micros®

Restaurant Enterprise Series

Chase Paymentech Credit Card Driver for 3700 POS

Version 4.10

November 21, 2012

MD0003-171

Declarations

Warranties

Although the best efforts are made to ensure that the information in this document is complete and correct, MICROS Systems, Inc. makes no warranty of any kind with regard to this material, including but not limited to the implied warranties of marketability and fitness for a particular purpose.

Information in this document is subject to change without notice.

MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

Trademarks

Installation and Setup

This section contains installation and setup instructions for the Version 4.10.21.2388 release of the Chase Paymentech (CaCP) Credit Card Driver. The release version is available on the MICROS web site Product Support page.

This version of the Chase Paymentech may be used on RES systems running Version 4.5 or higher.

In This Section...

Features

The following features have been implemented in the Chase Paymentech Driver:

- Communication Channels
    - Secure Network
- Prepaid Card Support
    - Partial Authorizations
    - Credit Card Balance Inquiry
- Authorization Reversal
    - Time out
    - Pre-settlement
- Duplicate Batch Prevention
- Auto Offline Authorization
- RFID Support
- AVS/CVV Support
- AMEX Direct/Network PIP
    - Authorizations are processed with the AMEX Driver and can be settled with the Chase Paymentech Driver.
- eCommerce Transactions
- Multi-Merchant Support

Installation

Site Requirements

Before installing the Chase Paymentech Driver on the RES system, the following configuration items should be considered:

- The installed version of 3700 POS should be Version RES 4.5 or higher.
- To use Internet Connectivity, an Internet connection must be configured and working. ISP software is needed to connect to the Internet.
- Security protocols, including firewalls and other protections, should be in place.
- The site's browser software will need to support 128-bit session keys.

Files Included

The following list the files installed for the driver:

\MICROS\Res\Pos\Bin\Paymentech\etc\linehandler.properties
\MICROS\Res\Pos\Bin\Paymentech\etc\log4cplus.properties
\MICROS\Res\Pos\Bin\Paymentech\etc\root2028.pem
\MICROS\Res\Pos\Bin\Paymentech\lib\log4plus.dll
\MICROS\Res\Pos\Bin\Paymentech\lib\ptCoreSDK.dll
\MICROS\Res\Pos\Bin\Paymentech\lib\SDKVersion.dll
\MICROS\Res\Pos\Bin\CaCP.dll
\MICROS\Res\Pos\etc\CaCP.cfg
\MICROS\Res\Pos\Bin\CaCP.hlp
\MICROS\Res\Pos\Bin\CaCP.cnt

Additional Files:

\WINDOWS\winsxs\MSVCP90.dll

Note *The MSVCP90.dll file is installed if it is not found in the \WINDOWS\winsxs directory when the installation program is executed.*

Note *If Paymentech Gift Cards were installed prior to loading the CaCP Driver, then the ETC folder will not be installed. It uses the equivalent files installed in \Program Files\Paymentech\Netconnect folder.*

Installation Instructions for a Site Running RES 4.5 or Higher

The installation of the credit card is now separate from the RES software. After each installation of RES software — whether it is a general release, service pack or hotfix — you MUST re-install the site's requisite credit card drivers.

The database can be at Front-of-House status while installing this driver.

1. Make sure all current batches have been settled. MICROS recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the latest Chase Paymentech Credit Card Driver from the MICROS web site. Copy this file to your RES Server's temp folder.
3. Double click on the **CaCP(4.10.21.2388).exe** file. This will install of the necessary files on RES Server and the BSM Client, and Windows Services will be restarted automatically.
4. If the server is RES 5.0 or higher, the server will need to rebooted after installing the driver. This will ensure that the environment variables are loaded properly.

NOTE: The following error will appear if the server has not been rebooted after installation:

- ***'Driver not programmed attempting credit auth'***

File	RES Server	Backup Server Client
linehandler.properties See Note 1 below	\MICROS\Res\Pos\Bin\Paymentech\Etc	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin\Paymentech\etc
log4cplus.properties	\MICROS\Res\Pos\Bin\Paymentech\Etc	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin\Paymentech\etc
root2028.pem	\MICROS\Res\Pos\Bin\Paymentech\Etc	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin\Paymentech\etc
log4plus.dll	\MICROS\Res\Pos\Bin\Paymentech\lib	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin\Paymentech\lib
ptCoreSDK.dll	\MICROS\Res\Pos\Bin\Paymentech\lib	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin\Paymentech\lib
SDKVersion.dll	\MICROS\Res\Pos\Bin\Paymentech\lib	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin\Paymentech\etc
CaCP.dll	\MICROS\Res\Pos\Bin	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin

File	RES Server	Backup Server Client
CaCP.cfg	\MICROS\Res\Pos\etc	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\etc
CaCP.hlp	\MICROS\Res\Pos\Bin	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin
CaCP.cnt	\MICROS\Res\Pos\Bin	\MICROS\Res\CAL\Win32\Packages\CaCP\Micros\Res\Pos\Bin
MSVCP90.dll/ Instmsvcr90.bat See Note 2 below	\WINDOWS\ winsxs	\MICROS\Res\CAL\Win32\Packages\CaCP

NOTE 1: The linehandler.properties file should not be edited. This file comes standard to communicate to the host.

NOTE 2: This batch file calls 'vcredist_x86.exe' to install required MSVCP90.dll, if not currently found on the client.'

- If changes have been made to the linehandler.properties file, the user will need to accomplish the following:

1. On the RES Server's Desktop: highlight 'My Computer', right-click mouse and select 'Properties'.

2. Select Advanced | Environment Variables, in System Variables, scroll down to 'PAYMENTECH_HOME'. Write down from the Value column, the current path location.

Note *This path will vary depending on what order Credit Card and/or Gift Card related files have been installed.*

---

3. In Windows Explorer, go to the path location written down Step 2 above. Highlight the ***linehandler.properties*** file, located in this folder.

4. Copy the ***linehandler.properties*** file into \MICROS\RES\CAL\Win32\Files\MICROS\RES\POS\BIN\Paymentech\Etc folder.

- In the event that the server is offline or goes down for any reason, the Backup Server Mode (BSM) client can take over handling all credit card authorizations; until the server is back online.

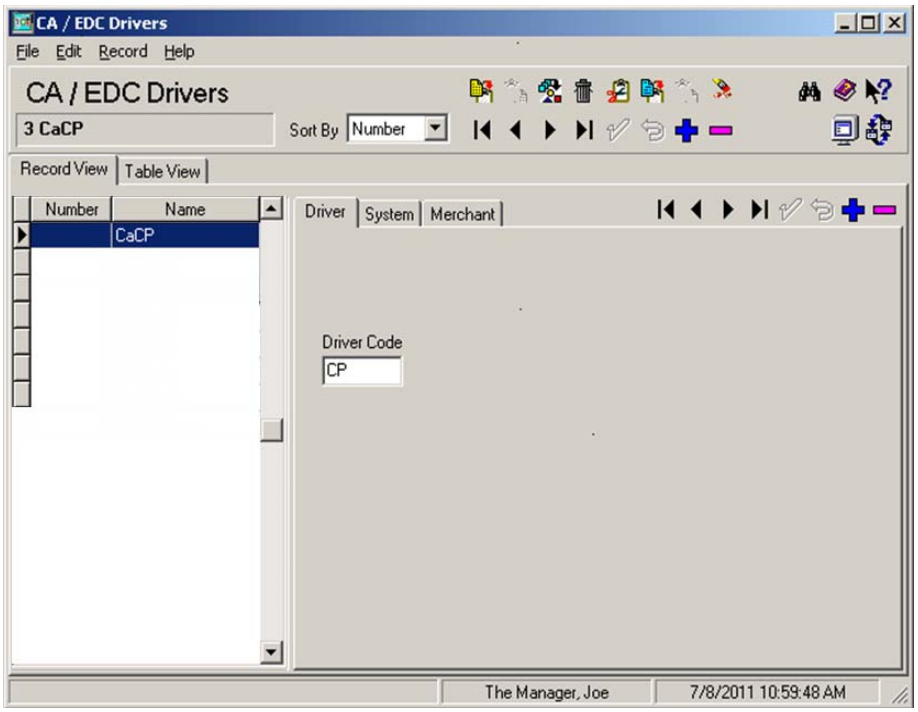
- Reboot the Win 32 client (BSM) after the driver installation. This is will ensure that all required Chase Paymentech environment variables load properly.

Configuration Instructions

Follow these steps to complete configuration for the driver:

1. Go to *POS Configurator* | *Devices* | *CA / EDC Drivers* and select the blue plus sign to add a record.

2. Enter a **Name** (For example: **Chase Paymentech** or **CaCP**) and a value of the **Driver Code** field (**CP**) and save the record.



3. Go to the *System* tab and configure the following settings:

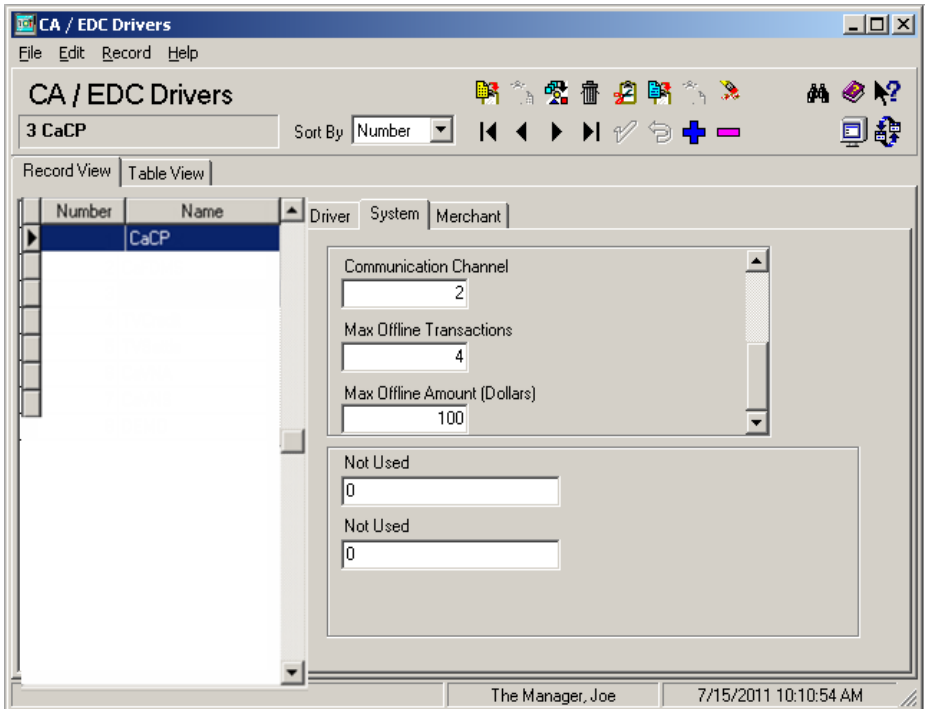
   - **Not Used** – Leave this field blank.
   - **Not Used** – Leave this field blank.
   - **Not Used** – Leave this field blank.
   - **Communication Channel** – This field specifies the type of interface connection used between the merchant and the credit card processor. At this time this field will default to 2 for internet connection.
   - **Max Offline Transaction** – This option controls the maximum number of automatic offline transactions that can be processed by the driver. When this limit is exceeded, the “Manual Auth Required” error message will be returned

to POS Operations. This value will accumulate until the time that a batch is successfully settled by the settlement driver. At that time, the value is re-set.

- **Max Offline Amount (Dollars)** – This option controls the maximum dollar value of automatic offline transactions that can be processed. The maximum offline amount is entered as dollars and cents with no decimal (e.g., 2500 is the equivalent of $25.00). When this limit is exceeded, the "Manual Auth Required" error message will be returned to POS Operations. This value will accumulate until the time that a batch is successfully settled by the settlement driver. At that time, the value is re-set.

> ***Note*** *Auth Offline At Settlement - This option works in conjunction with the Offline Auth feature and is enabled by default. This driver requires this option to always be enabled, therefore this option is no longer displayed. (The driver .cfg file sets this option to be enabled.) At the time of settlement is any transaction that needs to be authorized, will be processed during pre-settlement.*

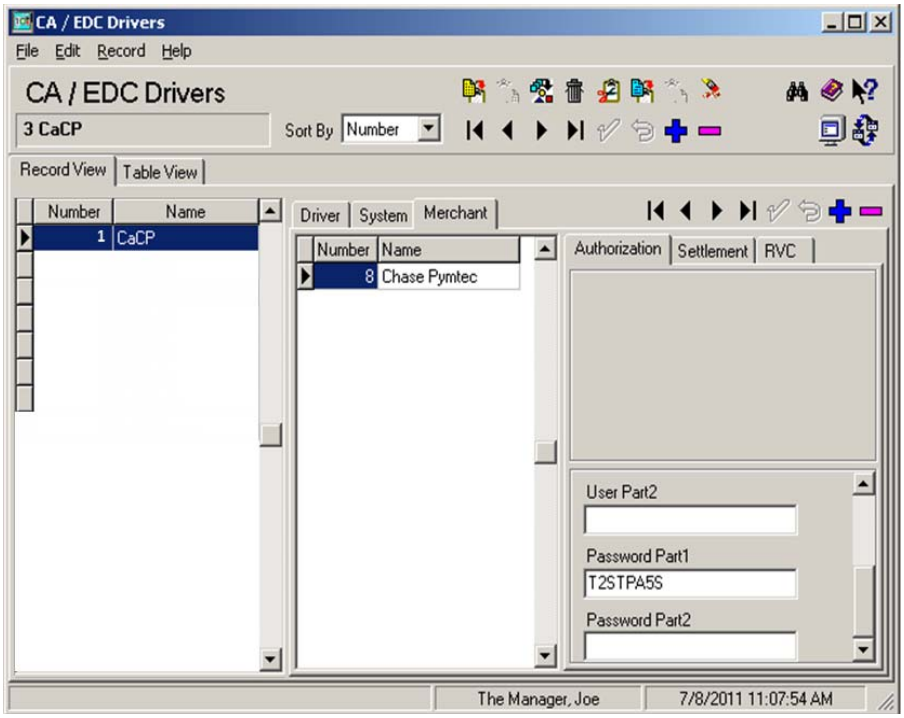
- **Not Used** – Leave this field blank.
- **Not Used** – Leave this field blank.



4. Go to the *Merchant* | *Authorization* tab and configure the following settings:

- **Merchant ID** – Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor

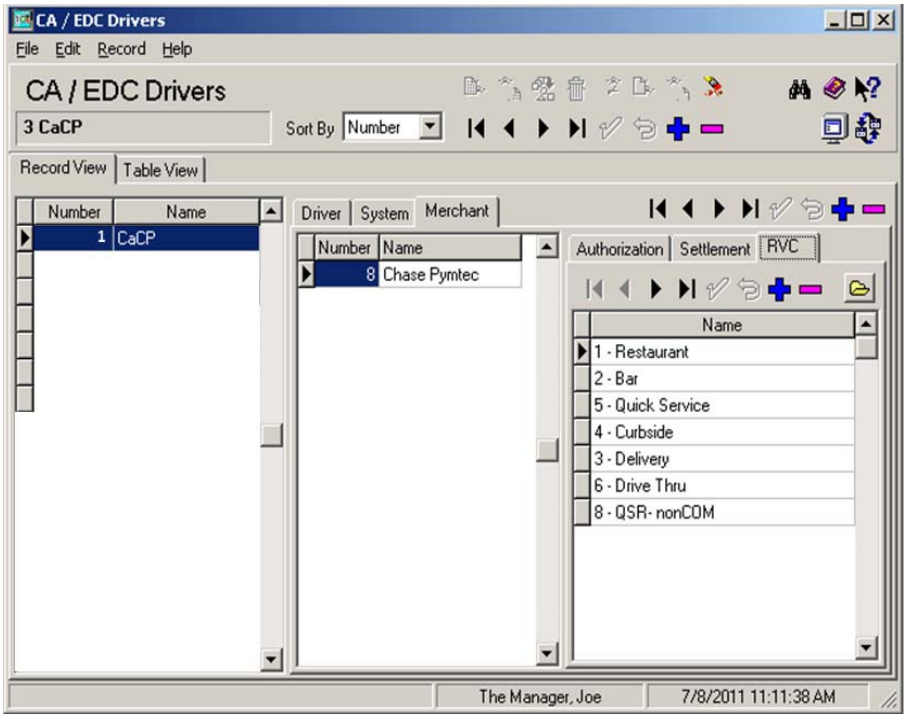
- **Terminal ID** – Enter the unique 1 to 3 digit Terminal ID number assigned by the Credit Card Processor.
  - **Important Note: All Merchant ID information must be obtained from your Chase Paymentech Representative.**
- **User Part1** – Enter the user name that is supplied by the bank. 25-digits are the maximum characters allowed in this field. If user name extends past 25-digits, the rest of the user name can be entered in the field *'User Part2'*.
- **User Part2** – If the user name extends past 25-digits in the field *'User Part1'*, enter the rest of the user name in this field.
- **Password Part1** – Enter the password that is supplied by the bank. 25-digits are the maximum characters allowed in this field. If password extends past 25-digits, the rest of the password can be entered in the field *'Password Part2'*.
- **Password Part2** – If the password extends past 25-digits in the field *'Password Part1'*, enter the rest of the password in this field.



5. Go to the *Merchant* | *RVC* tab and configure the following settings:

- **Merchant Name/Number** – Lists the names of each merchant associated with the POS System. This option allows a user to establish multiple merchant Ids for accounting and reporting purposes

- **RVC Name** – Lists the name of the revenue centers linked to the highlighted Merchant ID. When adding a new record, right click in the Name field to open the drop-down list of all the revenue centers configured across the POS System.
  - **Note: A revenue center may only be linked to one Merchant at a time. Attempts to link to more than one will result in an error message.**

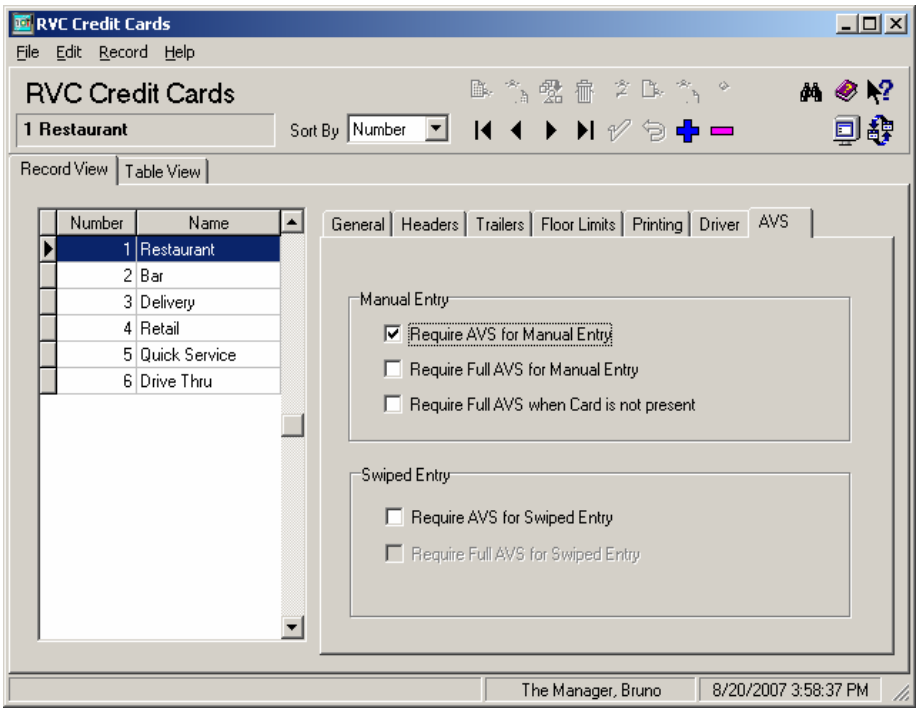


6. Go to *POS Configurator* | *SALES* | *Tender / Media* | *Credit Auth* form. Link all of the appropriate credit card tenders (e.g., Visa/Mastercard) to the CP driver by configuring the following fields:

   - **CA Driver** – Use the drop down box to select the CaCP driver.
   - **EDC Driver** – Use the drop down box to select the CaCP driver.

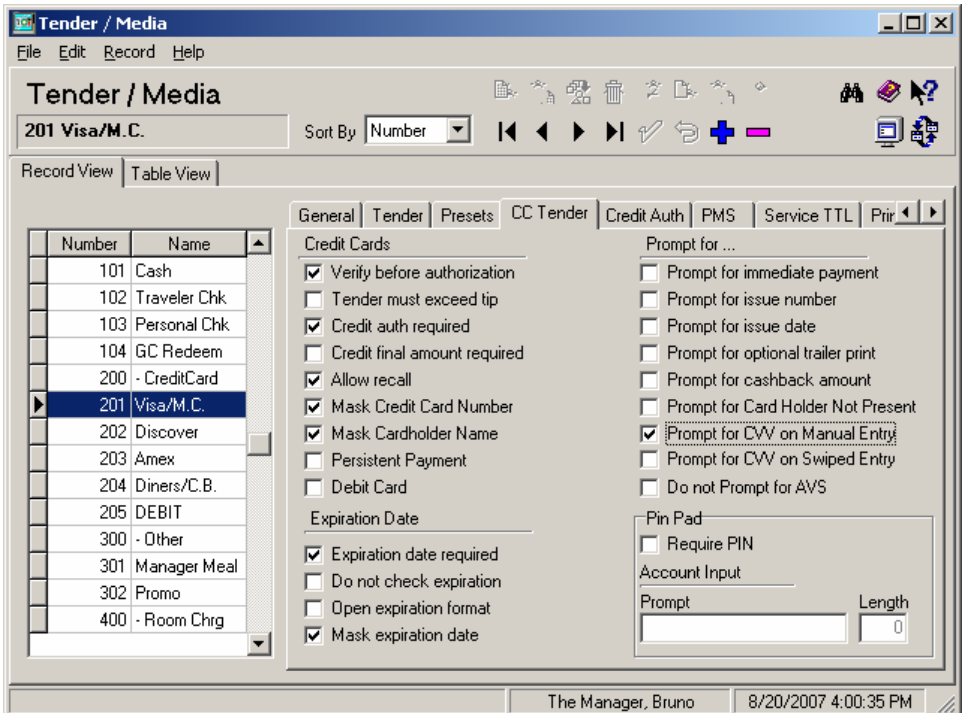
7. Go to *POS Configurator* | *SALES* | *Tender / Media* | *CC Tender.* Configure these options to mask the Card Number, Customer Name, and Expiration Date on all credit card transactions. This is required for Credit Card Security (PCI Compliance).

8. If AVS and CVV are configured at the site complete step 8. If not go to step 11. Go to the *Revenue Center* | *RVC Credit Cards* | *AVS* tab and enable the following options. Select the options as they are appropriate for the site.



- **Require AVS for Manual Entry -** Select this option to prompt for the cardholder's zip code before submitting a manual credit card authorization.
- **Require Full AVS for Manual Entry -** Select this option to prompt for the cardholder's address AND zip code before submitting a manual credit card authorization. This option is only enabled if the Require AVS for Manual Entry option is enabled.
- **Require Full AVS when Card is not present -** Select this option to determine whether the credit card is present before proceeding. If it is, the system will prompt for the zip code only. If it is not, the system will prompt for the cardholder's complete address and zip code. This option is only enabled with the Require AVS for Manual Entry option is also enabled.
- **Require AVS for Swiped Entry -** Select this option to prompt for the cardholder's zip code before proceeding with a swiped credit card transaction.
- **Require Full AVS for Swiped Entry -** Select this option to prompt for the cardholder's address AND zip code before proceeding with a swiped credit card authorization. This option is only enabled with the Require AVS for Swiped Entry option is also enabled.

Go to the *Sales* | *Tender / Media* | *CC Tender tab* and enable the following options. Select the options as they are appropriate for the site.



- **Prompt for CVV on Manual Entry**. Select this option to display the following menu of options when a credit card is manually entered. To proceed, the user must select one of these options and respond accordingly.
  - Intentionally not provided.
  - Present and will be provided.
  - Present but is illegible.
  - Not present.
- **Prompt for CVV on Swiped Entry**. Select this option to display the following menu of options when a credit card is swiped. To proceed, the user must select one of these options and respond accordingly.
  - Intentionally not provided.
  - Present and will be provided.

9. Go to the *Sales* | *Tender / Media* | *CC Tender* tab and enable the following options for all credit cards configured as they are appropriate for the site.

- **Verify before authorization** - Select this option to test for a valid credit card number before processing.

- This option is active only with the following setting:
  - Reference required (Tender/Media)

- **Prompt for Card Holder Not Present** - Select this option to prompt the server location when a credit card number is entered manually. If a confirmation message displays, the server can make three choices:
  - **Yes -** Select this option if the cardholder is present.
  - **No -** Select this option if the cardholder is not present.
  - **Cancel -** Select this option to abort the authorization attempt.
- This option works with the following setting:
  - Disable Prompt for Card Holder Not Present (RVC Credit Cards)

10. Go to the *Sales* | *Tender / Media* | *Credit Auth* tab and enable the following option for all credit cards configured as they are appropriate for the site.

- **Allow partial authorization**- Enable this option to allow this credit card tender to preform partial authorizations. A partial amount is any amount less than the amount required by the credit card driver.

11. Reload the database from the MICROS Control Panel.

12. Go to *Start* | *Programs* | *MICROS Applications* | *POS* | *Credit Card Batch*. Click on the Diagnostic tab and select the **Test Auth Connection** and the **Test Settlement Connection** buttons to verify that the drivers are up and running. A few test transactions can also be done to ensure all is working correctly.

NOTE: The Chase Paymentech Driver currently does not support the Authorization and Settlement Connection Diagnostics tests.

Removing the Software

Removing Software From a Site Running RES 4.5 or Higher

Follow these steps to remove the CaCP driver software from the RES Server and Backup Client:

1. Shut down the RES system from the **MICROS Control Panel**.
2. Delete the following files:
   - \MICROS\Res\Pos\Bin\Paymentech
   - \MICROS\Res\Pos\Bin\CaCP.dll
   - \MICROS\Res\Pos\etc\CaCP.cfg
   - \MICROS\Res\Pos\Bin\CaCP.hlp

- \MICROS\Res\Pos\Bin\CaCP.cnt

3. Delete the following files on the server:
   - MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\Paymentech
   - \MICROS\Res\CAL\Win32\Packages\CaCP
4. Shut down the RES System on the Backup Server Client (if applicable).

   Also on the BSM Client, delete the following driver files:
   - \Micros\Res\Pos\Bin\Paymentech
   - \Micros\Res\Pos\Bin\CaCP.dll
   - \Micros\Res\Pos\Bin\CaCP.hlp
   - \Micros\Res\Pos\Bin\CaCP.cnt
   - \Micros\Res\Pos\Etc\CaCP.cfg

Frequently Asked Questions

FAQ

Why is reading the Credit Card Transfer Report so important?

Errors during transmission are not always rectified automatically. To ensure a smooth and effective operation, end-users should regularly perform credit card batch and transfer processes along with an audit of the MICROS system. Frequent audits allow the end-user to identify problems quickly and, if necessary, place a call support to correct a batch with errors.

Audit procedures are generally done the next day. Information describing the 3700 POS Credit Card Process is provided below.

What is a credit card batch?

MICROS 3700 POS allows credit cards to be authorized throughout the day. This authorization process is done when a guest asks to pay his transaction with his credit card. The POS then stores that credit card information along with the transaction in the RES database.

At the end of the day, a process is run to combine all the credit card transactions into a batch. This groups all of these types of transactions into a single message that will be sent to the credit card host (during the transfer process). A batch report can also be run listing each individual credit card transaction, sorted by credit card type.

When a credit card batch is initiated (either through an end of night autosequence or manually using the Credit Card Batch Utility), the system takes all credit card transactions that occurred and combines them into batch files. Batches can be generated one of two ways:

1. One batch for all revenue centers (i.e, all transactions at the site).
2. One batch per revenue center

Batches can also be edited. MICROS allows any manually entered fields to be edited.

- Credit card number
- Expiration date

Once a batch is created, the site needs to transfer the batch. Typically, this is done once a day as part of the end-of-night procedures. The transfer process takes the batch created and sends it to the credit card host for processing.

MICROS supports two types of processing — Terminal-based and Host-based. The processing type is determined by the credit card driver selected.

Terminal-based processing requires that the entire batch be successful for the batch to be closed. Most of the 3700 POS drivers support terminal-based processing. The Chase Paymentech Credit Card driver uses this type.

Host-based processing requires each transaction to be successful. This means a batch could contain a single card that did not transfer to the credit card host. Once this transaction is adjusted, the batch could be re-sent to the host.

Transfer Status Report

The 3700 POS includes a Transfer Status Report, a one-page, easy-to-read summary for the end-user. The report shows each batch that was transferred and whether or not it was successful.

The Transfer Status Report should be added to the End-of-Night process and the site should be trained to read the report on a daily basis. Users can then call for support if an error condition appears.

IT IS IMPORTANT THAT A SITE READ THIS REPORT AFTER EACH TRANSFER. A BATCH MAY NOT PROCESS FOR SEVERAL REASONS SOME OF WHICH REQUIRE SUPPORT TO INTERVENE. IF THESE BATCHES ARE LEFT UNATTENDED, THE FOLLOWING ISSUES MAY ARISE:

1. A batch may never be processed which means the merchant may never receive the funds for those transactions.
2. A duplicate batch may be processed causing the customer to be charged twice.

How can a duplicate batch occur?

Duplicates occur when the system sends a batch to the credit card host and the host send back a response that does not makes it all the way to the 3700 POS. When this happens, the POS will send the message a second time.

Please note that credit card hosts may have rules in place to catch a second (duplicate) transmission of the batch, using criteria such as transaction amount or card numbers. These rules provide a temporary window for the user to rectify the problem before the batch is submitted again. *The resubmission is not dependent*

on action by the end-user. Eventually, if the 3700 POS continues to send the batch, a duplicate will be generated.

To correct this problem, MICROS has added enhancements to the Chase Paymentech Driver (CaCP) for the prevention of duplicate batches.