Infor Distribution FACTS Integration Guide for CenPOS

Release level: 9.3.0

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials (Purpose).

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

Publication Information

Release: Infor Distribution FACTS

Publication date: March 2, 2021

Contents

About this guide

This document describes the steps necessary to integrate CenPOS, a third-party credit card processing software package and service, with Infor Distribution FACTS.

Intended audience

This guide is for FACTS end users, managers, in-house analysts, and trainers who require an understanding of the automatic credit card processing and how to use it.

Related documents

Infor product documentation is available from the Infor Support Portal. System administrators must have a working knowledge of Distribution FACTS and be familiar with the current version of these documents:

- *Infor Distribution FACTS Installation Guide*
- *Infor Distribution FACTS Product Compatibility Matrix*
- *Infor Distribution FACTS Hardware Guide*
- *Infor Distribution FACTS Release Notes*

Contacting Infor

If you have questions about Infor products, go to the Infor Support Portal.

If we update this document after the product release, we will post the new version on this website. We recommend that you check this website periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1 Credit card handling

Distribution FACTS processes credit card payments using CenPOS, a credit card processor that provides a hosted payment solution.

How the interface works

The interface between FACTS and the CenPOS service uses CenPOS POS (point of sale) APIs and their web services. The CenPOS APIs are solely responsible for collecting all credit card data and processing the transaction. FACTS uses Internet Explorer on the client's PC to present CenPOS's URL for the user to complete each transaction.

This approach removes all direct handling of sensitive card information from FACTS.

Multi-merchant capabilities

Current standards in the PCI market require companies to have separate merchant accounts for each location. To accommodate this, FACTS supports setting up merchant IDs at the company level and at the warehouse level. When configured for multiple merchants, transactions generated from the Sales Order module for a specific document use the initiating warehouse's merchant ID.

All transactions originating from the Accounts Receivable module use the company-level merchant ID.

Valid characters for customer codes

In CenPOS, these characters are valid for customer codes.

>	-	0-9	A-Z	a-z
.	<empty space>	_	|	$
:	*	'	@	#
%				

The CenPOS field name reference for customers is `customercode`.

Tokenization

Many companies need to keep customer credit card numbers on file, with the customer's permission, for reuse on subsequent orders. Writing them down or keeping them in a spreadsheet or in a file is dangerous and is in direct conflict with PCI compliance rules.

CenPOS provides the ability to store credit card numbers in a form that can be used for transactions but that never exposes the card number information to your users. It does this by capturing the sensitive card information, storing it securely in the database, and providing the merchant with a name, or token, that refers to that card.

The token is merchant ID-specific, so it is useless to share that token ID with other parties. It cannot be used except with transactions for that merchant account.

FACTS provides an interface to the CenPOS token management system without displaying or storing any of the information.

Tokens are not only specific to the merchant ID, but they are assigned to a designated client ID. This client ID is either the FACTS customer number or the customer number combined with the ship-to number with a double colon (::) between them. This ensures that the stored credit card cannot be used for the wrong customer or the wrong customer ship-to.

The tokens are managed by using several web services and URL calls to retrieve, add, or delete tokens for a given client ID. The list of tokens is available in FACTS Order Entry programs. The ability to add, edit, and delete tokens is controlled by a user-level security setting. Without that setting enabled, the user can see and use tokens but cannot create, change, or delete them.

When using tokens and multi-merchant capabilities at the same time, it may be helpful to link your merchant IDs. A token created under one merchant ID can be used by any of the linked merchant IDs. To link merchant IDs, contact CenPOS.

EMV terminals

The FACTS integration with CenPOS works with any of the approved EMV terminals (chip readers), non-EMV terminals, and keyboard wedges approved by CenPOS and available for your operating environment.

When EMV terminals are used, they must be set up using CenPOS bridge software. This is software provided by CenPOS that allows multiple FACTS clients to share an EMV terminal.

A different PC must be assigned to control each EMV terminal. The bridge software must be installed on that PC and configured to find and control the EMV terminal.

In FACTS, the **EMV Terminal F/M** program is used to name and identify each PC and EMV terminal combination. This provides the IP address to the PC that is controlling the EMV terminal. When users begin a transaction that requires the use of a terminal, they select the PC and terminal to use.

Only one FACTS session can be actively using a terminal at a time. If the terminal is already in use, the transaction must be completed, or a different terminal must be used.

The PC's IP address is passed to the CenPOS credit card interface, which activates and interacts with the EMV terminal by way of the bridge software on the PC. The **EMV Terminal Search** dialog box is displayed for selecting which terminal to use during credit card processing. You can also click **EMV Terminal** on the **CenPOS Credit Card Entry** screen to display the terminals for selection.

Level III transmission data

Level III data processing provides more detailed information about the transaction, which is sent back to the buying organization via the issuing bank. By supplying this information, the merchant can secure a significantly lower transaction fee rate. In addition, a special interchange category called Large Ticket Interchange (LTI) requires Level III processing.

Level III payments require the most data out of the three processing levels. For comparison, Level II payments require this type of information.

- Transaction amount
- Customer code
- Sales tax

Level III payments require all the data for Level II payments, but also must include more detailed information.

- Item ID or SKU
- Item description
- Quantity
- Unit price
- Extended price
- Unit of measure (each)
- Commodity code
- Line discount

Level III transactions are cheaper for the merchant than Level I and Level II transactions because of the lowered interchange rates they can yield. Plus, with all the transaction details required, merchants can better track and monitor purchases. This increases efficiency and reporting power.

When you activate Level III data in FACTS, the data is sent on all relevant transactions.

When sent, Level III data must add up to the amount of the charge or the Level III data is ignored, and the financial benefit is lost. When the amount of the charge cannot be matched exactly with the totals of a single invoice, Level III summary data is sent instead. That applies to all charges performed from the cash and credit application side and to any deposits or partial charges on an invoice.

Level III Summary data qualifies for all fee discounts.

Pre-authorization/Force Capture

Also referred to as Book and Ship, use this feature to reserve a credit amount against a card. This helps protect against declined transactions during invoicing.

While the document is an order, you can process a pre-authorization for any selected amount. If the pre-authorization is approved, it is generally retained for seven days. Refer to CenPOS for specifics on how long pre-authorizations are valid. If the seven days pass without the pre-authorization being used or invoiced against, it expires. The credit amount is no longer reserved on the card.

It is important that you manage pre-authorizations properly to ensure that you do not end up with declined sales.

Re-authorizing a pre-authorization

You can re-authorize a pre-authorization automatically. You can also raise an alert when the pre-authorization is expiring or the automatic re-authorization failed. This is based on the customer settings and the **# days old** field in **Credit Card Control**.

If pre-authorization management is implemented on your system, an alert is raised when a pre-authorization transaction that qualifies for automatic re-authorization fails, or when pre-authorization transactions are expiring. From the pre-authorization alerts, you can access **Deposit/Payment Entry** to re-authorize the pre-authorization. You can also use the **Alert Control Center (POE400)** to re-authorize all pre-authorization lines that have raised the PreAuthExp or ReAuthFail alerts.

Voiding pre-authorizations

Voiding a pre-authorization within FACTS does not immediately release the funds encumbered on the credit card. The timing of the funds being released is between CenPOS and the merchant bank. FACTS has no control over this timing.

Pre-authorization example scenarios

A pre-authorization ties up available credit limit on the card. These are working examples of pre-authorizations.

Example 1: A customer has a total credit limit of $10,000. You have a large order for approximately $6,000. You create a pre-authorization for $6,500 to cover tax, shipping, and additional processing fees. The customer now only has $3,500 available credit remaining.

When you are ready to invoice, if you leave the pre-authorization and instead add a sale transaction, it would be declined because there is not enough credit available.

Instead, convert the pre-authorization to a sale. Double-click the pre-authorization line and specify the final invoice amount.

Example 2: The customer has a $10,000 credit limit. You have an order for approximately $3,000 and perform a pre-authorization for $3,000. The customer now has $7,000 in remaining credit. During invoicing, you do not convert the pre-authorization to a sale but instead add a new sale transaction. The transaction is successful, but the additional $3,000 reservation remains on the card.

This could cause your customer to have issues with other purchases.

Voiding a pre-authorization in FACTS or allowing it to expire does not immediately release the funds encumbered on the credit card. The timing of the funds being released is determined between CenPOS and the merchant bank. This timing is not controlled in FACTS, but it is important that you understand there is a delay.

Example 3: The customer has a $10,000 credit limit. You have pre-authorized $6,000, leaving $4,000 available. If you invoice on the seventh day, after the pre-authorization has expired, it will fail. Because of the timing of the funds being released, you may not be able to perform a sale transaction immediately.

Example 4: The customer has a $10,000 credit limit. You have pre-authorized $6,000, leaving $4,000 available. If the customer cancels the order and you void the pre-authorization, the reservation is not immediately released. Explain to the customer that you have voided the pre-authorization. Advise them to check with their bank to determine when the funds are available again.

Pre-authorizations can be created in the **Deposit/Payment Entry (SOC718)** program. To use or convert a pre-authorization to a sale, double-click the pre-authorization line in **Payment Entry**. You can update the pre-authorization amount to the amount of the actual invoice. When you save the pre-authorization amount, the CenPOS interface is automatically displayed so you can authorize the transaction.

Pre-authorizations/force captures work with swiped or entered credit cards or with tokens.

Setting up the merchant ID account

There is a setting within your CenPOS merchant ID, MID, that allows you to manage pre-authorizations and their associated force captures. This setting is called Force Management and can be found at **ADMINISTRATOR > MERCHANT > PROCESSING DATA** within the CenPOS Virtual Terminal.

If the **Force Management** check box is left cleared, then a force capture amount cannot exceed the original pre-authorization amount by more than 20%. When trying to force capture an amount that exceeds 120% of the original pre-authorization amount, the transaction is denied. This message is displayed within FACTS: *Invalid Amount (250)*.

If the **Force Management** check box is selected, then a force capture amount for any value, regardless of the original pre-authorization amount, is allowed.

Chapter 2 Integrating FACTS and CenPOS

This chapter provides information on the FACTS integration with the CenPOS credit card processing service. CenPOS is a third-party product, and Infor does not support or provide instructions for the use of CenPOS. Contact CenPOS directly to establish your merchant account and for any help with your product.

Access the Infor registration portal at https://www.cenpos.com/infor-registration/. Customers can register themselves directly into CenPOS Contact Resource Management for support.

You can also visit CenPOS on the web at http://www.cenpos.com.

Requirements

The FACTS integration with CenPOS must meet these requirements for credit card processing.

- Workstations must have Internet Explorer 7 or higher installed, TLS enabled, and SSL3 disabled. The entire CenPOS interface is managed through CenPOS and is displayed in an Internet Explorer window.
- The FACTS server must have secure Internet access and have TLS enabled. The FACTS server uses web services calls to the CenPOS servers to handle API transactions with credit cards.

Prerequisites

Prior to setting up FACTS for use with CenPOS you must determine this information.

- How many merchant IDs you need: one for each initiating warehouse and one company-level MID for AR transactions. Note that this can be the same MID as one of the warehouse MIDs unless you want a separate company-level MID.
- What type of terminals or readers you use and how many you require. Consult the CenPOS site for approved devices.
- The location of terminals or readers.

If using EMV terminals you must complete these tasks.

- Assign a 5-character name to each EMV terminal.
- Identify a PC for each EMV terminal. These PCs must have the CenPOS bridge software installed.
- Decide how the PC identifies the EMV terminal. The terminal can be connected directly to a network port. In this case the PC uses the EMV terminal's IP address to locate it. The EMV terminal can also be connected to the USB port on the PC.
- Record the PC, which terminal code it controls, and the PC's IP address.
- Establish your account with CenPOS.
- Order the needed terminals or card readers.
- Have CenPOS create each MID you require and optionally link all the MIDs. Linking MIDs is recommended but not required.
- Record the MIDs and the warehouse or company where they are used.
- Record the primary user name and password for each MID.
- Notify CenPOS whether each MID uses EMV readers so the MID can be configured correctly. Each MID should have one user account in FACTS. This user name and password should be kept strictly confidential.
- Set up any additional users for each MID. Tasks for additional users could include virtual terminal configuration or investigating transactions.
- Determine which of your FACTS users you allow to manage credit card tokens.

Configuring FACTS to use CenPOS

1 Select **System Management > File Maintenances > Company Control F/M**.

2 Select `CenPOS` in the **Credit Card Processor** field.

3 For the **Currency Code** field, specify the ISO standard currency code for this company.

This code is used when publishing XML and for CenPOS credit card processing. It does not change the fields throughout FACTS. It does not imply that FACTS is capable of handling multiple currencies or tracking conversion rates. To transmit Level III data to CenPOS, you must specify one of the active ISO 4217 currency codes. This value is populated into the <Destinationcountrycode> during Level III transmissions. For more information about ISO 4217 currency codes, refer to https://en.wikipedia.org/wiki/ISO_4217.

4 Select **Accounts Receivable > File Maintenances > Infrequent File Maintenances > Terms Code F/M**.

5 Set up a credit card terms code in **Accounts Receivable Terms Code F/M** if you have not already done so.

Credit cards must be set up as a cash type, Type 2 or 3. The General Ledger number you choose must be a cash GL account number.

Configuring credit card parameters

1 Select **System Management > File Maintenances > Credit Card Control**.

The information setup in the header portion of this entry is for the company-level merchant ID. This is the MID used for all AR transactions. If this MID is also used for a specific warehouse, it is not necessary to also add it in these lines.

2 Specify this information.

Base URL

The URL for the CenPOS interface. The default is
https://www4.cenpos.net/POSIntegration/POSIntegration-HTML5/.
After you have completed the information on this screen, click Test (the globe icon) to display the Test CenPOS Connectivity & Card Reader dialog box. Use this screen to submit a 1-cent test transaction.

Merchant ID

Specify the account ID for CenPOS.

Password

Specify the CenPOS password.

User ID

Specify the user id used with cookies to allow processing without logging in each time.

Transmit to CenPOS

Indicate whether you are ready to activate CenPOS and transmit transactions.

3 In the Lines section, optionally specify override merchant id and CenPOS settings for warehouses that need multi-merchant capability. Click **Add** and specify this information.

EMV Terminals

Indicate whether you use chip reader (EMV) terminals. EMV terminals are enabled with CenPOS. When changing to EMV readers, all readers must be EMV readers for all MIDs. You cannot mix EMV readers and non-EMV readers.

Columns for Receipt

This sets the width of your credit card receipts, which can range from 30 to 80 columns wide. Specify 0 if you do not want a receipt to print.

Transmit Level III Data

Indicate whether you want to transmit level III summary details for credit card/token transactions.

CenPOS Level III Strip Characters

Specify the characters that need to be stripped out of item descriptions when constructing and transmitting Level III data to CenPOS. CenPOS rejects item descriptions that contain ‘equals, =’, as well as ‘and, &’ characters in them. Use the **CenPOS Level III Strip Characters** field to control which item description characters get stripped out the L3 data. The characters specified apply to both the company merchant ID and warehouse merchant IDs if they exist.

The stripping action occurs on both detail Level III data as well as summary Level III data, in case there are characters in the two Level III Summary fields that need to be stripped out.

Level III UOM

From the drop-down specify the unit of measure type (F-Use FACTS Unit of Measure, I-Use ISO Unit of Measure, or A-Use Alternate Unit of Measure) for Level III data transmission. Some banks may require you to send UM codes that match their list of UMs. Specify those alternate UMs in **Unit of Measure F/M** in either the ISO standard or the alternate UM fields. Then select the field where you specified the CenPOS UMs.

Last Receipt Number Used

Specify the last credit card receipt number used.

AR Lvl 3 Summary Desc

Specify the description to use for AR Level III transmissions. When sending Level III data from cash receipts, this description is included in the Level III summary data.

SO Lvl 3 Summary Desc

Specify the description to use for SO Level III transmissions. When sending Level III data for sales order partial payments or deposits, this description is included in the Level III summary data.

4 If using re-authorization controls for pre-authorizations, specify this information.

Auto Re-Auth # Days

Specify the number of days old a pre-authorization is when the pre-auth is automatically reauthorized.

Existing Pre-Auth Alert # Days

Specify the number of days old a pre-authorization is when the pre-auth expiring alert is raised.

5 When the **EMV Terminal Search** window is displayed, you can select a default EMV terminal at this time or click **Cancel** and select a default EMV terminal later.

If you are setting up multiple merchant accounts, add a line for each warehouse-specific merchant ID that is not the MID setup in the header of this screen.

6 In the **Lines** section, specify override merchant id and CenPOS settings for warehouses that required multi-merchant capability.

7 Click **Add.**

8 Specify this information:

Warehouse

The warehouse for the override settings.

Merchant ID

Specify the account ID for CenPOS.

Password

Specify the CenPOS password.

User ID

Specify the user id used with cookies to allow processing without logging in each time.

Transmit to CenPOS

Indicate whether you are ready to activate CenPOS and transmit transactions. During initial setup, leave this setting cleared until configuration is complete and ready for use. Select the **Transmit to CenPOS** check box when you are ready for processing. When the **Transmit to CenPOS** check box is not selected, the **CC Token** button is not available in **Customer F/M (ARF910)**, **Ship To F/M (ARF920)** and **Quick Customer Add (ARF915)**.

EMV Terminals

Indicate whether you use chip reader (EMV) terminals. **Note**: All MIDs should have this either on or off.

Transmit Level III Data

Indicate whether you want to transmit level III summary details for credit card/token transactions.

Level III UOM

From the drop-down specify the unit of measure type (F-Use FACTS Unit of Measure, I-Use ISO Unit of Measure, or A-Use Alternate Unit of Measure) for level III data transmission.

9 When you have completed the information on this screen, click **Test** (the globe icon) beside the **Base URL** field.

The **Test CenPOS Connectivity & Card Reader** dialog box, where you can submit a 1-cent test transaction, is displayed. A warning message, indicating that there is no default EMV terminal setup for your workstation, may be displayed.

10 Click **OK**.

Your test connection with CenPOS is functional.

11 When the **EMV Terminal Search** window is displayed, you can select a default EMV terminal at this time or click **Cancel** and select a default EMV terminal later.

12 Click **Done**.

Configuring print parameters

You can optionally print credit card receipts.

1 Select **System Management > Menu Setup> Program F/M.**

2 Specify SOP610 in the **Program** field.

3 On the **Printer Defaults** tab, specify this information.

System-wide Default Printer

The printer id for the system printer to be used as a default if no other printer is specified. Specify a printer id (set in **Printer F/M**).

Company # Default Printer

The printer id for the system printer to be used as a default if no other printer is specified. Specify a printer id (set in **Printer F/M**).

By specifying printer usage and normal printer for each location you can have one credit card receipt printer for all terminals, or a different printer for some terminals, as necessary.

In the Location browser in the lower portion of the screen, the system displays the default locations for the program.

4 To add a default printer for the location for this program, double click the line in the browser to display the **Location Default Printer** field.

5 Specify the default printer for the location for the specified program.

Note: The fields are enabled for report and print programs.

6 Click **Save**.

7 Click **Exit**.

Credit card token management

These programs are used in credit card token management:

User Code F/M (SMF410) – Security tab

For each user allowed to manage credit card tokens, access **User Code F/M** and grant them the **CC Token Management Access** privilege.

Note: This is not required for users to access or charge tokens. It only controls creating, editing, and deleting tokens.

Customer F/M (ARF910) – Invoicing tab

For each customer who allows you to keep a credit card on file, determine whether their credit cards are only to be used for a specific customer or one of their ship-tos. If a customer wants you to store cards to use only for specific ship-tos, set the **CC Token Usage** field to **`S-Ship-To`**.

If a customer prefers that credit cards are saved at the customer level, instead of at the ship-to level, set the **CC Token Usage** field to `C-Customer`.

If a customer prefers that credit cards are not saved at all, set the **CC Token Usage** field to `N-Not used`.

CenPOS Token Management (SME958)

Token management can be accessed from many places in FACTS:

- Directly from the menu
- From within **Customer F/M** and **Ship-To F/M**
- Various credit card entry screens.

In all cases, only users with the **CC Token Management Access** check box selected can add, edit, or delete tokens. Any user can access the program for inquiry on tokens or to select tokens for use on a credit card transaction.

Tokens set up for `Ship-To SAME` are considered customer-level tokens and can be used for AR transactions.

Use **CenPOS Token Management** to optionally set up any known cards.

1. Specify the customer and, if used, ship-to location.
2. In the lines grid, you can complete these tasks:
    - To add a token, click **Add**. Specify the name of the token. The CenPOS token management URL is displayed. Specify the expiration date, name of card, zip, email address, tax exempt status, and address. Click **Submit**.
    - To edit a token, highlight the line and click **Edit**. The CenPOS token management URL is displayed. Update the card information. Click **Submit**.
    - To remove a token, highlight the line and click **Delete**. At the delete message, click **Yes**. Click **OK**.
3. When you are finished managing tokens, click **Done**. To exit, click **Done** again.

Special notes for tokens

Due to limitations of the CenPOS token management system, a token ID cannot be reused within the same MID. This applies to different customer and ship-to combinations. Once a token ID has been used for any customer and ship-to combination, that token ID cannot be reused for a different customer and ship-to unless the existing token ID is deleted from the customer and ship-to combination it was initially created for. A warning message is displayed if a duplication occurs. You are not transferred to the CenPOS POS web interface.

To ensure that tokens can only be used for their designated customer and ship-to client ID, all spaces are automatically removed before and after the customer and ship-to numbers. A double colon (::) is inserted between them.

In **CenPOS Token Management (SME958)**, you can select a linked MID, Customer and Ship to MIDS token for payment/deposit. Review the MID column in **CenPOS Token Management** to identify the MID. Editing or deleting a token created under one Mid (#1) is not allowed when working in the other MID (#2).

There are some limitations within the CenPOS virtual terminal. This applies to the use of the colons as a separator. We recommend that you use the FACTS interface to create all tokens.

Turbo Tokens

The turbo tokens workflow is available for faster use of CenPOS tokens credit card processing for deposits or payments on sales order documents.

The Turbo Tokens list is available in these programs:

- **Order Entry (SOE210)**
- **Order Confirmation (SOE310)**
- **Direct Invoice Entry (SOE320)**
- **Counter Sale Entry (SOE510)**
- **Credit Memo Entry (SOE330)**

The **Turbo Token** field is only available when these conditions are met:

- A customer and ship-to have been defined on the sales order document.
- In **User Code F/M (SMF410)**, the **Turbo Token Access** user security check box has been selected for the user creating the sales order document.

Processing details

This Turbo Token list is automatically populated with all available tokens for these options:

- The specified customer and ship-to combination if the **CC Token Usage** field in **Customer F/M (ARF910)** is set to **`S – Ship To.`**
- The specified customer if the **CC Token Usage** field in **Customer F/M (ARF910)**) is set to **`C – Customer`**

The Turbo Token list is disabled if the **CC Token Usage** field in **Customer F/M (ARF910)** is set to **`N – Not Used`**.

Initially the Turbo Token list is populated with blank lines.

Click the **Turbo Token** list button to display all available tokens. Selecting a token then sets the **Turbo Token** field to that token. This token is used in in **Deposit/Payment Entry (SOC718)**. The Turbo Token value is always encrypted and decrypted for display purposes and for transmission to CenPOS.

Transaction details

If a Turbo Token was selected in **Order Entry**, the token is displayed in **Order Confirmation**. If the **Turbo Token** field is available in **Order Confirmation**, the selected token can be changed or removed. After the **Deposit/Payment Entry (SOC718)** screen is displayed, normal payment processing continues.

In **Direct Invoice Entry** and **Counter Sale Entry,** only payment and deposit processing are available.

In **Credit Memo Entry**, only payment processing is available.

In **Deposit/Payment Entry** when a Turbo Token is selected for C – CC PreAuth transaction types with a terms code of Type 1 or for pre-authorizations with a terms code of Type 2, the entire CenPOS interface is suppressed. A properly formed web request is executed as if the user had selected the token in the normal fashion. If the transaction is approved, normal processing such as receipt printing continues.

If the transaction is not approved, then the **Turbo Token** field is cleared. The user is returned to the **Deposit/Payment Entry** program. When a transaction is not approved, a different Turbo Token can be selected. Normal payment mechanics continue. For example, if a PreAuth is selected and a Type 1 or Type 2 terms code is selected, click **OK** to display the CenPOS interface with the **CC Token** button at the bottom of the CenPOS interface panel.

The **Turbo Token** field is displayed on the **Header Document Detail** screen and on the **SO Document Inquiry (SOI620) Header Detail** screen for appropriate documents.

Security settings

These are the security settings for CenPOS processing:

- **Company Control F/M (SMF920)**

Turbo Token use also adheres to the **Credit Card Processor** value on the **General** view of **Company Control F/M (SMF920)**. If this value is changed from `C - CenPOS` processing to `D - Do Not Collect`, the **Turbo Token** field is cleared for subsequent documents that had a Turbo Token selected. No warning is issued.

- **User Code F/M (SMF410)**

In **User Code F/M**, the **Turbo Token Access** user security check box controls Turbo Token access for users entering sales order documents.

- **Customer F/M (ARF910)**

These programs adhere to the **CC Token Usage** field on the **Invoicing** view of **Customer F/M** for the specified customer:

- **Order Entry**
- **Order Confirmation**
- **Direct Invoice Entry**
- **Credit Memo Entry**

- **Counter Sales Entry**

These are the options for the **CC Token Usage** field:

- **N:** The Turbo Token field/drop down list is disabled.
- **C:** Only customer tokens are displayed, regardless of the specified ship-to.
- **S:** Both ship-to and customer tokens are displayed. The Turbo Token drop down list is initially populated with tokens for specified ship-to if any exist.

Modifying the ship-to on a document that already has a Turbo Token selected displays a warning notifying the user that the Turbo Token will be cleared due to changing the ship-to location.

If the **Turbo Token Access** setting on the **Security** view of **User Code F/M (SMF410)** is changed from `yes` to `no`, subsequent documents still display the Turbo Token if one was previously selected but the field is disabled. No adding, editing, or deleting of the Turbo Token is allowed.

Chapter 3 FACTS integration with EMV terminals via the CenPOS virtual bridge

When using EMV terminals, you must use the CenPOS virtual bridge software regardless of how you connect the EMV terminals. CenPOS has instructions for connecting EMV terminals without the use of the bridge software, but FACTS does not support that implementation.

For the purposes of this guide, it is assumed that you have the VeriFone MX915 EMV terminal/card reader. Regardless of which approved terminal you are using, always check the current CenPOS instructions, as they may have changed from those listed below.

These instructions should prove useful as a guide, but the specific steps, directories, and file names may be slightly different.

Requirements

Customers are required to run the latest version of the CenPOS Virtual Terminal Bridge, which is version 6.1.

Windows Firewall settings

If you have the Windows Firewall activated on the workstation running the Virtual Bridge software (v6.1 or greater) you must ensure these ports are open for both inbound and outbound traffic:

- 8055
- 50856
- 843
- 8000
- 8443

All workstations connecting to an EMV credit card terminal, through the CenPOS Virtual Bridge, must also have these ports are open for both inbound and outbound traffic on the Windows Firewall settings:

- 8055

- 50856
- 843
- 8000
- 8443

If the ports are not configured as specified, open communication fails between these components.

- the workstation attempting the charge transaction
- the workstation running the Virtual Bridge
- the EMV terminal
- the connection to CenPOS to transmit the charge transaction

Initial installation

These installation instructions only apply to a FACTS workstation with an active VT bridge connection to an approved EMV terminal or card reader.

Each EMV terminal is connected to a workstation either via USB or a direct connection to your intranet via an Ethernet cable. Only one workstation can establish a CenPOS VT bridge connection with that EMV terminal. Refer to the list of PCs and EMV terminals at the beginning of Chapter 2 for this list of PCs.

Those PCs must have the bridge software installed and configured for the EMV terminal that each one controls. All other workstations that only use an EMV terminal do not need the software installed.

1. Unpack the EMV terminal and connect it, via USB, to the FACTS workstation that will be bridged to it.

   At this point you can ignore the messages that are displayed on your workstation indicating no device drivers exist for the Mx915 EMV terminal that you just plugged into your workstation.

   Even if you eventually plan to connect this EMV terminal to an Ethernet port, we recommend that you first connect it to the workstation via a USB port and complete the setup steps.

   The steps to connect the terminal directly to your intranet are covered later in this chapter. Initially connecting to a USB port of the FACTS workstation also allows you to quickly ensure that the terminal is operational.

2. In a browser, access https://www3.cenpos.net/vtweb/v6/VirtualTerminalWeb.html.

3. In the lower left corner of the web page, click **Bridge Download** and download `VTB Service.zip`, the CenPOS virtual bridge software and drivers, to your desktop.

4. Open the zip file and drag the embedded VTB EMV folder to your desktop.

5. From your desktop, select **VTB EMV (folder) > Virtual Terminal Bridge.pdf** and start with step 3 described in *Installation Guide for VeriFone MX915*.

Skip steps 1 and 2, instructing you to download the MX915 driver, as the most current version of those drivers are in the VTB EMV folder on your desktop, inside the `Drivers\Verifone` sub folder.

6 When the proper drivers are installed, continue with the next section of the guide, *VTB Installation for the MX915*. This section guides you through the installation of the CenPOS virtual terminal bridge.

7 Be sure to test the connection as described in the Last Step references of the *Device Installation Guide*. This ensures that the entire connectivity chain between the card reader, the FACTS workstation, its installed CenPOS VT bridge, and the CenPOS Web UI is fully functional.

Note: It is likely that your card reader may not initially read EMV chip-enabled credit cards. Refer to the section: Setting the MX915 Profile for reading EMV chip- enabled credit cards for details. After setting the MX915 profile we recommend repeating step 7. Performing another test ensures that chip-enabled credit cards are being read successfully.

Keep in mind that each card reader is attached to only a single FACTS workstation. Every interaction between any FACTS user and the terminal, including the workstation that the reader is attached to, goes through the bridge software, not directly to the reader. This allows any FACTS workstation to use any EMV terminal set up on the system.

Updating the EMV profile

You must ensure that the newest EMV profile is loaded on the terminal and update it as needed. When credit card companies modify payment system public keys (PSPKs) and certificate authority public keys (CAPKs) a new EMV profile is required. The update is specific to the EMV profile loaded on the terminal.

1 Log into the workstation where the terminal is installed.

2 Select **Start > All Programs > Virtual Terminal Bridge > Check for Updates**.

3 If there is an update available, proceed with the installation.

4 After you have the latest version of the bridge, load the EMV profile. For details on loading the EMV profile, refer to the *Device Installation Guide*.

Ethernet connection

The card reader can be attached directly to your intranet via Ethernet cable. It must have a single FACTS workstation responsible for establishing and maintaining a VT bridge connection to it.

If the workstation maintaining the bridge software connection to the EMV terminal goes down or is turned off, or if the bridge software stops working for any reason, FACTS users cannot use the EMV terminal.

Connecting the bridge software to the EMV terminal via an Internet connection instead of the USB port may or may not have an advantage. Consult the CenPOS instructions to determine what is optimal for your environment.

One potential advantage of using a network connection as opposed to a USB connection is that the workstation running the bridge software does not need to be in physical proximity to the card reader. It could be in a secure area with easy access by IT staff.

Switching the MX915 card reader from USB communications to Ethernet communications

To switch from the previously configured USB configuration to a new TCP configuration, you must complete these tasks:

- Configure the card reader for TCP/IP communications.
- Reconfigure ports within the CenPOS VT bridge software.
- Stop the virtual terminal bridge service.
- Execute the VT bridge config.cmd program (`C:\VirtualTerminalBridge\config.cmd`) and specify the TCP connection.
- Restart the Virtual Terminal Bridge service.

Configuring the MX915 card reader for TCP/IP communications

Note: The card reader must be plugged into an Ethernet port before you continue.

1 Press and hold 1+5+9 for three seconds.

2 Specify the password,166832.

3 Select **Administration > Communications > Network > Ethernet**.

4 Set the device to **`Static`** for IP assign, Mask IP, default gateway ip.

5 Click **Apply**.

6 At the top of the screen, click the **Admin** directory.

7 Select **Config > usr1**.

8 Locate **`comm_type`** and select it.

9 Erase **`USB`** and type **`tcpip`**.

10 Press **Enter** on the keypad.

11 Click **Home** on the directory at the top of the screen.

12 Click **Reboot**.

Reconfiguring ports within the CenPOS VT bridge software

To switch from the previously configured USB configuration to a new TCP configuration, you must first stop the virtual terminal bridge service. If you do not know how to start and stop services on your computer, seek the assistance of an IT professional.

1 On the computer where you installed the MX915 drivers and VT bridge software, execute the VT Bridge config.cmd program (`C:\VirtualTerminalBridge\config.cmd`).

  The VT Bridge configuration screen is displayed.

2 In right corner of the panel, click **Verifone – Current configuration loaded**.

3 Click **Use TCP connection**.

4 Specify the static IP address that was assigned to the MX915 terminal in *Configuring the MX915 card reader for TCPIP communications*, step 4.

5 In the **Port** field, specify **`9001`**.

6 Click **Save and Close**.

7 On the computer where you installed the MX915 drivers and VT bridge software, execute `C:\VirtualTerminalBridge\init.cmd`.

  A DOS command window with commands running is displayed.

  In your computer's system tray the progress of the VT Bridge connection is displayed.

If you do not see a successful message, repeat the steps in the Switching the MX915 card reader from USB communications to Ethernet communications section. Ensure that the configuration is correct.

Starting the virtual terminal bridge service

The last step in switching from the previously configured USB configuration to a new TCP configuration is to restart the virtual terminal bridge service.

You must test the connection again as suggested in the Last Step references of the *Device Installation Guide* of the installation guide. This ensures that the entire connectivity chain between the MX915 card reader, the FACTS workstation, the CenPOS VT bridge, and the CenPOS Web UI is fully functional.

Note: It is likely that your MX915 card reader may not initially read EMV chip-enabled credit cards. Refer to the section Setting the MX915 Profile for reading EMV chip-enabled credit cards for details.

Setting the MX915 Profile for reading EMV chip-enabled credit cards

You must first stop the virtual terminal bridge service to set the MX915 profile for reading EMV.

1. On the computer where you installed the MX915 drivers and VT Bridge software, execute C:\VirtualTerminalBridge\init.cmd.
2. Click **VT Bridge** in the system tray and select **Show**.
3. Click **Settings** (wrench) to display the **VT Bridge Settings** screen.
4. Click **Advanced**.
5. From the **EMV Profile** list, select the appropriate MID. In the example screen, which is a test system, the US FDC EMV Nashville Platform profile was selected.
6. Click **Upload EMV config**.

   The progress bar indicates the progress of the new profile being loaded into the MX915 terminal.
7. Click **Save and Close**.
8. Close the command window that the CenPOS configuration opened automatically.
9. Start the virtual terminal bridge service.

   You must test the connection as described in Last Step references of the *Device Installation Guide* in the Virtual Terminal Bridge.pdf. This ensures that the entire connectivity chain between the card reader, the FACTS workstation and installed CenPOS VT bridge, and the CenPOS Web UI is fully functional for chip enabled credit cards.

EMV terminal maintenance in FACTS

Use **EMV Terminal FM** to set up EMV (chip reader) credit card terminals in FACTS. For each terminal, specify the terminal ID, description, and associated IP addresses.

Note that the IP address being requested in **EMV Terminal FM**, when adding a new record, is the IP address of the workstation that the EMV terminal is attached to. This is not the IP address of the EMV terminal itself.

The IP address for each terminal is passed to the CenPOS credit card integration. When you process a credit card transaction, the **EMV Terminal Search** dialog box is displayed so you can select which terminal to use during credit card processing. You can also click **EMV Terminal** on the **CenPOS Credit Card Entry** screen to display the terminals for selection.

Default EMV terminal

You have the option of selecting a default EMV terminal. It is not required but if you decide not to when initially requested to do so, you will receive a message to select a default EMV terminal every time you access the CenPOS POS interface. If specified, the EMV terminal that is set as the default is displayed in the title bar of the CenPOS POS interface to remind you which EMV terminal you are currently using.

Creating EMV terminals

1. Select **System Management > File Maintenances > EMV Terminal Maintenance**.
2. Specify the EMV terminal id and description.
3. Specify the IP address (in IVP4 or IVP6 format) of the workstation where the EMV terminal is attached.
4. Click **Save**.
5. Click **Test Connection** to determine if the IP address is correct.
6. Modify the value if needed and save your changes.
7. Click **Exit**.

Chapter 4 Using CenPOS with FACTS

This chapter provides information on processing credit cards using CenPOS and CenPOS tokens. Pre-authorizations, re-authorizations, and deleting deposits, pre-authorizations, and payments are also discussed.

Processing credit cards with FACTS and CenPOS

After specifying the credit card transaction amount in the SO Payment entry screen or AR cash and credit application, the **CenPOS Credit Card Entry** window is displayed with the amount and transaction type.

Note: The required fields are marked with an asterisk *and highlighted in red.

1. Specify the credit card number or swipe the card through the reader.
2. Specify the expiration date. If you swiped the card, the system automatically enters this data.
3. Specify additional information as needed based on your settings in CenPOS.
4. Click **Submit** to process the transaction.

   A dialog box is displayed, indicating that the system is waiting for a response.

   If there is no Internet connection, a recognition timeout is displayed. If the card processing company does not respond within the time set in CenPOS, a response timeout is displayed. In both cases, the transaction is cancelled. Nothing is charged on the credit card.

   Offline voice authorization is not supported with CenPOS due to PCI compliance rules.

   At the end of the transaction, a check is performed to determine if you are signed on to a cash drawer. If you are not, a message is displayed for you to sign on.

Using CenPOS tokens

Clicking the **CC Tokens** button at the bottom of the CenPOS screen displays the **CenPOS CC Token Management** screen. The customer and ship-to are automatically populated based on the document being processed.

When the screen is displayed, all available tokens for this customer and ship-to are displayed.

Users with CC Token Management security can select a token to use and add, edit, or remove tokens from this screen. Users without that security setting can only select a token to use.

To select a token to complete the transaction, highlight the token and click **Use Selected Token**. The transaction is processed automatically with the selected token.

Pre-authorization/Force Capture processing

To initiate a pre-authorization from **Deposit/Payment Entry**, add a transaction and select the pre-authorization transaction type. The transaction can be completed with a token by clicking **CC Tokens** on the CenPOS screen.

To use an existing pre-authorization transaction and convert it to a payment, double-click the pre-authorization line in the **Deposit/Payment Entry** browser. The **CenPOS ForceCapture CC Transaction** screen is displayed. The **Amount** field contains the value from the preauthorization line. You can change this amount to the full amount that you intend to charge the card.

When going to the footer of an order, invoice, or confirmation, if any pre-authorizations exist on this document, an ‘alert’ message, Note: PreAuths Exist, is displayed.

When running the **Daily Sales Register (SOR315)**, if a document is converted to a back order in whole and none of the pre-authorization is used, then it is retained. If part of the pre-authorization is used toward a partial shipment, then the remaining pre-authorization is removed.

If a document is completed and deleted when the **Daily Sales Register (SOR315)** is run, any existing pre-authorizations for that document are voided via a Web Service call to CenPOS and deleted from FACTS.

Re-authorizing a preauthorization

To manually re-authorize a pre-authorization that is about to expire, highlight the line and click **Re-Auth** in **Deposit/Payment Entry**. If pre-authorization management is implemented, an alert is raised when a pre-authorization transaction qualified for automatic re-authorization fails or pre-auth transactions are expiring. This is based on the customer’s settings and the **# days old** setting in **Credit Card Control**. From the alerts, you can also access **Deposit/Payment Entry** to re-authorize the pre-authorization.

Initiating force capture on a pre-authorization

1 Access the **Deposit/Payment Entry** window from an entry program.

2 Double-click a pre-authorization type C payment line in the line browser.

The amount from the pre-authorization is displayed in the **CC Charge Amount** field. You can specify a different amount as needed.

3 Click **OK** to complete the processing and send the CenPOS ProcessCreditCard/ForceCapture Transact Web Service call.

When you complete the CenPOS processing the original entry program is displayed.

Deleting deposits, pre-authorizations and payments

If the deposit or payment has been acted on, applied, earned, transferred, and so on, you must delete the transaction first and then delete the original deposit or payment.

Pre-authorizations are first voided via a Web Service call to CenPOS and then removed from the FACTS sales order processing files.

Transferred deposits cannot be deleted.

If a deposit or payment was made by a credit card, you cannot delete it. You must void the transaction or refund the payment.

1 Access the **Deposit/Payment Entry** window from an entry program.

2 Select the deposit, pre-authorization, or payment in the browser.

3 Click **Delete**.

4 Click **OK** to confirm.

Re-authorizing pre-authorizations (forced capture)

1 Access the **Deposit/Payment Entry** window from an entry program or alert.

2 In the browser highlight the pre-authorization line (type C payment line) that is about to expire.

3 Click **Re-Auth**.

Using Storefront with FACTS and CenPOS

When using CenPOS in FACTS, you must use version 3.5 of the FACTS Storefront Integration Server to also use CenPOS in Storefront.

Prior to FACTS Storefront Integration Server version 3.5, Storefront must be set up to pass the credit card information to FACTS to charge the card and store the payment as a deposit on the order.

Credit card processing with voice authorization

Credit card processing with voice authorization is not supported with FACTS and CenPOS.

Appendix A Processing credit card transactions during Internet outages

You may experience an Internet outage which could interrupt credit card processing. Business transactions within FACTS, including credit card transactions, must continue regardless of that outage.

These scenarios contain suggested workarounds for continuing with credit card transactions within FACTS during an Internet outage.

Keep in mind that the best practice is to avoid any further credit card processing until you are assured the Internet connection is available again.

n **Company Control F/M (SMF920)** change the **Credit Card Processor** field from **`C-CenPOS`** to **`D-Manual do not collect information`**. You must remember to change this setting back to **`C-CenPOS`** as soon as you have Internet access again.

You can now continue processing credit card transactions within FACTS. Note that any credit card transaction requires a voice authorization with your credit card banking institution.

Examples

In these examples, there are references to making changes in CenPOS or the CenPOS Virtual Terminal. This is an administrator-level function provided by CenPOS that only select authorized users should be allowed to access. It provides you with complete access to all the transactions and settings that have been made against the selected merchant account. For instructions on accessing and using the CenPOS virtual terminal, refer to CenPOS documentation and instructions.

When performing a credit card voice authorization, you are contacting your credit card banking institution, not CenPOS.

These are some example scenarios:

Scenario #1

The Internet is down. You need to process a credit card sale via **Order Confirmation**, **Direct Invoice Entry**, **Counter Sales**, or **AR Cash Receipts and Adjustment Entry**. In this example it is assumed that you want to make a credit card deposit against a new or existing sales order.

Continue with normal processing until you get to the point where you create the deposit with a credit card. Specify the credit card terms code and the amount of the deposit. At this point contact your credit card banking institution to get a voice authorization. You can use the **Payment Entry Memo** and **Notes** fields to specify any reference number or authorization number that you received over the phone. These fields are for reference only. Click **OK** and the new deposit entry is displayed within the **Deposit/Payment Entry** screen. You can continue with normal processing.

Scenario #2

The Internet is back up and you want to void or credit the voice-authorization deposit that you made in scenario #1.

Now that the Internet is back up, re-access **Company Control F/M (SMF920)** and change the **Credit Card Processor** field back to **`C-CenPOS`**. This is an important step and must be done when the Internet comes back online and before any further credit card processing occurs.

To void or credit the credit card deposit that was made in scenario #1. Access the sales order in **Order Entry** and click **Deposits/CC PreAuths**. On the **Deposit/Payment Entry** screen highlight the deposit created while the Internet was down and then click **Apply Trx**. Specify **`Refund/Void`** as the transaction type and the amount to be voided or click **Paid** for the full amount. Click **Save**.

The CenPOS POS interface is displayed, pre-populated as a credit with the amount indicated previously. Specify the same card number that was used when the deposit was made while the Internet was down. Fill out the remaining required fields. Click **Submit** on the CenPOS POS interface and the credit is issued to the cardholder. Normal processing continues.

Scenario #3:

In this scenario a pre-authorization on a sales order was processed while the Internet was up. The Internet went down but you must confirm and finalize the order by performing a special force transaction sale against the pre-authorization. Without an Internet connection you cannot perform a special force transaction, but the customer needs the sale finalized and processed against their credit card.

In **Company Control F/M (SMF920)** change the **Credit Card Processor** field from **`C-CenPOS`** to **`D-Manual do not collect information`**. You must remember to change this setting back to **`C-CenPOS`** as soon as you have Internet access again.

Access the sales order in **Order Confirmation** and process everything as normal until the **Payments** screen is displayed. Notice that the **Payments** screen contains the indicator, *PreAuths Exist*. Click **Payments** and then select the pre-authorization to process as a special force sale transaction. Delete the pre-authorization.

Keep in mind that deleting the pre-authorization only removes it from FACTS. The pre-authorization still exists in CenPOS. Access the CenPOS Virtual Terminal when the Internet comes back online to remove the pre-authorization from the CenPOS system too. If the pre-authorization is not a significant amount you can do nothing with the pre-authorization and let it expire at its normal expiration time, usually seven days.

After deleting the pre-authorization, follow the same steps as in scenario #1. Create a new sales or credit card transaction for the order. Specify the reference number and authorization number provided during the voice authorization process in the **Memo** and **Notes** fields of **Deposit/Payment Entry**.

You can run the **Daily Sales Register (SOR315)** at any time in this scenario, while the Internet is still down or once it is restored.

Note: Any time you leave a pre-authorization transaction in place and create a separate sale transaction, you have the possibility of exceeding the customer's credit limit. The pre-authorization holds that amount against their credit limit until it expires or is deleted.

Scenario #4

This scenario is the same as scenario #3 but the pre-authorization is not deleted. Then follow the same steps as in scenario #1 to create a new sales or credit card transaction for the order. Specify the reference number and authorization number, provided during the voice authorization process, in the **Memo** and **Notes** fields of the payment entry.

The difference between this scenario and scenario #3 is that you do not run the **Daily Sales Register (SOR315)** until you are certain that the Internet connection has been restored. By waiting for the Internet connection to be restored and then running the **Daily Sales Register (SOR315)**, the pre-authorization that was left on the sales order is deleted from FACTS and voided in CenPOS by the Daily Sales Register processing. This would be the preferable method instead of scenario #3 because you do not have to manually access the CenPOS Virtual Terminal and remove the pre-authorization.

Credit card tokens in an Internet outage

It is not possible to manage credit card tokens while the Internet connection is down. Adding, editing, or deleting credit card tokens requires an Internet connection.