ORACLE

Oracle Hospitality RES 3700

Transaction Vault Debit Card Driver Version 5.1

July 2016

Installation and Setup

This section contains installation and setup instructions for the Version 5.1 release of the Transaction Vault Debit (CaTVD) Card Driver. The Transaction Vault debit driver is available on the Oracle web site Product Support page.

The debit version of the Transaction Vault driver may be used on RES systems running Version 5.0 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 Oracle 3700 secures data for the customer minimizing the potential for security breaches.

The purpose of the TransactionVault feature is to remove sensitive credit and debit 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.

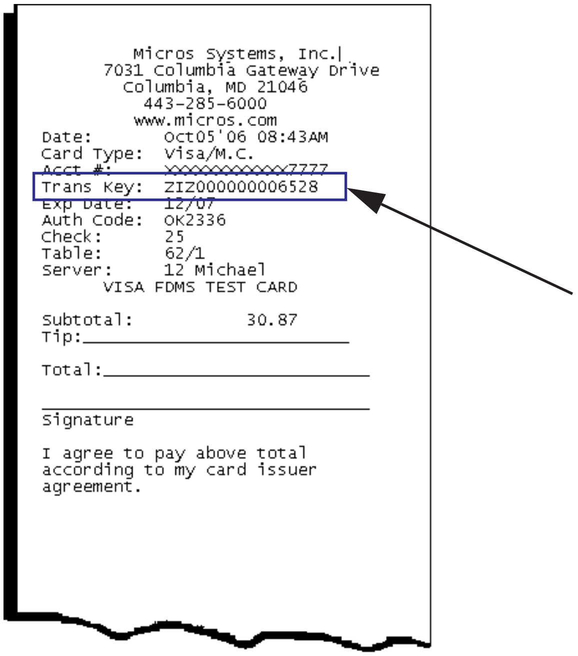
For additional information about TransactionVault see the *RES 4.1 HF2 ReadMe First, MD0003-098* or the *RES 3.2 SP7 HF6 Documentation*.

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 Oracle 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.



```
         Micros Systems, Inc.|
      7031 Columbia Gateway Drive
        Columbia, MD 21046
          443-285-6000
         www.micros.com
Date:         Oct05'06 08:43AM
Card Type:    Visa/M.C.
Acct #:       XXXXXXXXXXXX7777
Trans Key:    ZIZ000000006528
Exp Date:     12/07
Auth Code:    OK2336
Check:        25
Table:        62/1
Server:       12 Michael
      VISA FDMS TEST CARD

Subtotal:            30.87
Tip:_________________________

Total:_________________________

_______________________________
Signature

I agree to pay above total
according to my card issuer
agreement.
```

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/Debit 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.

Corrective Authorizations for Debit Transactions

With a debit transaction money is transferred at the time that the transaction is performed and cannot be edited after they are approved. For this reason corrective authorizations are not permitted for debit transactions. Corrective authorizations are only permitted for credit card transactions. If a Corrective Authorization is attempted with a debit driver the following message will display:

```
Corrective Auth Not Permitted
```

Secondary Level Encryption

This functionality uses a propriety 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.

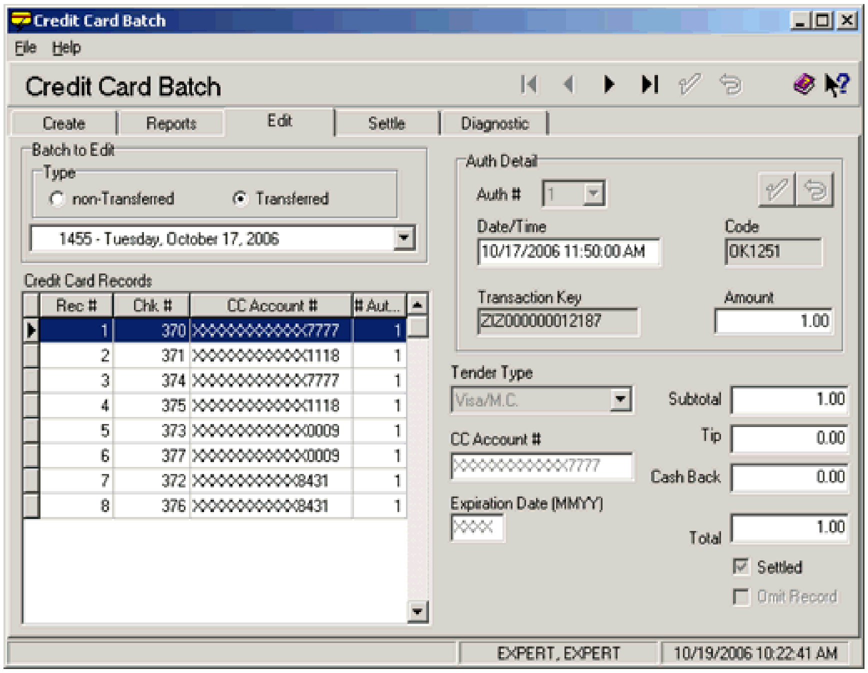
Following a successful batch, no customer information is stored in the RES system.

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.

The TransactionVault Key can be edited if it is entered manually due to a corrective authorization.



Batch to Edit

Type: ○ non-Transferred ● Transferred

1455 - Tuesday, October 17, 2006

Credit Card Records

Rec #	Chk #	CC Account #	# Aut...
1	370	XXXXXXXXXXXX7777	1
2	371	XXXXXXXXXXXX1118	1
3	374	XXXXXXXXXXXX7777	1
4	375	XXXXXXXXXXXX1118	1
5	373	XXXXXXXXXXXX0009	1
6	377	XXXXXXXXXXXX0009	1
7	372	XXXXXXXXXXX8431	1
8	376	XXXXXXXXXXX8431	1

Auth Detail

Auth #: 1

Date/Time: 10/17/2006 11:50:00 AM

Code: OK1251

Transaction Key: ZIZ000000012187

Amount: 1.00

Tender Type: Visa/M.C.

CC Account #: XXXXXXXXXXXX7777

Expiration Date (MMYY): XXXX

Subtotal: 1.00

Tip: 0.00

Cash Back: 0.00

Total: 1.00

☑ Settled

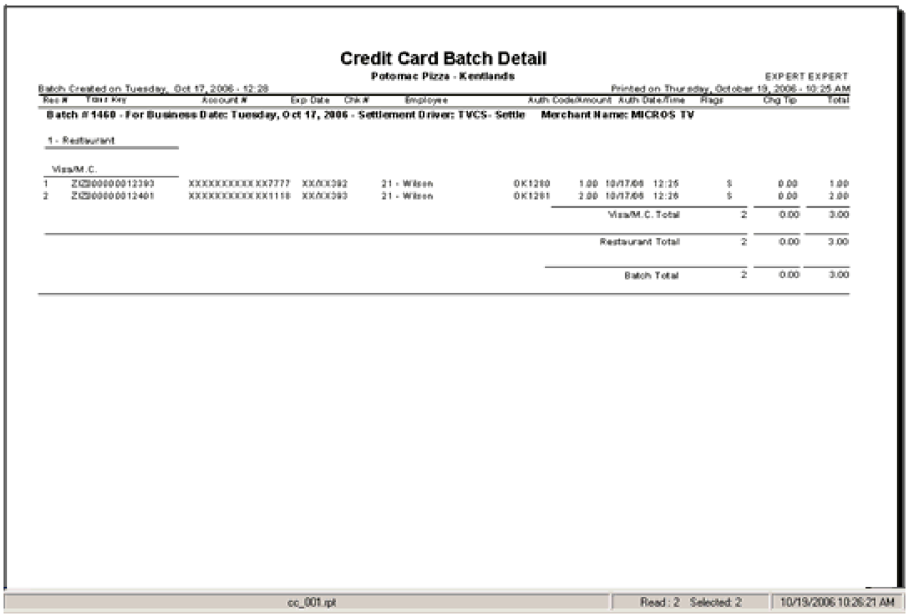
☐ Omit Record

EXPERT, EXPERT | 10/19/2006 10:22:41 AM

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.



Credit Card Batch Detail

Potomac Pizza - Kentlands

EXPERT EXPERT

Batch Created on Tuesday, Oct 17, 2006 - 12:28

Printed on Thursday, October 19, 2006 - 10:25 AM

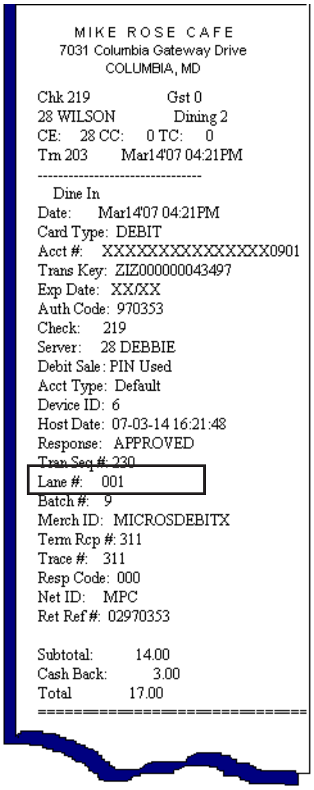
Rec #	TVau Key	Account #	Exp Date	Chk #	Employee	Auth Code/Amount		Auth Date/Time		Flags	Chg Tip	Total
Batch # 1460 - For Business Date: Tuesday, Oct 17, 2006 - Settlement Driver: TVCS- Settle						**Merchant Name: MICROS TV**						
1 - Restaurant												
Visa/M.C.												
1	ZZ00000012393	XXXXXXXXXXXX7777	XX/XX392		21 - Wilson	OK1280	1.00	10/17/06	12:25	$	0.00	1.00
2	ZZ00000012401	XXXXXXXXXXXX1118	XX/XX393		21 - Wilson	OK1281	2.00	10/17/06	12:26	$	0.00	2.00
							Visa/M.C. Total			2	0.00	3.00
							Restaurant Total			2	0.00	3.00
							Batch Total			2	0.00	3.00

cc_001.rpt | Read : 2 Selected: 2 | 10/19/2006 10:26:21 AM

Assigned Lane Numbers to VX670 Devices

A lane number is a unique identifier assigned to each workstation or handheld payment device when it is used for debit transactions requiring a PIN Pad entry. The Lane Number allows the system to keep track of the devices submitting debit authorization requests to the host processor.

When the Verifone device first submits a debit authorization, it will be assigned a Lane number automatically. The Lane Number will increment from 1 to 999. In the event that a Lane Number reaches the maximum (e.g., 999), all of the Lane Numbers will be deleted and the numbers will start again from 1. The number will appear on the voucher addendum returned by the driver to the workstation after the transaction is complete.

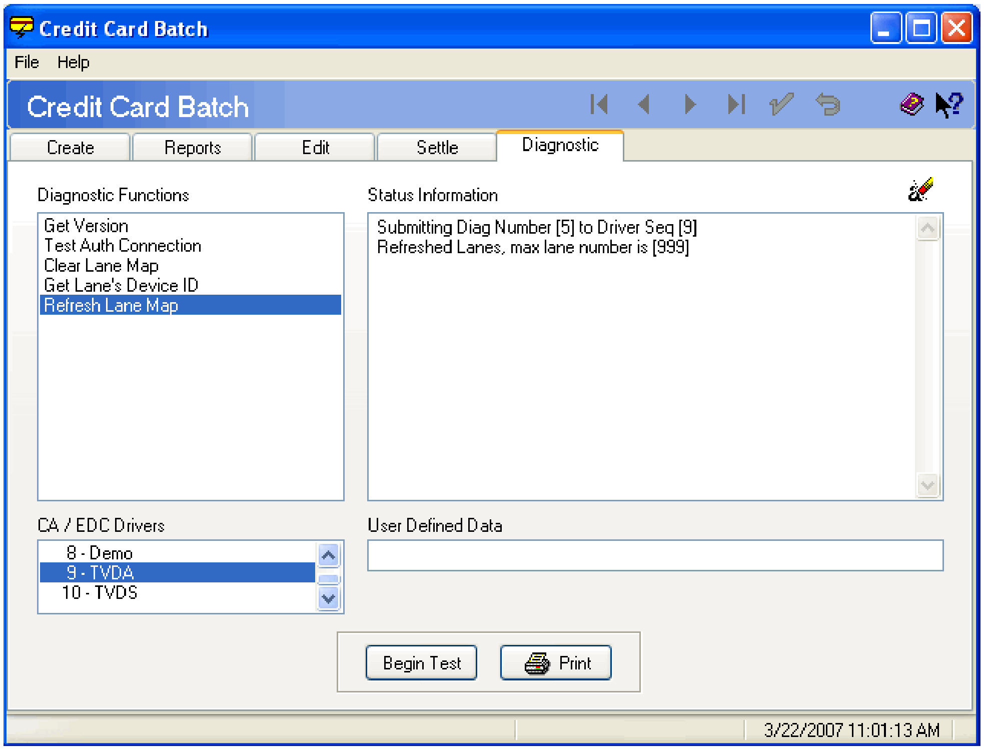


```
          MIKE ROSE CAFE
     7031 Columbia Gateway Drive
           COLUMBIA, MD

Chk 219              Gst 0
28 WILSON            Dining 2
CE:    28 CC:    0 TC:    0
Trn 203      Mar14'07 04:21PM
--------------------------------
   Dine In
Date:      Mar14'07 04:21PM
Card Type:  DEBIT
Acct #:    XXXXXXXXXXXXXXX0901
Trans Key:  ZIZ000000043497
Exp Date:   XX/XX
Auth Code:  970353
Check:      219
Server:     28 DEBBIE
Debit Sale : PIN Used
Acct Type:  Default
Device ID:  6
Host Date:  07-03-14 16:21:48
Response:   APPROVED
Tran Seq #: 230
Lane #:     001
Batch #:    9
Merch ID:   MICROSDEBITX
Term Rcp #: 311
Trace #:    311
Resp Code:  000
Net ID:     MPC
Ret Ref #:  02970353

Subtotal:        14.00
Cash Back:         3.00
Total            17.00
================================
```

The Pin debit device will maintain the same Lane Number after performing a reboot. Lane Numbers can be changed via the Credit Card Batch Utility by running the Refresh Lane Map function under the *Diagnostics* tab.

The TransactionVault Debit Driver uses the Windows registry to store the Lane Number device identifiers. A **LaneMap** registry key was added under the driver's configuration key. Each Vx670 device will represent a value name in the registry. The value data will be the Lane number associated with that device.

To support this feature the following diagnostic functions have been added. Each can be accessed by navigating to the *Credit Card Batch Utility | Diagnostic* tab and selecting **[Begin Test]**.



Diagnostic Functions

- Get Version
- Test Auth Connection
- Clear Lane Map
- Get Lane's Device ID
- Refresh Lane Map

Status Information

```
Submitting Diag Number [5] to Driver Seq [9]
Refreshed Lanes, max lane number is [999]
```

CA / EDC Drivers

- 8 - Demo
- 9 - TVDA
- 10 - TVDS

User Defined Data

3/22/2007 11:01:13 AM

- **Clear Lane Map –** This diagnostic will delete all lane map values from the registry.
- **Get Lane's Device ID –** This diagnostic displays the device ID corresponding to the Lane Number value entered in the **User Defined Data** field in the diagnostic.
- **Refresh Lane Map –** This diagnostic forces the drive to re-read all of the Lane Numbers in the registry. Use this function if one of the lane number values has been changed manually via the registry.

Debit Reversals

This section describes the scenarios which result in the transmission of a debit reversal, when the debited transaction amount is returned to the customer's card.

In a situation where the CaTVD driver times out, no amount is charged to the card, therefore no reversal will be performed.

Scenario 1

In this scenario, no confirmation is received from Oracle back to Merchant Link, which triggers a reversal.

1. Oracle sends a Debit Authorization request to Merchant Link. The TVD driver sets a 50 second timer awaiting a response.
2. Merchant Link forwards the request to the bank.
3. The bank sends a response but Oracle doesn't receive the host's response (e.g., lost in transit) before the timer expires. As a result, Oracle does not send back a Confirmation Record to the Merchant Link TransVault gateway.
4. Debit reversal is initiated from Merchant Link and sent to the bank.

Scenario 2

In this scenario, no host response is sent to Merchant Link, which results in a debit reversal.

1. Merchant Link TransVault does not receive a confirmation response back from Oracle before the 50 second timer expires.
2. A debit reversal is sent to the bank.
3. If no response is received for the reversal, then Merchant Link will retry up to 3 times.
4. If no response is received, then the transaction is terminated. In this case, the reversal is stored in the Merchant Link database until it can be resent.

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 5.0 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.)
- TransactionVault Debit requires the submissions of a Change of Service Request with MerchantLink.

Files Included

Transaction Vault supports both credit card and debit card transactions. The credit and debit drivers are divided into an authorization driver and a settlement driver.

The following lists the files installed for the Trans Vault Debit Driver:

Authorization for Debit Cards (CaTVDA)

\Micros\RES\POS\Bin\CaTVDA.dll
\Micros\RES\POS\Etc\CaTVDA.cfg
\Micros\RES\POS\Bin\CaTVDA.hlp
\Micros\RES\POS\Bin\CaTVDA.cnt

Settlement for Debit Cards (CaTVDS)

\Micros\RES\POS\Bin\CaTVDS.dll
\Micros\RES\POS\Etc\CaTVDS.cfg
\Micros\RES\POS\Bin\CaTVDS.hlp
\Micros\RES\POS\Bin\CaTVDS.cnt

Additional Files

\Micros\RES\Common\Bin\libeay32.dll

\Micros\RES\Common\Bin\ssleay32.dll

\Micros\RES\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 5.0 or Higher

The installation of debit card drivers are 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.

Transaction Vault Debit requires RES Version 4.1 HF2 or higher.

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. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
3. Download the latest Transaction Vault Debit Drivers from the Oracle web site. Copy the file to your RES Server's temp folder and unzip the files. The zip file includes the following:
   - Transaction Vault Debit Card Driver Documentation for RES 3700 POS (**CaTVD_V5.1_MD.pdf**)
   - Transaction Vault Debit Card Driver Software (**CaTVD(5.1).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 **CaTVD(5.1).exe** file. Skip this step if the CaTVD driver should not be installed.

   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
CaTVDA.dll	\MICROS\RES\POS\BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaTVDS.dll	\MICROS\RES\POS\BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaTVDA.cfg	\MICROS\RES\POS\ETC	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC
CaTVDS.cfg	\MICROS\RES\POS\ETC	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC
CaTVDA.hlp	\MICROS\RES\POS\BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaTVDS.hlp	\MICROS\RES\POS\BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaTVDA.cnt	\MICROS\RES\POS\BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaTVDS.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

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

Configuration Instructions

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

TV setup is not done until the CaTVDA, and CaTVDS 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 CaTVDA and CaTVDS Drivers

The TV Debit Drivers require RES Version 5.0 or higher.

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., **CaTVD-Auth**) and a value of the **Driver Code** field (e.g., **TVDA**) 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 Proxy IP Address Port information, if needed.

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., **CaTVD-Settle**) and a value of the **Driver Code** field (e.g., **TVDS**) 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.
```

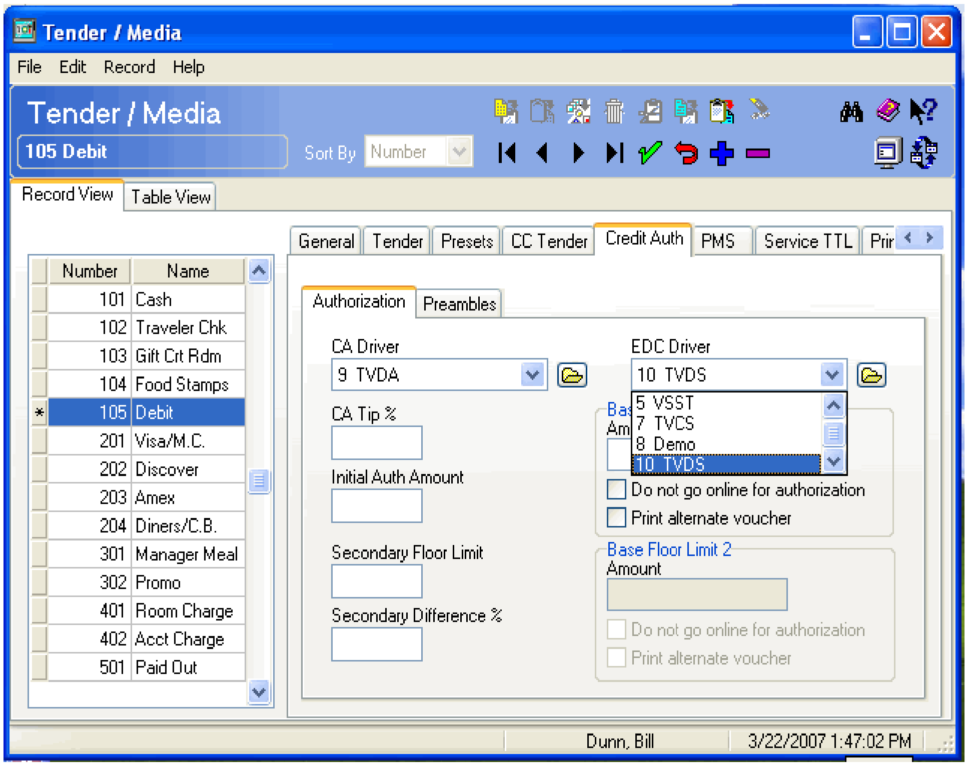
   - **Port Arbitration Enabled –** Enter a value of 1 to enable this driver.
   - **Communications Channel –** Indicate the communication type being used at the store (0 = dial-up, 1 = TCP, 2 = Internet).
   - **Batch Numbering Mode** – This field specifies the method to be used when assigning batch numbers during credit card settlement (0 = Static Batch Numbering Mode, 1 = Dynamic Batch Numbering Mode).
   - **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 Proxy IP Address Port information, if needed.

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 debit tender to the CaTVD driver by configuring the following fields:



105 Debit

	Number	Name
	101	Cash
	102	Traveler Chk
	103	Gift Crt Rdm
	104	Food Stamps
*	105	Debit
	201	Visa/M.C.
	202	Discover
	203	Amex
	204	Diners/C.B.
	301	Manager Meal
	302	Promo
	401	Room Charge
	402	Acct Charge
	501	Paid Out

CA Driver: 9 TVDA

CA Tip %

Initial Auth Amount

Secondary Floor Limit

Secondary Difference %

EDC Driver: 10 TVDS

5 VSST
7 TVCS
8 Demo
10 TVDS

Bas
Am

□ Do not go online for authorization
□ Print alternate voucher

Base Floor Limit 2
Amount

□ Do not go online for authorization
□ Print alternate voucher

Dunn, Bill | 3/22/2007 1:47:02 PM

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

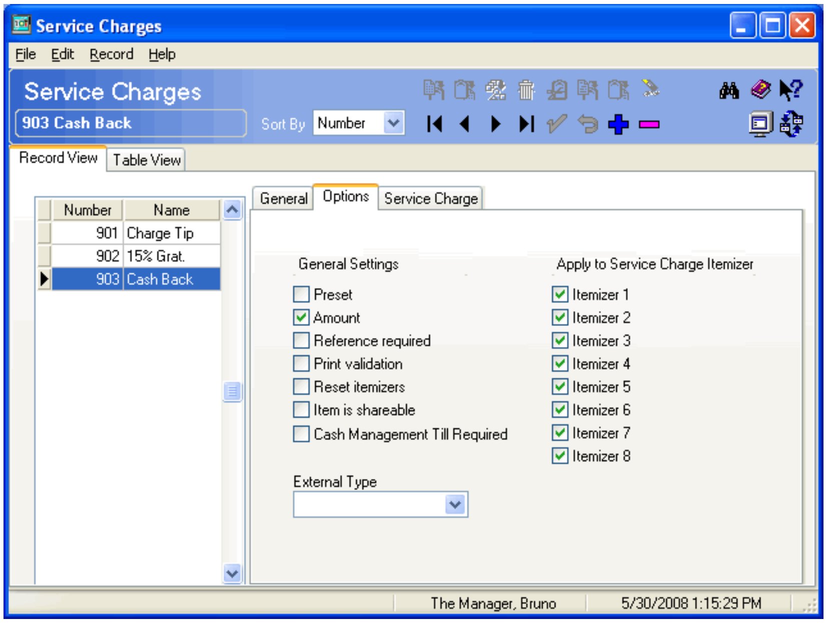
Configuring these options will automatically mask the Card Number, Customer Name, and Expiration Date on all debit card transactions.

10. If using the cash back feature with the Transaction Vault Debit Driver in RES Version 3.2 SP7 HF6, the user must enable the **Prompt for cash back amount** option on the *POS Configurator* | *Sales* | *Tender/Media* | *CC Tender* tab. If this option is not enabled then the requested cash back amount will not be transmitted.

11. If using the Verifone PinPad 1000SE Device, then you will also need to configure a Cash Back Service Charge in POS Configurator. If the PinPad 1000 SE is not used at the site, proceed to step 12. Oracle recommends configuring the service charge as follows. Only the steps necessary to configure this feature are described, perform additional configuration as desired.

Note *The Verifone Vx670 PinPad device does not support Cash Back.*

- Go to the *POS Configurator* | *Sales* | *Service Charges* form to configure a Cash Back service charge. Add a new record and use the *Name* field to assign a unique descriptor (e.g., Cash Back).
- Go to the *General* tab and select **All Levels** in the **Menu Level Class** drop down.
- Go to the *Options* tab and configure the following fields:



903 Cash Back

Sort By: Number

Number	Name
901	Charge Tip
902	15% Grat.
903	Cash Back

General Settings

- □ Preset
- ☑ Amount
- □ Reference required
- □ Print validation
- □ Reset itemizers
- □ Item is shareable
- □ Cash Management Till Required

External Type

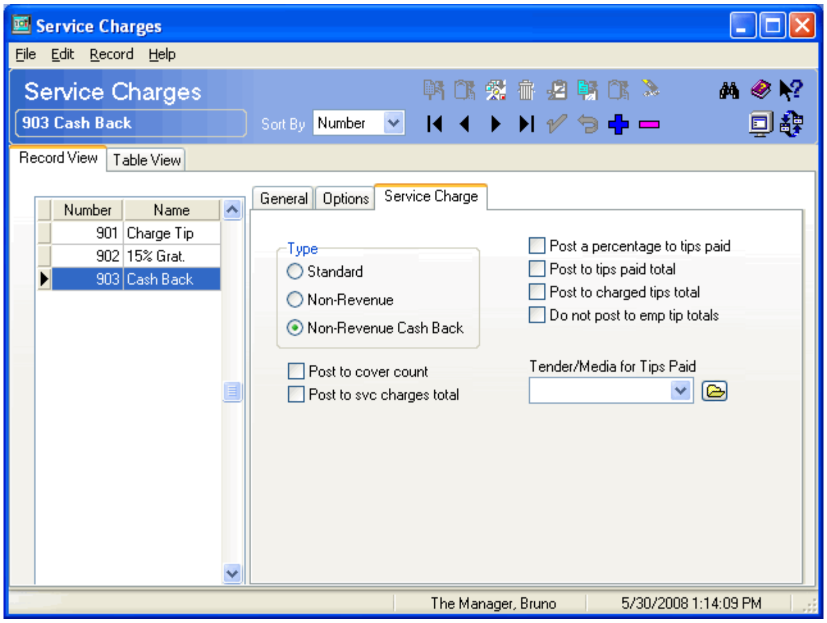
Apply to Service Charge Itemizer

- ☑ Itemizer 1
- ☑ Itemizer 2
- ☑ Itemizer 3
- ☑ Itemizer 4
- ☑ Itemizer 5
- ☑ Itemizer 6
- ☑ Itemizer 7
- ☑ Itemizer 8

The Manager, Bruno 5/30/2008 1:15:29 PM

- **Amount.** Enable this option.
- **Apply to Service Charge Itemizer.** Enable all 8 itemizers.

- Go to the *Service Charge* tab and enable the **Non-Revenue Cash Back** option.



Service Charges

903 Cash Back

Sort By: Number

Number	Name
901	Charge Tip
902	15% Grat.
903	Cash Back

Type
○ Standard
○ Non-Revenue
● Non-Revenue Cash Back

□ Post to cover count
□ Post to svc charges total

□ Post a percentage to tips paid
□ Post to tips paid total
□ Post to charged tips total
□ Do not post to emp tip totals

Tender/Media for Tips Paid

The Manager, Bruno   5/30/2008 1:14:09 PM

- Go to *Devices* | *Touchscreens* and select the Payment screen. Link the Debit Tender Key. Create a new Cash Back key, or select the existing Cash Back key, and link it to the TVD debit tender.
- Go to the *Tracking Groups* form and add the Debit Card tender key to the Tracking Groups in the standard tracking section.
    - Add the Cash Back to the tracking group where the Cash - Tips Paid are located.

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

Configuring Intermediate Certificates

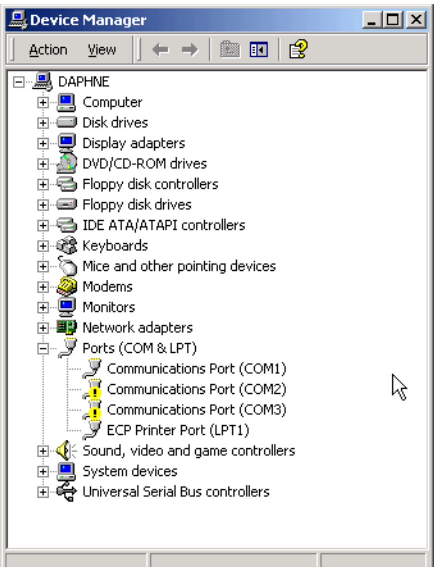
To establish a trusted end-to-end Internet connection, you must build and verify a certificate chain by downloading or adding intermediate certificates to the trust list on the credit card server. To enable automatic downloads, open outgoing connections to the URL for each intermediate certificate.

PinPad Device Setup

When performing PIN Debit transactions, the following configuration options are required to link a PinPad device to a user workstation. This is for the hard-wired Verifone PINPad 1000 device only.

For Win32 Clients

1. From the Windows Start menu, right-click the My Computer icon and select *Properties* | *Hardware*. Click the **[Device Manager]** button to open the form (right).



2. Select *Ports* | *Communication Port 1* | *Port Settings* and set the following options:

   - **Bits per second** — 1200
   - **Data bits** — 7
   - **Parity** — Even
   - **Stop bits** — 2
   - **Flow control** — None

3. In POS Configurator, select *Devices* | *Devices* | *Network Nodes*. Go to the *Com Port* tab and set the following options:

   - **Comm 1** — 1200
   - **Parity** — Even
   - **Num Data Bits** — 7
   - **Num Stop Bits** — 2

4. Go to *Devices* | *User Workstations* | *Peripherals* and configure the PinPad device.

For CE Clients

1. In POS Configurator, select *Devices* | *Devices* | *Network Nodes.* Go to the *Comm Port* tab and set the following options:

   - **Comm 1** — 1200

   - **Parity** — Even

   - **Num Data Bits** — 7

- **Num Stop Bits** — 2

Note *ComPORT 4 or 5 can also be configured on the PINPad using the separate cable.*

This is only available if the site is running RES 3.2 SP7 HF6 or higher, or RES 4.1 HF2 or higher.

Confidence Testing

Once the device is configured, test the PinPad hardware using the Micros Confidence Test (**MicrosCfdTest.exe**). Keep in mind that:

- A small keyboard and mouse will be needed to test the WS4.
- Before running the confidence test, close POS Operations by right-clicking the mouse and selecting the **Close** option.

Note *When starting the Micros Confidence Test, if the error message "PinPad.dll is currently in use or unavailable." displays, wait 30 seconds and try again.*

Removing the Software

Removing Software From a Site Running RES 5.0 or Higher

Follow these steps to remove the TV credit and debit 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\CaTVDA.dll
   - \Micros\Res\Pos\Etc\CaTVDA.cfg
   - \Micros\Res\Pos\Bin\CaTVDA.hlp
   - \Micros\Res\Pos\Bin\CaTVDA.cnt
   - \Micros\Res\Pos\Bin\CaTVDS.dll
   - \Micros\Res\Pos\Etc\CaTVDS.cfg
   - \Micros\Res\Pos\Bin\CaTVDS.hlp
   - \Micros\Res\Pos\Bin\CaTVDS.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\CaTVDA.dll
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTVDA.cfg
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVDA.hlp
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVDA.cnt
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVDS.dll
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTVDS.cfg
   - \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVDS.hlp

- \Micros\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTVDS.cnt
- \Micros\Res\CAL\Win32\Files\Micros\Res\Common\libeay32.dll*
- \Micros\Res\CAL\Win32\Files\Micros\Res\Common\ssleay32.dll*
- \Micros\Res\CAL\Win32\Files\Micros\Res\Common\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

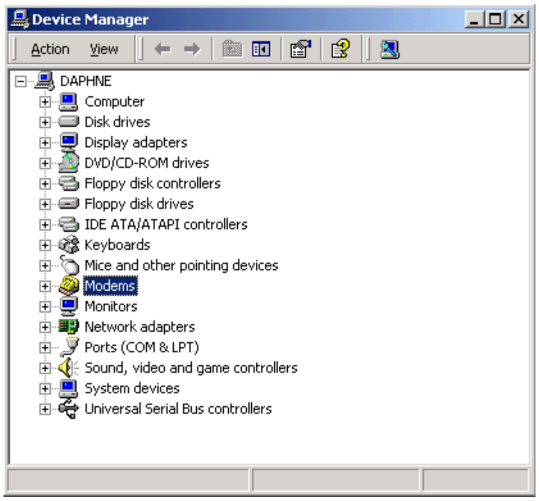
This section is provided as reference when installing the Transaction Vault Credit Card Driver.

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.

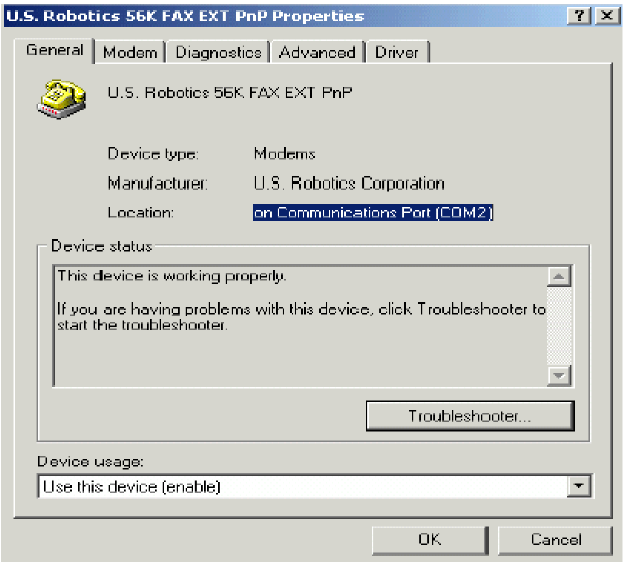
The following setup instructions are for Windows 2000 platforms or higher:

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.



U.S. Robotics 56K FAX EXT PnP Properties

U.S. Robotics 56K FAX EXT PnP

Device type: Modems
Manufacturer: U.S. Robotics Corporation
Location: on Communications Port (COM2)

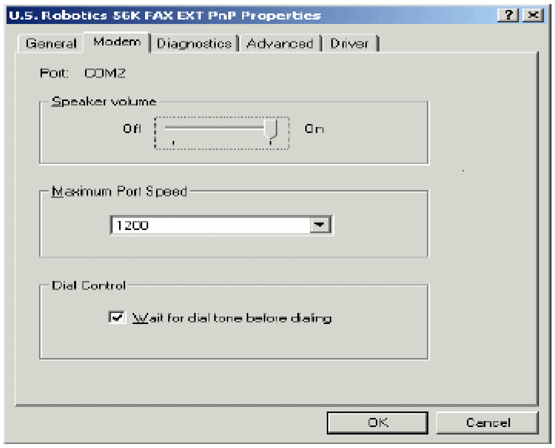
Device status

This device is working properly.

If you are having problems with this device, click Troubleshooter to start the troubleshooter.

Device usage:
Use this device (enable)

4. Go to the *Modem* tab.



U.S. Robotics 56K FAX EXT PnP Properties

Port: COM2

Speaker volume
Off On

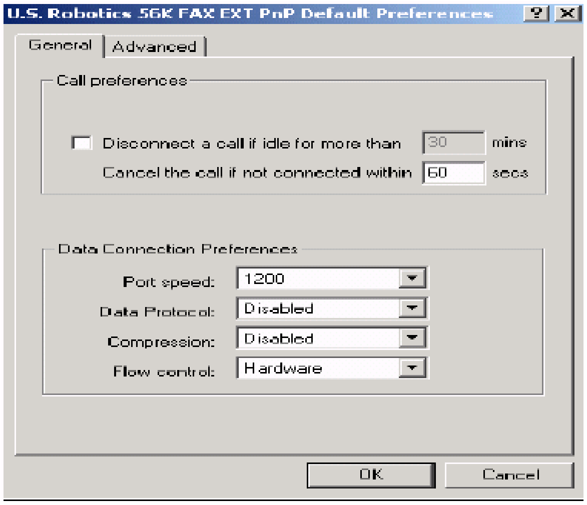
Maximum Port Speed
1200

Dial Control
☑ Wait for dial tone before dialing

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.



U.S. Robotics 56K FAX EXT PnP Default Preferences

Call preferences

□ Disconnect a call if idle for more than 30 mins

Cancel the call if not connected within 60 secs

Data Connection Preferences

Port speed: 1200

Data Protocol: Disabled

Compression: Disabled

Flow control: Hardware

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 Oracle 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, Oracle 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, Oracle 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.

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 Oracle 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, Oracle 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, Oracle 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 Oracle 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 Oracle network.

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

Frequently Asked Questions

Why is reading the Credit Card Transfer Report so important?

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

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

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

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

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

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

- Credit card number
- Expiration date

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

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

Terminal-based processing requires that the entire batch be successful for the batch to be closed. Most of the 3700 POS drivers support terminal-based processing. 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, Oracle has added enhancements to the Transaction Vault Debit Card Driver (CaTVD) for the prevention of duplicate batches.

ReadMe First
V. 5.1

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 5.1 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
Added support for Transport Layer Security 1.2 encryption protocol	38
Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols	38

New Features Detailed

Added Support for Transport Layer Security 1.2 Encryption Protocol

Version 5.1 of the Transaction Vault Debit (CaTVD) Card Driver contains support for the Transport Layer Security (TLS) 1.2 Encryption Protocol. The TLS protocol encrypts your data and provides a secure and reliable data transmission between the POS application (client) and server.

Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols

Version 5.1 of the Transaction Vault Debit (CaTVD) Card Driver removes support for all encryption protocols other than TLS 1.2. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

What's Enhanced

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

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

Enhancements Summarized

There are no enhancements included in this release.

What's Revised

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

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

Revisions Summarized

There are no revisions included in this release.