

TransArmor

from **fiserv.**

P2PE Validated

Point-to-Point Encryption (P2PE)
Instruction Manual
Ingenico iSC 250/480 Touch
Version 1.4



1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	First Data TransArmor P2PE Solution – Ingenico On-Guard
Solution reference number per PCI SSC website:	2022-00541.001

1.2 Solution Provider Contact Information

Company name:	First Data
Company address:	1600 Terrell Mill Road, Marietta, GA 30067
Company URL:	www.fiserv.com
Contact name:	Marco Mabante
Contact phone number:	(470) 508-6660
Contact e-mail address:	TransArmorProductTeam@fiserv.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. Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.

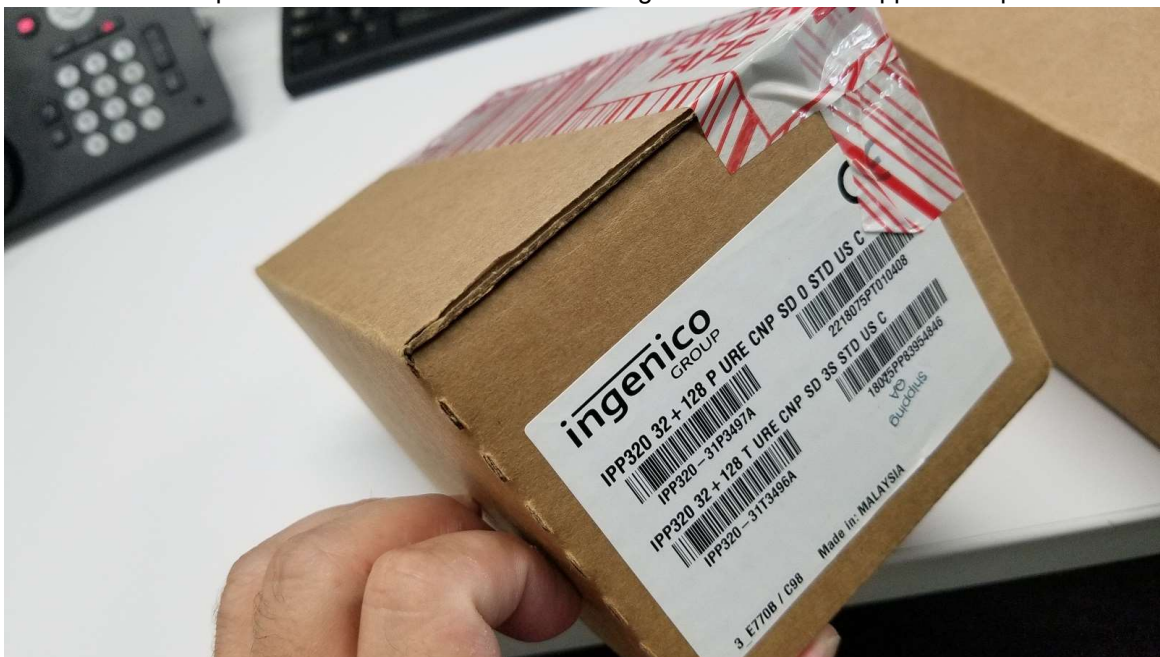
Ingenico terminals used as part of the First Data TransArmor P2PE Solution should only be deployed by approved personnel.

Do not purchase any Ingenico devices online or from a Key Injection Facility (KIF) that is not a component of the TransArmor P2PE Solution. You may use PCI Qualified Integrator Resellers to install and activate Ingenico POI devices. To request a return (RMA) for a POI that has been tampered with or defective follow the merchant's device tamper procedure and please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

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

Carefully inspect the shipping carton and its Tamper Evident packaging for damage. If the tamper evident packaging is damaged DO NOT put the device into service and follow the tamper package internal process and contact First Data or Ingenico Customer Support to report.



Inspect the Tamper Evident packaging to ensure no damage or an attempt made to reseal the package with clear tape.

- Photograph and retain pictures of the package (damaged or not).
- Confirm the serial number(s) of the devices against the serial numbers listed on the Advance Ship Notice (ASN) you should have received from the FDHS or Ingenico prior to receipt of the shipment.

NOTE: If serial numbers do not match do not put device into service and contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com
- Remove the contents from the box. The box contains the following items:
 - a. iSCxxx device
 - b. Multipoint Connector cable and cable mounting screws
 - c. Stylus
 - d. Power supply
 - e. Installation Guide
 - f. Privacy shield (optional)
- Remove the protective film from the graphical display screen.
- We recommend saving the carton and packing material for repackaging or moving the device in the future.

1. The box contains the following items:

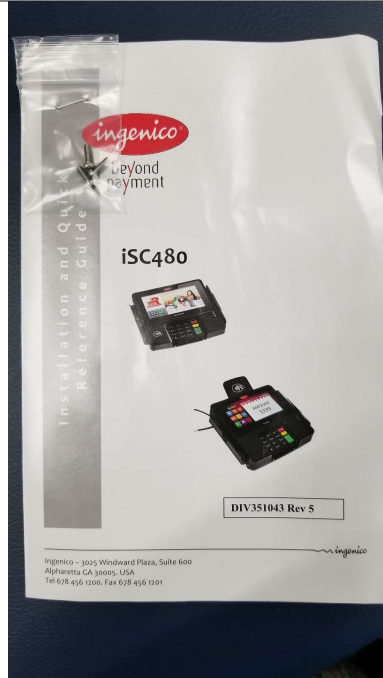


iSC250 or 480 device



Stylus





The box may also include the following optional items:

Multipoint Cable (specific to your connectivity requirements) and Power supply



2. Remove the protective film from the graphical display screen.
3. Save the carton and packing material for repackaging or moving the device in the future.

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

Physically secure POI devices in your possession, including devices:

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

2.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices.

First Data does not contract with any third-party personnel to install, troubleshoot, or repair any Ingenico devices.

Merchants may use internally approved associates or PCI Qualified Integrator Resellers (QIR) to install their devices using this P2PE Instruction Manual. Below is a link to PCI Certified QIR's:

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers

To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

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

3.1 POI Device Details

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

IMPORTANT NOTE: PCI-listed P2PE solutions (and applicable P2PE components) are allowed to revalidate and reassess their existing PCI P2PE approval with expired PTS POI devices for up to, but not exceeding, 5 years past the PTS POI device expiry dates (as listed on the PCI Approved PTS Devices list) for the POI device types used in the solution. In the case of the Ingenico iSC250/480 the PCI PTS expiry date is April 30, 2023 so that means you could use the device up until April 30, 2028. Be aware that the hardware manufacturer may end support for the device earlier than April 30, 2028.

All POI device information can be verified by visiting:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See also Section 9.2, "Instructions for how to confirm hardware, firmware, and application versions on POI devices."

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):
4-30132	Ingenico	iSC Touch 250	iSC2xx-21Txxxxx iSC2xx-31Txxxxx	820518 V12.xx SRED (CTLS): 820528V02.xx 820365 V02.xx (schemes),. 820073 V01.xx (Open Protocol module),. ,820554 V01.xx
4-30125	Ingenico	iSC Touch 480	ISC4xx-01Txxxxx ISC4xx-11Txxxxx	820518 V11.xx 820518 V12.xx 820528V02.xx 820365V02.xx (key schemes), . 820073V01.xx (Open Protocol module),,820554 V01.xx (SRED module)

3.2 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.

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.

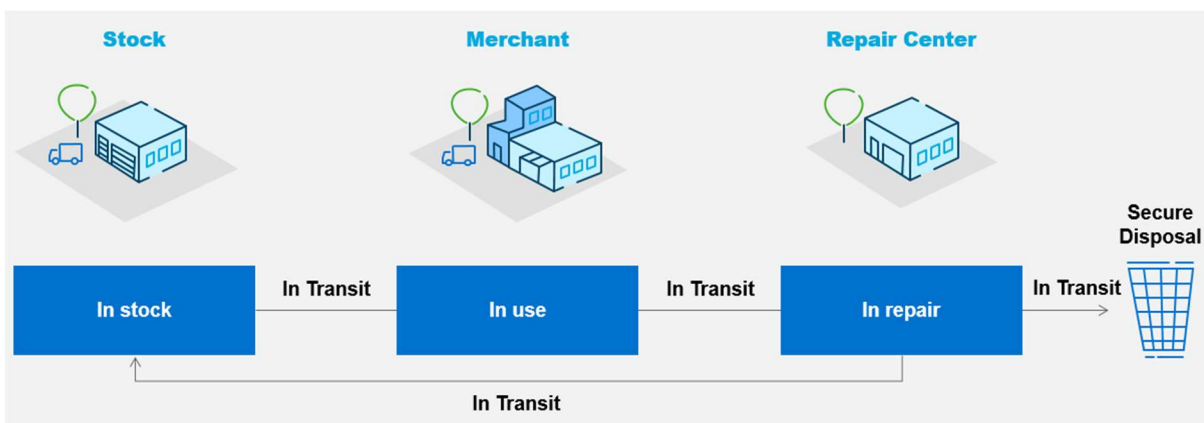
Application Vendor, Name, and Version #	POI Device Vendor	POI Device Model Name(s) and Number:	POI Device Hardware & Firmware Version #	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-text Account Data (Y/N)
Ingenico RBA v1.2	Ingenico	iSC Touch 250	Hardware # iSC2xx-21Txxxxx iSC2xx-31Txxxxx Firmware # 820518 V12.xx SRED (CTLS): 820528V02.xx 820365 V02.xx (schemes), 820073 V01.xx (Open Protocol module), 820554 V01.xx	Yes	Yes
Ingenico RBA v1.2	Ingenico	iSC Touch 480	Hardware # ISC4xx-01Txxxxx ISC4xx-11Txxxxx Firmware # 820518 V11.xx 820518 V12.xx 820528V02.xx 820365V02.xx (key schemes), 820073V01.xx (Open Protocol module), 820554 V01.xx (SRED module)	Yes	Yes

3.3 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 *First Data* via the contact information in Section 1.2 above.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

In order to maintain PCI P2PE compliance it is the Merchant's responsibility to keep track of all devices and regularly manage their inventory at the minimum of once per year. Merchants must track their POI devices for the following states:

- In secure storage awaiting deployment
- Deployed/In Service
- Disabled / Out for repair
- Decommissioned and returned for secure destruction
- In transit



POI's held in storage awaiting deployment or for repair should be stored in a secure area that restricts access to authorized personnel only. In addition to the above states, the Merchant will also need to track the following items to ensure their POI's have not been tampered with:

- Physical connections to POI's
- Hardware and Firmware versions on POI's
- Dates and locations of inspections for each POI
- Name of authorized staff that performed the inspections

Below is the URL that will provide detailed instructions on reviewing Hardware and Firmware versions:

- https://www.pcisecuritystandards.org/ptsdocs/ICO-OPE-01306-EN-V2_Security_Policy_ISC_Touch_2xx-4-30132.pdf

- https://www.pcisecuritystandards.org/ptsdocs/ICO-OPE-00930-EN-V3_Security_Policy_ISC4xx-4-30125.pdf

Merchants may use an Inventory tracking spreadsheet to keep track of all their devices similar to this sample below:

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory

4. 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 3.1 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.
-

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

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

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

4.1 Installation and connection instructions

This section describes how to install the iSC250 device.

The installation procedure includes:

- Connecting the stylus
- Connecting the device
- Connecting a power supply

Connecting the Stylus

1. With the stylus cable tab towards the bottom, insert the stylus connector into the iSC250 stylus port on the back of the iSC250.



Inserting the stylus connector into the stylus port

2. Place the stylus into the cradle on the left edge of the iSC250 device, or insert it upright into the hole in the cradle.



Stylus in the cradle



Stylus upright

Connecting the Device




⚠ *Do not connect power to the iSC250 device until instructed to do so.*

1. Place the iSC250 device in front of you with the bottom of the unit facing up. Be careful not to place the device on a surface where the device can be scratched or damaged.
2. If appropriate, connect a peripheral device to the appropriate available port on the rear of the device.



iSC250 Peripheral Ports

iSC250 Peripheral Ports


Icon	Port	Description
	USB	USB 2.0 Host high speed. 5V, 500mA max. Supports peripheral USB devices.
	Audio out	3.5 mm stereo audio jack. Use to connect external speakers.
	Stylus	Use to connect the stylus.

1. Connect the Multipoint cable (RS-232 cable, Tailgate (RS-485) cable, Ethernet cable, USB cable, or magic box) into the iSC250 HOST Multipoint port. Connect the other end into the POS or PC as appropriate (refer to Table 1: iSC250 Multipoint Port below for more information).



iSC250 Multipoint Port

Table 1: iSC250 Multipoint Port

Image	Port	Description
	Multipoint port	<p>Use to connect RS-232, Tailgate (RS-485), Ethernet, USB, Universal cable, or Magic box.</p> <p>Use this port to connect host devices (POS or PC) directly. The iSC250 receives power through this connection.</p> <p>⚠ For this device to be USB-IF compliant, only use the approved USB cable from Ingenico.</p>

Connecting a Power Supply

A separate Ingenico DC power supply (ALI0081A) is required when connecting the iSC250 device via RS-232, USB (5V), and Ethernet. When the device is powered from a POS, power may be provided via a USB (12V or 24V) or RS-485 cable.

⚠ Connect the cable to the Multipoint port before connecting the device to power.

Only use the power supply provided by Ingenico.

1. If your device came with a power supply, plug the power supply connector into the jack on the Multipoint cable.



Connecting a Power Supply

2. Plug the power supply into a power outlet.

⚠ To avoid accidental damage, secure cables and power cords prior to applying power to the device.

3. The iSC250 initializes when power is applied.

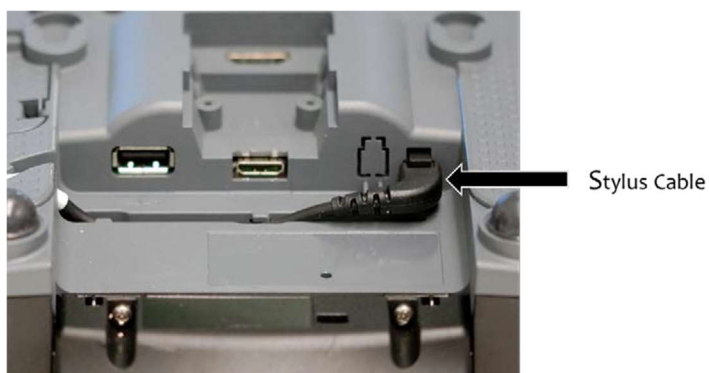
This section describes how to install the iSC480 device.

The installation procedure includes:

- Connecting the stylus
- Connecting the device
- Connecting a power supply

Connecting the Stylus

1. With the stylus cable tab towards the bottom, insert the stylus connector into the iSC480 stylus port on the back of the iSC480 as shown in figure below.



Stylus Cable Insertion

2. Place the stylus into the cradle on the left edge of the iSC480 device as shown in figure below.



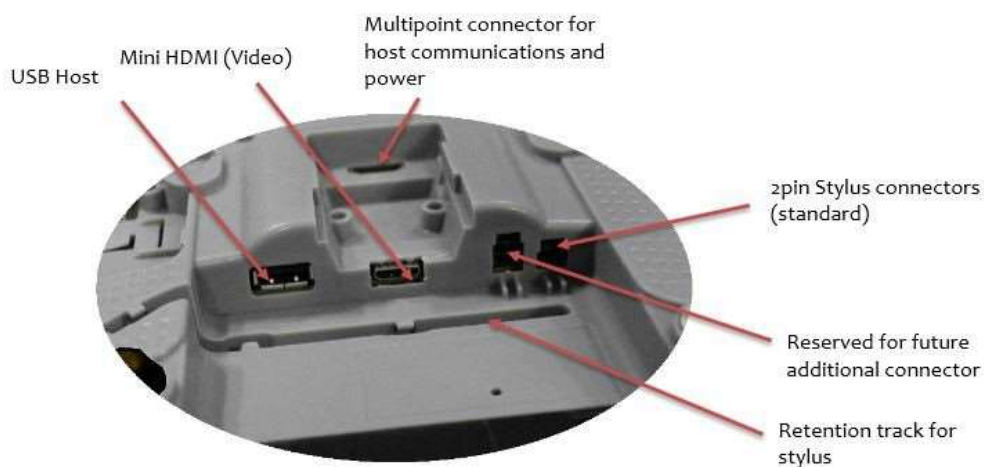
Stylus in the cradle

Connecting the Device




⚠ *Do not connect power to the iSC480 device until instructed to do so.*

The following procedure describes how to power and connect your iSC480.

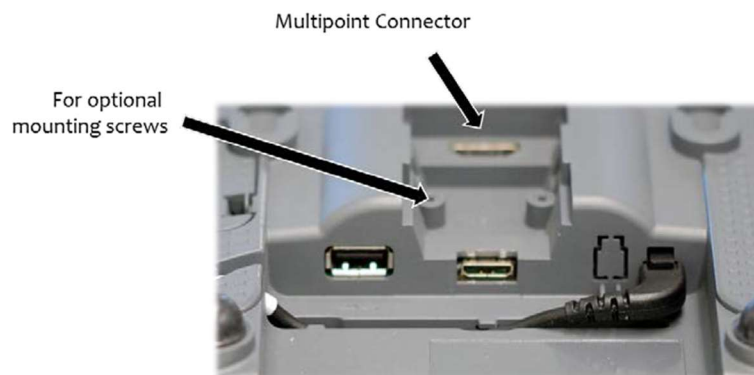
1. Place the iSC480 device in front of you with the bottom of the unit facing up. Be careful not to place the device on a surface where the device can be scratched or damaged.
2. Refer to figure below for port and connector locations on the iSC480.




iSC480 Peripheral Ports

Icon	Port	Description
	USB	USB 2.0 Host high speed, 5V, 500mA max. Supports peripheral USB devices.
	Audio out	3.5 mm stereo audio jack. Use to connect external speakers.
	Stylus	Use to connect the stylus.

1. If appropriate, connect a peripheral device to the appropriate available port on the rear of the device.
2. Connect the Multipoint cable (RS-232 cable, Tailgate (RS-485) cable, Ethernet cable, USB cable, or magic box) into the iSC480 HOST Multipoint port.



iSC480 Multipoint Port

Image	Port	Description
	Multipoint port	Use to connect RS-232, Tailgate (RS-485), Ethernet, USB, Universal cable, or Magic box. Use this port to connect host devices (POS or PC) directly. The iSC480 receives power through this connection.

A separate Ingenico DC power supply (192006210 and power cord 188413214) is required when connecting the iSC480 device via RS-232, USB (5V), and Ethernet. When the device is powered from a POS, power may be provided via a USB (12V or 24V) or RS-485 cable.

The following steps describe how to connect a power supply to the iSC480:

1. If your device came with a power supply, plug the power supply connector into the jack on the Multipoint cable.



Connecting a Power Supply

2. Plug the power supply into a power outlet.

⚠ To avoid accidental damage, secure cables and power cords prior to applying power to the device.

3. The iSC480 initializes when power is applied.

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

4.2 Guidance for selecting appropriate locations for deployed devices

The iSC250/480 device may be mounted on a flat surface, wall, or customer stand (recommended). Power may be provided from a host Point of Sale system or from an Ingenico power supply. If using an Ingenico power supply, the device must be placed close to an easily-accessible power outlet.

- *We recommend physically securing the stand to avoid theft.*
- *FDHS can provide a range of attractive stands to secure your device. Please contact your representative for further details.*

Checking the Installation Site

1. Ensure that there are NO objects close by in which cameras could be hidden.
2. Ensure that the device CANNOT be observed from outside (any window or door) during PIN entry.

When considering the prevention of theft once the device is installed, it is necessary to strike a balance between securing the asset and damaging usability and therefore, customer service. You should select a location for your POI that is secure, accessible by customers and always visible to staff.

It may be possible to attach the device to your payment station in such a way that prevents it being stolen but this will not necessarily deter the fraudulent engineer or collusive member of staff.

Therefore the physical location of the device and security of components should be considered. Can it be removed easily; are components hard wired together or physically protected to prevent easy tampering or theft?

Devices should always be placed in a location that allows the customer to use them in a manner that obscures their PIN entry from other customers and where practical should include PIN shielding. You should ensure that you treat your iSC250/480 device as you do your cash till and make sure that it is safe and secure. It is the merchants' responsibility to ensure the devices are secure at all times.

Do not place the iSC250/480 device on a PC monitor, adjacent to an electronically active security tag deactivation system, or near other sources of magnetic fields.

The iSC250/480 device must be at least 12 inches away from an electronically active type of security tag deactivation pad. There are two types of security tag deactivation systems:

An electronically active system sends out a powerful and potentially disruptive signal to deactivate the security tag. If the iSC250/480 device is placed too close to the system's pad, or placed above the pad, malfunction may occur.

A passive system is a permanent magnet type that does not send out a signal. This type does not affect the iSC250/480 device.

- ***When selecting the device location, keep in mind that you must perform daily tasks to ensure the security and compliance of your device. Refer to section 6 POI Device Tamper Monitoring and Skimming Prevention for more information.***

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

Devices should be examined at regular intervals to check for suspicious attachments and any signs that they have been altered or interfered with. It is the merchants' responsibility to check the devices for any interference, unsecure devices, or scanning devices.

Periodic physical inspections of devices should be performed to detect tampering or modification. Devices should also be examined at regular intervals to check for suspicious attachments and any signs that they have been altered or interfered with.

For POS devices located in areas away from merchant personnel, mechanism should be in place to ensure that suspicious attachments or alterations are found and investigated. It is the merchants' responsibility to ensure the devices are checked regularly.

POI's held in storage awaiting deployment or for repair should be stored in a secure area that restricts access to authorized personnel only.

- Physical connections to POI's
- Hardware and Firmware versions on POI's
- Dates and locations of inspections for each POI
- Name of authorized staff that performed the inspections

You should also perform the following for devices that cannot be secured:

- Secure devices in a locked room, drawer or cabinet when not in use.
- Assign responsibility to specific individuals when device is in use.
- Observe devices at all times.
- Sign devices in/out, etc.

For lost or stolen devices:

How do I report a stolen device?

You can report a device as stolen to one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com

- Ingenico: (800) 435-3014 or CSSRMARequesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

To address the issues of unsecured devices being stolen and illegally modified in the field, the iSC250 PIN pad features an optional anti-theft system. The Kensington lock mechanism is simple and universal, with key or code lock options available.

1. Secure the loop end of the cable to a permanent structure near the device.
2. Insert the cable into the secure lock port.
3. Lock the cable to the device using the key provided or by scrambling the number code.



Kensington anti-theft key lock

Additional Security

The iSC 250 has the optional use of screws for additional security. Screws can be used to secure the Multipoint cable and the access door. The iSC250 uses standard M2.5 x8 screws.

Securing the Multipoint Cable

1. Place the iSC250 device in front of you with the bottom of the unit facing up. Be careful not to place the device on a surface where the device can be damaged.
2. The Multipoint cable should be connected to the back of the PIN pad. See 2.4 Connecting the Device on page 11 for more information.
3. Screw in two standard M2.5 x8 screws on either side of the Multipoint cable.



Securing the Multipoint port

Securing the Access Door

1. Place the iSC250 device in front of you with the bottom of the unit facing up. Be careful not to place the device on a surface where the device can be scratched or damaged.
2. Ensure that the access door is securely closed.
3. Screw in one standard M2.5 x8 screw on the access door.



Securing the access door

Securing the iSC480 Device

Anti-Theft System

To address the issues of unsecured devices being stolen and illegally modified in the field, the iSC480 PIN pad features an optional anti-theft system. The Kensington lock mechanism is simple and universal, with key or code lock options available.

Secure the loop end of the cable to a permanent structure near the device.

Insert the cable into the secure lock port.

Lock the cable to the device using the key provided or, if a combination lock is used, by scrambling the number code.



Kensington Anti-theft Key Lock

Additional Security

If mounted on a stand, the iSC480 can also be secured using security screws for optional added security. Variations of security screw head styles may be used to further increase security (e.g., Key Rex screws). M2.5 x 8mm screws can be used to secure the Multipoint cable and the access door.

Securing the Multipoint Cable

Place the iSC480 device in front of you with the bottom of the unit facing up. Be careful not to place the device on a surface where the device can be scratched or damaged.

The Multipoint cable should be connected to the back of the PIN pad. Refer to figure below.



Securing the Multipoint port

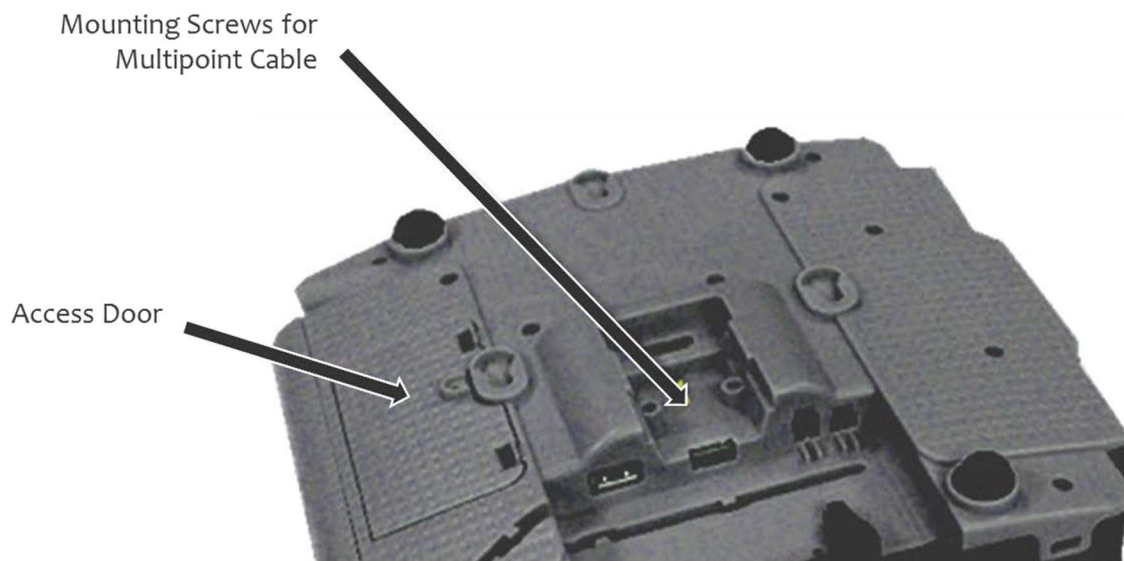
It's recommended to screw in two standard M2.5 x8 screws on either side of the Multipoint cable.

Securing the Access Door

Place the iSC480 device in front of you with the bottom of the unit facing up. Be careful not to place the device on a surface where the device can be scratched or damaged.

Ensure that the access door is securely closed.

Screw in one standard M2.5 x8 screw on the access door.



Securing the access door

5. POI Device Transit

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

Each party involved in organizing the shipping should follow these security requirements:

- Ensure that devices are sealed with tamper-proof tape prior to shipment and during shipping process. This can be obtained at an office supply store
- Wherever the device is stored, it should be secured in an access-controlled area with sealed tamper-proof packaging
- Shipments are transported using Customs-Trade Partnership Against Terrorism (C-TPAT) approved common carriers such as FedEx, UPS, DHL or merchant's approved shipping carriers.
- Advance Ship Notice (ASN) including device serial numbers shall be provided to the receiving company at time of physical shipment via electronic method
- Receiving company should always verify physical receipt (part number, serial numbers, qty, etc.) with separately provided ASN information to ensure no en-route tampering
- Tracking number must be provided to track shipment status including locations at any given time
- Inspection should be conducted upon receiving the device (see Section 2.2 for instructions). If the device is tampered, it must be returned

Physically secure POI devices in your possession, including devices:

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

5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only

Ingenico terminals used as part of the First Data TransArmor P2PE Solution can only be deployed by First Data Hardware Services or Ingenico.

Do not purchase any Ingenico devices online or from an unauthorized P2PE Solution Provider KIF. Use authorized personnel or PCI Qualified Integrator Resellers to install and activate Ingenico POI devices. To request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

6. POI Device Tamper & Modification Guidance

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

Additional guidance for inspecting POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants*, available at www.pcisecuritystandards.org.

Perform the following tasks daily to ensure the security and compliance of your device:

Ensure that no attempts have been made to tamper with the device, using the following method:

1. Check that there is NO external damage to the device, particularly around the keypad, display, and reader areas.
2. Check that the keypad is firmly in place.
3. Ensure that there are NO additional cables protruding from the device or associated equipment.
4. Check that there are NO holes drilled into the device's housing.
5. No changes to the resistance when inserting or removing a card from the EMV smart card slot or swiping a card through the magnetic stripe reader.



Ensure that this sticker is intact on the iSC250



Ensure that this sticker is intact on the iSC480



Inspect for case modifications, new stickers covering holes or signs of case separation. This photo illustrates a snap-on skimmer.

Inspect the EMV reader slot and MSR slot for obstructions and alterations



Inspect for case modifications, new stickers covering holes or signs of case separation

6.2 Instructions for responding to evidence of POI device tampering

The iSC250/480 device detects any “tampered state”. In this state the PIN pad will repeatedly flash the message **“Alert Irruption!”** and further use of the PIN pad will not be possible. If you observe the **“Alert Irruption!”** message, you should follow the merchant’s device tamper procedure and contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

What does it mean if my device has been tampered?

This can happen for a number of reasons, such as a credit card skimmer is applied to the device or someone has attempted to break the device open. This can also happen if the device is dropped hard enough during shipment or by the merchant or a customer.

What should I do if my device has been tampered?

Follow the merchant’s device tamper procedure and request a return (RMA) for a POI that has been tampered with or defective, please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com

- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

If First Data has contacted the Merchant to inform them of encryption errors, OR the merchant experiences an **“Alert Interruption!”** the POI must be taken out of service immediately and replaced.

To request a swap (RMA) for a POI that has been tampered with or defective, follow the merchant’s device tamper procedure and please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

This section covers basic troubleshooting.

To request a swap (RMA) for a POI that has been tampered with or defective, follow the merchant’s device tamper procedure and please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

Magnetic Card Reader Does Not Work Properly

1. Slide the card through the magnetic stripe reader
2. Swipe the card at a faster or slower steady speed.
3. Swipe the card in a different direction.
4. Inspect the magnetic stripe on the card to make sure it is not scratched or badly worn.
5. To determine if the problem is with the card:
 - a. If your host device has a magnetic stripe reader, try swiping the card there.
 - b. If you have another working iSC250/480 device, try swiping the card there.
6. If there is still a problem, contact your internal Help Desk.

No Information is Visible on Screen

7. Make sure the iSC250/480 device cable is fully inserted and secured into the device.

8. Restart the device.
9. If you have another working iSC250/480 device, swap the devices to determine if the problem is with the device, cable, POS, or power supply.
10. Replace the cable.
11. Reset the host by turning it off and back on again.

Checking the Device's Integrity

Ensure that no attempts have been made to tamper with the device, using the following method:

12. Check that there is NO external damage to the device, particularly around the keypad, display, and reader areas.
13. Check that the keypad is firmly in place.
14. Ensure that there are NO additional cables protruding from the device or associated equipment.
15. Check that there are NO holes drilled into the device's housing.

Alert Irruption!

The iSC250/480 device detects any "tampered state". In this state the PIN pad will repeatedly flash the message **"Alert Irruption!"** and further use of the PIN pad will not be possible. If you observe the **"Alert Irruption!"** message, you should follow the merchant's tamper device procedure and contact one of the following immediately:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

9. Additional Guidance

9.1 Additional Solution Provider Information

What should I do if I do not find the answer to my question or want to leave feedback?

Please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorProductTeam@fiserv.com
- Ingenico: (800) 435-3014 or CSSRMAResquesting@ingenico.com
- ScanSource: (800) 944-2439 or paymentsolutions@scansource.com
- POS Portal: (855) 838-4611, option 2 or support@posportal.com

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices

Below is the URL that will provide detailed instructions on reviewing Hardware and Firmware versions:

- https://www.pcisecuritystandards.org/ptsdocs/ICO-OPE-01306-EN-V2_Security_Policy_ISC_Touch_2xx-4-30132.pdf
- https://www.pcisecuritystandards.org/ptsdocs/ICO-OPE-00930-EN-V3_Security_Policy_ISC4xx-4-30125.pdf