when necessary. No one outside of CardConnect, and their fulfilment partners are authorized to troubleshoot or repair terminals.

8. Additional Solution Provider Information

Please contact cardpointesupport@cardconnect.com with any questions or concerns regarding your POI device. You can also contact CardPointe Support by phone at 877-828-0720 > option 1 > option 1.

Appendix A – Supplemental Information for Ingenico Devices running PANpad

A.1 Setup and Installation

Your CardConnect device is shipped to you pre-programmed and ready to use. There is no need for you to perform any update or download once you receive your device. Simply unpack the device from the box, connect the included cabling, connect the USB, Ethernet, or Serial cable to your network, and then plug the power supply in to a wall outlet to power up your device.

Your device will now go through boot cycle to power up. Once your device has completed booting up it will display "PANpad No Connection." If your device displays another message, or you are unable to process a transaction contact the CardPointe support team at 877-828-0720 option 1 > option 1.

A.2 Troubleshooting

Misconfigured device from supplier:

If keys are wrong or missing, the device should be returned to Ingenico for a replacement.

Device is not communicating with the gateway:

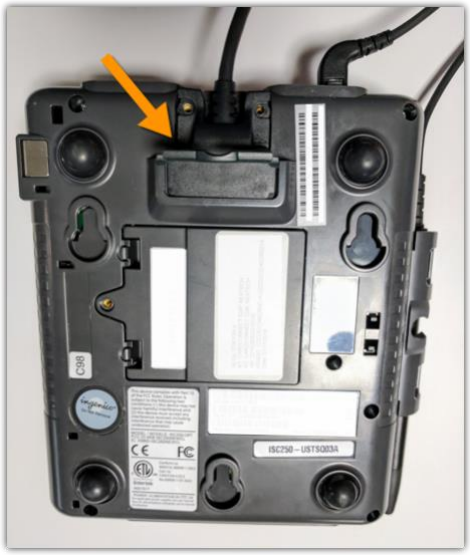
1. Ensure that the Ethernet cable is plugged in properly between the device and the router/switch.
2. Ensure that TCP ports 443, 8443, 8553 are open on your firewall from your device to the gateway.

Device is communicating but not processing transactions:

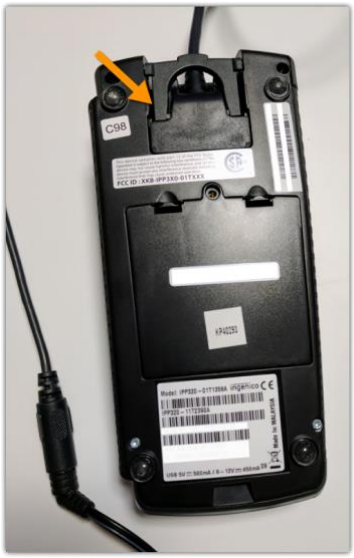
Contact CardPointe Support via email, or by calling 877-828-0720 > option 1 > option 1.

Device does not start:

1. Ensure that the power supply is securely connected to your device.

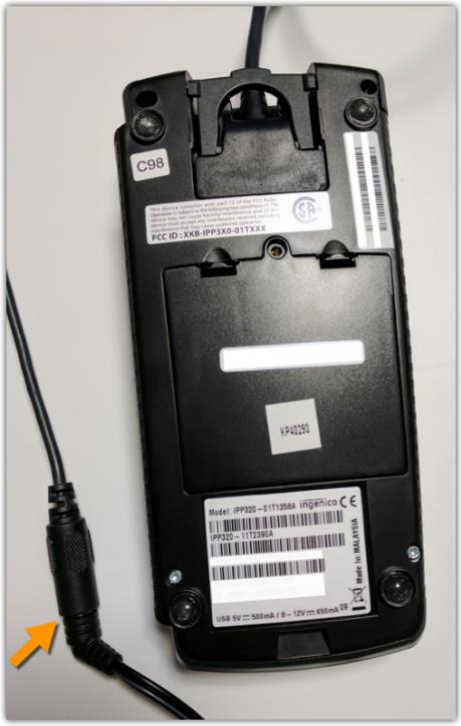


ISC250



IPP320

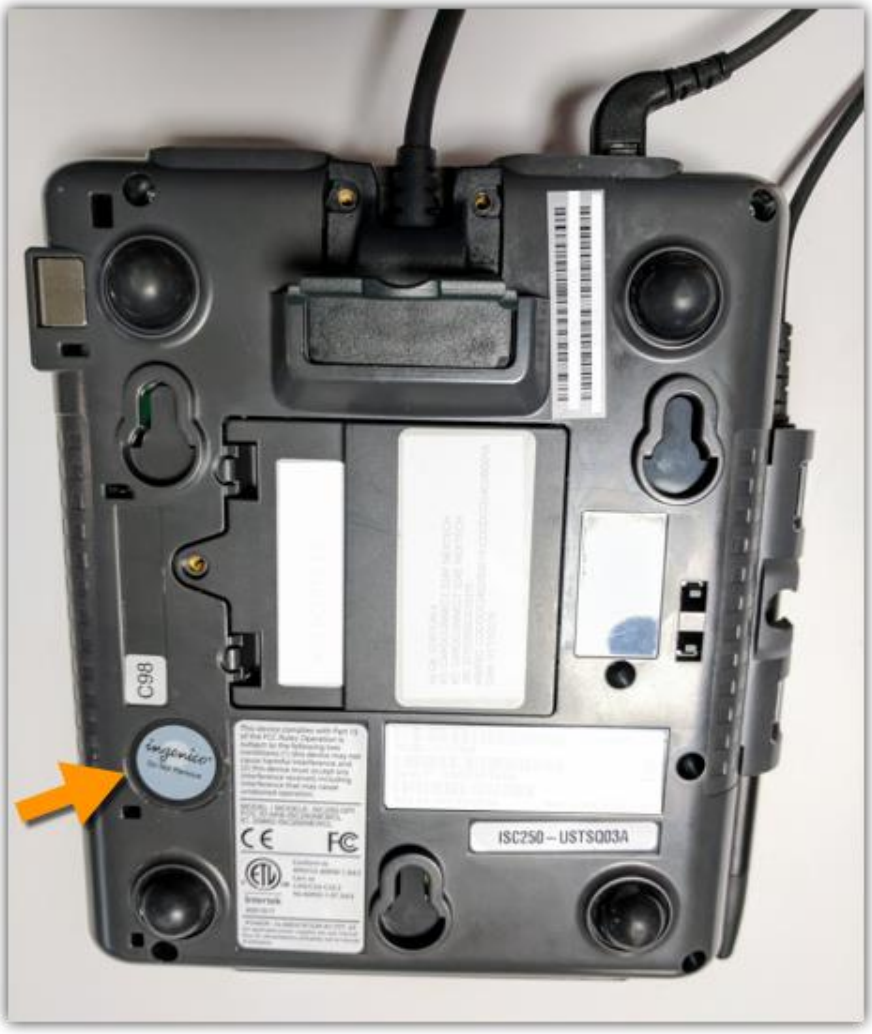
2. Ensure that the power cable is securely connected to the power supply and plugged into the wall.



You will hear an audible chime when the device is powered on. If the device still does not power on, please contact CardPointe Support via email, or by phone at 877-828-0720 > option 1 > option 1.

A.3 Anti-Tampering Inspection

Below is a photo of an anti-tamper seal. Verify that the seal is not broken and has not been replaced or masked over.



Appendix B – Supplemental Information for Ingenico Devices running CardPointe TRA

B.1 Setup and Installation

Your CardPointe terminal is shipped to you pre-programmed and ready to use. There is no need for you to perform any update or download once you receive your terminal. Simply unpack the terminal from the box, connect the included cabling, connect the Ethernet cable to your network, and then plugin the power supply to a wall outlet to power up your device.

Your terminal will now go through boot cycle to power up. Depending on the model of terminal you have, either one of two idle screens should display. Telium 2 series devices will say “CardPointe” in plain text. Tetra terminals will have a blue CardPointe image as the idle screen. If your terminal displays another message, or you are unable to process a transaction contact the CardPointe support team at 877-828-0720 > option 1 > option 1.

B.2 Troubleshooting

Device is not communicating with the gateway:

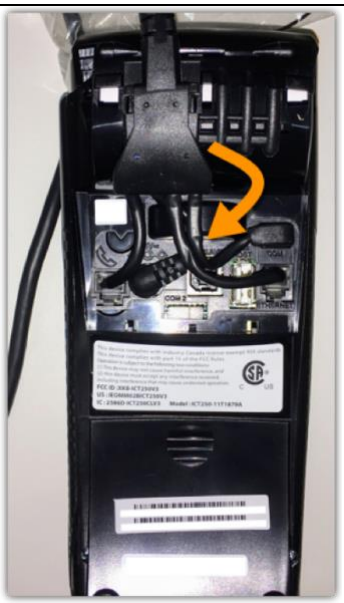
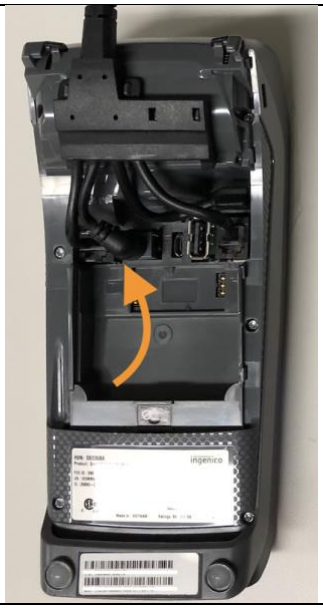
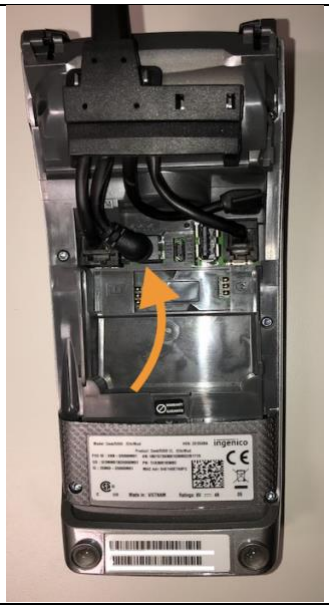
1. Ensure the Ethernet cable is plugged in properly between the device and the router/switch.
2. Ensure that TCP ports 443, 8443, 8553 are open on your firewall from your device to the gateway.

Device is communicating but not processing transactions:

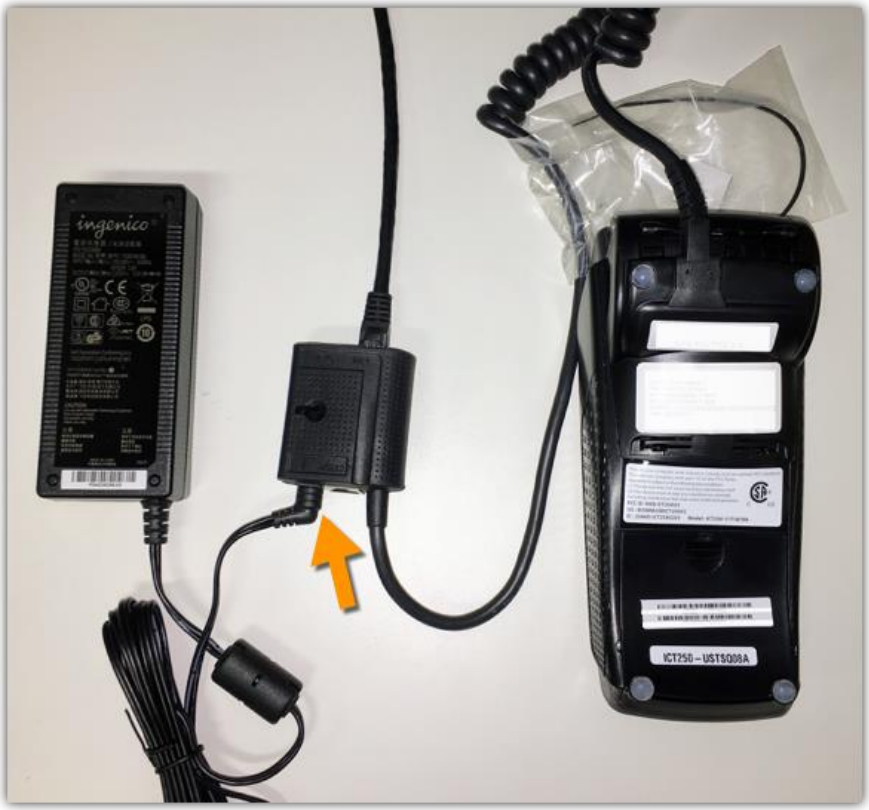
Contact CardPointe Support via email, or by calling 877-828-0720 > option 1 > option 1.

Device does not start:

1. Ensure that the power supply is securely connected to your device.

ICT220/ICT250	DESK 3500	DESK 5000
		

2. Ensure that the power cable is securely connected to the power supply and plugged into the wall.



You will hear an audible chime when the device is powered on. If the device still does not power on, please contact CardPointe Support via email, or by phone at 877-828-0720 > option 1 > option 1.

Appendix C – Supplemental Information for ID Tech SREDKey

C.1 Setup and Installation

1. Connect the device to a USB port.
2. Verify that the device is ready to transact. The device will display “Swipe Card or Key-in Card Number” when ready.

C.2 Troubleshooting

Admin Settings

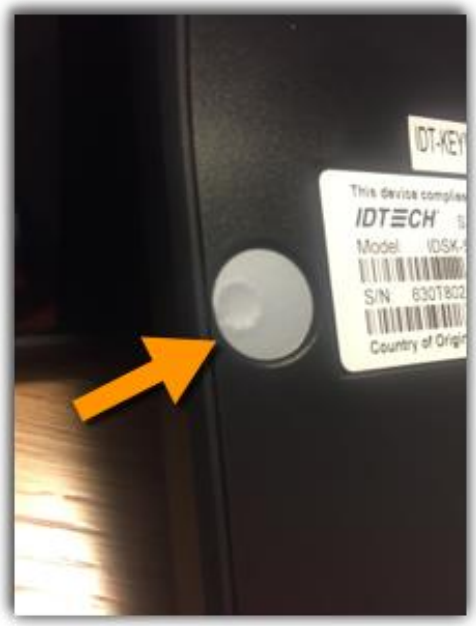
Selecting the Admin button opens a menu with various settings. By default, the Admin mode is set to "1." If you inadvertently change it to another mode number, you must change it back to "1," otherwise the device will not work properly.

Device is Faulty

If the device's screen blue and nothing else displays on the screen, please return it to CardConnect for a replacement.

C.3 Anti-Tampering Inspection

The following photo illustrates the anti-tamper seal. Verify that the seal is not broken and has not been replaced or masked over.



Appendix D – Supplemental Information for Bolt Terminals

D.1 Setup and Installation

1. Once your equipment is unboxed, plug the power supply connector into the jack on the Multipoint Interface Cable.
2. Connect the Multipoint Interface Cable into the Multipoint Port on the back of the Bolt P2PE device.
3. Connect the other end of the Multipoint Interface Cable to an ethernet port (POS, PC, modem, etc.).
4. Plug the power supply adapter into an available power outlet.

Confirming Connectivity

1. Once power is supplied to the Bolt P2PE device, an initiation process begins.
2. Once the device has successfully established its IP Address, it will attempt to call the Bolt service.
3. If the connection is successful, the Bolt P2PE device displays Bolted.
4. If the connection is unsuccessful, the device displays Unbolted, at which point you can contact us for troubleshooting.
5. Once Bolted, the device is ready for use. The device may be left on indefinitely or may be disconnected from power as necessary.

D.2 Troubleshooting

Restarting the Device

1. To restart, press [clear] and [-] simultaneously.
2. Alternatively, disconnect and reconnect the power supply to power cycle the device.

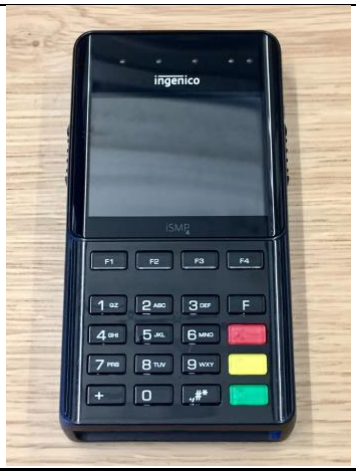
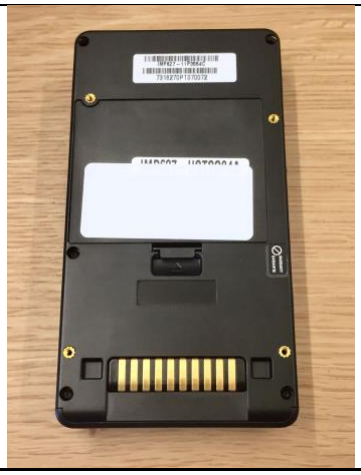
Device is Faulty

If the device's screen blue and nothing else displays on the screen, please return it to CardConnect for a replacement.

D.3 Anti-Tampering Inspection

The device includes pressurized tamper detectors. If a tamper detector is triggered, the device enters an 'Alert Irruption' state and the keys installed on the device are erased. In this case, the device must be returned for repair and reactivation before it can be used again.

If the device shows any signs of tampering, contact CardPointe Support via email, or by phone at 877-828-0720 > option 1 > option 1. For assistance.

iSMP4 Front	iSMP4 Rear
	

Appendix E – Supplemental Information for IDTECH Spectrum Pro Devices

E.1 Setup and Installation

Mounting Instructions

The Spectrum Pro Device can be mounted in either a horizontal or vertical orientation. The removal detection points must be pressed down when the unit is mounted.

LED Management

There are two LEDs. One is the user-interface LED on the front bezel of the reader; the other (diagnostic) LED is on the back.

Front LED Status:

- The LED turns green in idle waiting.

LED handling for Magstripe card operation:

- The LED will turn red to indicate that the recent magstripe card read was bad.

LED handling for smart card operation:

- The Green LED will flash after powering on the smart card.
- The solid Green LED indicates smart card processing is complete and the ICC powered off. The user can remove the smart card.

E.2 Troubleshooting

Diagnostic LED Status

The LED on the back of Spectrum Pro can be used for diagnostic purposes.

LED status:

- Off
- Solid – No communication with its host.
- Flashing (1 sec on, 1 sec off) – Communicating with its host.

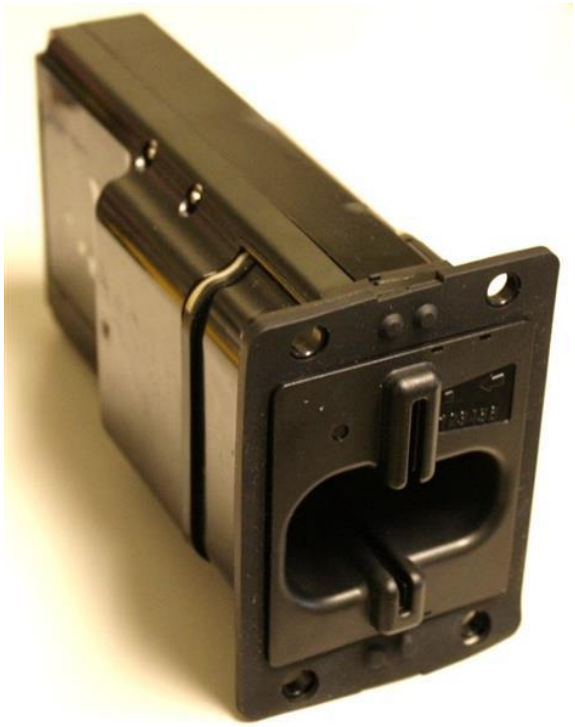
LED Colors:

- Amber – Reader requires on-site service actions.
- Green – Reader is ready to read cards.
- Red – Reader needs to be sent back to the manufacturer.

E.3 Anti-Tampering Inspection

Below is a photo of a Spectrum Pro Device. To check for evidence of tampering:

- Inspect the devices, make sure they are intact
- Power on the device, check the LED display, make sure there is not RED LED display shows the tamper was triggered.
- Connect device to Host to read the tamper flag, make sure no tamper flags are set.
- Check the hardware version on the label and power on the device to check the firmware/hardware version that conform to the version purchased.
- Check the slot of the ICC, make sure there is not overlay adaptor in the slot or ICC acceptor for shim devices.



The device uses multiple “active tamper” detection mechanisms that will detect physical intrusion into the device, and invoke a “tamper event”. A tamper event causes immediate erasure of all sensitive data and cryptographic keys. Once tampered, the device is in a non-operational state.

A merchant or acquirer can easily determine if a device is in a tamper state by observing not operating with solid red LED on.
Information about tamper events is contained in the Installation Guide.

In the case where a device is tampered, the merchant or acquirer should contact the service help desk and make arrangements to have the device removed from service, and returned to the factory for repair or forensics review.