Feature Focus Guide: Point-to-Point Encryption

Core Product: Aloha Quick Service, Aloha Table Service Last Updated: April 3, 2025

Contents

About Point-to-Point Encryption (P2PE)	4
P2PE overview for TSYS (visa net)	5
P2PE overview for First Data (CES)	7
Hardware support for P2PE	9
Additional documentation	11
Configuring Aloha EDC for Point-to-Point Encryption	11
Defining additional EDC settings	11
Configure a CES (First Data) processor for P2PE	13
Assigning cards to processors	15
Configure a TSYS (Visa Net) processor for P2PE	16
Configuring Aloha POS system for Point-to-Point Encryption	17
1. Enable P2PE in store settings	17
2. Assign a PIN pad device to a terminal	18
3. Create an integrations profile	20
4. Create a P2PE tender	21
5. Add a P2PE tender to a panel for QS	24
6. Limit access to card tenders from the FOH (optional)	25
Refresh the data	26
Perform the RegiStart process for First Data (CES)	26
Using Point-to-Point Encryption functionality	28

NCR V:YIX

© 2023 NCR Voyix. All rights reserved. NCR Voyix – Confidential Use and Disclose Solely Pursuant to Company Instructions

Copyright and Trademark Information

The products described in this document are proprietary works of NCR Voyix.

NCR Voyix is a registered trademark of NCR Voyix.

Aloha is a registered trademark of NCR Voyix.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are the property of their respective owners.

It is the policy of NCR Voyix to improve products as technology, components, software, and firmware become available. NCR Voyix, therefore, reserves the right to change specifications without prior notice.

Not all features, functions and operations described herein are available in all parts of the world. In some instances, photographs are of equipment prototypes; therefore, before using this document, consult with your NCR Voyix representative or NCR Voyix office for the most current information.

© 2023 NCR Voyix Atlanta Georgia USA www.ncrvoyix.com All Rights Reserved



© 2023 NCR Voyix. All rights reserved. NCR Voyix — Confidential Use and Disclose Solely Pursuant to Company Instructions

Revision Record

Date	Version #	Description
Prior to 11/23/2022	v12.3+	Implemented support for P2PE for TSYS (Visa Net) and First Data (CES) processors.
11/23/2022		Converted document to use new templates.
01/12/2023		Updated front cover and back page to reflect new NCR branding.
06/13/2024		Updated document to reflect NCR Voyix branding.
04/03/2025		Added statement clarifying P2PE is optional and is not received just by upgrading but requires deliberate implementation.



About Point-to-Point Encryption (P2PE)

P2PE at a Glance	
Core Product	Aloha Quick Service, Aloha Table Service, Aloha EDC
Complementary Products	No
Separate License Required?	No
Other References	Aloha Quick Service Reference Guide, Aloha Quick Service Reports Guide, Aloha EDC User Guide

Effective with Aloha[®] Point-of-Sale (POS) system v12.3 and EDC v12.3, or later, Point-to-Point Encryption (P2PE) provides sites regulated by Payment Card Industry Data Security Standards (PCI DSS) with the potential to reduce their compliance obligations. Using P2PE removes cardholder data from your environment by encrypting the data at the moment of capture, without the ability to decrypt. When the data is sent to a secure on-premises vault or the payment processor, Format-Preserving Encryption (FPE) is enforced. In the case of First Data, (CES), a token is provided to the Aloha system in place of the cardholder data.

Once you implement P2PE functionality, guests and employees can only process credit, debit, and EBT payment cards with the PIN pad device. Any attempt to slide one of these cards with an MSR attached to a POS terminal, results in an error that guides you to use the PIN pad device instead. For other types of payment cards, such as gift cards, you still use a magnetic stripe reader (MSR).

In summary, the PIN pad device supports only the following transactions:

- Credit cards
- Debit cards
- EBT cards

You must still use a magnetic stripe reader for these features:

- Employee MAG cards
- Gift cards

P2PE is an optional feature and is not implemented by default when you upgrade to an EDC version in which it is supported. Should you decide to implement P2PE, it is necessary to work with TSYS or First Data CES to ensure all requirements are in place and you order and receive the PIN pad devices preloaded with encryption software specific to your sites. If you currently pass payment information to the Aloha POS system from another Aloha application, such as Aloha Orderman, you cannot implement a P2PE solution at this time.



P2PE functionality is certified with the following processor and hardware combinations within the Aloha system.

Processor:	Encryption Platform:	Hardware Device:	Communication Type
TSYS (aka Visa Net)	Voltage SecureData™	Ingenico iPP350 PIN pad device	USB only.
First Data (aka CES)	TransArmor	VeriFone VX820 PIN pad device	USB only.
The above PIN pad devi	ces are EMV-canable devi		

paa aevices are EMV-capable devices.

Before you configure Aloha EDC for P2PE. There are some existing EDC functionality that is not supported with P2PE. These features are:

- You cannot use multiple processor indexes in EDC.
- You cannot use more than one processor at the site, such as for split dialing. All payment cards must be processed with the same processor. For example, your P2PE solution does not work if you have all your MasterCard tenders processing via CES and all your Visa tenders processing via TSYS.

This document references industry standard verbiage. To help you, you should be aware of the following glossary of terms:

Acronym	Term
P2PE	Point-to-Point Encryption
PCI DSS	Payment Card Industry Data Security Standards
FPE	Format-Preserving Encryption
PAN	Primary Account Number
AES	Advanced Encryption Standard

P2PE overview for TSYS (visa net)

You can use P2PE functionality with the TSYS (Visa Net) processor with the Ingenico iPP350 PIN pad device. Cardholder data is captured and encrypted using the Voltage Security encryption and then sent to TSYS for decryption, using the Voltage SecureData Payments host. TSYS then sends the unencrypted card data to the payment brands and issuing banks for further processing over a secure connection. Once TSYS receives a response from the card payment brands and issuing bank, TSYS sends the response back to the Aloha POS system.

You must enter all cardholder data on the iPP350 device. If the guest or employee attempts to swipe a card at the POS terminal, an error appears, instructing them to use the PIN pad device instead.



Cardholder data is never in clear text in the Aloha environment. Only TSYS can decrypt the cardholder data for further processing.

R Note

Keep in mind, this is not a PCI P2PE validated solution; however, the merchant's PCI QSA or the acquirer shall determine the PCI scope reduction. Refer to the NCR Aloha POS Data Security Implementation Guide for more information regarding this solution. We encourage Aloha customers to read it prior to implementation.



Figure 1 TSYS and Voltage P2PE Transaction Flow

Voltage Security offers an FPE that keeps credit card numbers protected without the need to modify or alter their format or structure. FPE is a form of strong encryption that uses the Advanced Encryption Standard (AES) algorithm to protect cardholder data according to industry standards, while preserving the original data syntax and thus minimizing the impact on existing systems. Voltage uses AES FFX-mode encryption to protect data.

Voltage provides a software development kit (SDK) to Aloha that allows the use of two encryption methods: TEP1 (whole track encryption) and TEP2 (structure preserving encryption). Aloha uses TEP2 to allow card processing through Aloha EDC and for reporting purposes.



© 2023 NCR Voyix. All rights reserved. NCR Voyix — Confidential Use and Disclose Solely Pursuant to Company Instructions Please refer to <u>http://www.voltage.com</u> for more information.

Here are some examples of how Voltage encrypts cardholder data:

• PAN – Primary Account Number - The first six and the last four digits are kept intact, while the remaining digits are encrypted:



P2PE overview for First Data (CES)

You can use P2PE functionality with the First Data (CES) processor and the Verifone VX820 PIN pad device. Cardholder data is captured and encrypted using the First Data TransArmor security encryption and then sent to First Data for decryption at the TransArmor vault. First Data then sends the unencrypted cardholder data to the payment brands and issuing banks for further processing over a secure connection. Once First Data receives a response from the card payment brands and issuing



bank, First Data sends the response back to the Aloha POS system with a token that replaces the account number (PAN). A token ID is listed in the .txn file, for reference.

Note

Keep in mind, this is not a PCI P2PE validated solution; however, the merchant's PCI QSA or the acquirer shall determine the PCI scope reduction. Refer to the NCR Aloha POS Data Security Implementation Guide for more information regarding this solution. We encourage Aloha customers to read it prior to implementation.



Figure 2 First Data and TransArmor P2PE Flow

TransArmor and VeriFone offer an FPE that keeps cardholder numbers protected without the need to modify or alter their format or structure. FPE is a form of strong encryption that uses an Advanced Encryption Standard (AES) 128-bit algorithm to protect cardholder data according to industry standards, while preserving the original data syntax and thus minimizing the impact on existing systems.

First Data partners with VeriFone to provide merchants a format-preserving encryption, which secures cardholder data on a tamper-resistant device before it enters your environment in a format that other applications interpret as valid cardholder data.



© 2023 NCR Voyix. All rights reserved. NCR Voyix — Confidential Use and Disclose Solely Pursuant to Company Instructions Here are some examples of how TransArmor encrypts cardholder data:



The algorithm encrypts data so the output is in the same length and character set as in the input. This is beneficial for bin routing in Aloha environments. TransArmor then provides a token to replace sensitive data post authorization. A PAN is sent to a centralized First Data server called a "vault" to tokenize a transaction. After authorization, TransArmor generates a unique and random token number for use in place of a PAN. In the Aloha system, only the last four digits of the credit card number are stored.



Please refer to the following link for more information:

http://www.firstdata.com/en_us/products/merchants/security-and-fraud-solutions/encryption-and-to kenization.html

Hardware support for P2PE

Effective with Aloha v12.3, you can use the Ingenico iPP350 and VeriFone VX820 PIN pad devices to process credit, debit, EBT cash, and EBT food cards. These devices support a card slide, card tap, or manual entry.

) Tip

You cannot use a combination of Ingenico and VeriFone devices at the site. You also cannot use one of these devices with a lower model number, such as VeriFone SE1000.



The Ingenico iPP350 is used with the Voltage TSYS P2PE solution, which requires a USB driver. You can find the driver on Aloha Update and more information is found in RKS ID 14728 USB Driver for Ingenico iPP350.



Figure 3 Ingenico iPP350 PIN Pad Device

The VeriFone VX820 is used with the TransArmor First Data P2PE solution, which uses a USB driver. You can find the driver on Aloha Update and more information is found in RKS ID 14727 USB Driver for VeriFone VX820.



Figure 4 VeriFone VX820 PIN Pad Device



Additional documentation

You can find additional documentation at these locations:

Documentation:

- RKS ID14736 How to Change a Communication Type to USB on the Ingenico iPP350.
- RKS ID 14729 Setting the VX820 to Use USB as the Communication Type.

For the Ingenico iPP350 PIN pad:

• <u>http://ingenico.us/terminals/iPP350/.</u>

For the VeriFone VX820 PIN pad:

• http://www.verifone.com/products/hardware/pin-pad/vx-820.

Configuring Aloha EDC for Point-to-Point Encryption

After you configure the Aloha POS system, you must configure Aloha EDC for P2PE.

Defining additional EDC settings

Additional EDC options include defining the maximum refund amount for credit cards and defining how many times an SSL attempts to connect, enabling Store and Forward, and more.

1. Select Maintenance > Electronic Draft Capture > EDC Settings.

EDO O Minana	
EDC Settings	
EDC Settings: 1 EDC Settings	~
EDC Settings Custom	
Settings	
Number	1
Name	EDC Settings
Credit card refund limit	200.00
Retry SSL every this many connections	30
Offline recovery	
Mock authorize until offline transactions are processed	
Start live processing with this many queued transactions	0
Store and forward	
Enable store and forward	
Authorization timeout threshold	0
Number of seconds to wait before attempting recovery	30
Floor for transaction amount	0
Maximum number of offline transactions	0

Figure 5 Electronic Draft Capture - EDC Settings

 Under the 'Settings' group bar, type the maximum dollar amount, up to \$9999.00, you can refund a credit card. Use this function to prevent employees from entering incorrect amounts accidentally. For example, '200.00.'



- 3. Type the **consecutive number of attempts** that Aloha EDC uses to retry SSL connection. **Is Why is this in two places? (see Business > Store > refund...***
- 4. Under the 'Offline recovery' group bar, select Mock authorize until offline transactions are processed to allow the Front-of-House (FOH) to perform 'mock' authorizations for sales less than the pre-defined amount if the EDC server is down. When the FOH loses connection to the EDC server and attempts to do a credit card authorization, the system approves the authorization and the transaction is held as an .spl (spooling) file in the EDC directory. When the connection is restored, the EDC program scans all spooling files to send them for approval.

Caution

The monies from spooling files are not realized until EDC receives an authorization and settles a batch

The 'mock authorization' mode is only activated when the Back-of-House (BOH) is down. If the BOH is up, 'mock authorizations' do not occur, even if the EDC program is turned off and is not processing requests. EDC is able to go into spool-down without losing network connection.

- 5. Specify the **number of queued transactions** for the system to reach to initiate live processing. For example, '20.' Once the system reaches 20 queued transactions, the system initiates live processing.
- 6. Under the 'Store and forward' group bar, select **Enable store and forward** to enable the Store and Forward feature which allows the system to provide a premature authorization and store the transaction until the system reconnects to the processor and reprocesses the store transactions in queue.
- 7. Type the **number of seconds**, from zero to 30, allowed to attempt to authorize a transaction.
- 8. Type the **number of seconds**, from zero to 900, to wait before attempting to authorize the oldest transaction placed in the queue by Store and Forward.
- 9. Type the **dollar amount** above which the system will not 'store and forward' the transaction, in 'Floor for transaction amount.' If EDC does not receive an authorization before the allotted time frame for a transaction greater than this amount, the system declines the transaction. If you define the floor limit as zero, the system allows EDC to 'store and forward' any transaction amount.
- 10. Type the **highest number of transactions**, per processor, to allow EDC to 'store and forward' in 'Maximum number of offline transactions.'

Reference

Refer to the Store and Forward (SAF) Feature Focus Guide - HKS381 for more information.

11. Click **Save** and exit **EDC Settings**.



Configure a CES (First Data) processor for P2PE

If you are using First Data (CES) as your processor, in combination with the Verifone VX820, for P2PE, you must configure the CES processor for P2PE and then go to the FOH and activate the PIN pad. **Note**: You must be on CFC 14.6, or later, to configure the CES processor for P2PE.

To configure the CES processor for P2PE:

- 1. Select Maintenance > Electronic Draft Capture > Processors.
- 2. Select **CES** from the drop-down list or click the **New** drop-down arrow, select the **processor**, and click **OK**.

Processor Options TCP/IP Dialing Reversals Custo	0	
Processor Options TCP/IP Dialing Reversals Custo		-
	m	
Identification		
Number	4	ł
Name	CES - 0	
Active	V	
Index	😮 0	
Туре	CES	
Terminal ID	999999	
Terminal ID BOH terminal ID	999999	
Terminal ID BOH terminal ID Gift card alternate merchant ID	999999 0000000000	
Terminal ID BOH terminal ID Gift card alternate merchant ID Enable multiple transactions	999999 0000000000 V	
Terminal ID BOH terminal ID Gift card alternate merchant ID Enable multiple transactions Remove rejected transactions	999999 0000000000 V	
Terminal ID BOH terminal ID Gift card alternate merchant ID Enable multiple transactions Remove rejected transactions EBT merchant FNS ID	999999 00000000000 2000000000 0000000	
Terminal ID BOH terminal ID Gift card alternate merchant ID Enable multiple transactions Remove rejected transactions EBT merchant FNS ID Point to point encryption	999999 00000000000 000000000 0000000	
Terminal ID BOH terminal ID Gift card alternate merchant ID Enable multiple transactions Remove rejected transactions EBT merchant FNS ID Point to point encryption Enable point to point encryption and disable credit.	999999 0000000000 000000000 0000000 201,	
Terminal ID BOH terminal ID Gift card alternate merchant ID Enable multiple transactions Remove rejected transactions EBT merchant FNS ID Point to point encryption Enable point to point encryption and disable credit VSP domain	999999 0000000000 00000000 0000000 201000	

Figure 6 Processors - Processor Tab (CES)

3. Under the 'CES' group bar, enter the **BOH terminal ID** (CES Terminal ID) provided by CES.

R Note

This terminal ID must be associated with the 'Credit Card Terminal ID (DID) option on the TCP/IP tab. Both of these values are provided by the processor.

- 4. Under the 'Point to point encryption' group bar, select **Enable point to point encryption and disable credit card entry in EDC**.
- 5. Type the **VSP domain** provided by CES.
- 6. Type the **VSP brand** provided by CES.
- 7. Type the **Token ID** provided by CES.

NCR V:YIX

8. Select the **TCP/IP** tab.



Figure 7 Processors - TCP/IP Tab

9. Type the Datawire ID (DID) provided by the processor in 'Credit Card Terminal ID.'

B Note

The Datawire ID is ONLY required on the BOH computer (BOH terminal ID). Aloha EDC does not require a DID for each POS terminal.

- 10. If you are configuring the processor for the first time, complete the remaining **options** as you would for any other processor.
- 11. Click Save and exit the Processor function.
- 12. Select **Utilities > Refresh POS & All Products** to transfer the new information to the FOH terminals.

Additionally, if you are implementing a CES (First Data)/TransArmor solution, you must have debit configured in the Cards function, even if you do not accept debit at the store. This is required when you perform a RegiStart on the FOH terminals in <u>"Perform the RegiStart process for First Data (CES)"</u> on page 26. If you already have debit configured, you should have this procedure already in place.

Note

This procedure is only for CES (First Data)/TransArmor sites that do not have debit configured. If you want to begin using debit, you must configure the debit tender, as normal. Also note, this does not change the way you configure your credit cards. They are configured, as normal.



Assigning cards to processors

Currently, Aloha EDC provides for these major credit cards: MasterCard, VISA, American Express, Diners, Carte Blanche, Discover, Enroute, JCB, and Military. The Aloha system recognizes Diners and Carte Blanche as being the same, thus you should configure Diners/Carte Blanche as one credit card type in the Maintenance > Payments > Tenders function.

To assign cards to processors:

1. After you configure your processors, select Maintenance > Electronic Draft Capture > Cards.

Cards		
Cards: 1 EDC Ca	ards	•
Cards		
Common Credit Cards		
Number	1	
Name	EDC Cards	
MC	CES	•
Visa	CES	•
AMEX	CES	•
Diners/CB	None	•
Discover	CES	•
Enroute	None	•
JCB	None	•
Military	None	•
Private Label Credit Cards		
Private Label 1	None	•
Private Label 2	None	•
Private Label 3	None	Ψ
Private Label 4	None	•
Private Label 5	None	•
🖬 Gift Cards		
Paymentech	None	•
ValueLink	None	•
Comdata	None	•
Vantiv	None	•
Private	None	•
Heartland Payment Systems	None	•
Debit Cards		
US Debit	CES	•
Other cards		
Chip 'N Pin	None	•
EBT	CES	•
Campus card	None	•

Figure 8	Electronic	Draft	Capture -	Cards
----------	------------	-------	-----------	-------

- 2. Under the 'Common Credit Cards' group bar, select **CES** to use for each card type. Unless you are using multiple processors, you would use the same processor for all types. Select 'None' for any card you do not accept.
- Under the 'Private Label Credit Cards' group bar, select CES to use for each private label card type. Unless you are using multiple processors, you would use the same processor for all types. Select 'None' for any card you do not accept.
- 4. Under the 'Gift Cards' group bar, select the **CES** to use for the corresponding gift card you accept. In most cases, such as Paymentech and Stored Value, you can select only one supporting processor for the gift card. Select 'None' for any card you do not accept.



- 5. Under the 'Debit Cards' group bar, select the **CES** from the 'US Debit' drop-down list. **Note**: Selecting a processor as the US Debit processor disables the Canadian Debit option.
- 6. Under the 'Other cards' group bar, select the **CES** to use for 'EBT,' if necessary.
- 7. Click **Save** and exit the **Card** function.

Configure a TSYS (Visa Net) processor for P2PE

If you are using TSYS (Visa Net) as your processor, in combination with the Ingenico iPP350 PIN pad, you must configure the Visa Net processor for P2PE.

To configure the TSYS (Visa Net) processor for P2PE:

- 1. Select Maintenance > Electronic Draft Capture > Processor.
- 2. Select **Visa Net** from the drop-down list or click the **New** drop-down arrow, select the **processor**, and click **OK**.

Processor		
Processor: 2 Visa Net	- 0 Visa Net 0	-
Processor Options TCP/IP Dialing Reversals Au	to Settlement Custom	
Identification		
Number	2	
Name	Visa Net - 0	
Active	\checkmark	
Index	😆 0	
Type	Visa Net	
1700		
Industry	Food/Restaurant	•
Industry Currency	Food/Restaurant US Dollars	v
Industry Currency Country	Food/Restaurant US Dollars USA	•
Industry Currency Country Sharing group	Food/Restaurant US Dollars USA	v A v
Industry Currency Country Sharing group Reimbursement attribute	Food/Restaurant US Dollars USA	Y Y
Industry Currency Country Sharing group Reimbursement attribute Enable multiple transactions	Food/Restaurant US Dollars USA	V
Industry Currency Country Sharing group Reimbursement attribute Enable multiple transactions Remove rejected transactions	Food/Restaurant US Dollars USA	▼ ▼ ▼
Industry Currency Country Sharing group Reimbursement attribute Enable multiple transactions Remove rejected transactions EBT FCS ID	Food/Restaurant US Dollars USA C C C C C C C O000000	
Industry Currency Country Sharing group Reimbursement attribute Enable multiple transactions Remove rejected transactions EBT FCS ID Point to point encryption	Food/Restaurant US Dollars USA S OCOUDOU USA	• A • •
Industry Currency Country Sharing group Reimbursement attribute Enable multiple transactions Remove rejected transactions BBT FCS ID Point to point encryption Enable point to point encryption and disable cred	Food/Restaurant US Dollars USA © 0000000 edit car	▼ ▼ ▼

Figure 9 Processors - Processor Tab (Visa Net)

- 3. Under the 'Visa Net' group bar, enter the **BOH terminal ID** (TSYS Terminal ID) provided by TSYS.
- 4. Under the 'Point to point encryption' group bar, select **Enable point to point encryption and disable credit card entry in EDC**.
- 5. Type the **authentication code** provided by TSYS.
- 6. If you are configuring the processor for the first time, complete the remaining **options** as you would for any other processor.
- 7. Click Save and exit the Processor function.



Configuring Aloha POS system for Point-to-Point Encryption

Prior to configuring the Aloha POS system for Point-to-Point Encryption (P2PE), you must be in contact with either First Data (CES) or TSYS (Visa Net) for the proper requirements, such as obtaining unique terminal IDs, and the appropriate PIN pad, which is injected specifically for the NCR Aloha software and the merchant. You must also have Aloha POS system and Aloha EDC v12.3 and later, installed at the site.

Caution

Prior to implementing P2PE functionality, we highly recommend you remove all existing sensitive cardholder data from the Aloha environment and settle all credit card batches. Refer to the NCR Aloha CleanPan guide for instructions on removing stored cardholder data.

1. Enable P2PE in store settings

For the first step, you must access Store Settings, to enable P2PE and define the encryption service you want to use. Once defined, the system only allows you to select the applicable PIN pad in Terminal Maintenance.

To enable P2PE in Store Settings:

- 1. Select Maintenance > Business > Store > Store Settings tab.
- 2. Select the **Credit Card** group at the bottom of the screen.

Store: 264 Al	oha Cafe	-
ocation Information Licensing Custom Store	Settings Aloha Manager	
Display message upon close check	V	-
Authorize transactions less than 1.00		
Include transactions authorized from BOH.	••	
Maximum amount of credit card refunds	0.00	
Number of IC verify terminals	1	
Credit Card Lookup ID	None	-
Eood stamp category	None	-
Use Canadian Debit	None	•
Show Last Settlement alert		
Tab or table name when customer name n.	Prompt user for tab or table name	
Enable point to point encryption and disa	. Voltage	-
EMV processor	None	-
Authorization		
🔢 Enable automatic pre-authorization		
Initial pre-authorization amount	50.00	
Subsequent pre-authorization amount	25.00	
Threshold for subsequent pre-authoriz.	15.00	
1st Preauthorization amount to be sel	. 0.00	
2nd Preauthorization amount to be sel.	0.00	-

Figure 10 Store - Store Settings Tab - Credit Card Group

- Under the 'EDC Setup' group bar, select either Voltage or TransArmor from the 'Enable point to point encryption and disable credit card entry on all POS terminals' drop-down list.
- 4. Click **Save** and exit the **Store** function.



© 2023 NCR Voyix. All rights reserved. NCR Voyix — Confidential Use and Disclose Solely Pursuant to Company Instructions

2. Assign a PIN pad device to a terminal

You must assign a PIN pad device to each terminal that drives a PIN pad device. The system displays Verifone VX820 if you have TransArmor selected in Store Settings, and displays Ingenico IPP350 if you have Voltage selected in Store Settings. As a P2PE requirement, you must also assign a unique terminal ID to each terminal driving a PIN pad. These IDs are supplied by the processor. If you already have unique terminal IDs assigned, you may have to obtain new terminal IDs.

P Note

Prior to configuring, you must ensure you install the latest drivers for the respective PIN pad.

Once you install the latest drivers, you need to confirm and identify the port on which the PIN pad is installed. To do this, you can access Device Manager on each FOH terminal. You associate these ports in Terminal Maintenance.



Figure 11 Device Manager Screen

As an additional feature for the Ingenico iPP350 PIN pad, you can also configure Aloha to direct the PIN pad to not display confirmation prompts to the guest on the PIN pad. By default, all prompts from the PIN pad appears. You can optionally select 'Customer-facing PIN pad' in Terminal Maintenance to do this. The prompts this option suppresses tip and amount confirmations to enhance your speed of service.

To assign a PIN pad device to a terminal:

- 1. Select Maintenance > Hardware > Terminals.
- 2. Select a terminal you want to assign a PIN pad device from the drop-down list.



3. Select the **Output Devices** tab.

Terminal: 1 SERVER STAT #1		-
Terminal Readers Output Devices EDC Settings		
Pole display		
Use pole display		
🖬 Coin changer		
Туре	None	•
🖬 Aloha spy server		
Port	0	
IP address		
Fiscal manager		
Port	0	
IP address		
E PIN pad		
Туре	Ingenico IPP350	•
Port	COM 9	•
Customer-racing PIN pad		
S Assign an order number when	• The first item is entered	
	O The check is sent	

Figure 12 Terminals - Output Devices Tab

- 4. Select either Ingenico IPP350 or Verifone VX820 from the 'Type' drop-down list.
- 5. Select the **USB port** to use for the PIN pad device.
- 6. If you are using Ingenico iPP350 PIN pad device, clear **Customer-facing PIN pad** if you want to reduce the prompts initiated by the PIN pad. This is not supported with the VeriFone PIN pad.
- 7. To assign a unique terminal ID, select the **EDC Settings** tab.

Terminals		
Т	erminal: 2 STATION 2	•
Terminal Readers Output D	Devices EDC Settings	
Unique terminal ID	for each processor	
Processor	△ Terminal ID	Add
I CES - 1	1234	
		Remove
		Processor

Figure 13 Terminals - EDC Settings Tab

8. Click **Add** to start a new processor and terminal ID record for the terminal.



© 2023 NCR Voyix. All rights reserved. NCR Voyix — Confidential Use and Disclose Solely Pursuant to Company Instructions

- 9. Select the **processor** from the drop-down list.
- 10. Type the **terminal ID number** supplied by the processor in 'Terminal ID.'
- 11. Click Save.
- 12. Repeat this **procedure** for each terminal using a PIN pad device.
- 13. Exit the **Terminals** function.

3. Create an integrations profile

As an internal function, the Aloha system uses the Integrations (formerly called Aloha Transaction Gateway) functionality to enable P2PE. You must at least open the Integrations function and create an Integrations profile for the system to use.

Caution

Δ

To enable P2PE and create an Integrations profile, you must use CFC/new Aloha Manager v13.9, and later. Create an Integrations profile by accessing the Integrations function and saving a record, with no additional configuration. If you already have an Integrations profile record defined, you can skip this step.

B Note

Effective in CFC/new Aloha Manager v14.9, the function is named Integrations.



To create an Integrations or ATG profile:

- Select Maintenance > System Settings > Integrations. Note: If you use CFC/new Aloha Manager v14.8 and earlier, select Maintenance > System Settings > Aloha Transaction Gateway.
- 2. Click New.

Integrations			
Integrations: 10 Aloha Café	v		
Integrations Custom			
Settings		-	
Polling time in seconds	35		
Interface server terminal	None	•	
Interface terminal	None	•	
Type of operation	Table Service 🔹	•	
Additional POS Parameters			
Start the POS if not already running			
Force start of POS even if instance found			
IP address in case of dual NIC			
Print intercept timeout (in seconds)	5		
Maximum debout file size (in MB)	2		
Enable boh functions			
PayPal payments		-	
Custom Debouts			
Custom debouts		_	
	Add		
	Remove		

Figure 14 System Settings - Integrations

3. Click Save and exit the Aloha Transaction Gateway or Integrations function.

4. Create a P2PE tender

You must create a new P2PE tender to enable the system to divert responses from the MSR to the PIN pad device. When the cashier touches this tender in the FOH, Aloha sends the amount due to the PIN pad for initialization. The PIN pad device detects the card type and guides the cardholder or employee through the rest of the transaction flow.

To create a P2PE tender:

- 1. Select Maintenance > Payments > Tenders.
- 2. Click the New drop-down arrow, select Credit Card, and click OK.
- 3. Type a tender name, such as 'P2PE Credit Card'
- 4. Select Active.



5. Select the **Type** tab.

Type settings		
Credit card provider	Not Applicable	•
Prompt for payment using the following PIN pad	None	
Apply a surcharge to this tender	None	•
Chip 'N Pin reader ID required		
Property management settings		
Post to PMS		
Foreign Currency		
Foreign currency	None	•
Options settings		
Use magnetic card only		
Expiration		
Verify signature		
🙀 Get common service tender prefix		

Figure 15 Tenders - Type Tab

6. Select Not Applicable from the 'Credit card provider' drop-down list.

Note

You need only configure the P2PE tender as 'Not Applicable.' Configure all other card tenders as their respective card type.



7. Select the Authorization tab.

Tender: 50 P2PE Credit card			
Tender Type Identification Authorization Reconciliation Printers Rounding			
- Authorization			
Require authorization			✓
Authorization prompt		Auth:	
Maximum length		0	
Print on check			✓
Authorize using EDC			✓
Allow pre-auth with EDC			
Do not print vouchers			
Apply signature line rules for	vouchers		

Figure 16 Tenders - Authorization Tab

- 8. Select **Require authorization** to initiate an authorization prompt on the order entry screens.
- 9. Type the **text** to appear on the order entry terminal to prompt for the authorization number, such as 'Auth.'
- 10. Type **O** (zero) as the maximum length, to allow the system to accept blank authorization codes if a code is not entered.
- 11. Select **Print on check** to print the authorization code on the guest check.
- 12. Select Authorize using EDC to specify Aloha EDC is used for credit card authorization.
- 13. Click **Save** and exit the **Tenders** function.

Additionally, if you are implementing a CES (First Data)/TransArmor solution, you must have a debit tender configured in the Tenders function, even if you do not accept debit at the store. We recommend you leave the debit tender as inactive since you will not use the tender in production. This is required when you perform a RegiStart on the FOH terminals in <u>"Perform the RegiStart process for First Data (CES)" on page 26.</u>

Tip

This procedure is only for CES (First Data)/TransArmor sites that do not have debit configured. If you want to begin using debit, you must configure the debit tender, as normal. Also note, this does not change the way you configure your credit cards. They are configured, as normal.



To create a debit card tender for CES sites not using a debit solution:

1. Select Maintenance > Payments > Tenders.

Tender:	6 Debit Debit 🔹	
Tender Type Identification Authorizati	on Reconciliation Printers Rounding	O New ▼
Settings		
Number	6	
Name	Debit	Cash
Туре	Debit	Check
First available button position		Credit card
Button position	None	··· Debit
Button image	None	▼ Gift card
Report as	Current	 House account
Default amount behavior	Ask for amount	Property management
Active		Accounts receivable
Track		Saved customer C.C.
Can refund		Generic 👻
Affect deposit		
Print check on close		OK Cancel
Open drawer on close		Circ Cancer
Print signature line		X
Combine on check		
Close check upon payment		
Do not verify amount		
Overpayment		
Allow overpayment		
Auto fix balance without prompt		•

Figure 17 Debit Tender Configuration for Non-Debit Solutions

- 2. Click the New drop-down arrow, select Debit, and click OK.
- 3. Type a **tender name**, such as 'Debit.'
- 4. Clear Active.
- 5. Leave all settings as their default values, since you will not use this tender in production.
- 6. Click **Save** and exit the **Tenders** function.

5. Add a P2PE tender to a panel for QS

For Quick Service environments, you must also add the P2PE tender button to a panel in use.

To add a P2PE tender to a panel for QS:

- 1. Select Maintenance > Screen Designer > Quick Service Screen Designer.
- 2. Select Work with Panels.
- 3. Select Panel > Open Panel and select a panel containing your tenders.
- 4. Select **Panel > New Button**.
- 5. In the Properties dialog box, select **Tender** from the 'Action' drop-down list.
- 6. Select the P2PE tender from the 'Tender' drop-down list.
- 7. Configure the remaining **options**, such as appearance, font and color, as you would for any other tender.
- 8. Click Panel > Save Panel.
- 9. Exit the **Screen Designer** function.



6. Limit access to card tenders from the FOH (optional)

As previously noted, all card transactions will be processed in the FOH using the P2PE tender. As a best practice, we recommend you remove all other card tender buttons from the FOH. This prevents the employee from needlessly selecting a card tender.

To limit access to card tenders from the FOH in Table Service:

- 1. Select Maintenance > Payments > Tenders.
- 2. Select a card tender, such as 'Visa,' from the drop-down list.
- 3. Click the **ellipses button** in 'Button position' to display the Select New Button Position dialog box.

Select New Button Position		
Cash	Mastercard	Check
Exact \$	Cut	Account
Next\$	Discorrei	Gift Cert
\$1.00	AMEX	
\$5.00	Diners	
\$10.00	Debit Card	
\$20.00	Cash Card	
\$50.00	Paymentech	
		\leq
×		

Figure 18 Select New Button Position Dialog Box

- 4. Right-click on the **appropriate position** and select **Delete**.
- 5. Click Save.
- 6. Repeat this **procedure** for each card tender you will process, using the P2PE tender.



Refresh the data

After all settings are in place in both Aloha POS system and EDC, you must select **Utilities > Refresh POS & All Products** to transfer the new information to the FOH terminals, or wait for the End-of-Day (EOD) process to accomplish the data refresh for you. After the data refresh is complete, all new settings become operational across the Aloha network.

Perform the RegiStart process for First Data (CES)

Once you configure the CES processor for P2PE, and after you refresh data, you must ensure activation between the POS and the TransArmor Vault. This requires a "RegiStart" card (provided by CES) and it is necessary to perform the following steps on each VeriFone PIN pad. You must be on-line to activate P2PE on a VeriFone PIN pad. You cannot process off-line.

Tip

Remember, you must have debit cards configured even if you are not using debit at the store. Refer to <u>"Configure a CES (First Data) processor for P2PE" on page 13</u> and <u>"4. Create a P2PE tender" on page 21</u> for more information.

To perform the RegiStart process:

- 1. Log in to a **FOH terminal** with a VeriFone PIN pad device attached.
- 2. Start a new check.
- 3. Add an item for \$1.00 to the check. This can be an open item.
- 4. Order the item.
- 5. Navigate to the tender screen/panel.
- 6. Touch the 'P2PE tender.' The tender screen appears.



7. Reduce or adjust the **amount** down to \$1.00, using the **keypad**.



Figure 19 Tender Screen

8. Slide the **RegiStart card** through the MSR on the PIN pad. In the on-screen guest check, the response returns as declined, and "RegiStart Successful."



On the PIN pad, a 'RegiStart' message appears, followed by a 'Declined' message.

- 9. Once successfully registered, **void or delete the declined transaction** from the check and log out of the **terminal**.
- 10. Repeat this **procedure** for each POS terminal attached with a VeriFone PIN pad. You can use the same check for each terminal.
- 11. Run a test transaction to confirm the POS terminal is accepting approvals.

Tip

If you move the PIN pad to a different POS terminal, you must perform RegiStart again.



Using Point-to-Point Encryption functionality

Once implemented, you can start using P2PE functionality. When enabled, you cannot use the magnetic stripe reader to capture cardholder information for a credit, debit, or EBT card. You must use the PIN pad to complete the transaction.

To use P2PE functionality:

- 1. Start a **check**.
- 2. Add and order **items** on the check.
- 3. Access your tender screen.
- 4. Select the **PIN Pad tender** configured for P2PE. The tender screen appears with the sales amount populated in the 'Amount' prompt.
- 5. Confirm the **amount** by touching **OK**. The PIN pad takes over and the guest or employee must complete the transaction using the PIN pad device.
- 6. Follow the **prompts on the PIN pad** to manually enter the data, or slide or tap the card across the PIN pad reader. To manually enter card data on the VX820 PIN pad payment device, when the 'Please swipe card' prompt appears:
 - a. Press the **Cancel (red)** button. The 'Enter account number and Exp date' prompt appears on the VX820 PIN pad payment device.
 - b. Manually enter card number data and expiration date.
- 7. Enter the **tip amount**, if necessary.
- 8. Touch **OK** to approve the **amount** of the transaction. The system sends the transaction to the appropriate vault or issuing bank for further encryption. If you are using First Data (CES), a token is inserted in the cardholder number.



Point-to-Point Encryption, Feature Focus Guide

NCR Voyix welcomes your feedback on this document. Your comments can be of great value in helping us improve our information products. Please contact us using the following email address: Documentation.HSR@NCRVoyix.com

