First Data®

TransArmor®

Point-to-Point Encryption (P2PE)
Instruction Manual

Equinox Luxe 8500i
Version 1.0

First Data.

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	First Data TransArmor P2PE Solution – PKI/RSA
Solution reference number per PCI SSC website:	*2019-00541.003*

1.2 Solution Provider Contact Information	
Company name:	*First Data*
Company address:	*5565 Glenridge Connector, Atlanta, GA 30342*
Company URL:	*www.firstdata.com*
Contact name:	*Marco Mabante*
Contact phone number:	*(404) 890-3666*
Contact e-mail address:	*TransArmorP2PE@firstdata.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 Point of Interaction (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.

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 Equinox Luxe 8500i the PCI PTS expiry date is April 30, 2026. This means you could use the device until April 30, 2031. Be aware that the hardware manufacturer may end support for the device earlier than April 30, 2031.

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:	*Equinox Payments*
POI device model name and number:	*Luxe 8500i*

Hardware version #(s):	*LX85xx-0100xx*
Firmware version #(s):	*LXMQX1-0100xx*
PCI PTS Approval #(s):	*4-70030*

<Add additional tables for each POI device type used in this solution, if applicable>

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)
N/A	N/A	N/A	N/A	N/A	N/A

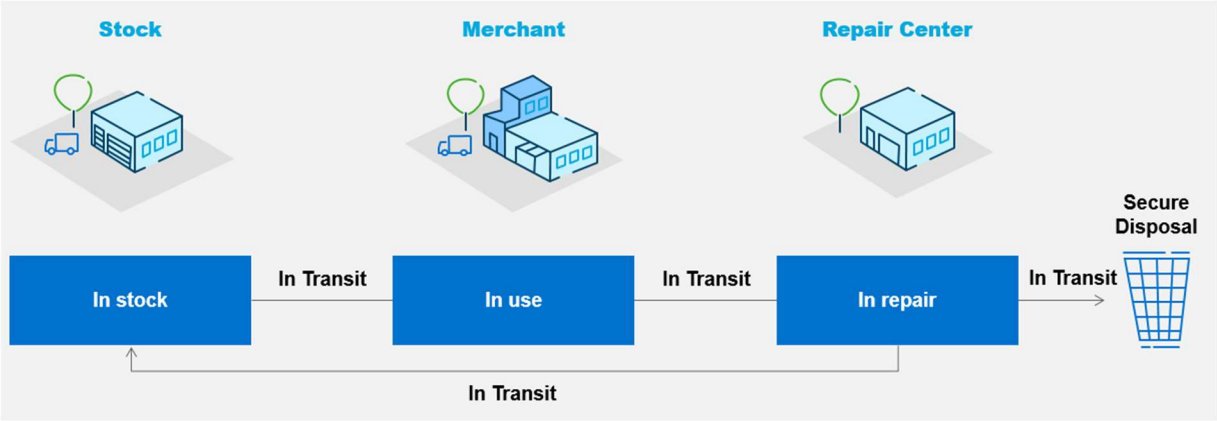
<Add additional rows for each application on a POI device used in this solution, if applicable>

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 *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/4-70030_950222-203E_PCI_PTS_POI_Security_Policy_v21_20170830-1510933485.17142.pdf

Merchants may also 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

First Data.

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

First Data.

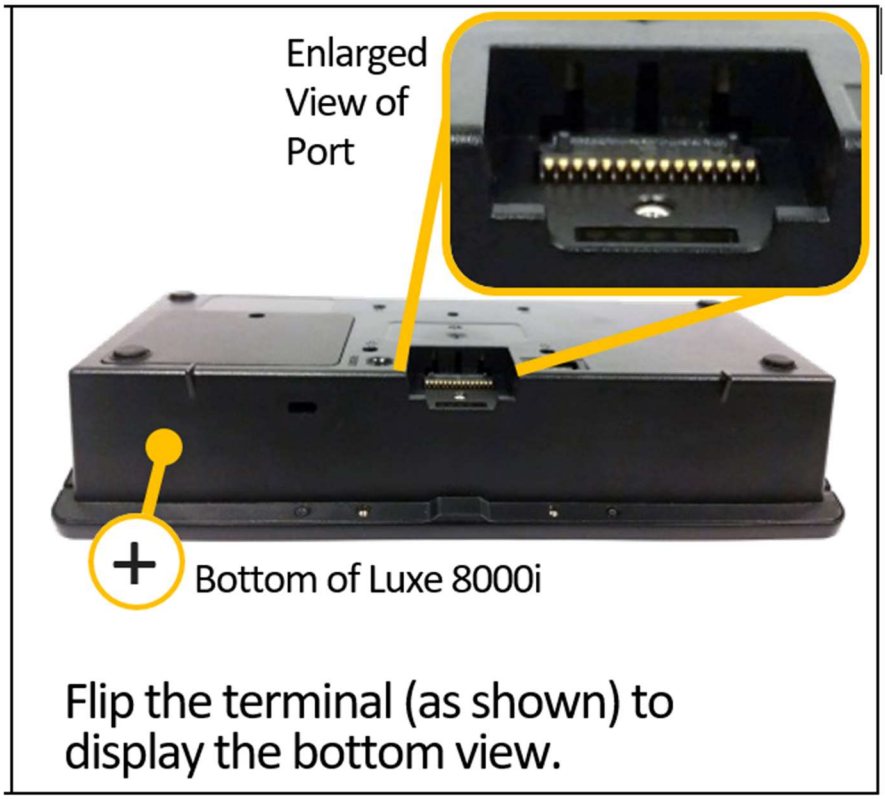
3.1 Installation and connection instructions

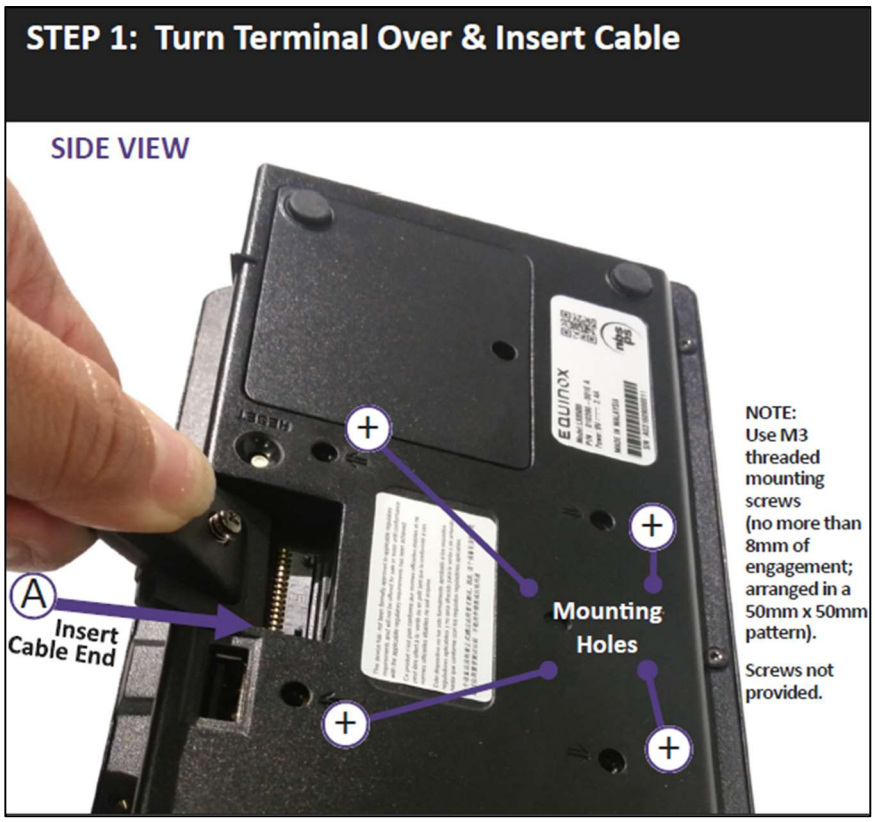
This section describes how to install the Luxe 8500i device.

The installation procedure includes:

- Connecting the communications cable/power supply

Connecting the Communications/Power Supply





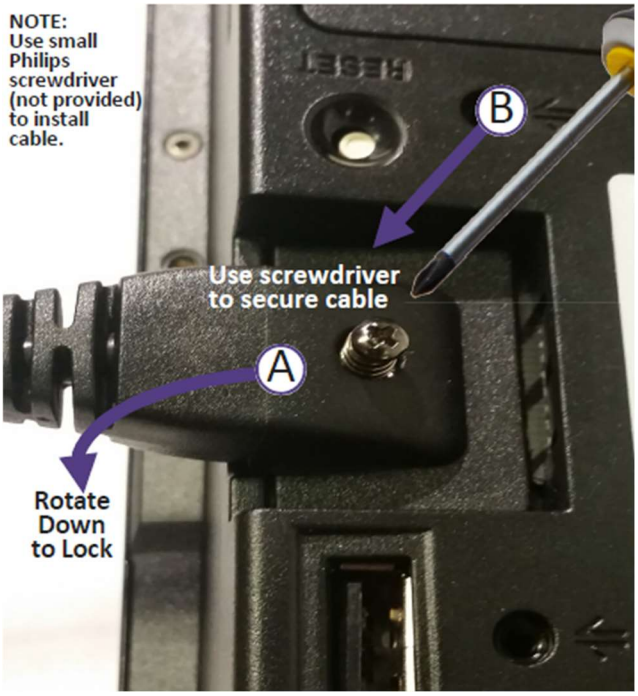
First Data.

STEP 2: Angle and Push Cable In Against Terminal

ENLARGED VIEW

STEP 3: Rotate Cable Down & Press Firmly to Lock in Place, then Screw to Secure

ENLARGED VIEW



STEP 4: Turn Terminal Over & Connect Power Source

NOTE: To remove cable, disconnect power source and then turn the terminal over. Use screwdriver to remove the screw from the cable end. Push cable end in (against the terminal), then lift (rotate) cable up to remove.

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

The Luxe 8500i 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 Equinox power supply. If using an Equinox power supply, the device must be placed close to an easily-accessible power outlet.

- *We recommend physically securing the device 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 security cameras focusing on the device.
2. Ensure that there are NO objects close by in which cameras could be hidden.
3. 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 POS 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. Secure mounts should be used to minimize opportunities for theft but care must be taken to balance security needs with the requirements of the Americans with Disabilities Act (ADA).

Where the needs of the ADA can be met with the device in a mounting bracket, consideration should be given to modifying the bracket from a 'support only' mechanism to one that physically restrains the device reducing the potential for a 'smash and grab' type theft.

Where locking the device into the mounting bracket would contravene the ADA, consideration should be given to connecting a security wire cable to the device and the mounting bracket so giving a degree of movement but maintaining security against theft.

You should ensure that you treat your Luxe 8500i 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 Luxe 8500i device on a PC monitor, adjacent to an electronically active security tag deactivation system, or near other sources of magnetic fields. The Luxe 8500i device must be at least 12 inches away from an electronically active type of security tag deactivation pad. This is specifically defined as:
    - An electronically active system that sends out a powerful and potentially disruptive signal to deactivate the security tag. If the Luxe device is placed too close to the system's pad or placed too close above the pad, malfunction may occur.

- ***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 5 POI Device Tamper Monitoring and Skimming Prevention for more information.***

3.3 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 be 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.

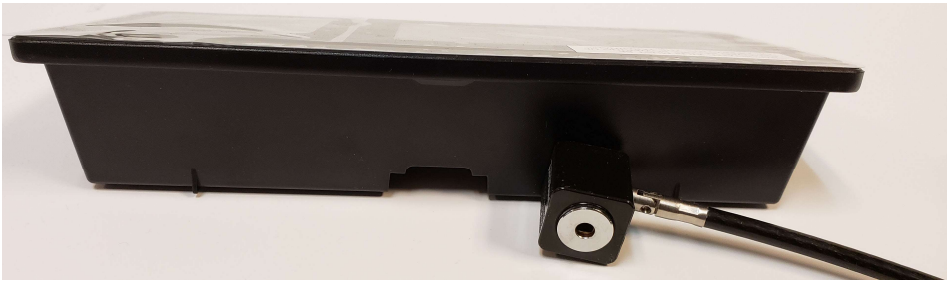
For lost or stolen devices:

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: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

To address the issues of unsecured devices being stolen and illegally modified in the field, the Luxe 8500i PIN pad features an optional anti-theft system. The Kensington lock mechanism is simple and universal, with key or code lock options available.



Kensington anti-theft lock attached to Luxe

Luxe anti-theft lock hole

Kensington anti-theft key lock

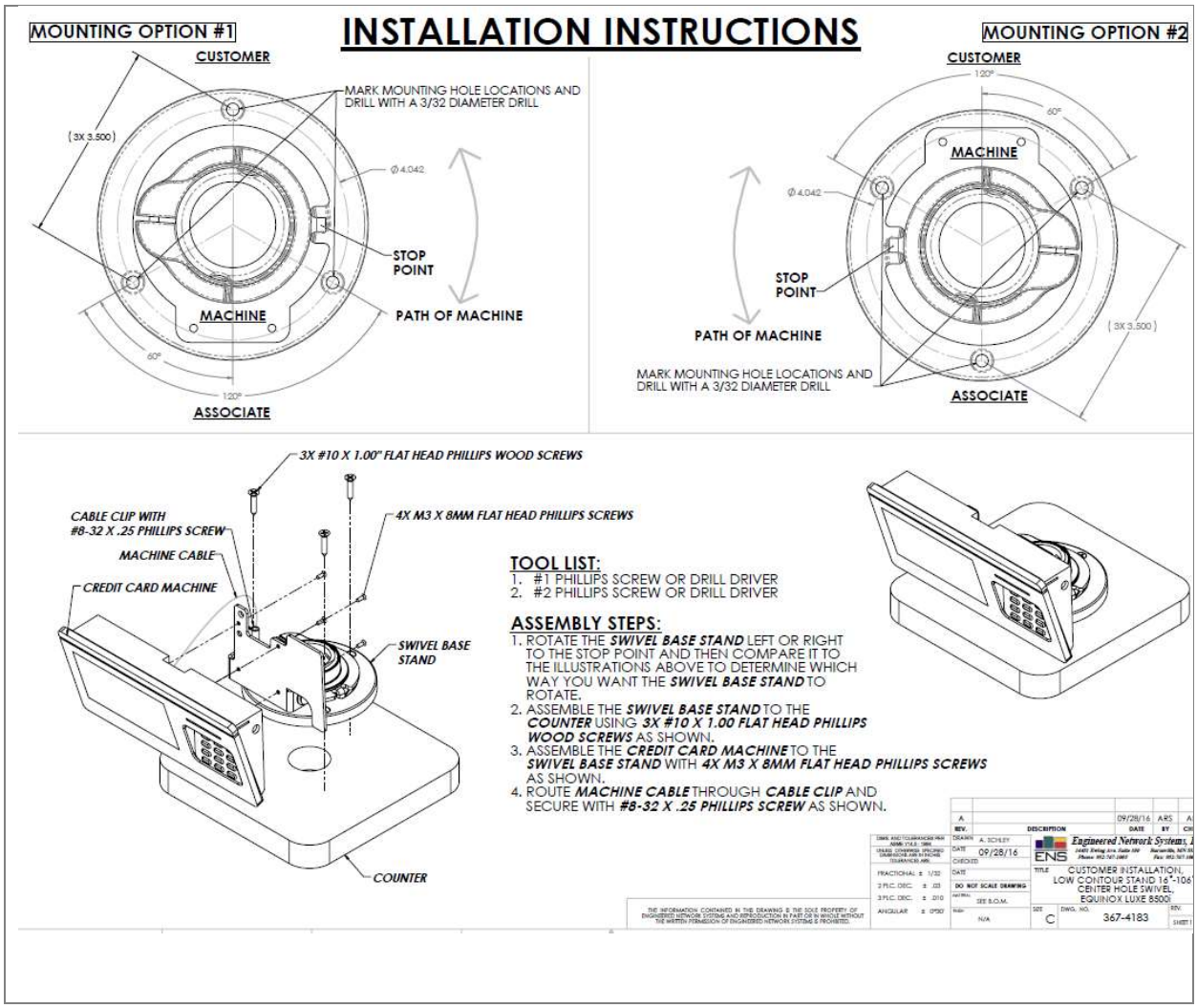
Securing the anti-theft cable

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.

Additional Security

We highly recommend that you use a secure mounting device like the ENS stand (part # 367-4183) which is available from First Data Hardware Services.

If mounted on a stand, the Luxe 8500i 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). Follow instructions from the stand manufacturer to install.



4. POI Device Transit

4.1 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 or DHL
- 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 5.3 for instructions). If the device is tampered, it must be returned

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

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

Do not purchase any Equinox devices online or from an unauthorized P2PE Solution Provider KIF. Only use PCI Qualified Integrator Resellers to install and activate Equinox 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: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

5. POI Device Tamper Monitoring and Skimming Prevention

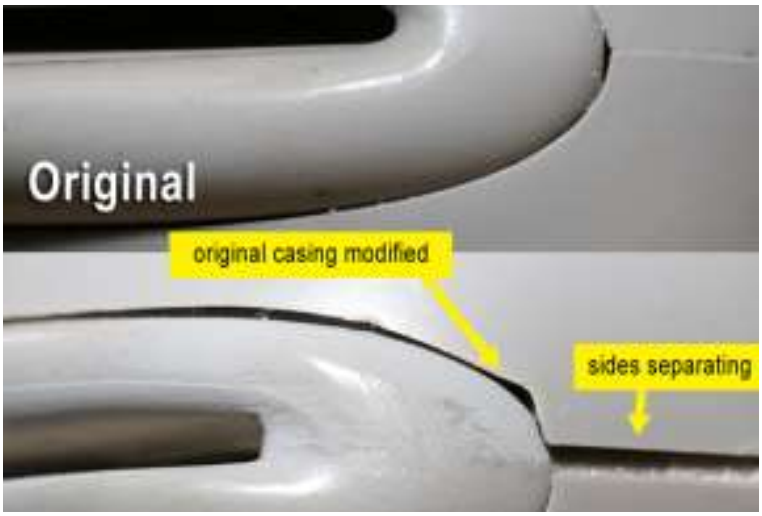
5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

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.

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:

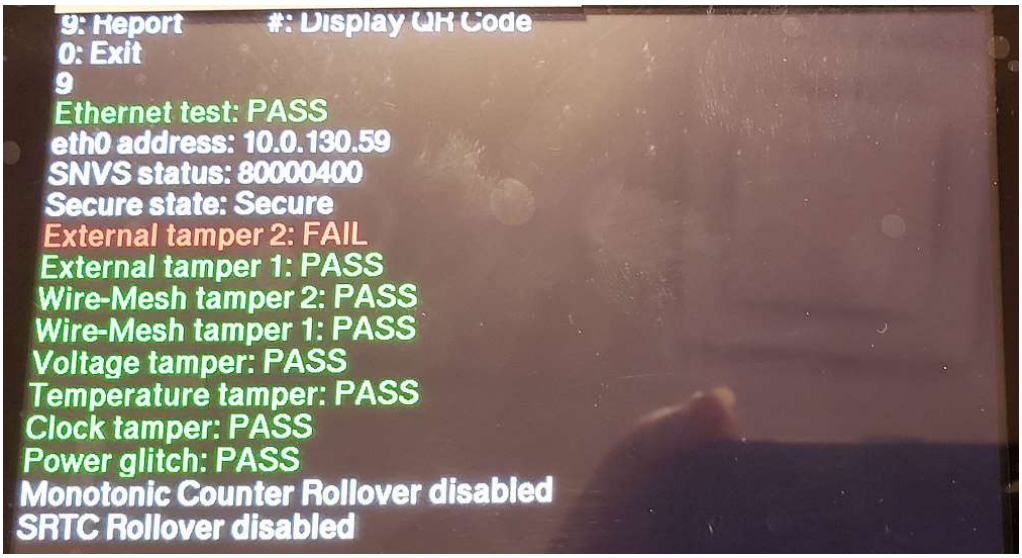
1. Check that there is NO external damage to the device, particularly around the keypad, display, and reader areas.
2. Check that the keypad is firmly in place.
3. Ensure that there are NO additional cables protruding from the device or associated equipment.
4. Check that there are NO holes drilled into 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.



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

5.2 Instructions for responding to evidence of POI device tampering

Your Luxe device detects any “tampered state”. In this state the PIN pad will repeatedly flash the message “**!!!Security Alert!!!**” and further use of the PIN pad will not be possible.



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?

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

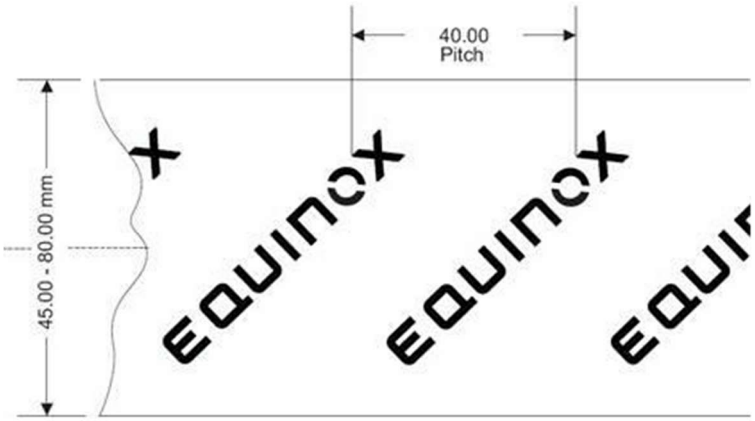
- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com

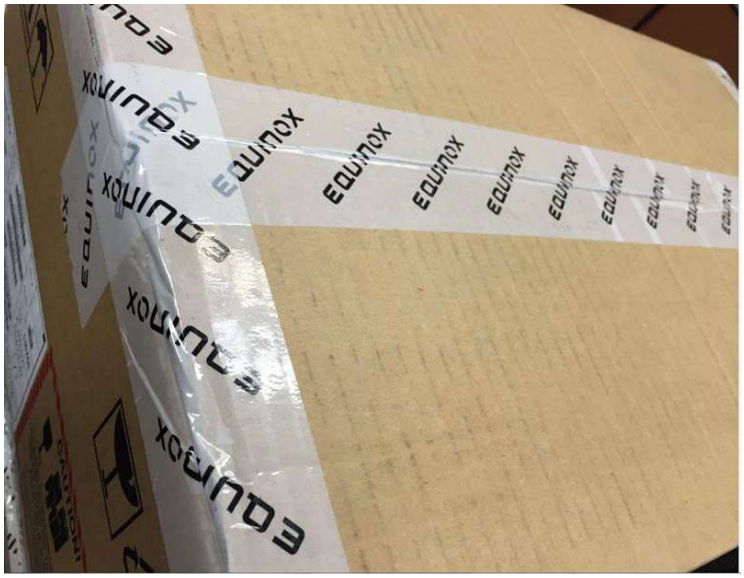
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

5.3 Instructions for confirming 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 immediately contact First Data or Equinox Customer Support to report.

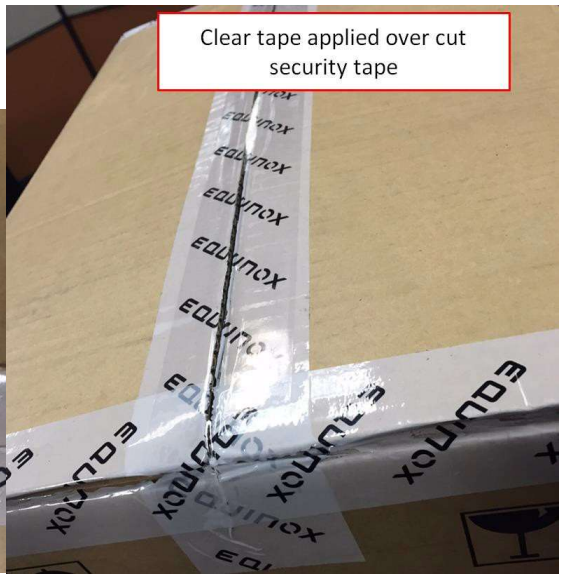
Equinox shipping tape has a white background with black “EQUINOX” logo printing. See dimensional specifications below.





Standard Overpack Carton (sealed)

Standard Overpack Carton (re-sealed with new tape)



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

1. Photograph and retain pictures of the package (damaged or not).
2. Confirm the serial number(s) of the devices against the serial numbers listed on the Advance Ship Notice (ASN) the merchant should have received from the KIF 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: TransArmorP2PE@FirstData.com

Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

3. Remove the contents from the box. The box contains the following items:
   a. Luxe 8500i device
   b. Screen cleaner
   c. Installation Guide:
4. Remove the protective film from the graphical display screen.
5. Save the carton and packing material for repackaging or moving the device in the future.

The following is an example of content inside the box:

Cables and power supply will be shipped separately specifically to suit the connectivity requirements of the merchant.

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: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

First Data.

5.4 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 Equinox devices.

Merchants should use PCI Qualified Integrator Resellers (QIR) to install their devices using this P2PE Implementation 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: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

6. Device Encryption Issues

6.1 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 a "**!!!Security Alert!!!**" the POI must be taken out of service immediately and replaced.

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: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

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

You may choose to opt-out of using the protection of the P2PE solution. However, this involves transitioning you to a different solution that is not P2PE validated. If you choose to opt out, understand you accept the following responsibility:

1. The security impact to your account data and potential risks associated with processing transactions without P2PE protection.

2. Responsibility for implementing alternative controls to protect account data in lieu of the P2PE solution

3. That you are no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution

4. You must advise your acquirer that you are no longer using the P2PE solution

5. That processing transactions without P2PE protection may impact your PCI DSS compliance validation and you should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected.

First Data.

To request to opt-out please contact one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com

7. POI Device Troubleshooting

7.1 Instructions for troubleshooting a POI device

This section covers basic troubleshooting.

To request a return (RMA) for a POI that has been tampered with or defective, please contact 1 of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.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.

1. Inspect the magnetic stripe on the card to make sure it is not scratched or badly worn.
2. 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 Luxe device, try swiping the card there.
3. If there is still a problem, contact your internal Help Desk.

No Information is Visible on Screen

1. Make sure the Luxe cable is fully inserted and secured into the device.
2. Restart the device
3. If you have another working Luxe device, swap the devices to determine if the problem is with the device, cable, POS, or power supply.
4. Replace the cable.
5. 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:

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.

First Data.

!!!Security Alert!!!

Your Luxe device detects any "tampered state". In this state the PIN pad will flash the message **"!!!Security Alert!!!"** and further use of the PIN pad will not be possible. If you observe the **"!!!Security Alert!!!"** message, you should contact the PIN pad helpdesk immediately or one of the following:

- Your Banking/Acquiring Relationship or Account Manager
- First Data TransArmor: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com

8. 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: TransArmorP2PE@FirstData.com
- Equinox: (877) 497-3726 or RMArequests@equinoxpayments.com