

**ORACLE**

**Oracle Hospitality RES 3700**

*TSYS*

*Credit Card Driver*

*Version 5.1*

**July 2016**

Copyright © 2013, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Installation and Setup

---

This section contains installation and setup instructions for the Version 5.1 release of the TSYS Acquiring Solutions (CaTSYS) Credit Card Driver. The release version is available on the Oracle web site Product Support page.

This version of the TSYS driver may be used on RES systems running Version 5.0 or higher.

## In This Section...

• Features .....	3
• Installation .....	4
• Pre Installation Requirements .....	4
• Site Requirements .....	5
• Files Included .....	5
• Installation Instructions .....	6
• Configuration Instructions .....	7
• Configuring Intermediate Certificates .....	15
• Feature Support .....	16
• Password Support .....	20
• End of Day Procedures .....	21
• Removing the Software .....	23
• Password Handling Process .....	24
• Troubleshooting Tips .....	27
• Frequently Asked Questions .....	28

---

## Features

The following features have been implemented in the CaTSYS Driver:

- Communication Channels
  - HTTPS
- Prepaid Card Support
  - Partial Authorizations
  - Credit Card Balance Inquiry
- Authorization Reversal
  - Time out
  - Un-used Authorizations
- Zero Dollar Verification
- Auto Offline Authorization
- AVS/CVV Support
- eCommerce Transactions
- Multi-Merchant Support
- Host Based Settlement
- Automatic Password Rotation (with encryption)

## *Installation*

### **Pre Installation Requirements**

Before installing the TSYS Driver on the RES system, the site must contact TSYS Acquiring Solutions to obtain the following:

- Documentation for using the Merchant Center web site.
- Internet Host Header
- Internet Target Name
- Host URL
- Backup Host URL
- Automated e-mail with the Administrator User Name, Password and Device ID

#### **Important:**

Before installing the TSYS Driver, the merchant must work with their TSYS representative to establish an account to connect to the TransIT processor. An email from the TSYS Merchant Center will confirm the account has been created. The email will contain an Administrator User ID and Password as well as the URL address needed to connect the Oracle system to the TSYS Acquiring Processor.

Once logged in using the Administrator User ID, it will be necessary to create a Store Operator User ID. This User will be used by the Oracle system for all credit authorizations for this location. In Merchant Center, click on Preferences | Admin | Employee Configuration. Select ADD A USER to create the new user giving it the name of your choice. Give this user the Supervisor function. Check all the available boxes. Make a note of the Store User ID as it will be used in the configuration of the TSYS Driver in the Micros POS Configurator.

Log out of the Administrator User ID and log back in with the Store Operator ID.

Please read the Password Handling Process (page 24) before installing the TSYS Credit Card Driver.

---

**Note**     *If you have any questions related to the TSYS Merchant Center Website, please contact TSYS representative.*

---

The site will get the Merchant ID directly from the bank.

## Site Requirements

Before installing the TSYS 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\CaTSYS.dll*  
*\MICROS\Res\Pos\Etc\CaTSYS.cfg*  
*\MICROS\Res\Pos\Bin\CaTSYS.hlp*  
*\MICROS\Res\Pos\Bin\CaTSYS.cnt*  
*\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.dll*  
*\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTSYS.cfg*  
*\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.hlp*  
*\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.cnt*  
*\WINDOWS\system32\MSVCR71.dll*

---

**Note**     *The MSVCR71.dll file is installed if it is not found in the \WINDOWS\system32 directory when the installation program is executed.*

---

## **Installation Instructions for a Site Running RES 5.0 or Higher**

The installation of the credit card driver is separate from the RES software. When a site loads a new version of RES software, the TSYS driver files and configuration will remain on the system. They do not need to be reinstalled.

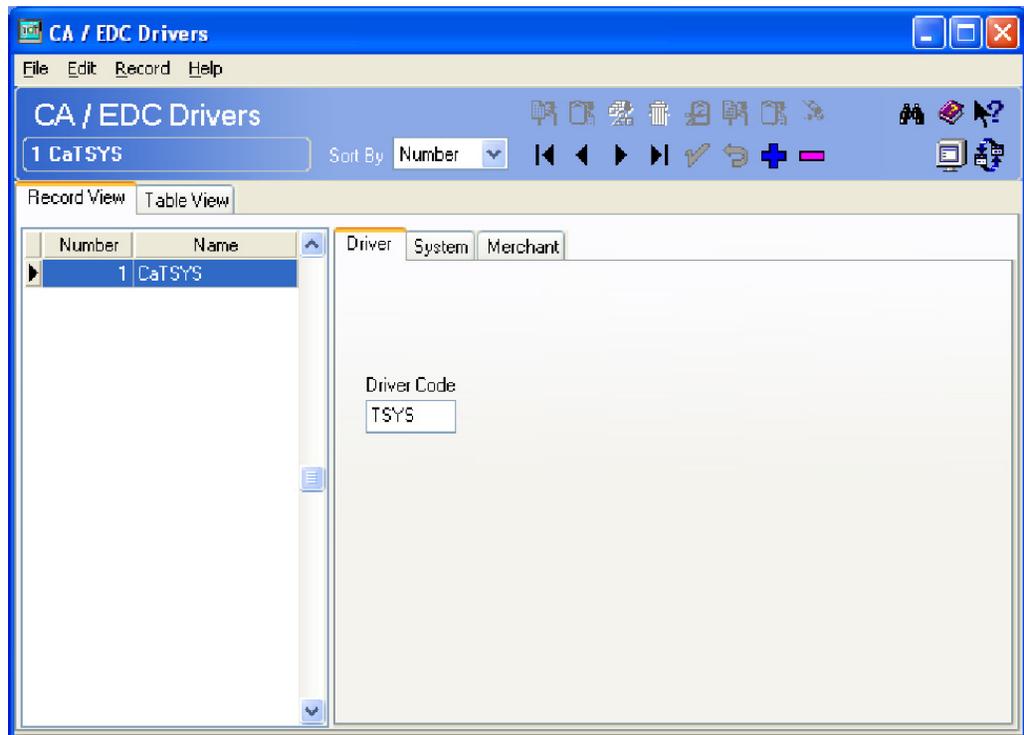
The database can be at Front-of-House status while installing this driver.

1. Make sure all current batches have been settled. Oracle 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 TSYS Credit Card Driver from the Oracle web site. Copy this file to your RES Server's temp folder.
3. Double click on the **CaTSYS(5.1).exe** file. This will install of the necessary files on RES Server and the BSM Client, and Windows Services will be restarted automatically.
4. Reboot the RES Server.

## Configuration Instructions

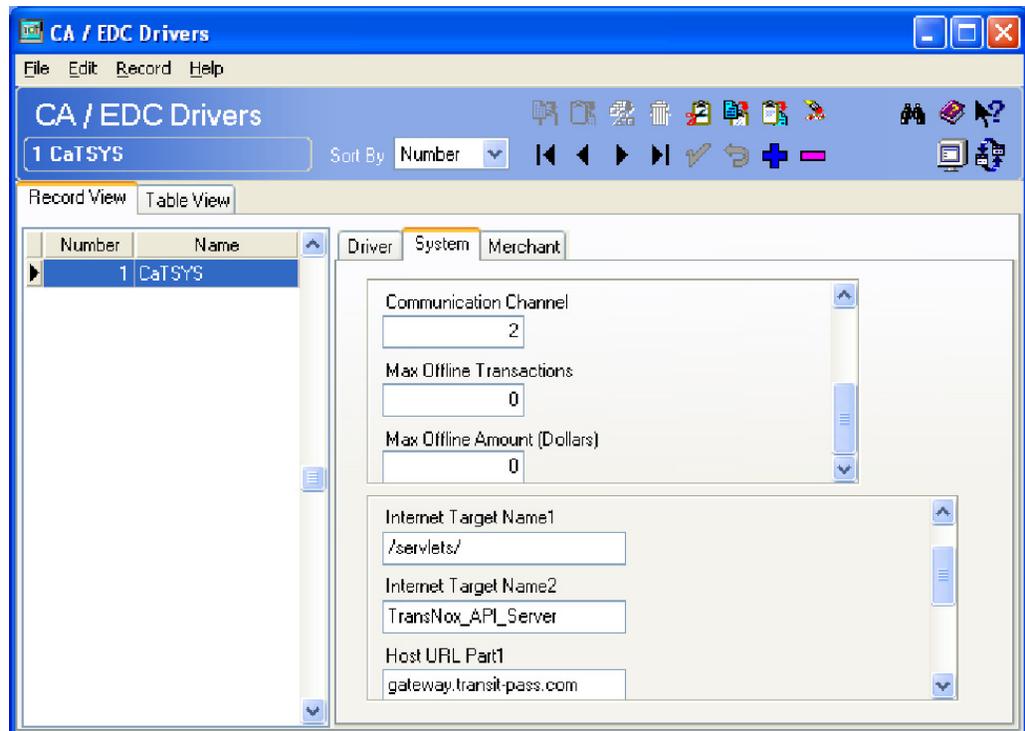
Follow these steps to complete the configuration for the driver:

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



- Enter a **Name** (For example: **TSYS** or **CaTSYS**) and a value of the **Driver Code** field (**TSYS**) and save the record.

2. 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. This field will default to 2 for an 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.

When either limit is exceeded the driver will return the 'Manual Auth Required' error to OPS. For Auth&Pay (e.g., the CC Lookup function key) tenders OPS will automatically prompt for a manual authorization code.

The total count and dollar value of the offline authorizations is reset any time a batch is successfully settled by the settlement driver. In addition a new driver diagnostic has been added which will reset the totals to zero. This diagnostic is available through both the credit card GUI and the command line settlement application.

The system wide limits are not enforced when the workstations are operating in SAR mode.

---

**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, any transaction that needs to be authorized will be processed during pre-settlement.*

---

For additional information on **Auto Offline Authorizations**, please refer to page 16.

- **Internet Host Header** – Enter the HTTP host name to be included in every outgoing authorization request. Up to 25 characters is allowed.
- **Internet Target Name1** – Enter the HTTP target name to be included in every outgoing authorization request. Up to 25 characters is allowed. If no existing data exists, it will default to the following:

```
/servlets/
```

- **Internet Target Name2** – Enter the remaining target name if longer than 25 characters from the previous field. If no existing data exists, it will default to the following:

```
TransNox_API_Server
```

- **Host URL Part1** – Enter the first part of the URL address of the primary host connection. This consists of the protocol and site name. If no existing data exists, it will default to the following:

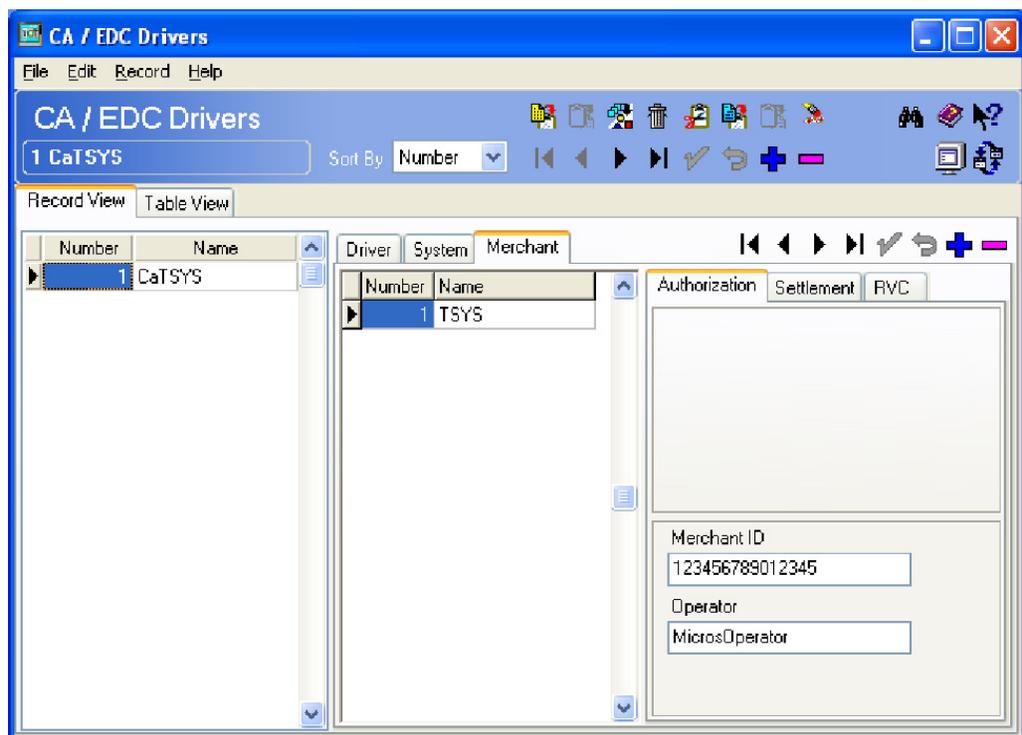
```
gateway.transit-pass.com
```

- **Host URL Part2:Port** – Enter the second part of the URL address of the primary host connection. This consists of the domain and port number.

```
leave this field blank
```

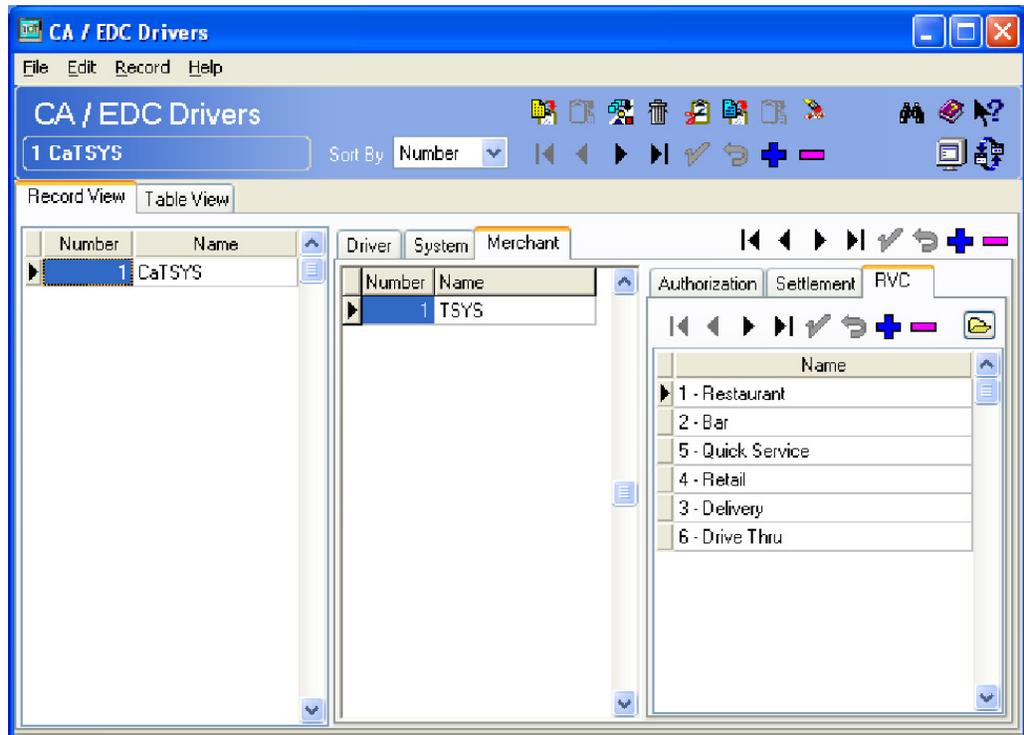
- **BackUP URL Part1** – Enter the first part of the URL address of the backup host connection. This consists of the protocol and site name. Backup connections are triggered when the system cannot establish communication via the primary host address.
- **BackUP URL Part2:Port** – Enter the second part of the URL address of the backup host connection. This consists of the domain and port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

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



- **Merchant ID** – Enter the number used to identify the merchant. This number is assigned by the Credit Card Processor (bank). The valid range is 3-20 digits.
- **Operator** – Enter the Operator User ID added to TSYS Merchant Center as described on page 4. chosen for this site. The valid range is 6-20 alphanumeric characters. This is the *Operator* name that is used to identify this store. For example, *Store1234* and the second site to be rolled out might be *Store5678*. Each site that the driver is installed in requires it's own Operator name. Per *Pre Installation Requirements* note on Page 4, your TSYS representative will provide instructions on how to access the TSYS Website and obtain a temporary password for each installation.

4. 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 ID's 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.**

### Single Merchant Site

If only one Merchant ID is issued by the bank for this site, then in Credit Card Batch | Diagnostics | Set Host Password only use the first Revenue Center number to enter the Password (see page 20).

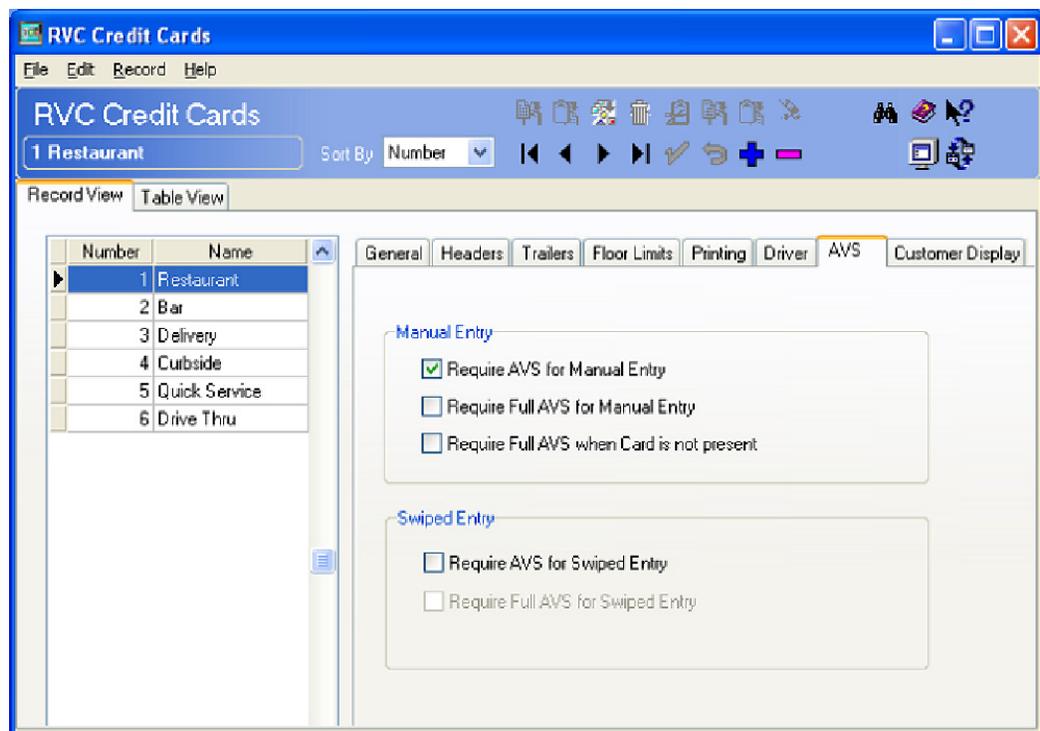
## Multiple Merchant Site

If there are two or more Merchant ID's issued by the bank for this site, then add Merchant 2 and link the appropriate RVC's to each Merchant IFD. For example, above there are six RVC's. If RVC 6 (Drive Thru) is assigned Merchant ID 2, then in Credit Card Batch | Diagnostics | Set Host Password, enter Merchant ID 2's Operator ID and Password (see page 20).

Merchant ID 1 = 1|Password@123 (this will cover RVC's 1-5)

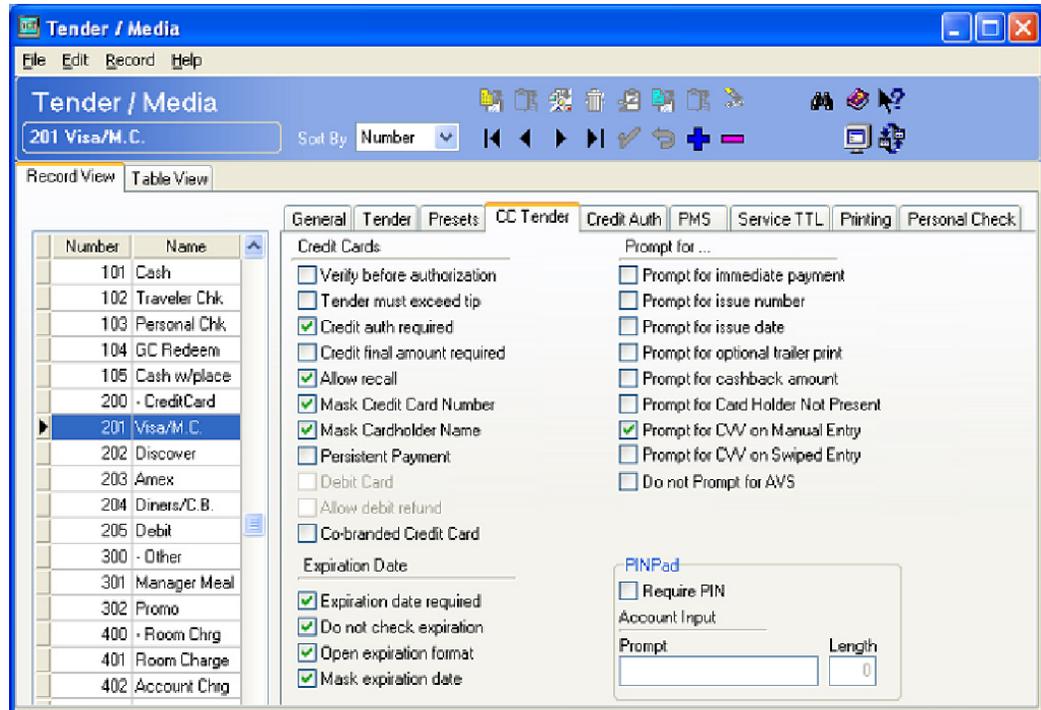
Merchant ID 2 = 6|Password@123 (this will cover RVC 6)

5. Go to *POS Configurator* | *Sales* | *Tender / Media* | *Credit Auth* form. Link all of the appropriate credit card tenders (e.g., Visa/Mastercard) to the TSYS driver by configuring the following fields for each card type:
  - **CA Driver** – Use the drop down box to select the CaTSYS driver.
  - **EDC Driver** – Use the drop down box to select the CaTSYS driver.
6. 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).



7. 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 password needs to be set in the Diagnostics tab prior to the Authorization and Settlement Connection Diagnostics tests.

## **Configuring Intermediate Certificates**

To establish a trusted end-to-end Internet connection, you must build and verify a certificate chain by downloading or adding intermediate certificates to the trust list on the credit card server. To enable automatic downloads, open outgoing connections to the URL for each intermediate certificate.

## Features Supported

### Auto Offline Credit Card Authorization Support

When a site goes offline, and their credit card network connection is unavailable, the site must perform manual credit card authorizations by selecting the [Manual Authorization] key and entering an authorization code. In many situations, a site may not want to spend the time to obtain a voice authorization over the phone from the credit card processor because of the business disruption this poses. Instead, the site will make up their own authorization code, and assume the risk of a charge back.

RES has enhanced the manual authorization process so that a site can configure the manual authorization code to generate automatically. This feature streamlines the manual authorization process so that employees do not spend additional time manually entering authorization codes. This feature is ideal for an environment where voice authorizations are not sought for manual credit card transactions.

Additionally, this feature minimizes the risk of fraud that could arise from employees who realize that the network is down, and that the site is not obtaining card authorizations from the credit card processor. An automatically generated code would prevent the operator from realizing that the system is down.

### Basic Use Cases

**Example 1:** In a quick service environment transaction amounts are small and the number of declined transactions are small. When a restaurant goes offline, rather than slow down service by obtaining a voice authorization for every transaction, the restaurant would prefer to risk a charge back by forcing transactions through without an authorization code.

**Example 2:** A restaurant is concerned that while offline, the employees will be able to fraudulently tender transactions to known bad credit cards. By removing the error message presented to the employee when an online authorization fails, the employee can no longer distinguish between online and offline transactions. This prevents the employees from knowing when the system is unable to contact the credit card processor for authorization.

### How It Works

When the Automatic Offline Credit Card Authorization feature is enabled, the transaction will flow as follows:

#### Authorization

1. The driver is unable to contact the credit card host through the primary and backup Host URL's.

2. The driver will generate a random 6-digit authorization code and return an approval to POS Operations (Approval is dependent upon whether floor limits are used, continue reading for more information).

The credit card driver will only generate an automatic offline authorization code when it is unable to contact the credit card host. Other errors which can cause the driver to reject a transaction (e.g., invalid driver configuration) will continue to generate errors in POS Operations.

POS Operations pauses before responding so that it is not obvious that no attempt was made to contact the host. Only the random 6-digit auth code appears on the credit voucher.

3. The transaction is flagged as having been automatically approved.
4. POS Operations will mark the authorization detail as having been auto approved but will not indicate that the auth code was manually generated on either the voucher or the display.

### Settlement

5. At settlement, Automatic Offline Credit Card Authorizations are passed to the settlement driver and are flagged as auto offline auth transactions.

The settlement driver will attempt to obtain an online authorization from the issuing bank to replace the authorization generated by the credit driver. These authorizations will occur before the actual settlement in an operation known as pre-settlement. The authorization request in pre-settlement will treat the authorization as a card present / manually keyed transaction.

6. The batch settlement report will show an **L** flag next to transactions where an auto offline auth was generated. The “L” flag has been added to the Credit Card Batch Detail report, in the flags column, to indicate an Auto Offline Authorization. This occurs if the Host Processor is down and the transaction amount is below the designated floor limit. An auto offline auth transaction was obtained rather than an actual authorization. The L flag will appear in the same column as the manual authorization flag since the two flags can not both appear for the same transaction.
7. If an authorization request is declined in pre-settlement, the settlement driver will change the authorization code on the record to ‘DECLINED’ and mark the record as omitted by the driver (a ‘D’ flag on the batch detail report). These transactions will also be shown in the omitted record summary of the batch transfer report.  
*Note: Omitted by the driver (Dflag) will only occur if the driver option ‘Auth Offline Transactions’ is set to one ‘1’ (enabled).*

This feature can be enabled either with a floor limit, or without a floor limit.

- **With No Floor Limit.** If the feature is enabled without a floor limit, all transactions will be automatically authorized with a random 6-digit numeric authorization code during a network outage.
- **With the Floor Limit Enabled.** If the floor limit is enabled then transactions under the floor limit will be automatically authorized and transactions above the floor limit will continue to return an error when the credit card driver is unable to contact the host. POS Operations passes the auto offline auth setting and floor limit, to the driver as part of every authorization request.

The existing floor limit functionality is not changed by this feature. If the existing base floor limit is programmed not to go online for authorization, then transactions which are under the base floor limit will continue to generate a voucher in POS Operations without contacting the driver.

If the floor limit is enabled and the authorization amount exceeds the amount of the floor limit, and POS Operations is unable to obtain an authorization from the credit card host, then POS Operations will display the error message `Manual Auth Required`. For these transactions it is necessary to obtain a voice authorization to complete the transaction. For Auth&Pay (e.g., the CC Lookup function key) tenders POS Operations will automatically prompt for a manual authorization code after displaying the error message. If the transaction employee is not privileged to add a manual authorization to the check a manager's authorization will be required. For standard credit authorizations (CC Auth / CC Final keys) there is no automatic prompt and the Manual Auth key must be used to complete the transaction as a separate step.

### **POS Configuration**

To support this functionality, the following options are at the revenue center level.

- **Enable auto offline auth** (*Revenue Center | RVC Credit Cards | General*). Highlight the appropriate tender and enable this option if Automatic Offline Credit Card Authorizations are supported.

By default the option is not enabled and the operator will receive an error message any time the driver is unable to contact the credit card host. When this option is enabled and the driver is unable to contact the credit card host for authorization a random, auth code is generated and the transaction will appear to have been approved normally.

By enabling this feature by revenue center, transactions in one revenue center can receive an auto offline authorization while transactions in another revenue center continue to require voice authorization during a network outage.

- **Enable auto offline floor limit** (*Revenue Center | RVC Credit Cards | Floor Limit*). Enable this option if using floor limits to designate a maximum amount that can be authorized when using the Automatic Offline Credit Card Authorization feature.

If the auto offline floor limit is enabled, then the **Auto offline floor limit**, (*Revenue Center | RVC Credit Cards | Floor Limit*) is used to set the upper limit on the amount of the authorization which can receive an auto offline authorization. The amount is programmed in dollars and cents (or local currency).

Unlike the existing base floor limits which are programmed by tender and can only be enabled and disabled by revenue center, the auto offline floor limit is set by revenue center. As a result, each revenue center can have a different floor limit or no floor limit at all by disabling the **Enable auto offline floor limit** for the revenue center. The floor limit applies to all authorizations within the revenue center.

If the floor limit is enabled, and the authorization amount exceeds the amount of the floor limit, and POS Operations is unable to obtain an authorization from the credit card host, then POS Operations will display the error message `Manual Auth Required`. In this situation, it is necessary to obtain a voice authorization to complete the transaction.

## Support Zero Dollar Account Verification

With zero-dollar initial auth, the open-to-buy limit on the customer's account will not be affected and the initial auth will not have to be reversed during pre-settlement. The use case for initial auths is the bar tab scenario.

The option **Initial Auth as Zero Dollar Account Verification** (*POS Configurator | Revenue Center | RVC Credit Cards | General*) must be enabled for POS Operation to ignore the tender's configured amount or keyed amount and do the initial auth for zero dollars. This option is disabled by default.

This credit card driver feature is only available when used in conjunction with RES v4.11 and higher or RES 5.1 and higher.

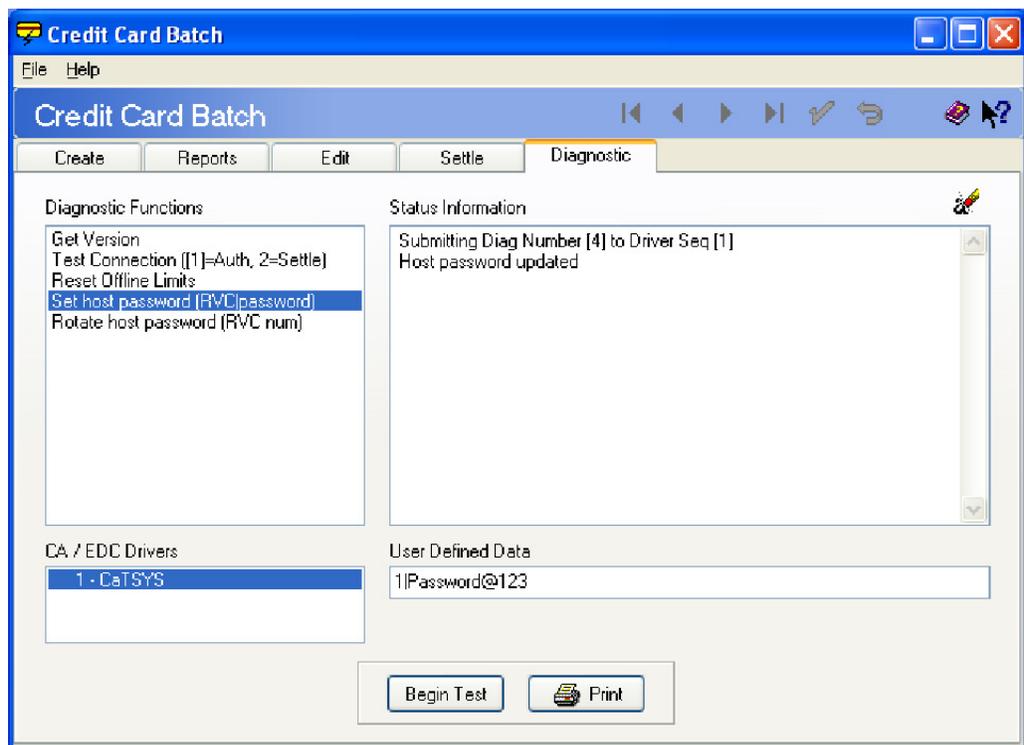
## eCommerce Transactions Support

An eCommerce transaction is one that occurs online. Authorization for payments submitted online are sent with a different set of authorization data. When transactions come through Transaction Services will have a flag set that distinguishes them as eCommerce.

## Password Support

Once the software is installed and configured, the password obtained from TSYS must be entered. Once the password has been entered it must be rotated. Following these steps to set the password:

1. Go to *Start | Programs | MICROS Applications | POS | Credit Card Batch* and click on the Diagnostic tab.
2. Select **Set host password (RVC|password)**.
3. In the **User Defined Data** field, enter the Revenue Center number followed by a pipe then the password. Click on the **Begin Test** button.
  - Example - 1|Password@123



4. To rotate the password, select **Rotate host password (RVC num)**, enter the Revenue Center number as **User Defined Data** and click on **Begin Test**.

The TSYS Administrator password will expire every 45 days.

The TSYS Store Operator password, used for credit transactions, will automatically update every seven days once the initial password has been entered in *Credit Card Batch | Diagnostic* and used for the first week.

## End of Day Procedures

TSYS does 'Host Based Settlement' but all credit card transactions still need to be batched and settled during the sites EOD procedures. This will mark the transactions in the Merchant Center web site as Pending Settlement. All applicable transactions will be settled by the Host 15 minutes before the hour, for example 3:45am, 4:45am, etc.

---

**Warning** *If the site does not batch and settle credit cards through the RES, the Host Based Settlement will not occur. This could result in the site not being paid for the credit card transactions.*

---

The Credit Card Batch Transfer Status report will have the Host System Reports and the Driver Reports. In the following example, the Driver Reports will show one reversal and one settled. The Host System Reports will show two settled, the reversals are included in the settled totals.

### Credit Card Batch Transfer Status

MICROS Cafe -

**Batch Created on Wednesday, Sep 19, 2012 - 15:20**

**Batch # 1 - For Business Date: Wednesday, Sep 19, 2012 - Settlement Driver: CaTSYS Merchant Name: TSYS**

**Attempt # 1 - 2012/09/19 15:20:10.43 Previous Settle Count - 0 901 - Bruno The Manager**

Batch Status: Omitted | Reversed | Settled | Total

Host System Reports: - | - | 2 | 29.80

Driver Reports: 0 | 1 | 1 | 29.80

### Sample Credit Card Voucher

Below is a sample of a printed credit card voucher when using the TSYS driver. A Reference number has been added that can be used to cross reference to the Transaction ID on the Merchant Center web site.

```
Date:          Sep18'12 01:47PM
Card Type:    Visa/M.C.
Acct #:       XXXXXXXXXXXXXXX1111*
Card Entry:   KEYED
Trans Type:   PURCHASE
Auth Code:    836248
Check:        8
Table:        61/1
Server:       101 Sally S
Reference:    2543375

Subtotal:     18.88
Date:          Sep18'12 01:47PM
Card Type:    Visa/M.C.
Acct #:       XXXXXXXXXXXXXXX1111*
Card Entry:   KEYED
Trans Type:   PURCHASE
Auth Code:    836248
Check:        8
Table:        61/1
Server:       101 Sally S
Reference:    2543375 ← Transaction ID

Subtotal:     18.88
```

The TSYS Transaction ID (Reference number on the credit card voucher) may be needed if there is an issue with the batch settlement amount and the user needs to logon to the TSYS Merchant Center web site to review the days transactions. Contact your TSYS representative for web site URL address and for further details on editing host-based batches.

## Removing the Software

### Removing Software From a Site Running RES 4.5 or Higher

Follow these steps to remove the CaTSYS 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\CaTSYS.dll
  - \MICROS\Res\Pos\Etc\CaTSYS.cfg
  - \MICROS\Res\Pos\Bin\CaTSYS.hlp
  - \MICROS\Res\Pos\Bin\CaTSYS.cnt
3. Delete the following files on the server:
  - \MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.dll
  - \MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTSYS.cfg
  - \MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.hlp
  - \MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.cnt
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\CaTSYS.dll
- \MICROS\Res\Pos\Etc\CaTSYS.cfg
- \MICROS\Res\Pos\Bin\CaTSYS.hlp
- \MICROS\Res\Pos\Bin\CaTSYS.cnt

## Password Handling Process

The TSYS Credit Card Driver utilizes a special process that requires store operator passwords to be encrypted and rotated on a regular basis. To accommodate this requirement, the password information is encrypted using the *Micros Credit Card Batch | Diagnostic* functions, specific for the TSYS Driver. These functions are explained below.

1. The TSYS Administrator password expires every 45 days. When attempting to login to the TSYS Merchant Center, you may receive an error that the password has expired. Follow the instructions on the web site to reset your Administrator password, or contact your TSYS Representative if you need assistance.

---

**Warning** *The Administrator password, received via e-mail from the TSYS Merchant Center when first setting up the driver, cannot be used for credit transactions in RES. The Administrator password is to be used only for management purposes (i.e. - checking on Pending Batches, Settled Batches, or possible adjustments).*

---

2. A separate store 'Operator' password needs to be created, using the TSYS Merchant Center Web Site, for daily credit transactions. This is the only password that is automatically updated after the initial password is entered via Credit Card Batch | Diagnostics.
  - Choose a password that is at least eight (8) characters long, it must have numbers (0-9), upper, lowercase letters (A-Z, a-z) and special character (!,@,\$,^,\*,-,\_,.) but no spaces. You are not allowed to reuse any of the last 6 Passwords used. (It is recommended doubling this to the last 12 passwords, to be extra secure).
  - The 'Operator' password will be automatically rotated every 7 days (default), by sending a change password request to the host. This can be changed (See #3 below).
3. What Password Information is stored in the registry?
  - The encrypted password, represented in ASCII HEX.
  - The last time the password was updated - formatted as mm-dd-yyyy.
  - Optional DWORD value to configure how often to update the password (indicating number of days). Registry name = RotatePasswordEveryXDays.
  - This parameter will default to 7 days if not configured in the registry.

4. Before each transaction the driver:
  - Checks if it is time to update the password by reading the last time the password was updated from registry and comparing it to the current time. If more than X days have passed (where X is a configurable value, see 3 above) then a change password request is sent.
  - TransIT MultiPASS responds in the following three ways to a Change Password XML Request:
    - **Approved**
    - **Invalid user or Password**
    - **Locked user**
  - If a change password request is approved then the new password will be saved in the registry.
  - If the change password request fails nothing will be updated in the registry, and the driver will proceed with the current request processing (auth or batch detail), which is expected to fail with the same error as the change password request (invalid user or password, locked user). This error will be returned to the user in POS Operations or in CreditCards.exe.
5. The driver reads the password from the registry for each transaction.
6. The driver will offer the following additional operations:
  - **Set the password** in *Credit Card Batch | Diagnostic*, which is used during the setup process and requires password input. The driver will store the given password in the registry. No change password request will be sent to the processor.
  - **Rotate password**, which is used to “manually” initiate the password update process and it does not require password input. In this case, the driver will generate a password and will send a change password request to the processor.
7. For optimization purposes when processing a batch, if a password rotate is needed, only the first transaction will check this and rotate the password until it succeeds.
8. With this version of the driver, there is no way for the user to know the current operator password. That is why it is highly recommended that the merchant not use their Administrator user assigned by TSYS, and instead create an extra operator/user which will be used only to process transactions.
9. The generated password format is:
  - 12 characters in length total
  - 8 (at least one Upper, one lower, one digit, one special chars) + mmdd (the current time)

10. Backup Server Mode (BSM) Client- Password Update will occur immediately after the Server Password is updated. If the BSM client is down for any reason, and the server cannot update the client at this time, a pending update flag is set in the registry indicating that an update is needed. As soon as the client is back up and online, the password will be updated.

---

## Troubleshooting Tips

When troubleshooting the TSYS driver, there are several settings that will add additional logging and/or create TSYS specific log files.

- **Verbosity** = 5 in the MICROS Control Panel  
This will log extra information in the 3700d.log.

To make the logging more useful for troubleshooting, there are several registry keys that can be added in the following directory:

HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROS\Common\CCS\DrvrCfg\Drvr#\Support

The following keys can be created as **DWORD Value**:

- **DiskLog** = 1
- **LogCaMsgs** = 1
- **LogSettleMsgs** = 1  
These will create a TSYS.log file in the \MICROS\Res\Pos\Etc folder.
- **LogXMLMsgs** = 1  
This will log each XML message in a separate XML file in the \MICROS\Res\Pos\Etc\TSYS folder.

---

## *Frequently Asked Questions*

### **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 Oracle 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?**

Oracle 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. Oracle 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.

Oracle 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.

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. The TSYS Credit Card Driver is host-based.

### **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.

# *ReadMe First*

## *V. 5.1*

---

This section contains a comprehensive guide to the Version 5.1 release of the TSYS Acquiring Solutions (CaTSYS) Credit Card Driver.

### **In This Section...**

• What's New .....	31
• Summarized .....	31
• Detailed .....	31
• What's Enhanced .....	32
• Summarized .....	32
• What's Revised .....	33
• Summarized .....	33

---

## What's New

A new feature is defined as one that provides capabilities that were not available in previous versions of the application.

### New Features Summarized

The following table summarizes the new features included in this version

Feature	Page
Added support for Transport Layer Security 1.2 encryption protocol	31
Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols	31

### New Features Detailed

#### **Added Support for Transport Layer Security 1.2 Encryption Protocol**

Version 5.1 of the TSYS Acquiring Solutions (CaTSYS) Credit Card Driver contains support for the Transport Layer Security (TLS) 1.2 Encryption Protocol. The TLS protocol encrypts your data and provides a secure and reliable data transmission between the POS application (client) and server.

#### **Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols**

Version 5.1 of the TSYS Acquiring Solutions (CaTSYS) Credit Card Driver removes support for all encryption protocols other than TLS 1.2. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

---

## ***What's Enhanced***

An enhancement is defined as a change made to improve or extend the current functionality. To qualify as an enhancement, the change must satisfy the following criteria:

- The basic feature or functionality already exists in the previous release of the software.
- The change adds to or extends the current process. This differs from a revision (i.e., a bug fix) which corrects a problem not caught in previous versions.

## **Enhancements Summarized**

There are no enhancements included in this release.

---

## ***What's Revised***

A revision is defined as a correction made to any existing form, feature, or function currently resident in the 3700 POS software. To qualify as a revision, the change must satisfy the following criteria:

- The basic form, feature, or functionality must be a part of the previous version of the software.
- The change must replace or repair the current item or remove it from the application.

## **Revisions Summarized**

There are no revisions included in this release.