micros®

**Restaurant Enterprise Series**

# *Transaction Vault Credit Card Driver for 3700 POS*

**April 3, 2013**

**********************Important**********************

*When upgrading the Transaction Vault Credit Card Driver from v4.7.20.2065 or earlier to v4.9.21.2292 or higher, the user must go into POS Configurator | Devices | CA / EDC Drivers and select both the TVCA and TVCS records. This will update the database with the new configuration file.*

*Authorization reversals are only supported in RES Version 4.5 or higher.*

*Corrective authorizations are not compatible with authorization reversals and are therefore no longer supported. If you currently have corrective authorizations configured, you should remove this.*

********************************************************



**MD0003-118**

# 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

# Compatibility

The following charts explain which versions of RES and the Transaction Vault credit card driver are compatible.

| CaTVC 4.14 | | |
|---|---|---|
| RES Versions | EMSR ON | EMSR OFF |
| RES 4.x | YES | YES |
| RES 5.0 - 5.1 | NO | YES |
| RES 5.1 MR1 and higher | YES | YES |

| CaTVC 4.13 | | |
|---|---|---|
| RES Versions | EMSR ON | EMSR OFF |
| RES 4.x | YES | YES |
| RES 5.0 - 5.1 | YES | YES |
| RES 5.1 MR1 and higher | NO | YES |

For example:

If RES 5.1 MR1 or higher is installed and **Encrypted MSR Mode** (*POS Configurator* | *System* | *Restaurant* | *Security*) is enabled, then the CaTVC v4.14 driver is required to coincide with changes made to POS Operations.

# Installation and Setup

This section contains installation and setup instructions for the Version 4.14 release of the Transaction Vault Credit (CaTVC) Card Driver. The TVC driver is available on the MICROS web site Product Support page.

The credit version of the Transaction Vault driver may be used on RES systems running Version 3.2 SP7 HF5 or higher, or Version 4.1 or higher.

## In This Section...

# Introduction

The Merchant Link TransactionVault solution minimizes the ability for a merchant's cardholder data to be compromised. All sensitive data is stored in the TransactionVault, a hosted database at Merchant Link, instead of in the merchant's local RES database. Merchant Link's TransactionVault coupled with MICROS 3700 secures data for the customer minimizing the potential for security breaches.

The purpose of the TransactionVault feature is to remove sensitive credit card information from the RES data store. This is done by using Merchant Link to provide the card storage at their data center. In exchange, Merchant Link provides a TransactionVault key that replaces all cardholder information at the customer site. The key utilizes leading edge encryption technology, which helps to ensure that only TransactionVault can match the key to access the cardholder information.

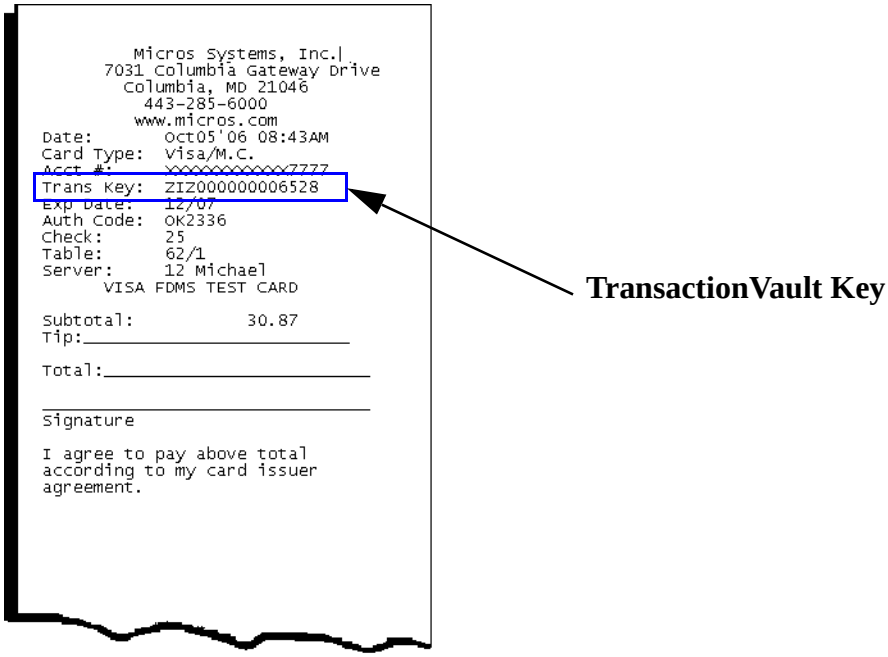
For additional information about TransactionVault see the *RES 4.1 ReadMe First, MD0003-098* or the *RES 3.2 SP7 HF5 Documentation*.

## How it Works

Traditionally, cardholder data (card number, expiration date, and the cardholder name) is stored by the RES system until it is purged from the system, typically within 90-180 days after settlement. RES automatically detects when TransactionVault payment drivers are installed.

When obtaining an authorization for a transaction, the MICROS database will delete the cardholder data from the system, replacing it with a 15-character **TransactionVault Key** obtained from Merchant Link during the authorization process. All cardholder data is stored in Merchant Link's TransactionVault. The TransactionVault Key becomes the reference number for merchants if it is necessary to lookup cardholder data.

The TransactionVault Key is printed on the authorization voucher.




> ***Note*** *Keep a record of the authorization voucher. Referencing the TransactionVault Key will be the only way to correct a transaction if an issue should arise.*

There are several instances when cardholder data will be stored on the RES system. We refer to these instances as offline transactions. The following are the four types of offline transactions available through RES:

- Credit Transaction
- SAR/BSM Transaction
- Manual Authorization
- Below Floor Limit Transaction

Additionally, during authorization, the user will not be prompted to enter Address Verification (AVS) and Credit Card Verification (CVV) for transactions performed offline except for Below Floor Limit Transactions.

When an offline transaction is performed, the system will encrypt and store the cardholder data until the system is online and does a settlement. The settlement process has been enhanced to first process offline transactions, obtaining a TransactionVault Key for each of these transactions, and then deleting cardholder data from the system. Once complete, normal settlement will occur processing all transactions via their TransactionVault Key.

## Secondary Level Encryption

This functionality uses a proprietary protocol. It is not available for use at this time.

## Settlement

Batch settlement with the Transaction Vault Driver is a two step process. The first step is to submit all offline authorizations to the processor. During this step, the settlement process scans the batch records for any offline authorizations. All offline transactions are processed to Merchant Link where they receive a TransactionVault Key.

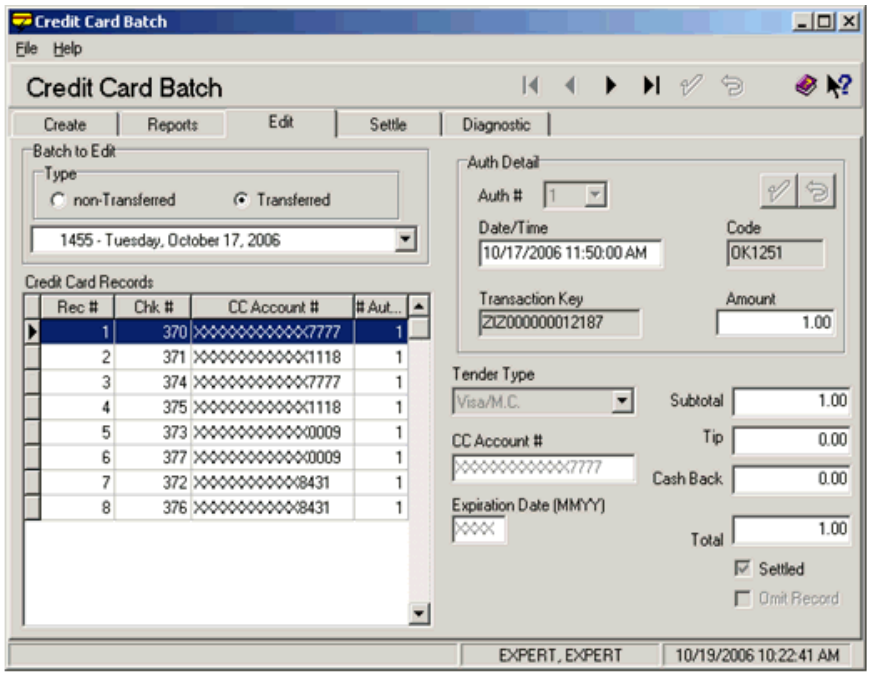
After all of the records have been issued TransactionVault Keys, the settlement process begins to transmit the batch to the processor. Unlike traditional drivers, TV does not transmit customer information. Instead the RES system sends the TransactionVault Key and the total amount owed to the processor. The processor will then match the TransactionVault Key to the appropriate customer account.

Following a successful batch, no customer information is stored in the RES system.

In previous Credit Card Drivers, an option to **Disable Auth Code Limit** was available. This option has been omitted from the POS Configurator with the Transaction Vault Driver and it is now enabled by default. If a manual authorization is performed, and the user enters a value greater than 6 characters in the Auth Code field, the settlement driver will truncate the code down to the first 6 characters only. The record will then be settled with the truncated Auth Code.

## Credit Card Batch Utility

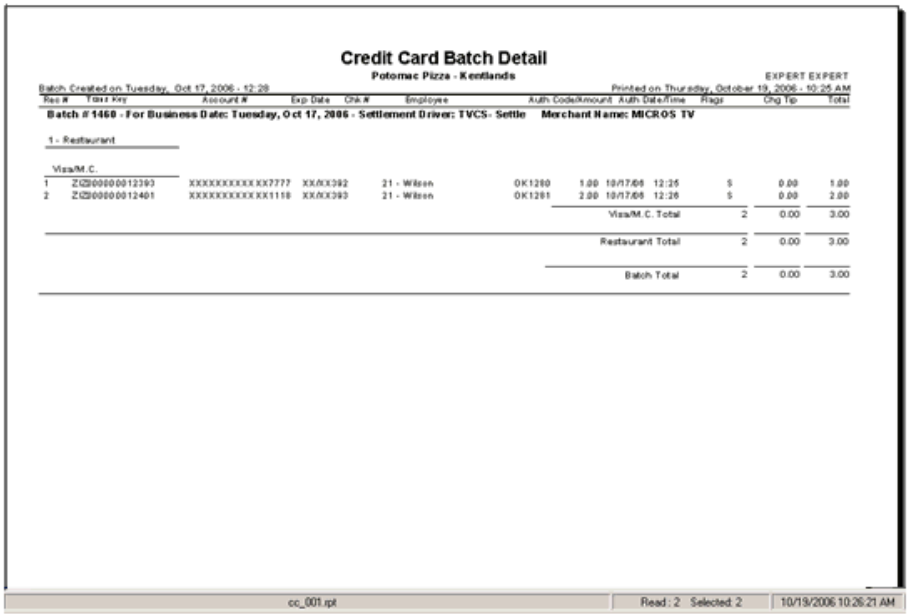
To support the TransactionVault Key, a field has been added to the *Credit Card Batch Utility* | *Edit* form. The **TransactionVault Key** field will display the assigned transaction key.



## Reports

The following report has been altered to support the Transaction Vault Payment Driver.

**Credit Card Batch Detail Report** – A TransactionVault Key column has been added to this report. The 15-digit TransactionVault Key associated with the transaction will be listed in this column. The customer name column has been removed from the report.



# Installation

## Site Requirements

Before installing the Transaction Vault Driver on the RES system, the following configuration items should be considered:

- The installed version of 3700 POS should be Version 3.2 SP7 HF5 or higher, or Version 4.1 or higher.
- To use Internet Connectivity, an Internet connection must be configured and working. ISP software may be needed to connect to the Internet.
- A dedicated modem and phone line are required for dial-up connectivity or fallback to dial-up when using TCP/IP or Internet connectivity.
- Security protocols, including firewalls and other protections, should be in place.
- The site's browser software will need to support 128-bit session keys. (See section Internet Explorer Cipher Strength, for a method to check this.)

## Files Included

This version of the Transaction Vault Driver supports credit card transactions only. The credit card driver is divided into an authorization driver, and a settlement driver. The following lists the files installed for each driver:

### Authorization for Credit Cards (CaTVCA)

*\Micros\RES\POS\Bin\CaTVCA.dll*
*\Micros\RES\POS\Etc\CaTVCA.cfg*
*\Micros\RES\POS\Bin\CaTVCA.hlp*
*\Micros\RES\POS\Bin\CaTVCA.cnt*

### Settlement for Credit Cards (CaTVCS)

*\Micros\RES\POS\Bin\CaTVCS.dll*
*\Micros\RES\POS\Etc\CaTVCS.cfg*
*\Micros\RES\POS\Bin\CaTVCS.hlp*
*\Micros\RES\POS\Bin\CaTVCS.cnt*

### Additional Files

*\Micros\Common\Bin\libeay32.dll*
*\Micros\Common\Bin\ssleay32.dll*
*\Micros\Common\Bin\McrsOpenSSLHelper.dll*
*\WINNT\System32\MSVCR71.dll*

***Note*** *The MSVCR71.dll file is installed if it is not found in the \WINNT\System32 directory when the installation program is executed.*

## Installation Instructions for a Site Running RES 3.2 SP7 HF5 or higher

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

1. Prior to installation, a new order form (new site) or a change of service form (existing site) must be submitted to Merchant Link, LLC. and you must contact their implementation department for TransactionVault setup information.
2. 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.
3. Download the latest Transaction Vault Credit Driver from the MICROS web site. Copy the files to your RES Server's temp folder and unzip the files. These zip files include the following:
   - Transaction Vault Credit Card Driver for RES 3700 POS (**CaTVC_V4.14_MD.pdf**)
   - Transaction Vault Credit Card Driver Software (**CaTVC(4.14.0.2481).exe**)
4. Shutdown the RES system from the **MICROS Control Panel**.
5. Double-click on the **CaTVC(4.14.0.2481).exe** file to execute the installation program.

   During installation, the following files will be automatically copied into the Windows directories for the Server:

| File | RES Server |
|---|---|
| CaTVCA.dll | \MICROS\RES\POS\BIN |
| CaTVCS.dll | \MICROS\RES\POS\BIN |
| CaTVCA.cfg | \MICROS\RES\POS\ETC |
| CaTVCS.cfg | \MICROS\RES\POS\ETC |
| CaTVCA.hlp | \MICROS\RES\POS\BIN |

| File | RES Server |
|---|---|
| CaTVCS.hlp | \MICROS\RES\POS\BIN |
| CaTVCA.cnt | \MICROS\RES\POS\BIN |
| CaTVCS.cnt | \MICROS\RES\POS\BIN |
| libeay32.dll | \MICROS\COMMON\BIN |
| ssleay32.dll | \MICROS\COMMON\BIN |
| McrsOpenSSLHelper.dll | \MICROS\COMMON\BIN |
| MSVCR71.dll | \WINNT\System32 |

6. If a Backup Server Mode (BSM) Client is configured (*POS Configurator* | *System* | *Restaurant* | *Descriptions* | *Backup Server Network Node*) copy the **CaTVC(4.14.0.2481).exe** file to a Temp directory and run the installation program on this client. Verify that all required files listed in step 5 are copied to the correct directory paths.
7. Take the RES system to *Front Of House* from the **MICROS Control Panel**.
8. If upgrading from TVC v4.7.20.2065 or earlier to TVC v4.9.21.2292 or later, open *POS Configurator* | *Devices* | *CA / EDC Drivers* and select both the TVCA and TVCS records. This will update the database with the new configuration file.
9. If upgrading, CA/EDC should be operational. A few test transactions should be done to ensure all is working correctly.

## Installation Instructions for a Site Running RES 4.1 or Higher

The installation of the credit card driver is separate from RES software. When a site loads a new version of RES software the TransactionVault 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. Prior to installation, a new order form (new site) or a change of service form (existing site) must be submitted to Merchant Link, LLC. and you must contact their implementation department for Transaction Vault setup information.
2. 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.
3. Download the latest Transaction Vault Credit Driver from the MICROS web site. Copy the files to your RES Server's temp folder and unzip them. The zip files include the following:
   - Transaction Vault Credit Card Driver Documentation for RES 3700 POS (**CaTVC_V4.14_MD.pdf**)
   - Transaction Vault Credit Card Driver Software (**CaTVC(4.14.0.2481).exe**)

4. It is not necessary to shut down your RES system during installation. There cannot be any credit card transactions in progress so be cautious and take your RES system to the database level via the Control Panel.

   Double click on the **CaTVC(4.14.0.2481).exe** file. This will install of the necessary files on RES Server and the BSM Client, and Windows Services will be restarted automatically. The credit card server will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started.

| File | RES Server | Backup Server Client |
|---|---|---|
| CaTVCA.dll | \MICROS\RES\POS\BIN | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN |
| CaTVCS.dll | \MICROS\RES\POS\BIN | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN |
| CaTVCA.cfg | \MICROS\RES\POS\ETC | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC |
| CaTVCS.cfg | \MICROS\RES\POS\ETC | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC |
| CaTVCA.hlp | \MICROS\RES\POS\BIN | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN |
| CaTVCS.hlp | \MICROS\RES\POS\BIN | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN |
| CaTVCA.cnt | \MICROS\RES\POS\BIN | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN |
| CaTVCS.cnt | \MICROS\RES\POS\BIN | \Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN |
| libeay32.dll | \MICROS\COMMON\BIN | \Micros\RES\CAL\Win32\Files\MICROS\COMMON\BIN |
| ssleay32.dll | \MICROS\COMMON\BIN | \Micros\RES\CAL\Win32\Files\MICROS\COMMON\BIN |
| McrsOpenSSLHelper.dll | \MICROS\COMMON\BIN | \Micros\RES\CAL\Win32\Files\MICROS\COMMON\BIN |
| MSVCR71.dll | \WINDOWS\System32 | \Micros\RES\CAL\Win32\Files |

5. Take the RES system to *Front Of House* from the **MICROS Control Panel**.

6. If upgrading from TVC v4.7.20.2065 or earlier to TVC v4.9.21.2292 or later, open *POS Configurator* | *Devices* | *CA / EDC Drivers* and select both the TVCA and TVCS records. This will update the database with the new configuration file.

7. If upgrading, CA/EDC should be operational. A few test transactions should be done to ensure all is working correctly.

> ***Note*** *Once the driver files have been installed using the CaTVC executable into the \MICROS\RES\CAL\Win32|Files path, an automatic update will occur to all harddisk clients (including the Backup Server).*

## Configuration Instructions

Each of the Transaction Vault drivers (i.e., CaTVCA, and CaTVCS) must be configured separately.

TV setup is not done until the CaTVCA, and CaTVCS driver forms are completed in *POS Configurator* | *Devices* | *CA/EDC Drivers*. An online help file is available to explain the general configuration requirements. However, entries for some options will be provided by the credit card processor. If so, be sure to enter this data exactly as given, as some fields may be case-sensitive. Entering the correct entry in the wrong format may result in communication failure at the Host Processor.

### Configuring the CaTVCA and CaTVCS Drivers

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

2. Enter a **Name** (e.g., **CaTVC-Auth**) and a value of the **Driver Code** field (e.g., **TVCA**) and save the record.

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

   - **Authorization Device** – Complete this step if you are using a modem for primary or fallback authorizations. If you are unsure of the device number, go to the command prompt in the *\POS\bin* directory and enter settle –m for a Version 3.2 RES Server or go to the command prompt in the *\Common\Bin* directory for a Version 4.1 RES Server. The following sample message will display:

     ```
     Device [1]: Boca 28.8 Kbps V.34 MV.34E
     Device [2]: Standard 1200bps Modem
     Device [3]: Standard 2400 bps Modem
     Select the appropriate device number.
     ```

   - **Not Used** – Leave this field blank.
   - **Port Arbitration Enabled** – Enter a value of 1 to enable this driver.

- **Communications Channel** – Indicate the communication type enabled at the store (0= Dial-up, 1 = TCP, 2 = Internet).
- **Phone Number** – Enter the phone number that will be used for authorizations, if necessary. This number will be provided by the credit card processor.
- **Backup Phone Number** – Enter the secondary phone number that will be used for authorizations, if necessary. This number will be provided by the credit card processor.
- **Host IP Address: Port** – Enter the IP address and port of the primary host connection. This field is only applicable if a TCP or an Internet connection is enabled.
- **Backup IP Address: Port –** Enter the IP address and port of the secondary host connection. This field is only applicable if a TCP or an Internet connection is enabled.
- Enter the **City, State** and **Zip Code** where the merchant is located.
- **SiteNET Customer ID** – Enter the siteNET customer identification information provided by Merchant Link.
- **Proxy IP Address: Port** – Enter the IP Address and Port of the Proxy Server provided by your Network Support Personnel.

4. Go to the *Merchant* tab and configure the following settings:
   - All settings under the *Merchant* **|** *Authorization* tab should be completed using the instructions provided by the bank. The following information is needed:
     - Acquirer BIN
     - Merchant ID Number
     - Store Number
     - Terminal Number
     - Merchant Name
   - Go to the *Merchant* | *RVC* tab and use the blue plus arrow to add all Revenue Centers that will use this driver.
5. Go to *POS Configurator* | *Devices* | *CA/EDC Drivers* and select the blue plus sign to add a record.
6. Enter a **Name** (e.g., **CaTVC-Settle**) and a value of the **Driver Code** field (e.g., **TVCS**) and save the record.
7. Go to the *System* tab and configure the following settings:
   - **Not Used** – Leave this field blank.

- **Settlement Device** – Complete this step if you are using a modem for primary or fallback settlements. If you are unsure of the device number, go to the command prompt in the *\POS\bin* directory and enter settle –m for a Version 3.2 RES Server or go to the command prompt in the *\Common\Bin* directory for a Version 4.1 RES Server. The following sample message will display:

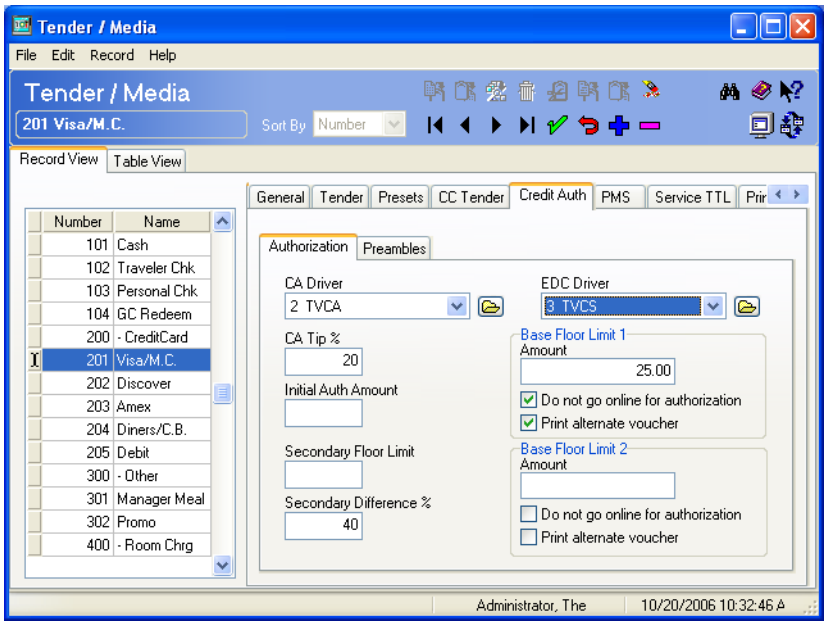
```
Device [1]: Boca 28.8 Kbps V.34 MV.34E
Device [2]: Standard 1200bps Modem
Device [3]: Standard 2400 bps Modem
Select the appropriate device number.
```

- **Port Arbitration Enabled –** Enter a value of 1 to enable this driver.
- **Communications Channel –** Indicate the communication type being used at the store (0= Dial-up, 1 = TCP, 2 = Internet).
- **Phone Number** – Enter the phone number that will be used for settlement, if necessary. This number will be provided by the credit card processor.
- **Backup Phone Number** – Enter the secondary phone number that will be used for settlement, if necessary. This number will be provided by the credit card processor.
- **Host IP Address: Port** – Enter the IP address and port of the primary host connection. This field is only applicable if a TCP or an Internet connection is enabled.
- **Backup IP Address: Port –** Enter the IP address and port of the secondary host connection. This field is only applicable if a TCP or an Internet connection is enabled.
- Enter the **City, State** and **Zip Code** where the merchant is located.
- **SiteNET Customer ID** – Enter the siteNET customer identification information provided by Merchant Link.
- **Proxy IP Address: Port** – Enter the IP Address and Port of the Proxy Server provided by your Network Support Personnel.

8. Go to the *Merchant* tab and configure the following settings:

   - All settings under the *Merchant* | *Settlement* tab should be completed using the instructions provided by the bank.
   - Go to the *Merchant* | *RVC* tab and use the blue plus arrow to add all Revenue Centers that will use this driver. The following information is needed:
     - Acquirer BIN
     - Merchant ID Number
     - Store Number
     - Terminal Number
     - Merchant Name

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




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

   Configuring these options will automatically mask the Card Number, Customer Name, and Expiration Date on all credit card transactions.

10. If using second level encryption complete this step. If second level encryption is not used, proceed to step 11. To enable second level encryption, enter a value in the **Secondary CC Encryption Key** option on the *POS Configurator* | *Revenue Center* | *RVC Credit Cards* | *General* tab. This is an alphanumeric value up to 40-characters that is assigned by MerchantLink.

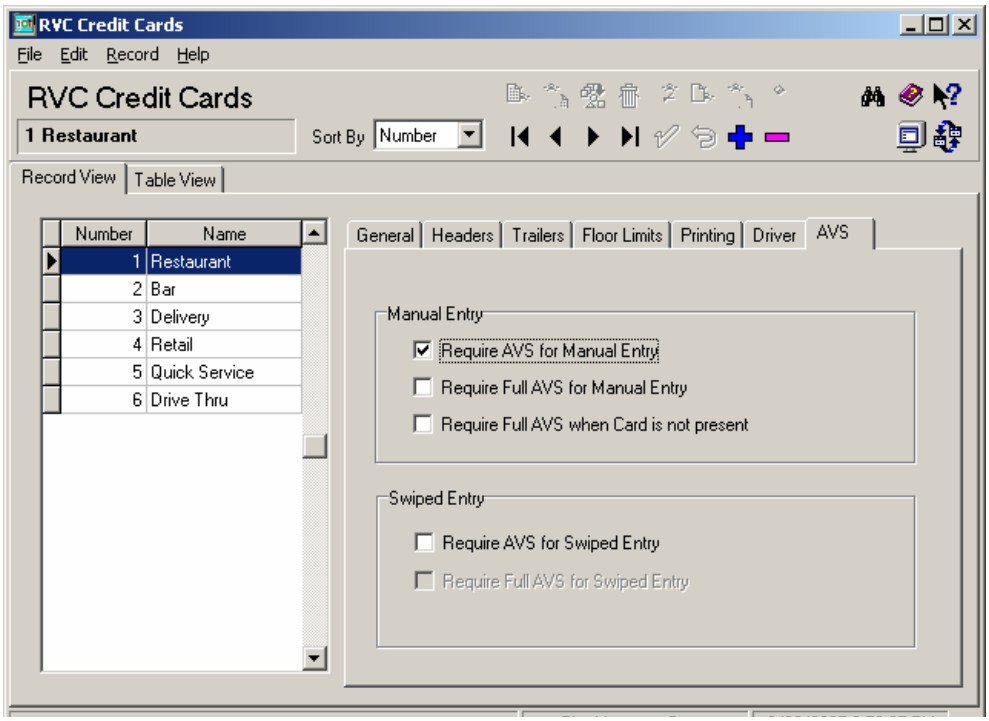
11. Go to *Start* | *Programs* | *Micros Applications* | *POS* | *Credit Card Batch*. Click on the Diagnostic tab and select the **Test Auth Connection** and the **Test Settlement Connection** buttons to verify that the drivers are up and running. A few test transactions can also be done to ensure all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

## AVS and CVV Configuration - Credit Only

The TVC driver includes Address Verification (AVS) and Card Verification Value (CVV) as part of the authorization request.

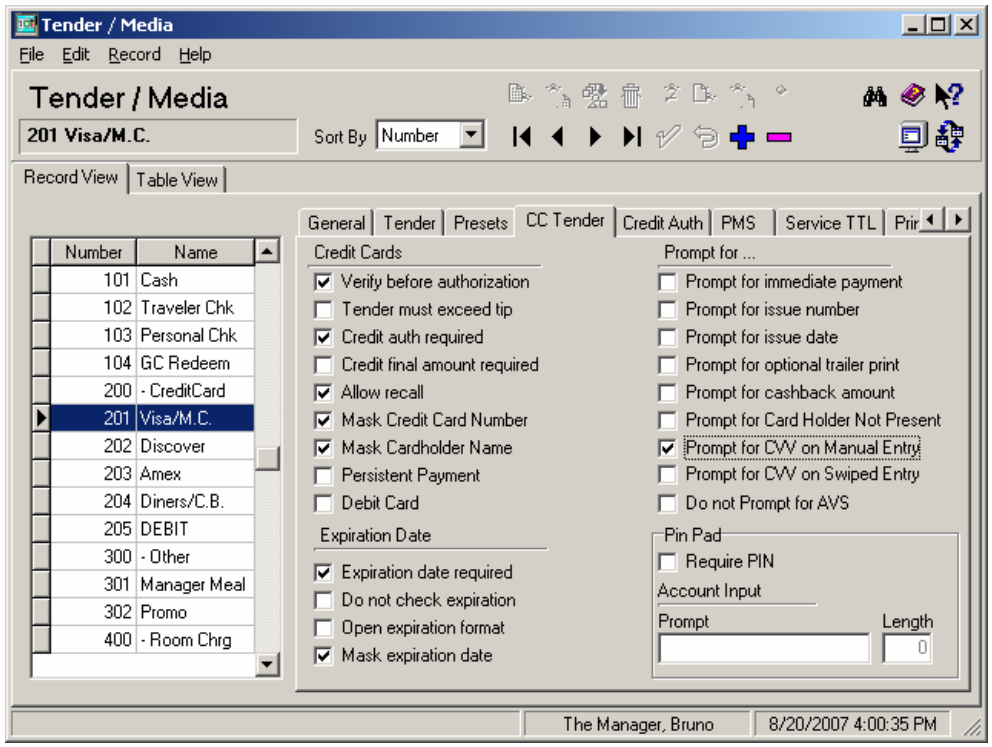
AVS is a system check that matches the address provided in the transaction to the address on file with the bank. CVV is the three or four-digit number listed on the back of the card that provides an additional level of security for the user. AVS and CVV data is transmitted in the Cardholder Identification Code field of the authorization request.

The AVS feature can be enabled by going to the *Revenue Center* | *RVC Credit Cards* | *AVS* tab and enabling 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** and the **Require Full AVS when Card is not present** options are also 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.

The CVV feature can be enabled by going to the *Sales* | *Tender/Media* | *CC Tender* tab and enabling 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 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.

This support is only included when the driver is sending authorization requests using the default VisaD format. Custom modes, which use the older VisaK format will ignore CVV and AVS fields.

## Removing the Software

### Removing Software From a Site Running RES 3.2 SP7 HF5 or Higher

Follow these steps to remove the CaTVC 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\CaTVCA.dll
   - \Micros\Res\Pos\Etc\CaTVCA.cfg
   - \Micros\Res\Pos\Bin\CaTVCA.hlp
   - \Micros\Res\Pos\Bin\CaTVCA.cnt
   - \Micros\Res\Pos\Bin\CaTVCS.dll
   - \Micros\Res\Pos\Etc\CaTVCS.cfg
   - \Micros\Res\Pos\Bin\CaTVCS.hlp

- \Micros\Res\Pos\Bin\CaTVCS.cnt
- \Micros\Common\Bin\libeay32.dll*
- \Micros\Common\Bin\ssleay32.dll*
- \Micros\Common\Bin\McrsOpenSSLHelper.dll*

** These are shared .dlls that may be used by other drivers/applications. Proceed with caution when deleting them.*

3. Shut down the RES System on the Backup Server Client (if applicable).
4. Delete the following files:
   - \Micros\Res\Pos\Bin\CaTVCA.dll
   - \Micros\Res\Pos\Etc\CaTVCA.cfg
   - \Micros\Res\Pos\Bin\CaTVCA.hlp
   - \Micros\Res\Pos\Bin\CaTVCA.cnt
   - \Micros\Res\Pos\Bin\CaTVCS.dll
   - \Micros\Res\Pos\Etc\CaTVCS.cfg
   - \Micros\Res\Pos\Bin\CaTVCS.hlp
   - \Micros\Res\Pos\Bin\CaTVCS.cnt
   - \Micros\Common\Bin\libeay32.dll*
   - \Micros\Common\Bin\ssleay32.dll*
   - \Micros\Common\Bin\McrsOpenSSLHelper.dll*

   ** These are shared .dlls that may be used by other drivers/applications. Proceed with caution when deleting them.*

### Removing Software From a Site Running RES 4.1 or Higher

Follow these steps to remove the TV credit 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\CaTVCA.dll
   - \Micros\Res\Pos\Etc\CaTVCA.cfg
   - \Micros\Res\Pos\Bin\CaTVCA.hlp

- \Micros\Res\Pos\Bin\CaTVCA.cnt
- \Micros\Res\Pos\Bin\CaTVCS.dll
- \Micros\Res\Pos\Etc\CaTVCS.cfg
- \Micros\Res\Pos\Bin\CaTVCS.hlp
- \Micros\Res\Pos\Bin\CaTVCS.cnt
- \Micros\Common\Bin\libeay32.dll*
- \Micros\Common\Bin\ssleay32.dll*
- \Micros\Common\Bin\McrsOpenSSLHelper.dll*

** These are shared .dlls that may be used by other drivers/applications. Proceed with caution when deleting them.*

3. Shut down the RES System on the Backup Server Client (if applicable).
4. Delete the following files:
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVCA.dll
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTVCA.cfg
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVCA.hlp
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVCA.cnt
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVCS.dll
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTVCS.cfg
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVCS.hlp
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVCS.cnt
   - \Micros\Res\CAL\Win32\Files\Micros\Common\Bin\libeay32.dll*
   - \Micros\Res\CAL\Win32\Files\Micros\Common\Bin\ssleay32.dll*
   - \Micros\Res\CAL\Win32\Files\Micros\Common\Bin\McrsOpenSSLHelper.dll*

   ** These are shared .dlls that may be used by other drivers/applications. Proceed with caution when deleting them.*

# Setup

## Communication Channels Supported

- Dial-Up (Channel 0, system default)
- TCP (Channel 1)
- Internet, Encrypted via Merchant Link's siteNET gateway (Channel 2)

**Communication Channel** setup is done when setting up the driver in *POS Configurator* | *Devices* | *CA/EDC Drivers*.

## Connectivity Considerations

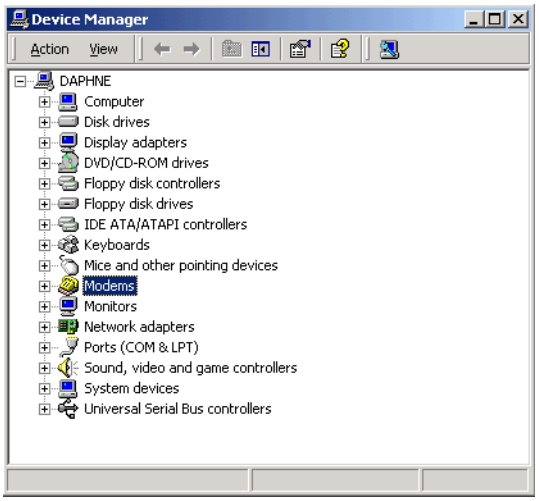
This section is provided as reference when installing the Transaction Vault Credit Card Driver.

### Configuring Dial-Up Connectivity

Before beginning, make sure that the phone line being used is dedicated for credit cards only, and will not be used for other purposes.

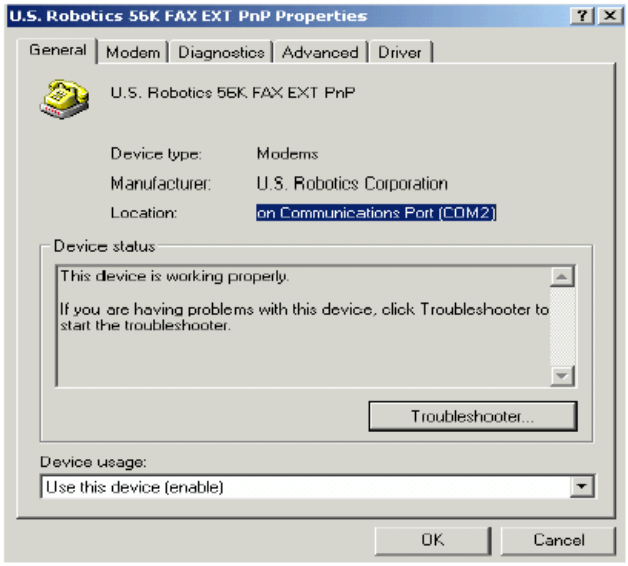
The following setup instructions are for Windows 2000 platforms or higher:

1. From the **Windows Start** menu, select *Settings* | *Control Panel* | *System*. Go to the *Hardware* tab and press the **[Device Manager]** button to open the form.

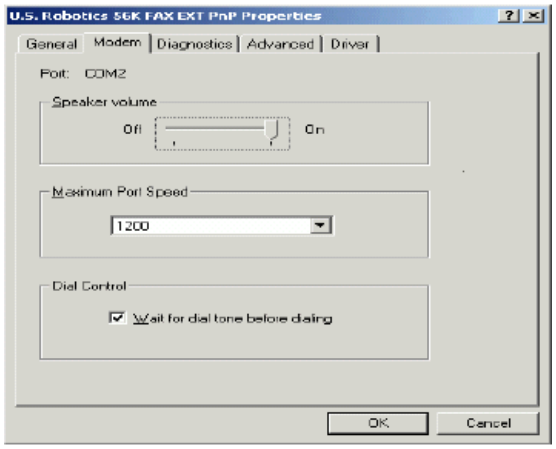


2. Expand the **Modems** entry and double-click on the modem to be used for credit card processing. The properties form will be displayed.

3. From the *General* tab, refer to the **Location** field. Write down the COM Port number, as it will be needed shortly.



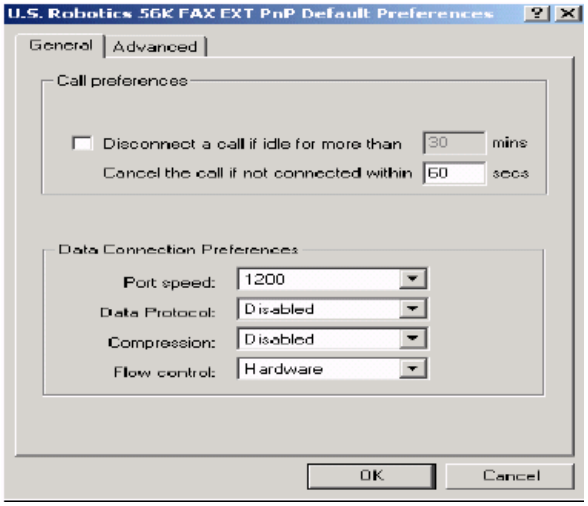

4. Go to the *Modem* tab.




5. Enable the **Dial Control** option and set the **Maximum Port Speed** to *1200*.

   **NOTE:** In some cases, port speed may need to be set to 2400. If so, this value must be changed to 2400 wherever else it appears in the configuration.

6. Go to the *Advanced* tab and click the **[Change Default Preferences]** button to open the preferences form.




7. On the *General* tab, set the options as follows:

   - **Port speed** — 1200 (or 2400, as discussed in step 4)
   - **Data Protocol** — Disabled
   - **Compression** — Disabled
   - **Flow control** — Hardware

8. Go to the *Advanced* tab and set the options as follows:

   - **Data bits** — 7
   - **Parity** — Even
   - **Stop bits** — 1
   - **Modulation** — Standard

9. Click the **[OK]** button (twice) to accept the changes and return to the Device Manager screen.

10. Expand the **Ports** menu entry and double-click on the COM Port identified in Step 2.

11. Go to the **Port Settings** table and select the following options:

    - **Bits per second** — 1200 (or 2400, as discussed in step 4)
    - **Parity** — Even
    - **Stop bits** — 1
    - **Flow Control** — Hardware

12. Click **[OK]** to save and close the **System** forms.
13. Exit the Control Panel and reboot the PC.

## Configuring TCP Connectivity

Merchants can use a private network to process credit card transactions. A secure corporate network is closed to the public and uses security protocols to prevent unauthorized access. Message traffic on a private network is not encrypted. When a private network is used, the 3700 POS can be configured to either connect directly to Merchant Link (ML) or via a corporate WAN connected to Merchant Link.

Network configurations are typically setup one of two ways:

- Satellite connection from each site to ML. This requires contracting with a satellite vendor that has a TCP connection from their satellite hub to Merchant Link.
- Connection from each site to a corporate WAN and TCP connection from corporate to ML.

### 1. Host And Backup Host Configuration

In order to process via TCP, contact ML for Host configuration information.

### 2. Fallback Configuration

The TV has a built-in feature to support failover or “fallback” capability for authorizations using either TCP or Internet Connectivity. This feature enables the driver to automatically switch from a TCP protocol to dial-up if the connection to Merchant Link fails. In other words, fallback is initiated when the MICROS 3700 POS cannot connect to the credit card host.

Fallback is **not** initiated if the POS makes the connection but then an error occurs (i.e., the connection is lost). In this case, the user receives an error and can try the transaction again. If the system consistently connects and then errors out, MICROS recommends the following:

1. Place a call to your support desk.
2. Change the **Communication Channel** option to Dial-up (0) until the situation is resolved.

For this functionality to work, a modem must be installed on the RES Server. The device number and network phone numbers must also be entered into the driver configuration.

As a first step in setting up **Fallback** mode, MICROS recommends testing the TV with a communications channel configured for Dial-up (0). Once the system can process credit card transactions in this mode, the communications channel can be changed and the modem can be configured in *POS Configurator* | *Devices* | *CA/EDC Drivers*. This includes specifying the **Authorization** and **Backup Authorization Phone Numbers**.

### 3. Confirmation Of Connectivity With Network Default Gateway

Most networks have specified gateway routers where connections need to be routed before they can get to the "outside world." To confirm a connection is getting through the merchant's network, ping the address of the Default Gateway router. If the address is unknown, follow these steps to determine the default gateway's IP address:

1. Go to a command prompt.
2. Type **ipconfig /all**
3. Find the line that reads default gateway.
4. Type **ping**, then the **IP address** from Step 3.

If pings to the Default Gateway are unsuccessful, then the Merchant's IT group will need to troubleshoot and fix the issue within their network.

### 4. Confirmation Of Connectivity With The Merchant Link Network

The easiest way to test the connection from the RES Server to the Merchant Link Network through a frame circuit is by pinging from a command line on the RES Server. This can be done in conjunction with Merchant Link. For more information, contact ML for connection information.

### 5. Test TCP/IP Connectivity via Credit Card Utility

Another way to test the connection (from the RES Server to the Merchant Link Network through a frame circuit) is to use the diagnostic tools in the Credit Card Batch Utility. This can be done as follows:

1. Open the **Credit Card Batch Program** on the RES Server.
2. Go to the *Diagnostics* tab.
3. In the **CA/EDC Drivers list** box, select one of the TV's authorization or settlement drivers.
4. From the *Diagnostic Functions* window, highlight the **Test Settle Connection** option.
5. Click the **[Begin Test]** button to run the test.

If all is configured correctly, a **Connection Successful** message will display. If no connection is made, an error message will be shown.

In the event of a problem, Merchant Link support personnel should provide assistance in discussing the issue with their IT Group.

## Configuring Internet Connectivity

The following are considerations when configuring a system to use Internet Connectivity as the communications channel.

### 1. Internet Configuration

Normal configuration of a site's Internet must be done prior to testing MICROS CA/EDC transactions.

### 2. Internet Connectivity

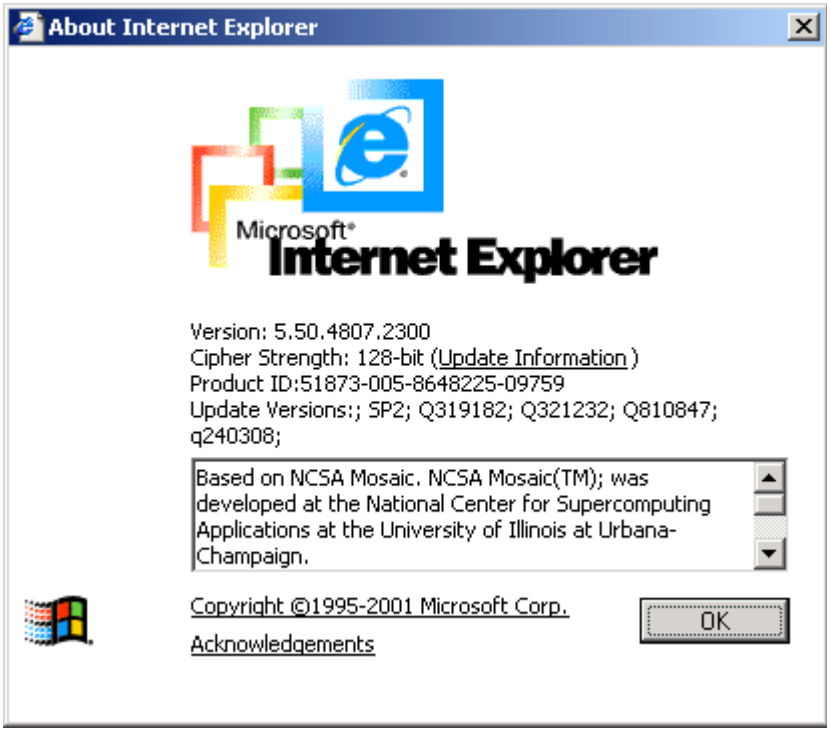
Merchants must have an ISP account that supports DSL, ISDN, or Cable modem connectivity. Connection to the Internet can also be established through a corporate LAN or WAN.

### 3. Internet Explorer Cipher Strength

In order for the 3700 POS CA/EDC software to properly make connections with **g1.merchantlink.com** and **g2.merchantlink.com**, the encryption strength (or Cipher Strength) of the MICROS RES Server must be 128-bit. The Cipher strength on a given server can be easily checked as follows:

1. Open Internet Explorer
2. Click on the **Help** menu.

3. Select the **About Internet Explorer** option. The following window will display:




The second line is the Cipher Strength. If that is anything less than 128-bit, the server will need to be updated. The specifics on what is needed for the update is dependent upon the RES Server's Operating System and/or Internet Explorer version. The URL for the Microsoft High Encryption Pack update page is:

http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp

### 4. Test Internet Connectivity

The site must be able to connect to ML's siteNET gateway through port 8443. To create a successful round trip test to the siteNET Gateway, open Internet Explorer on the RES Server and attempt to access the following URL from the browser:

*https://g1.merchantlink.com:8443/test.cgi*

This does an HTTPS GET request to the siteNET Gateway. Internet Explorer responds with a File Download request.

If the GET request makes it to siteNET, a plain text message of *cgi is working* is sent back. This response is necessary before continuing with the CA/EDC installation.

If a problem is encountered, and you do not receive the *cgi is working* message, one of the following issues may be responsible:

- Something is blocking the connection. Check the firewall settings.
- The site's network configuration is not resolving the URL correctly.

Should either of these errors occur, a trained network person may be required to configure the site's network for access to the siteNET gateway.

### 5. Host and Backup Host Configuration

To process via a high-speed internet connection, the site must be able to connect to ML's siteNET gateway through port 8443. This requires configuring the following fields on the *System* tab (*POS Configurator* | *Devices* | *CA/EDC Drivers*) for both the authorization and settlement drivers:

- **Host IP Address: Port** — g1.merchantlink.com:8443
- **Backup IP Address: Port** — g2.merchantlink.com:8443

### 6. Test Internet Connectivity via Credit Card Utility

If a browser is not available on the RES Server, use the test connection tool in the MICROS Credit Card Batch Utility.

This can be done as follows:

1. Open the **Credit Card Batch** Program on the RES Server.
2. Go to the *Diagnostics* tab.
3. In the **CA/EDC Drivers list** box, select one of the TV's authorization or settlement drivers.
4. From the *Diagnostic Functions* window, highlight the **Test Settle Connection** option.
5. Click the **[Begin Test]** button to run the test.

If all is configured correctly, a **Connection Successful** message will display. If no connection is made, an error message will be shown. Problems related to the Internet or ISP will require further investigation from the Merchants ISP. Merchant Link support personnel should provide assistance in discussing these issues with the ISP.

### 7. Fallback Configuration

The TV has a built-in feature to support failover or "fallback" capability for authorizations using either TCP/IP or Internet Connectivity. This feature enables the driver to automatically switch from a TCP/IP protocol to dial-up if the connection to the ML fails. In other words, fallback is initiated when the MICROS 3700 POS cannot connect to the credit card host.

Fallback is **not** initiated if the POS makes the connection but then error out (i.e., the connection is lost). In this case, the user receives an error and can try the transaction again. If the system consistently connects and then errors out, MICROS recommends the following:

1. Place a call to your support desk.
2. Change the **Communication Channel** option to Dial-up (0) until the situation is resolved.

For this functionality to work, a modem must be installed on the RES Server. The device number and network phone numbers must also be entered into the driver configuration.

As a first step in setting up **Fallback** mode, MICROS recommends testing the TV with a communications channel configured for Dial-up (0). Once the system can process credit card transactions in this mode, the communications channel can be changed and the modem can be configured in *POS Configurator* | *Devices* | *CA/EDC Drivers*. This includes specifying the **Authorization** and **Backup Authorization Phone Numbers**.

## 8. Internet Security

The security and protection of the MICROS network, and the data and applications on that network, are solely and entirely the responsibility of the customer. A properly configured firewall is required for each site that uses a persistent connection to the Internet or any private internal network where there is a potential for unauthorized access to the MICROS network.

The customer is solely and entirely responsible for the security of the MICROS network, 3700 POS, and their data against unauthorized access and any damage and support costs incurred as a result of said access.

# Licenses

This driver is subject to the following license agreements:

- OpenSSL License
- SSLeay license

The terms of both licenses are listed below:

## OpenSSL License

Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com).”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

# *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 MICROS system. Frequent audits allow the end-user to identify problems quickly and, if necessary, place a call to 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 Transaction Vault 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 Transaction Vault Credit Card Driver (CaTV) for the prevention of duplicate batches.

# ReadMe First
# V. 4.14.0.2481

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.14 release of the Transaction Vault Driver.

## In This Section...

# 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

There are no new features in this release.

# 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

The following table summarizes the revisions included in this version:

| Feature | Page |
|---|---|
| Driver Could Timeout Waiting for Response with Multi-Threaded Transactions | 42 |
| Decryption of EMSR Data could fail during Pre-Settlement | 42 |
| Auth transaction sent wrong merchant data in multi-merchant environment | 43 |

## Revisions Detailed

### Driver Could Timeout Waiting for Response with Multi-Threaded Transactions

**CR ID #: N/A**

Previously, when processing multi-threaded Credit Card transactions, the driver would timeout waiting for a response. This has been corrected. Now, each request will be processed in a separate connection and each connection will process one request.

### Decryption of EMSR Data could fail during Pre-Settlement

**CR ID #: N/A**

Previously, decryption of IDTECH EMSR data could fail during pre-settlement when processing a voice authorization. This would happen if there were two auths for the same account number, the credit card driver would pick the 'best' auth to use during pre-settlement, which may not have the EMSR indicator stored in the driver data. This has been corrected.

### Auth transaction sent wrong merchant data in multi-merchant environment

**CR ID #: N/A**

Previously, when the driver was sending multi-threaded authorizations in a multi-merchant environment, in some instances, the wrong authorization data was sent during settlement. This would cause settlement to fail. This has been corrected.

# ReadMe First
# V. 4.13.0.2468

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.13 release of the Transaction Vault Driver.

## In This Section...

# 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 |
|---|---|
| Support Added For ID TECH Devices | 45 |

## New Features Detailed

### Support Added For ID TECH Devices

#### CR ID #: N/A

With this release, support for the ID TECH SecureMag and SecureKey devices has been added. The SecureMag device is an integrated Encrypted Magnetic Stripe Reader (EMSR) that replaces the current workstations Magnetic Card reader. The SecureKey device is used to enter credit card numbers when the credit card cannot be read with the SecureMag device.

Please refer to the RES410_RMF.pdf for more information about EMSR Mode configuration.

***Note*** *ID TECH devices require RES v5.1 or higher.*

# 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

The following table summarizes the enhancements included in this version:

| Feature | Page |
|---|---|
| Support Added For Multi-Threaded Authorizations | 46 |

## Enhancements Detailed

### Support Added For Multi-Threaded Authorizations

#### CR ID #: N/A

With this release, the Transaction Vault authorization driver has been updated to process credit card authorizations as multi-threaded transactions versus single-threaded transaction. This allows credit card authorizations to be processed concurrently instead of the authorizations queuing and processing consecutively.

# 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

The following table summarizes the revisions included in this version:

| Feature | Page |
|---|---|
| Credit Card Service Could Fail To Start | 47 |
| Driver Locked Up During Settlement | 47 |

## Revisions Detailed

### Credit Card Service Could Fail To Start

**CR ID #: N/A**

Previously, when the Credit Card Service (CCS) was being started, which loads the drivers; the driver initialization process could fail. This resulted in CCS hanging in the Windows Services with a status of 'Starting'. This has been corrected.

### Driver Locked Up During Settlement

**CR ID #: N/A**

Previously, under certain scenarios the credit card driver would lock-up during settlement. This kept the batch from settling successfully. This has been corrected.

# ReadMe First
# V. 4.11.21.2418

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.11 release of the Transaction Vault Driver.

## In This Section...

# 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

There are no new features in this release.

# 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

The following table summarizes the enhancements included in this version:

| Feature | Page |
|---|---|
| Open SSL Libraries have been Updated | 50 |
| McrsOpenSSLHelper.dll Included in the Install | 50 |

## Enhancements Detailed

### Open SSL Libraries have been Updated

#### CR ID #: N/A

With this release, the Secure Sockets Layer (SSL) Libraries (libeay32.dll and ssleay32.dll), which are used when Communication Channel 2 (Internet) is enabled, have been updated to version 1.0.0.4.

### McrsOpenSSLHelper.dll Included in the Install

#### CR ID #: N/A

With this release, the McrsOpenSSLHelper.dll has been added to the install. This dll will allow two or more drivers that use the Open SSL format to run on the same system simultaneously.

# 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

The following table summarizes the revisions included in this version:

| Feature | Page |
|---|---|
| Settlement Could Error if a Credit Card was a Keyed Entry | 51 |
| Settlement Could Omit Records if Batch Contains Reversals | 51 |
| Credit Card Batch Detail Report had Incorrect Forward Count | 52 |

## Revisions Detailed

### Settlement Could Error if a Credit Card was a Keyed Entry

**CR ID #: N/A**

Previously with Transaction Vault Driver version 4.10, if a credit card batch contained a record that was manually keyed, settlement could fail during transmission to certain host processors. This only occurred when not using TransactionShield™. This has been corrected.

### Settlement Could Omit Records if Batch Contains Reversals

**CR ID #: N/A**

When a check has multiple auths, the credit card driver selects the 'best auth' to use during settlement. If the batch contained reversals, the driver will complete all reversal first. In previous Version of the driver under certain scenarios, the driver would reverse an unused auth, then would use the same auth code to try to settle the batch record. This could result in the batch failing to settle all records correctly. This has been corrected.

### Credit Card Batch Detail Report had Incorrect Forward Count

**CR ID #: N/A**

Previously, the Credit Card Batch Report would not have the Forward Count when the batch contained auto offline or manual/voice auth records. This was due to the driver not properly updating the records as settled.

For example:

Offline Count: 2

This number represents the auto offline auths that are processed online and then settled.

Forward Count: 2 + 0  Forward Balance: 15.08

The forward count is the number of credit card transactions that have been settled. The first number is the total amount of credit card transactions. The second number is the amount of credit reversals that have been completed and all zero payment records that are discarded from processing because they are not used (auto offline auths, manual auths).

The forward balance is the total dollar amount of all the transactions. The auth reversal will always be zero dollars.

# ReadMe First
# V. 4.10.21.2365

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.10 release of the Transaction Vault Driver.

## In This Section...

# 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 |
|---|---|
| TransactionShield™ Authorizations Now Supported | 54 |

## New Features Detailed

### TransactionShield™ Authorizations Now Supported

#### CR ID #: N/A

With this release, support for TransactionShield™ Credit Card Authorization has been added. TransactionShield™ provides a means to eliminate cardholder data at the customer system level and now encrypts the data as the card is swiped through the external Magtek IPAD device. The data is then stored in a secure, hosted 'vault' via transmission to Merchant Link. This feature utilizes cloud-based decryption, so the merchant no longer has decrypted data on site; providing protection of the cardholder's personal information.

Additional logging has been added to the credit auth request message. The following are examples of the possible messages that will be in the 3700d.log:

'...IPAD is loaded with test key' - with Credit Card Server verbosity set to 5 or higher.

'...IPAD is loaded with production key' - with Credit Card Server verbosity set to 5 or higher.

'...IPAD is loaded with unknown key' - with Credit Card Server verbosity set to 0 or higher.

For information on this feature, see the *RES 4.10 RMF, MD0003-175*.

> ***Note*** *TransactionShield™ requires RES v4.10 or v5.1 or higher.*

# 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.

# ReadMe First
# V. 4.9.21.2292

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.8 release of the Transaction Vault Driver.

## In This Section...

# 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 enhancements included in this version:



## New Features Detailed

### RFID for MX870 PinPad Device Now Supported

#### CR ID #: N/A

With this release, RFID card entry for authorizations and settlements are now supported on the MX870 PinPad Device.

Note: The MX870 only supports credit transactions. Debit is not supported.

### Authorization Reversals Are Now Supported

#### CR ID #: N/A

With this release, authorization reversals are now supported. Card associations are now mandating that merchants submit authorization reversals for fully-approved or partially-approved transactions that will not be settled.

The authorization reversal transaction negates the approved amount that has been 'on hold' on the cardholder's account. It is intended as a clearing transaction that will release the customer's open-to-buy.

For example:

Authorizations on a guest check that receive an Auth Code and TransVault Key, but are then closed to Cash; will now be reversed at Settlement time. This occurs during the Pre-Settlement Process.

In the case of multiple authorizations for the same account on a single guest check (i.e.- secondary auths), the 'best' authorization is used to settle the transaction and the remaining authorizations on this check will be reversed.

Only authorizations that receive an Auth Code and TransVault key will be reversed. Manual Authorizations, Auto-offline Auths, and Below Floor Limit Offline auths will not be reversed.

There is a limitation that at most two auths can be reversed for each account on a single guest check.

---

***Note*** *Authorization reversals are only supported in RES Version 4.5 or higher.*

*Corrective authorizations are not compatible with authorization reversals and are therefore no longer supported. If you currently have corrective authorizations configured, you should remove this.*

---

### Batch Number Mode Now Defaults to One

**CR ID #: N/A**

With this release, the Batch Number Mode will default to one. This is the most common configuration required by the processors.

This default is only used when the driver is installed in *POS Configuration* | *Devices* | *CA/EDC Drivers*.

This change will not affect the configuration of a driver that is already installed.

# 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

The following table summarizes the enhancements included in this version:

| Feature | Page |
|---|---|
| Credit Card Batch Report Now Includes Reversal Count | 60 |

## Enhancements Detailed

### Credit Card Batch Report Now Includes Reversal Count

**CR ID #: N/A**

With this release, the 'Credit Card Batch Report' will now support the reversal count. If no reversals have been done, the report will reflect a zero.

For example:

Forward Count: 2 + 0  Forward Balance: 15.08

The forward count is the number of credit card transactions that have been settled. The first number is the total amount of credit card transactions. The second number is the amount of credit reversals that have been completed.

The forward balance is the total dollar amount of all the transactions. The auth reversal will always be zero dollars.

# 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

The following table summarizes the revisions included in this version:

| Feature | CR ID # | Page |
|---|---|---|
| Rejected Credit Card Batch Record Being Reported Off By One | N/A | 61 |
| Large Batch Settlements Fail Over Dial Up Connection | N/A | 61 |
| EOT Results in a Timeout When in Multitrans Mode | N/A | 62 |
| Multiple Credit Card Authorization Results in Memory Leak | N/A | 62 |

### Rejected Credit Card Batch Record Being Reported Off By One

**CR ID #: N/A**

Previously, the Transaction Vault Settlement Driver was reporting the wrong record number being rejected by the batch. For example, when two records are created in a Credit Card Batch and record two was rejected. The driver would report that record one had failed, when actually record two failed. This has been corrected.

### Large Batch Settlements Fail Over Dial Up Connection

**CR ID #: N/A**

Previously, the Transaction Vault Settlement Driver failed during large batch settlements when the connection was over dial up. The error message 'No response from CA driver' would appear after batch settlement failed. This has been corrected.

### EOT Results in a Timeout When in Multitrans Mode

**CR ID #: N/A**

Previously, Transaction Vault would timeout when the host would send out an EOT (End of Transmission) instead of an ENQ (Enquiry) when in multitrans mode. This has been corrected.

With this version, when the host sends out an EOT, the connection will close and a request for a new connection is queued.

### Multiple Credit Card Authorization Results in Memory Leak

**CR ID #: N/A**

Previously, if multiple credit card transactions were submitted, the CCS memory usage would increase, and would not release after the authorizations were completed. This has been corrected.

# ReadMe First
# V. 4.7.20.2065

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.7 release of the Transaction Vault Driver.

## In This Section...

# 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 enhancements included in this version:

| Feature | Page |
|---|---|
| Auto Offline Credit Card Authorization Support Introduced | 64 |
| Partial Auth Support for Prepaid Credit Cards Introduced | 68 |
| Second Level Encryption for Transaction Vault | 68 |
| RFID Transactions Not Supported | 69 |

## New Features Detailed

### Auto Offline Credit Card Authorization Support Introduced

#### CR ID #: N/A

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 IP addresses and through dial backup.
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.
6. The **Auth Offline Transactions** option (*Devices* | *CA/EDC Drivers* | *System*) was added to the TVC settlement driver to control how these transactions are handled at settlement.

- By default the option is disabled, and the settlement driver will treat these transactions as manually keyed and manually authorized transactions, and will attempt to settle them as though they were regular manual authorizations. ***Note:*** *If these records fail to settle, they will cause the entire batch to fail to settle.*
- With the option enabled the settlement driver will attempt to obtain a real 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.

7. 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.

8. 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.

## TVC Driver Configuration

To prevent a restaurant from being offline for an extended period without being aware of the network outage, the following options were added to the TVC driver.

- **Max offline transactions** (*Devices* | *CA/EDC Drivers* | *System*). This option controls the maximum number of automatic offline transactions that can be processed by the driver.
- **Max offline amount** (*Devices* | *CA/EDC Drivers* | *System*). This option controls the maximum dollar value of automatic offline transactions that can be processed. The maximum cumulative offline amount is entered as dollars (e.g., 2500 is the equivalent of $2500.00).

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.

## POS Configuration

To support this functionality, the following options were added 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.

## Partial Auth Support for Prepaid Credit Cards Introduced

### CR ID #: N/A

With this release, support has been added for the RES partial authorization feature, which permits a site to accept prepaid credit cards more conveniently and reliably

This credit card driver feature is only available when used in conjunction with RES v 4.3 hot fix 2 or RES v 4.5 or greater. For information on how to configure this feature in RES, see the *RES v 4.3 Hotfix 2 Documentation*.

## Second Level Encryption for Transaction Vault

Previously, the credit card number, expiration date, and track data was encrypted at the time of transmission. Now, the Transaction Vault Credit Card Driver when used in conjunction with RES v. 4.3 Hotfix 2 and greater encrypts the data from the moment the card is swiped and this encrypted data is then encrypted a second time, as though it were still sensitive data. This functionality must be enabled separately for credit and

debit drivers. For more information, see the *RES Version 4.3 Hotfix 2 Documentation, MD0003-139*.

### RFID Transactions Not Supported

RFID transactions are not supported by the Transaction Vault Credit Card Driver. When an attempt is made to submit an RFID authorization to the CaTVCA driver, the user will receive the message "RFID not supported."

# 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

The following table summarizes the revisions included in this version:

| Feature | CR ID #/ SCR # | Page |
|---|---|---|
| Text Was Truncated at First Space | N/A/ 35690 | 72 |
| Manual Authorization Could be Settled with Incorrect Transaction Time | N/A 34879 | 72 |

## Revisions Detailed

### Text Was Truncated at First Space

**CR ID #: N/A**

**SCR #: 35690**

Previously, the TVCA and TVCS Drivers would incorrectly truncate text present in the driver configuration at the first space. For example, Mike Rose Cafe would appear as Mike. This has been corrected.

### Manual Authorization Could be Settled with Incorrect Transaction Time

**CR ID #: N/A**

**SCR #: 34879**

When a manual auth is settled the driver pre-settles the transaction to obtain a TransactionVault ID number. If the settlement batch fails after receiving the TransactionVault ID, then the driver saves the TransactionVault ID, and the date and time of the pre-settled transaction. Previously, when the driver attempted a second time to settle the transaction, the time sent in the settlement record would be the time of the pre-settlement, not the original transaction time. This has been corrected.

# ReadMe First
# V. 4.6.19.1900

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.6 release of the Transaction Vault Driver.

## In This Section...

# 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 enhancements included in this version:

| Feature | Page |
|---|---|
| Driver Checks to Verify that the User Enters a Valid TransactionVault Key Number During a Corrective Authorization | 74 |

## New Features Detailed

### Driver Checks to Verify that the User Enters a Valid TransactionVault Key Number During a Corrective Authorization

The TransactionVault Driver will now check to verify that a valid TransactionVault Key number is entered when performing a corrective authorization.

# 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

The following table summarizes the revisions included in this version:

| Feature | CR ID # | Page |
|---|---|---|
| CaTVCA and CaTVCS Drivers Encounter an Error When Handling Back-to-Back Responses Over a Dialup Connection | N/A | 77 |
| CaTVCA and CaTVCS Drivers Unable to Authorize or Settle if the SiteNET ID Contained a Either a Leading or a Trailing Space | N/A | 77 |
| CaTVCS Driver Does Not Correctly Quarantine Batch After Local Settlement Failure | N/A | 77 |
| CaTVCS Driver Incorrectly Re-sends Batch After Timeout | N/A | 77 |
| If the CaTVCA and TVCS Drivers Did not Receive an ENQ-byte During a Multiple-Transaction Connection, then the Drivers Would Not Close the Connection | N/A | 78 |
| If the Driver Encountered an Error Condition During Authorization or Settlement it Would Close the Connection and Fail to Retransmit the Request | N/A | 78 |
| Transactions Failed to Settle if TransVault Key Duplicate | 24653 | 78 |

## Revisions Detailed

### CaTVCA and CaTVCS Drivers Encounter an Error When Handling Back-to-Back Responses Over a Dialup Connection

**CR ID #: N/A**

Previously, the CaTVCA and CaTVCS drivers would encounter an error when attempting to process multiple back-to-back authorization or settlement responses when a dialup connection was used. This would only occur in situations where there was no delay between receiving messages. This has been corrected.

### CaTVCA and CaTVCS Drivers Unable to Authorize or Settle if the SiteNET ID Contained a Either a Leading or a Trailing Space

**CR ID #: N/A**

Previously, the CaTVCA, and the CaTVCS drivers would fail to authorize or settle if the SiteNET ID contained either a leading, or a trailing space. An error, "TIMEOUT AWAITING POLL" would occur due to the space(s) in the SiteNET ID. This has been corrected and the SiteNET ID will automatically truncate any leading or trailing spaces.

### CaTVCS Driver Does Not Correctly Quarantine Batch After Local Settlement Failure

**CR ID #: N/A**

Previously, when a local settlement attempt failed, it was possible for the TransferStatus to inaccurately record the batch status as *BatchOpen Submitted*. As a result, the credit card application would duplicate the batch thinking that the previous attempt failed when attempting to transmit to Merchant Link.

Now, the driver will always set the TransferStatus to *Local Accept* for all locally settled batches. In the event of a failure, the batch will be quarantined, until another local settlement attempt is made.

### CaTVCS Driver Incorrectly Re-sends Batch After Timeout

**CR ID #: N/A**

Previously, if the CaTVCS driver timed out while waiting for a response to close the batch, then the driver would incorrectly flag the batch with a BatchClose Error, indicating that the batch should be resubmitted to the host. The correct behavior is to flag the batch with a Response Failure status, which results in the batch being quarantined. This has been corrected.

### If the CaTVCA and TVCS Drivers Did not Receive an ENQ-byte During a Multiple-Transaction Connection, then the Drivers Would Not Close the Connection

**CR ID #: N/A**

During a multiple-transaction connection, the CaTVCA and the CaTVCS drivers expect the host to transmit an ENQ-byte after the host has received the ACK from the driver. If the driver does not receive the ENQ-byte, the credit card connections should be closed. However, regardless of whether the ENQ-byte was sent or not, the drivers would continue to process the transaction. This has been corrected.

### If the Driver Encountered an Error Condition During Authorization or Settlement it Would Close the Connection and Fail to Retransmit the Request

**CR ID #: N/A**

When using a TCP/IP or an Internet connection, the driver could receive an "Unexpected Host Response" error message. When this occurred, the driver would close the connection and not attempt to retransmit the request to the host. The correct behavior is to re-transmit the request. This issue has been corrected, and the driver will now attempt to retransmit up to 3 times before disconnecting with the Host.

### Transactions Failed to Settle if TransVault Key Duplicate

**CR ID #: 24653**

Previously, TransVault settlement could fail if two records had the same TransVault Key. This would occur when there was a protocol error between two consecutive authorization requests when using TCP/IP or Internet Communication. This has been corrected.

# ReadMe First
# V. 4.5.19.1614

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.5 release of the Transaction Vault Driver.

## In This Section...

# 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 enhancements included in this version:

| Feature | Page |
|---|---|
| Allow Settlement of Authorizations Performed by the Universal Credit Card Driver | 81 |
| Communication Through a Proxy Server is Supported | 81 |
| Credit Card Server Faulting When Trying to Settle a Batch Containing Authorizations from Different Driver | 83 |

# New Features Detailed

## Allow Settlement of Authorizations Performed by the Universal Credit Card Driver

The Transaction Vault Settlement drivers will now support the settlement of authorization requests submitted using the Universal Credit Card Driver (UCCD). This feature is useful in a situation where the site performs authorizations using the UCCD driver and then switches to the Transaction Vault driver without batching and settling all transactions.

When settlement is initiated, the UCCD authorizations will be submitted to the host processor for pre-settlement and will be assigned a TransactionVault key.

To compensate for missing information that is present in a Transaction Vault authorization but not in a UCCD authorization (e.g., Cardholder ID, Account Data Source), the TV driver will use default values.

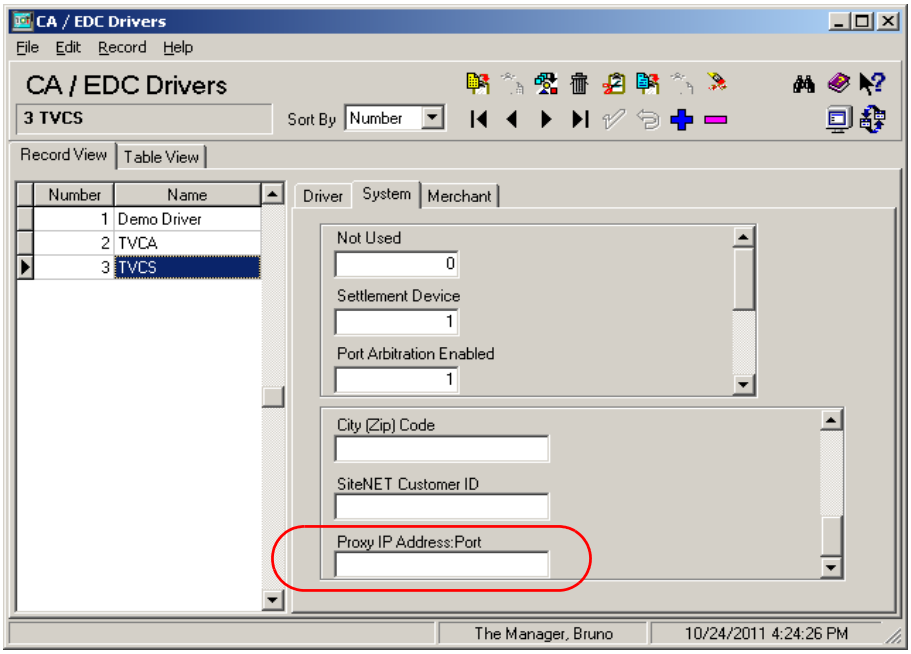
This feature supports all released versions of the UCCD driver.

## Communication Through a Proxy Server is Supported

The Transaction Vault credit driver now supports communication through a Proxy Server when using the Internet Communications Channel (COMM Channel 2).

The Proxy Server is typically a single computer within a Local Area Network (LAN) that acts as a gateway to the internet for all other computers on the LAN. Devices located outside of the network can also relay data to a Proxy Server.

To support this feature a new option has been added to the *Devices* | *Ca/EDC Drivers* | *System* tab in POS Configurator.




The **Proxy IP Address:Port** option can be configured with the address and port number of the proxy server on the local network. This information can be provided by your Network Support Personnel. If left blank, the Proxy Server will not be used.

If used, this field must be configured for the TVCA, and the TVCS drivers.

### Credit Card Server Faulting When Trying to Settle a Batch Containing Authorizations from Different Driver

Previously, the Credit Card Server would fault during settlement if the batch contained transactions authorized by a different driver (e.g., the Demo Driver).

Now, if the user attempts to settle a transaction using a driver other than the Transaction Vault Driver, then settlement will abort and the following error message will display on the Credit Card Batch Utility and print on the settlement report:

```
Record not allowed.
```

**Note** *One exception to this new rule is the UCCD Driver. If the user has just upgraded from the UCCD Driver to the Transaction Vault Driver, and there are open batches that have not been settled, then the TV Driver will perform pre-settlement for these records. During pre-settlement a TransactionVault Key number will be assigned to each record so that these records can be transmitted to the Host Processor.*

# 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

The following table summarizes the revisions included in this version:

| Feature | CR ID # | Page |
|---|---|---|
| Cannot Print Credit Card Voucher When the Amount Due is the Same as the Initial Authorization Amount | N/A | 86 |
| CaTVCA and CaTVCS Drivers Logging Extra Information at Verbosity 0 | N/A | 86 |
| CaTVCA and CaTVCS Drivers Logging Improperly | N/A | 86 |
| CaTVCA Driver can Log Invalid Characters Causing the Credit Card Server to Close Unexpectedly | N/A | 86 |
| CVV Value Would Log in the 3700d.log | N/A | 87 |
| Multi-Transaction Mode Not Working Properly if the Transaction Vault Driver is Configured for Multiple Merchants | N/A | 87 |
| Dynamic Batch Numbering Mode Sending Wrong Batch When it Hits Batch #999 | N/A | 87 |
| The Occurrence of an Error During Local Batch Settlement Could Result in an Incorrect Transfer Status and the Batch Being Sent Online Twice | N/A | 87 |
| Unable to Load the TransactionVault Drivers on a Windows XP Pro Server Running RES 4.1 | N/A | 87 |
| Unable to Set Batch Number After Installing a New Driver | N/A | 88 |

## Revisions Detailed

### Cannot Print Credit Card Voucher When the Amount Due is the Same as the Initial Authorization Amount

**CR ID #: N/A**

When the amount due matched the amount of the initial authorization, the user received the "Must Print Voucher" error message. This error condition prevented the user from finalizing the guest check. This has been corrected.

### CaTVCA and CaTVCS Drivers Logging Extra Information at Verbosity 0

**CR ID #: N/A**

The CaTVCA and CaTVCS drivers were logging the following normal information at the verbosity setting of 0:

```
Error connecting SSL object
```

This message will now only be logged at a verbosity setting of 2 or higher. This additional messaging may be needed if the failure resulted in an inability to connect to the host.

### CaTVCA and CaTVCS Drivers Logging Improperly

**CR ID #: N/A**

The version 4.3 CaTVCA and CaTVCS drivers were logging all information about the driver when the verbosity was set to 0. Detailed message logging was being sent to the 3700d.log and not the individual driver logs. This issue has been corrected.

### CaTVCA Driver can Log Invalid Characters Causing the Credit Card Server to Close Unexpectedly

**CR ID #: N/A**

Previously, the CaTVCA driver could log invalid characters causing the Credit Card Server to close unexpectedly. This issue would occur in the following situations:

- Verbosity is configured to be higher than 4.
- During a transaction that immediately followed a transaction that went into fallback mode.

This has been corrected.

### CVV Value Would Log in the 3700d.log

**CR ID #: N/A**

The Card Verification Value (CVV) for the CaTVCA driver was not being masked in the authorization request message and would then log in the 3700d.log. This has been corrected.

### Multi-Transaction Mode Not Working Properly if the Transaction Vault Driver is Configured for Multiple Merchants

**CR ID #: N/A**

Previously, if multiple merchants were configured at a site, and two or more transactions occurred at the same time, some authorizations would fail. This has been corrected.

### Dynamic Batch Numbering Mode Sending Wrong Batch When it Hits Batch #999

**CR ID #: N/A**

When the CaTVCS driver was in dynamic batch numbering mode, and the batch number reached 999, the driver would mistakenly send batch number 1. This has been corrected.

### The Occurrence of an Error During Local Batch Settlement Could Result in an Incorrect Transfer Status and the Batch Being Sent Online Twice

**CR ID #: N/A**

If an error occurred during local settlement, the batch would be interrupted and the Transfer Status would be incorrect. When the user attempted to settle the batch again, the incorrect Transfer Status caused the batch to be settled a second time (online), rather than treat it as a local settlement. This resulted in a duplicated batch being sent to the Host. This issue has been corrected.

### Unable to Load the TransactionVault Drivers on a Windows XP Pro Server Running RES 4.1

**CR ID #: N/A**

A server running Windows XP Pro with RES Version 4.1 installed was unable to load the TransactionVault authorization and settlement drivers. This was due to a second instance of the required libeay32.dll file in the *\Windows\System32* directory that was being used by another Windows application. As a result the TV driver DLLs were prohibited from loading properly.

To ensure that the libeay32.dll and the ssleay32.dll files do not compete with any other Windows applications, these files are now installed in the *\Micros\Common\Bin* folder.

### Unable to Set Batch Number After Installing a New Driver

**CR ID#: N/A**

Previously, when performing 'Set Batch Number' in *CC Batch Utility | Diagnostics*, for a new settlement driver installation; the error "Can't set Batch Number to..." would appear if there were no previous batches. Now, if no batches have been attempted, the diagnostic function will allow setting the batch number for the next batch attempt.