Oracle® Hospitality RES 3700 Credit Card Interface

User Guide
Release 5.2
E81083-04

September 2017

ORACLE

Contents

Preface **7**
Audience 7
Customer Support 7
Documentation 7
Revision History 7
1 Oracle Payment Interface (OPI) **9**
Installing the Oracle Payment Interface Driver (CaOPI) 9
Configuring the Credit Card Batch for OPI 10
Configuring Tender/Media for OPI 10
Configuring Revenue Centers for OPI 11
Changing the Driver Passphrase for OPI 11
Update Checks with Initial Authorization 12
Enabling Tender with Initial Authorization 12
2 FDMS North **13**
Installation 13
Site Requirements 13
Files Included 13
Before You Begin 14
Installation Instructions 14
Setup 15
Communication Channels 15
Configuring the Driver 15
PinPad Device Setup 19
Configuring Intermediate Certificates 20
Usage 21
Running an Authorization and Settlement Simultaneously 21
3 Transaction Vault Credit Card Driver **22**
How the Driver Works 22
Secondary Level Encryption 23
Settlement 23
Credit Card Batch Utility 23
Reports 24
Compatibility 24
Installation 25
Site Requirements 25

Files Included 25
Installation Instructions for a Site Running RES 5.0 or Higher 26
Configuration Instructions 28
Configuring Intermediate Certificates 31
Removing the Software 32
Setup 32
Communication Channels Supported 32
Connectivity Considerations 33
Frequently Asked Questions 38
Why is reading the Credit Card Transfer Report so important? 38
What is a credit card batch? 38
How can a duplicate batch occur? 39
4 Transaction Vault Debit Card Driver 40
How the Driver Works 40
Corrective Authorizations for Debit Transactions 41
Secondary Level Encryption 42
Settlement 42
Assigned Lane Numbers to VX670 Devices 42
Debit Reversals 44
Installation 44
Site Requirements 44
Files Included 45
Installation Instructions for a Site Running RES 5.0 or Higher 45
Configuration Instructions 47
Configuring the CaTVDA and CaTVDS Drivers 47
Configuring Intermediate Certificates 50
PinPad Device Setup 50
Removing the Software 51
Setup 52
Communication Channels Supported 52
Connectivity Considerations 52
Frequently Asked Questions 57
Why is reading the Credit Card Transfer Report so important? 57
What is a credit card batch? 57
How can a duplicate batch occur? 58
5 Heartland 59
Installation 59
Site Requirements 59

Files Included 59
Installation Instructions 59
Setup 60
Configuring the Drivers 60
Configuring Intermediate Certificates 67
6 TSYS Acquiring Solutions 68
Installation 68
Pre Installation Requirements 68
Site Requirements 69
Files Included 69
Installation Instructions for a Site Running RES 5.0 or Higher 69
Configuration Instructions 70
Configuring Intermediate Certificates 74
Features Supported 74
Auto Offline Credit Card Authorization Support 74
Support Zero Dollar Account Verification 77
eCommerce Transactions Support 77
Password Support 77
End of Day Procedures 78
Sample Credit Card Voucher 79
Removing the Software 79
Removing Software From a Site Running RES 4.5 or Higher 79
Password Handling Process 80
Troubleshooting Tips 82
Frequently Asked Questions 82
Why is reading the Credit Card Transfer Report so important? 82
What is a credit card batch? 82
7 American Express Authorization 84
Installation 84
Site Requirements 84
Files Included 84
Installation Instructions 84
Setup 85
Configuring the Drivers 85
Configuring Intermediate Certificates 86
8 Universal Credit Card Driver (UCCD) including Ventiv 87
Installation 87
Site Requirements 87

Files Included 87
Installation Instructions 88
Removing the Software 91
Setup 92
Communication Channels Supported 92
Connectivity Considerations 92
Configuring the Drivers 98
Change Maximum Batch Size 99
AVS and CVV Configuration 99
Configuring Intermediate Certificates 100
Frequently Asked Questions 100
Why is reading the Credit Card Transfer Report so important? 100
What is a credit card batch? 101
How can a duplicate batch occur? 102
9 Worldpay 103
Installation 103
Site Requirements 103
Files Included 103
Installation Instructions 104
Setup 111
Communication Channels Supported 111
Connectivity Considerations 111
Configuring the Drivers 117
Configuring Intermediate Certificates 118
Frequently Asked Questions 118
Why do I have to take down the entire system when loading the new credit card drivers? 118
What happens if I forget to shut down the Credit Card Server or the system? 118
Why is reading the Credit Card Transfer Report so important? 118
What is a credit card batch? 118
How can a duplicate batch occur? 120

Preface

The Oracle Hospitality RES 3700 Credit Card Interfaces are a collection of credit card drivers that submit payments and communicate with the credit card processor. This document provides instructions for configuring RES credit card drivers and information regarding functionality and limitations.

Audience

This document is for RES 3700 system administrators.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
November 2016	• Initial publication
May 2017	• Update checks with initial authorization. • Configuring the printed credit card voucher.
July 2017	• Added instructions for enabling Card Verification Value responses for CaFDMS. • Added information and instructions for CaFDMS, CaTVC, CaTVD, CaHL, CaTSYS, CaAMEX, CaUCCD, and CaVN.

October 2017	• Corrected compatibility table for CaTVC.

1 Oracle Payment Interface (OPI)

The Oracle Payment Interface (OPI) with the RES native CaOPI driver supports features and functionality not supported by the MICROS Gateway Device Handler (MGDH), such as:

- Beverage control
- Place holders
- Splitting checks with auths
- Adding checks with auths
- More than five auths per check
- Associating auths with specific seats
- Voiding credit card tenders before batch and settle
- Printing credit auths to the CA Voucher printer

OPI does not support the following RES 3700 features:

- Gift Cards
- TopUp Auth
- Balance Inquiry
- Void a refund
- Debit
- SaleCashBack
- CC Voice for QSR (offline sales)
- Backup OPI Server

This chapter provides instructions and information for installing and setting up the Oracle Payment Interface (OPI) credit card driver.

This version of the OPI Driver only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

Installing the Oracle Payment Interface Driver (CaOPI)

1. Make sure Microsoft .NET Framework 4.6.1 is installed.
2. Batch and settle all current transactions.
3. In the MICROS Control Panel, set **Restaurant** to `OFF`, and then close the MICROS Control Panel.
4. Stop the MICROS Credit Card Server service.
5. Double-click `CaOPI.exe` and follow the instructions to complete the installation.
6. Download and run `CaOPI.exe` on the Backup Server.
7. Start the MICROS Control Panel, and then set **Restaurant** to `Back of House`.
8. In the POS Configurator, click the **Devices** tab, and then click **CA/EDC Drivers**.

a) Create a record named `OPI`.

b) On the **Driver** tab, enter `OPI` as the **Driver Code**.

c) On the **System** tab, enter `http://OPI server IP:port` in **Host URL Part 1**, and then enter `/JSON` in **Host URL Part 2**. By default, OPI uses port 5098.
Do not enter `127.0.0.1` even when OPI is installed on the RES server.

d) On the **Merchant** tab, click the **Authorization** tab, and then enter the merchant ID number.

e) On the **RVC** tab, link the revenue centers.

9. In the MICROS Control Panel, select **Restaurant**, and then click **Reload DB**.

Configuring the Credit Card Batch for OPI

1. From Microsoft Windows, click **Start**, click **Run**, and then enter `CreditCards.exe` to start the Credit Card Batch application.
2. On the **OPI** tab, enter the OPI passphrase created during OPI installation, click **Save**, and then verify that the application saves the passphrase without errors.

   If your environment includes a backup server and you receive a save error, the Credit Card Batch application may be encountering issues saving the passphrase to the backup PC.

   If you enter a passphrase that is different from the passphrase created during the OPI installation, you must change the passphrase in OPI.
3. On the **Diagnostics** tab, select **OPI**, select **Update OPI PassPhrase**, click **Begin Test**, and make sure the application shows the message `OPI Passphrase update succeeded`.

Configuring Tender/Media for OPI

1. In the POS Configurator, click the **Sales** tab, and then click **Tender/Media**.
2. Create a tender and name it **Default OPI Tender**.
3. On the **Tender** tab:
   a. Select **Reference required** and **Assume paid in full**.
   b. For Table Service Restaurants, select a **Charged Tip**. If only Quick Service revenue centers will use this tender, clear any selection in **Charged Tip**.
4. On the **CC Tender** tab, select **Credit Auth required**, **Mask Credit Card Number**, and **Mask expiration date**.
5. On the **Credit Auth** tab:
   a. On the **Authorization** tab, select the OPI driver for **CA Driver** and **EDC Driver**.
   b. Select **Allow partial authorization** unless it is not supported by the 3rd-party application.
   c. Make sure to leave the **Card Type** blank.
   d. On the **Preamble** tab, delete existing preambles.

6. On the **PMS** tab, select **Allow 19 reference characters**.
7. On the **Personal Check** tab, select **Authorization required**, and then select the OPI driver for **Check Driver**.
8. Create or configure other credit card types using the same settings. Use the following table for the **Card Type** value for each credit card:

Table 1 - Card Type Values

Credit Card	Card Type for OPI 6.1.1 and Later	Card Type for OPI 6.1.0.9
Visa	00	00
Master Card	01	01
American Express	02	02
Diners	03	03
JCB	04	04
CUP	10	10
Visa Electron	17	19
Maestro	19	29
VPAY	20	24
Alliance	21	25
EC Chip	22	26
Bancomat Card	23	40
Discover	26	08
PayPal	27	32

Configuring Revenue Centers for OPI

1. In the POS Configurator, click the **Revenue Center** tab, and then click **RVC Credit Cards**.
2. For each applicable revenue center:
    a. On the **General** tab, select **Enable OPI mode**.

    If OPI is not enabled for all revenue centers, you cannot transfer checks with credit auths between differing revenue centers.

    b. Select the D**efault OPI Tender**.
    c. Select **Allow 20 reference characters**.

Changing the Driver Passphrase for OPI

1. On the server with the OPI installation, right-click *root*`\OraclePaymentInterface\Bin\RWregistry\RWregistry.exe`, and then click **Run as administrator**.

2. Log in using the Microsoft Windows administrator credentials.
3. Select **POS Passphrase** from the drop-down list.
4. Enter the new password, click **Confirm**, and then restart the OPI service.

Update Checks with Initial Authorization

With RES 5.5.2 and later, you can re-authorize a credit card to update a check without needing the card present. For example, if a customer orders a drink at a bar, and then later orders another drink, the customer does not need to swipe the card again on the second drink.

POS Operations prompts you for whether the transaction should use the existing card information or a new card. When re-using the existing card for a new authorization amount, the previous authorizations are marked as reversed. These authorizations are excluded from batch operations, are not shown, and cannot be selected or settled. You cannot service total the check while waiting for a response from the Oracle Payment Interface.

Enabling Tender with Initial Authorization

If you are using RES 5.5.1, you can assign employee classes with the ability to select `CC Final` on a workstation to close checks to the initial credit card authorization.

For example, a bartender begins a check and does an initial authorization. By default, if the customer leaves without paying their bill, the bartender cannot perform another authorization without having the credit card. This permission allows the bartender to close the check using the initial authorization.

Update Checks with Initial Authorization deprecated this functionality in RES 5.5.2 and later.

1. In the POS Configurator, click the **Employees** tab, and then click **Employee Classes**.
2. For each employee class that should be able to authorize special transactions or services:
    a. Select the employee class.
    b. On the **Options** tab, select **Tender with initial authorization**.

2 FDMS North

This version of the driver may be used on RES systems running Version 5.0 or higher. Certain features of this driver may require later releases of RES.

This version of the FMDS North Driver only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

Installation

Site Requirements

Before installing the CaFDMS North Credit Card 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.
- A dedicated modem and phone line are required for dial-up connectivity.

Files Included

The CaFDMS North Driver contains both an authorization driver and a settlement driver. The following lists the files installed with this driver:

- `\Micros\RES\POS\Bin\CaFDMS.dll`
- `\Micros\RES\POS\etc\CaFDMS.cfg`
- `\Micros\RES\POS\Bin\CaFDMS.hlp`
- `\Micros\RES\POS\Bin\CaFDMS.cnt`
- `\Micros\Res\Pos\Bin\Vxnapi.dll`
- `\Micros\Common\Bin\libeay32.dll`
- `\Micros\Common\Bin\McrsOpenSSLHelper.dll`
- `\Micros\Common\Bin\ssleay32.dll`

For sites running RES Version 4.5 or higher, the driver will create a win32 CAL package to be distributed to RES clients via the CAL service. The following lists the files installed as part of this package:

- `\Micros\RES\CAL\Win32\Files\Micros\RES\Pos\Bin\CaFDMS.dll`
- `\Micros\RES\CAL\Win32\Files\Micros\RES\Pos\etc\CaFDMS.cfg`
- `\Micros\RES\CAL\Win32\Files\Micros\RES\Pos\Bin\CaFDMS.hlp`
- `\Micros\RES\CAL\Win32\Files\Micros\RES\Pos\Bin\CaFDMS.cnt`
- `\Micros\RES\CAL\Win32\Files\Micros\RES\Pos\Bin\Vxnapi.dll`
- `\Micros\RES\CAL\Win32\Files\Micros\Common\Bin\libeay32.dll`
- `\Micros\RES\CAL\Win32\Files\Micros\Common\Bin\McrsOpenSSLHelper.dll`
- `\Micros\RES\CAL\Win32\Files\Micros\Common\Bin\ssleay32.dll`

All logging is recorded to the %WinDir%\MICROSCaFDMSInstall.log file located on the root Oracle Windows directory as defined by WinDir.

Before You Begin

Before you begin installation make sure that you have the following information available. This information can be obtained by contacting your credit card processor:

- Merchant ID (MID).
- Terminal ID (TID).
- Primary phone number for authorization and settlement functions (if using dial-up for fallback mode if the internet fails).
- Secondary phone number for authorization and settlement functions (if using dialup for fallback mode if the internet fails).

Installation Instructions

CaFDMS is a single driver that performs both Authorization and Settlement functions. Authorization and settlement, however, cannot be performed simultaneously. Usage contains more information.

Follow these steps to install the FDMS North Credit Card Driver:

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the `FDMS_5.2.zip` file from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
    - CaFDMS North Credit Card Driver Installation Documentation (`CaFDMSV 5.2_MD.pdf`).
    - CaFDMS North Driver Executable (`CaFDMS(5.2).exe`).
3. Shutdown all Oracle applications from the MICROS Control Panel and turn the Database to off.
4. Copy the `CaFDMS(5.2).exe` to a TEMP directory on the RES Server.
5. Double-click the `CaFDMS(5.2).exe` file to install the driver. The driver executable will install the following files to the folder locations listed below:
    - `CaFDMS.dll` to `\Micros\Res\Pos\bin`
    - `CaFDMS.cfg` to `\Micros\Res\Pos\etc`
    - `CaFDMS.hlp` to `\Micros\Res\Pos\bin`
    - `CaFDMS.cnt` to `\Micros\Res\Pos\bin`

    The executable will also install the following three DLL files that are required if using the Datawire SSL Internet Protocol as your mode of communication:
    - `vxnapi.dll` to `\Micros\Res\Pos\bin`
    - `libeay32.dll` to `\Micros\Common\bin`
    - `ssleay32.dll` to `\Micros\Common\bin`

6. For CaFDMS versions 4.7.20.2216 and greater, the Credit Driver Installation Package enters the following driver related information to Windows Registry:

   `[HKEY_LOCAL_MACHINE\SOFTWARE\MICROS\CreditCardDrivers\XXXXXX]`

   Where *XXXXXX* is the driver package name

   InstallationVersion = `4.X.XX.XXXX`

   The version of the driver being installed

   Installed = *Day MM/DD/YYYY*

   The installation date of the installed driver (for example, Tue 03/31/2009)

7. Configuring the Driver contains further instructions for configuring the credit card driver.

Setup

Communication Channels

Communication Channel can be configured on the **POS Configurator** | **Devices** | **CA/EDC Drivers** | **FDMS North** | **System** form. Configuring the Driver contains further information about configuring the Communication Channel.

The following communication types are supported by this driver:

- Dial-Up – Enable Channel 0 to select this option. This is the system's default configuration.
- TCP – Enable Channel 1 to select this option. Uses a private network to transmit unenrcypted credit card data to the processor via Frame Circuit Connectivity or VSAT Connectivity. The user can configure this option to use dial-up as a fallback connection type.
- Datawire/IPN – Enable Channel 2 to select this option. Uses a network to transmit information to the credit card processor. The user can configure this option to use dial-up as a fallback connection type.

The fallback dial-up connection will only activate if the initial connection attempt by the primary communication type is unsuccessful. For authorizations when there is a failure, the fallback connection will always attempt to connect. For batch settlement, however, if the primary connection attempt is initially successful, but a failure occurs prior to the batch being settled, then the batch will fail without attempting to connect using the fallback connection. However, if the primary connection fails before any contact is made with the processor, then the driver will use the fallback option.

For example, suppose the Mike Rose Cafe is using the CaFDMS North Driver and has configured TCP/IP as their communication channel. Their fallback connection is dialup. At the end of the night they attempt to settle a batch with the processor. Initially the TCP connection works during the Batch Open request. However, before the batch is settled and closed, the connection fails. The driver does not try to re-send the batch using the dial-up connection and registers the batch as failed.

Configuring the Driver

Follow these steps to configure the CaFDMS North Credit Card Driver.

If using the cashback feature with the CaFDMS Debit Driver on a system running RES Version 3.2, the user must enable the Prompt for cashback 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.

1. Go to **POS Configurator** | **Devices** | **CA/EDC Drivers**.
2. Click the blue plus sign to add a record.
3. Enter a **Name** for this record and its corresponding code in the **Driver Code** field (such as FDMS). Save the record.
4. Select the **System** tab and configure the following fields:
   - 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 `\3700\bin` directory and enter `settle -m`. 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.
     ```
   - 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 `\3700\bin` directory and enter `settle -m`. 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 – This field prevents communication error by testing port availability before attempting an authorization request. Select **1** to enable this feature.
   - Authorization Channel – This field specifies the type of interface connection used for authorization requests between the merchant and the credit card processor. Make sure that the Authorization and Settlement channels match. The options are:
     - Channel 0: Dial-up connection
     - Channel 1: TCP/IP connection
     - Channel 2: Datawire/IPN connection
   - Settlement Channel – This field specifies the type of interface connection used for settlement requests between the merchant and the credit card processor. Make sure that the Authorization and Settlement channels match. The options are:
     - Channel 0: Dial-up connection
     - Channel 1: TCP/IP connection
     - Channel 2: Datawire/IPN connection

- Transient Connection – Use this option to determine whether the transient TCP connection is enabled or not. A transient TCP connection connects each authorization transmission, and will disconnect once the authorization response is received from the processor. Select **0** to disable this functionality (default) and the connection will remain open between authorizations. Select **1** to enable it and the connection will be closed between authorizations.
- Max Offline Amount (Dollars) – This option controls the maximum dollar value of automatic offline transactions that can be processed. The maximum offline amount is entered in dollars (e.g. 2500 is the equivalent of $2500.00).
- Auth Offline At Settlement – Automatic Offline Credit Card Authorization allows the settlement driver to obtain an on-line authorization from the issuing bank to replace the offline authorization code generated by the CC driver.
  Enter **1** to enable this option, enter **0** to disable.
  This option defaults to zero (0) disabled. When the option is disabled, the settlement driver will treat these as manually authorized transactions and attempt to settle them along with all other transactions during the normal batch transfer.
- Auth Phone Number – Enter the authorization phone number provided by your credit card processor. The following formatting issues apply when entering a value:
  - Do not include hyphens.
  - Include any long distance access codes or area codes (e.g., 14105551212)
  - Include any dialing prefixes necessary to get an outside line (such as 914105551212)
- Backup Auth Phone Number – Enter the backup phone number provided by the credit card processor. This is an optional field.
- Auth Host IP Address: Port – Enter the IP address and port of the primary host connection to be used for authorization requests. This option is only applicable when TCP/IP is enabled.
- Backup Auth Host IP Address: Port – Enter a backup IP address and port of the primary host connection to be used for authorization requests. The backup auth host is triggered when the primary host address fails.
- Settle Phone Number – Enter the authorization phone number provided by your credit card processor. The following formatting issues apply when entering a value:
  - Do not include hyphens
  - Include any long distance access codes or area codes (e.g., 14105551212)
  - Include any dialing prefixes necessary to get an outside line (e.g., 914105551212)
- Backup Settle Phone Number – Enter the backup phone number provided by the credit card processor. This is an optional field.

- Settle Host IP Address: Port – Enter the IP address and port of the primary host connection to be used for settlement requests. This option is only applicable when TCP/IP is enabled.
- Backup Settle Host IP Address: Port – Enter a backup IP address and port of the primary host connection to be used for settlement requests. The backup settle host is triggered when the primary host address fails.

5. Go to the **Merchant** tab. All fields on this tab should be completed using the settings provided by the bank. The following fields must be configured:
   - Merchant ID – A number that identifies the credit card merchant.
   - Terminal ID – A number that identifies the credit card terminal within the store.
   - Merchant Type – Enter a 1 in this field to add a Hotel Restaurant charge type of "92" to the settlement message. Enter a zero (0) if this restaurant does not need a charge type in the settlement record. The default is 0.
6. Go to the **POS Configurator** | **Sales** | **Tender/Media** | **Credit Auth** tab. Go to the following fields and select **FDMS** from the drop down box:
   - CA Driver
   - EDC Driver
7. Go to the **CC Tender** tab and enable the following options. Configure other CC options as needed:
   - Verify Before Authorization
   - Credit Auth Required
   - Expiration Date Required
   - Mask Credit Card Number
   - Mask Cardholder Name
   - Mask expiration date
8. Save the record and bring the MICROS Control panel back to **Front-of-House** status.
9. CA/EDC should be operational. A few test transactions should be done to ensure all is working correctly. Test connections option is located on the **Micros Applications** | **POS** | **Credit Card Batch** | **Diagnostics tab**.
10. If you are configuring a Datawire/IPN (Channel 2) connection, you must register the Merchant Settings with the Datawire Server prior to going live. Follow these steps to register the driver:
    a. Go to the **MICROS Applications** | **POS** | **Credit Card Batch** | **Diagnostic** tab and select the **CaFDMS North** driver.
    b. Select the **[Test Connection]** button.
    c. Click **[Begin Test]**. The status window will display the results of the registration process.
11. The Datawire registry settings need to be updated on the BSM Client. The following steps should only be taken by a knowledgeable IT staff person and after consulting with Oracle IT personnel.
    The Datawire registry settings are located in the

`HKLM\Software\MICROS\Common\CCS\DrvrCfg\DrvrX\Support` folder. Follow these steps to update the registry settings on the BSM Client:

a. On the RES Server select **Start** | **Run** and enter **Regedit**. Click **[Ok]**.

b. Navigate to the following location of the CaFDMS driver number: `HKLM\Software\MICROS\Common\CCS\DrvrCfg\DrvrX\Support`

c. Highlight the `Support` folder and select **File** | **Export**.

d. To be certain that the registry data will export properly, verify that the CaFDMS Driver number selected as well as the following path to the Support folder. Only export from the support folder in the registry. `HKLM\Software\MICROS\Common\CCS\DrvrCfg\DrvrX\Support`.

e. Use the **Browse** feature to locate a shared network drive or a flash drive to save this portion of the Registry file.

f. Copy the registry file from the location designated in Step e to the BSM client's `TEMP` directory.

g. To import the registry file onto the BSM client double-click on the `.reg` file that you exported or saved from the server registry. This will import the support key information into the proper registry location on the BSM client.

h. To verify that the data was imported properly, select **Start** | **Run** and type in **REGEDIT**.

i. Navigate to `HKLM\Software\MICROS\Common\CCS\DrvCfg\` and compare the data in the BSM client's registry to the RES Server's registry.

12. Enable Card Verification Value (CVV) responses:

a. Go to the **POS Configurator** | **Devices** | **CA/EDC Drivers**. Select the FDMS driver, and then click the **Authorization** tab.

b. When an authorization request including CVV data is sent to FDMS, the transaction will be approved even if the CVV data does not match the card issuer's records. Enter `1` in **Require CVV Match** to treat transactions without matching CVV data as declined.

c. In the **CVV Decline Message** field, enter the message to be shown to the operator when an authorization is declined due to the issuer indicating that the supplied CVV data does match the expected value.

13. Bring the system back to **Front-of-House** status using the Control Panel.

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

- Bits per second — 1200
- Data bits — 7
- Parity — Even
- Stop bits — 1
- Flow control — None

2. 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 — 1
3. Go to **Devices** | **User Workstations** | **Peripherals** and configure the PinPad device.

For WS4 Clients

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 — 1

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.

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.

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.

Usage

Running an Authorization and Settlement Simultaneously

CaFDMS is a single driver that performs both Authorizations and Settlements. Therefore, authorizations and settlements must be performed separately.

If an authorization is performed in the POS system and the manager goes to settle a batch, any PCWS(s) that attempts to authorize a credit card will receive the following error message:

"`Settlement In Progress`"

It is recommended that settlement occur during off hours (i.e., during End-Of-Night Autosequence; or outside of normal hours of operation).

3 Transaction Vault Credit Card Driver

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 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.

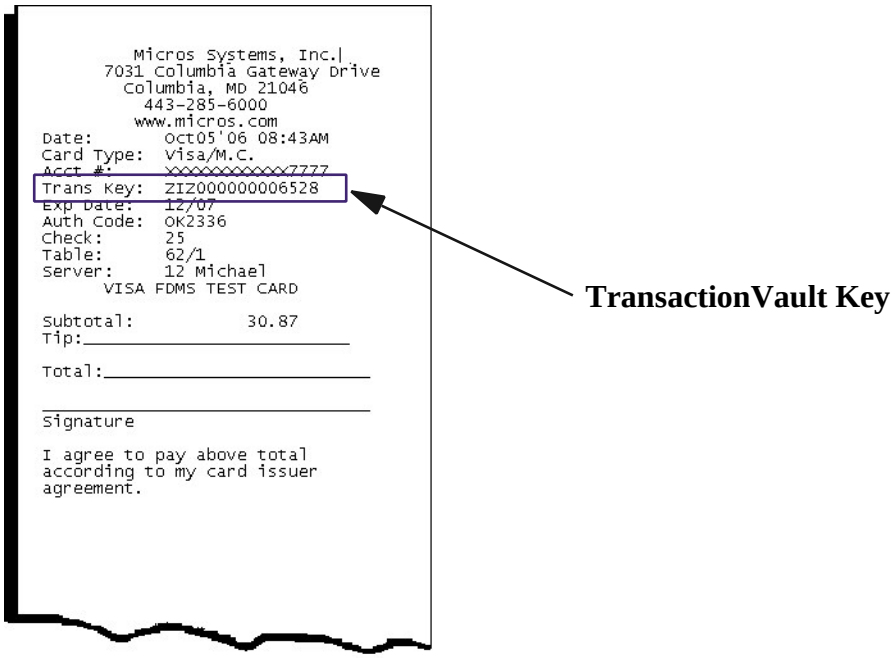
The key utilizes leading edge encryption technology, which helps to ensure that only TransactionVault can match the key to access the cardholder information.

How the Driver 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:



You must 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.

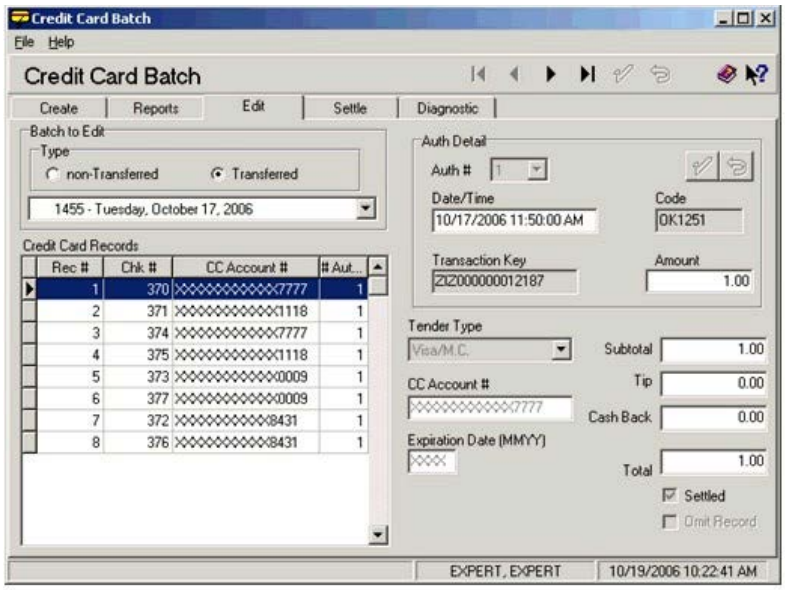
After all of the records have been issued TransactionVault Keys, the settlement process begins to transmit the batch to the processor. Unlike traditional drivers, TV does not transmit customer information. Instead the RES system sends the TransactionVault Key and the total amount owed to the processor.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

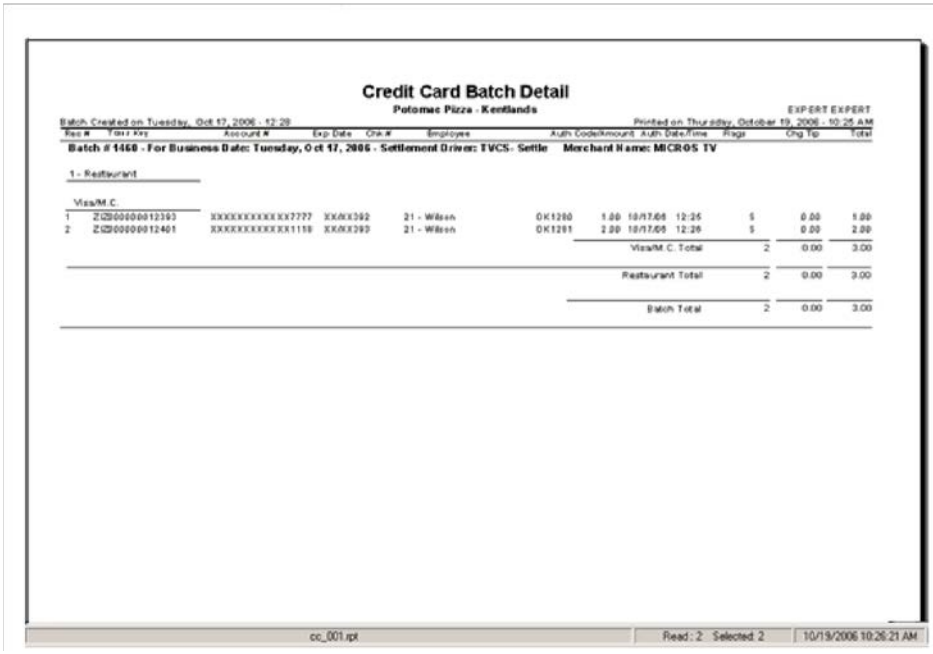
To support the TransactionVault Key, a field has been added to the **Credit Card Batch Utility | Edit** form. The **TransactionVault Key** field will display the assigned transaction key.



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.



Compatibility

The credit version of the Transaction Vault driver may be used on RES systems running Version 5.0 or higher.

This version of the Transaction Vault Credit Card Driver only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

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

Table 2 – Compatibility for CaTVC 4.14 or later

CaTVC 4.14 or Later		
RES Versions	EMSR On	EMSR Off
RES 5.0 to 5.1	No	Yes
RES 5.1 MR1 and later	Yes	Yes

Table 3 - Compatibility for CaTVC 4.13

CaTVC 4.13		
RES Versions	EMSR On	EMSR Off
RES 5.0 to 5.1	Yes	Yes
RES 5.1 MR1 and later	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

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.

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
```

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 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. 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 Credit Driver from the Oracle 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_V5.2_MD.pdf`)
    - Transaction Vault Credit Card Driver Software (`CaTVC(5.2).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(5.2).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 v5.0 or higher, 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.

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

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 40characters 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.

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.

At this time, the URL for the merchant link intermediate certificate is:
http://ss.symcb.com

Removing the Software

Removing Software From a Site Running RES 5.0 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\McrsOpenSSLHe
   lper.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

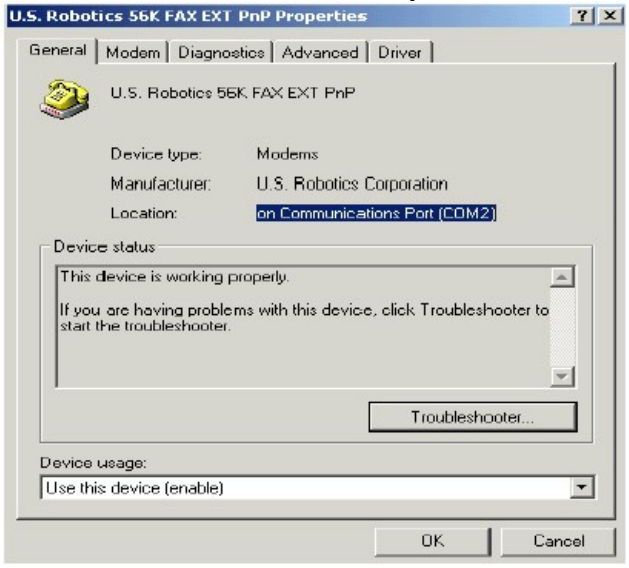
This section is provided as reference when installing the Transaction Vault Credit Card Driver.

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`.

   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 3.
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.

Host And Backup Host Configuration

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

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**.

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.

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.

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.

Internet Configuration

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

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.

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.

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

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.

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**.

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:

- One batch for all revenue centers (i.e, all transactions at the site).
- 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 Credit Card Driver (CaTV) for the prevention of duplicate batches.

4 Transaction Vault Debit Card Driver

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.

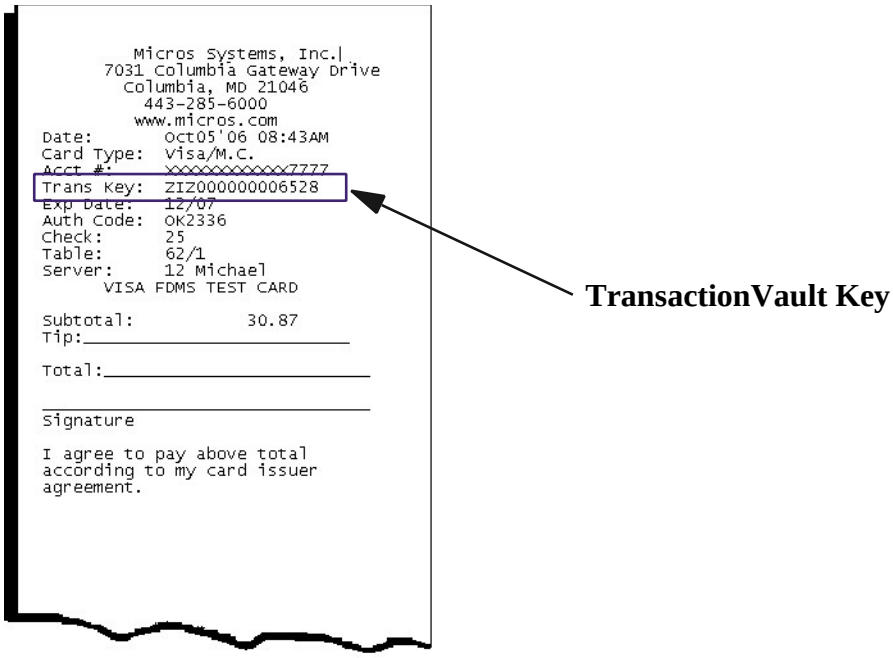
This version of the Transaction Vault Debit Card Driver only supports the Transport Layer Security (TLS) 1.2 Encryption Protocol. The TLS protocol encrypts your data and provides a secure and reliable data transmission between the POS application (client) and server. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

How the Driver 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.



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.

Reports

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

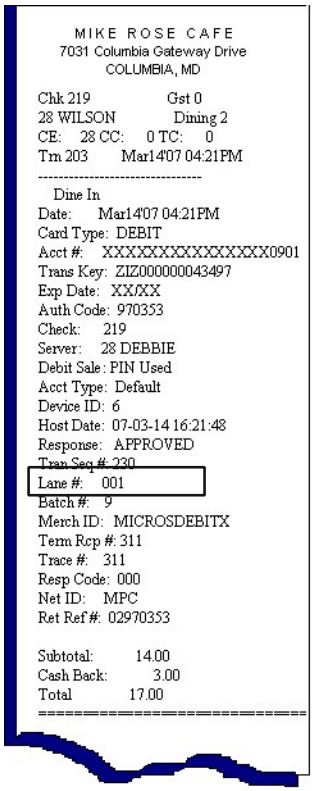
Credit Card Batch Detail Report – A TransactionVault Key column has been added to this report. The 15-digit TransactionVault Key associated with the transaction will be listed in this column. The customer name column has been removed from the report.

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 Assigned Lane

Numbers to VX670 Devices 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]**.

- 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.

Debit Reversals

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

This section contains installation and setup instructions for the Version 5.2 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.

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.

- 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
```

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
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_V5.2_MD.pdf)

- Transaction Vault Debit Card Driver Software (CaTVD(5.2).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(5.2).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

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:
    - 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.

    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:
  - **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.
- 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

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
- PinPad Device Setup
- Num Stop Bits — 2

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.

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

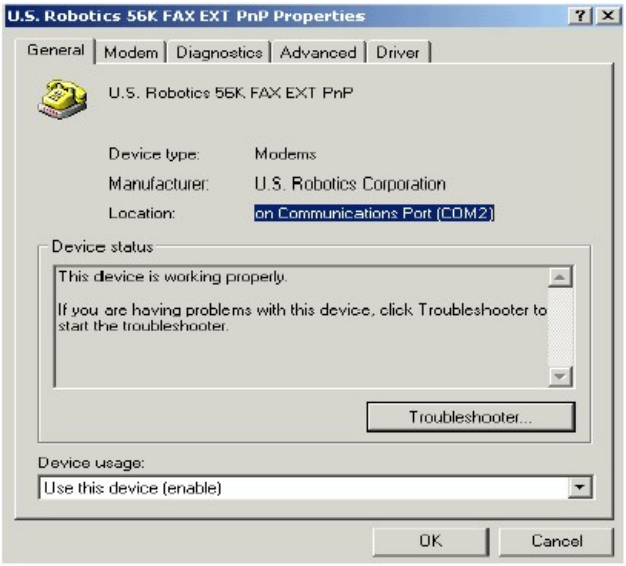
This section is provided as reference when installing the Transaction Vault Credit Card Driver.

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.



4. Go to the **Modem** tab.
5. Enable the **Dial Control** option and set the **Maximum Port Speed** to `1200`.

   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 3.
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.

Host And Backup Host Configuration

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

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**.

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.

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.

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.

Internet Configuration

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

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.

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.

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

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.

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**.

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.

5 Heartland

This section contains installation and setup instructions for the Version 5.2 release of the Heartland (HL) Credit Card Driver. The release version is available on the Oracle web site Product Support page.

This version of the Heartland:

- May be used on RES systems running Version 5.0 or higher.
- Only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

Installation

Site Requirements

Before installing the HL Credit Card 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.
- A dedicated modem and phone line are required for dial-up connectivity.

Files Included

The HL driver includes the following files:

```
\Micros\RES\POS\Bin\CaHLA.dll
\Micros\RES\POS\Bin\CaHLS.dll
\Micros\RES\POS\etc\CaHLA.cfg
\Micros\RES\POS\etc\CaHLS.cfg
\Micros\RES\POS\Bin\CaHLA.hlp
\Micros\RES\POS\Bin\CaHLS.hlp
\Micros\RES\POS\Bin\CaHLA.cnt
\Micros\RES\POS\Bin\CaHLS.cnt
```

Installation Instructions

The installation of the credit card drivers are separate from the RES software.

The Heartland driver is an independent install. When upgrading RES, the Heartland driver will not be affected.

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the `HL49212298.zip` file from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:

- HL Credit Card Driver Installation Documentation (`CaHL_MD.pdf`).
- `CaHL (5.2).exe`

3. Shutdown all Oracle applications from the MICROS Control Panel.
4. Double click the `CaHL(5.2).exe`.
5. Turn on the RES System from the MICROS Control Panel.
6. Configure the drives. Follow the setup starting on page 6.

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

Setup

Configuring the Drivers

Credit card drivers are setup through the **POS Configurator** | **Devices** | **CA/EDC Drivers**. A separate record should be added for each of the following, using the specified **Driver Codes**.

- HLA - CaHLA Authorizations
- HLS - CaHLS Settlements

Configuring the CaHLA and CaHLS 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., CaHLA) and a value of the **Driver Code** field (e.g., HLA) and save the record.
3. Go to the **System** tab and configure the following settings:
   - Authorization Device – Specify the modem to use for authorization requests. Reference the modem using a one-digit number. Use 1 for the first modem listed in Control Panel, 2 for the second, etc. Use 0 for no device.

     To determine the number to enter, type settle -m from a command prompt in the \POS\bin directory. The following sample messages 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.
     ```

     The modem must be configured in Control Panel before it can be assigned as an authorization device.
   - Not Used – Leave this field blank.
   - Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter 1 to enable port arbitration when more than one credit card driver is being used. Enter 0 to disable the option.

     Port arbitration is usually enabled.

- Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor. The options are:

  0: dial-up (phone/modem)

  1: TCP/IP (Not Used)

  2: internet
- Auth Phone Number – Enter the telephone number used for authorizations. Your Credit Card Processor will provide this number. Enter the number as follows:
  - Do not include hyphens.
  - Include any necessary long distance access code and area code, for example, 14105551212.
  - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- Backup Auth Phone Number – Enter the backup authorization phone number provided by your Credit Card Processor. (This field is optional. You may not have a backup number.)

  If the system attempts to perform an authorization but cannot get a telephone connection using the Auth Phone Number (for example, if the line is busy or the modem cannot make a connection), the backup number will be used. Enter the number as follows:
  - Do not include hyphens.
  - Include any necessary long distance access code and area code, for example, 14105551212.
  - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- Not Used- This field is not used.
- Not Used- This field is not used.
- City (Zip) Code – Enter the 3-digit number assigned by the Credit Card Processor to further identify the merchant location within a country. In the USA, the 5- or 9-digit Zip code for the merchant is used. Merchants located outside of the USA will be assigned a number by the Credit Card Processor.
- Time Zone – Enter the 3-digit number assigned by the Credit Card Processor used to calculate the local time within the Heartland.Net Authorization System (i.e., standard local time zone differential from Greenwich Mean Time (GMT).
- Host URL Part 1 – Enter the first part of the URL address of the primary host connection. This consists of the protocol and the site name.

  Example: `sslprod.secureexchange`
- Host URL Part 2:Port – Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.

Example: `.net:22345`

- BackUP URL Part 1 – Enter the first part of the URL address of the backup host connection. This consists of the protocol and the site name. Backup connections are triggered when the system cannot establish communication via the primary host address.

  Example: `sslprod.secureexchange`

- BackUP URL Part 2:Port - Enter the second part of the URL address of the backup host connection. This consists of the domain and the port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

  Example: `.net:22345`

4. Go to the **Merchant | Authorization** tab and configure the following settings:
   - Not Used – Leave this field blank.
   - Industry Code – This field is used to identify the type of industry for this merchant.
     - Enter 1 if the merchant business is a retail establishment.
     - Enter 0 if the merchant business is a restaurant.
   - Language Code – This field is used to identify the language in which authorization response messages will be returned for display and/ or printing.
   - Select the language code from the following list:
     - 0 (zero) English
     - 1 Spanish
     - 2 Portuguese
     - 3 Irish
     - 4 French
     - 5 German
     - 6 Italian
   - Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.
   - Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.
   - Merchant Type – This field support eCommerce transactions. An eCommerce transaction is one that occurs online. Authorizations for payments submitted online are set with a different set of authorization data. To support this functionality.
     - Enter a 0 in this field to designate restaurant transactions (default setting).
     - Enter a 1 in this field to designate eCommerce transaction.

- Bin Number – Enter the 6-digit Bank Identification Number assigned by the Credit Card Processor.
- Merchant Number – Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor.
- Store Number – Enter the 4-digit number used to identify the merchant store. This number is assigned by the Credit Card Processor.
- Terminal Number – Enter the 4-digit number used to identify a specific terminal within an establishment.This number is assigned by the Credit Card Processor. Each terminal in the establishment must have a unique number.
- Merchant Category – Enter the 4-digit number used to identify the merchant type. This number is assigned by the Credit Card Processor.
- Merchant Name – Enter the name of the merchant (up to 25-characters). This name must correspond to the name that prints on the credit card voucher.
- *Reserved* - This field is not used.
- Merchant State - Enter the 2-character state/province code assigned by the Credit Card Processor used to identify the merchant. The 2-characters entered here must correspond to the state/province that prints on the credit card voucher.
- Merchant City - Enter the name of the city where the merchant is located.
- *Reserved* - This field is not used.

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., CaHLS) and a value of the **Driver Code** field (e.g., HLS) and save the record.
7. Go to the **System** tab and configure the following settings:
    - Not Used – Leave this field blank.
    - Settlement Device – Specify the modem to use for settlement requests. Reference the modem using a one-digit number. Use 1 for the first modem listed in Control Panel, 2 for the second, etc. Use 0 for no device.

      To determine the number to enter, type settle -m from a command prompt in the `\POS\bin` directory. The following sample message displays:

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

      The modem must be configured in Control Panel before it can be assigned as settlement device.
    - Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter `1` to enable port arbitration when more than one credit card driver is being used. Enter `0` to disable the option.

Port arbitration is usually enabled.

- Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor. The options are:
    - 0 - dial-up
    - 1 - TCP/IP (Not Used)
    - 2 - internet
- Settle Phone Number - Enter the telephone number used for settlement. Your Credit Card Processor will provide this number. Enter the number as follows:
    - Do not include hyphens.
    - Include any necessary long distance access code and area code, for example, 14105551212.
    - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- Backup Settle Phone Number - Enter the backup settlement phone number provided by your Credit Card Processor. (This field is optional. You may not have a backup number.)

  If the system attempts to perform a settlement but cannot get a telephone connection using the Settle Phone Number (e.g., the line is busy, modem cannot make a connection, etc.), the backup number will be used. Enter the number as follows:
    - Do not include hyphens.
    - Include any necessary long distance access code and area code, for example, 14105551212.
    - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- Merchant City - Enter the name of the city where the merchant is located.
- Merchant State - Enter the 2-character state/province code assigned by the Credit Card Processor used to identify the merchant. The 2-characters entered here must correspond to the state/province that prints on.
- City (Zip) Code - Enter the 3-digit number assigned by the Credit Card Processor to further identify the merchant location within a country. In the USA, the 5- or 9digit Zip code for the merchant is used. Merchants located outside of the USA, will be assigned a number by the Credit Card Processor.
- Time Zone - Enter the 3-digit number assigned by the Credit Card Processor used to calculate the local time within the HEARTLANDNet Settlement System (i.e., standard local time zone differential from Greenwich Mean Time (GMT).
- Host URL Part 1 - Enter the first part of the URL address of the primary host connection. This consists of the protocol and the site name.

Example: `sslprod.secureexchange`

- Host URL Part 2:Port - Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.

  Example: `.net:22346`

- BackUP URL Part 1 - Enter the first part of the URL address of the backup host connection. This consists of the protocol and the site name. Backup connections are triggered when the system cannot establish communication via the primary host address.

  Example: `sslprod.secureexchange`

- BackUP URL Part 2:Port - Enter the second part of the URL address of the backup host connection. This consists of the domain and the port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

  Example: `.net:22346`

8. Go to the **Merchant** | **Settlement** tab and configure the following settings:
   - Industry Code - This field is used to identify the type of industry for this merchant.
     - Enter 1 if the merchant business is a retail establishment.
     - Enter 0 if the merchant business is a restaurant.
   - Language Code – This field is used to identify the language in which settlement response messages will be returned for display and/ or printing. Select the language code from the following list:
     - 0 (zero) English
     - 1 Spanish
     - 2 Portuguese
     - 3 Irish
     - 4 French
     - 5 German
     - 6 Italian
   - Not Used – Leave this field blank.
   - Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.
   - Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.
   - Merchant Type - This field supports eCommerce transactions. An eCommerce transaction is one that occurs online. Authorizations for payments submitted online are set with a different set of authorization data. To support this functionality.

    - Enter a 0 in this field to designate restaurant transactions (default setting).
    - Enter a 1 in this field to designate eCommerce transactions.
- Acquirer BIN Number - Enter the 6-digit Bank Identification Number assigned by the Credit Card Processor.
- Merchant ID Number - Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor.
- Store Number - Enter the 4-digit number used to identify the merchant store. This number is assigned by the Credit Card Processor.
- Terminal Number - Enter the 4-digit number used to identify a specific terminal within an establishment. This number is assigned by the Credit Card Processor. Each terminal in the establishment must have a unique number.
- Merchant Category - Enter the 4-digit number used to identify the merchant type. This number is assigned by the Credit Card Processor.
- Merchant Name - Enter the name of the merchant (up to 25-characters). This name must correspond to the name that prints on the credit card voucher.
- Agent Number - Enter the 6-digit number that identifies the merchant. This number is assigned by the Credit Card Processor.
- Chain Number - Enter the 6-digit number that identifies the merchant chain. This number is assigned by the Credit Card Processor.
- Merchant Location Number - Enter the 5-digit number that provides additional information on the location of the merchant. This number is assigned by the Credit Card Processor. Unless specified otherwise by the merchant's bank or processor, the default for this field should be 00001.

9. Go to **POS Configurator** | **Sales** | **Tender Media** | **Credit Auth** tab. Link all of the appropriate credit card tenders (e.g., Visa/Mastercard) to the HL drivers by configuring the following fields:
    - CA Driver – Use the drop down box to select the CaHLA driver.
    - EDC Driver – Use the drop down box to select the CaHLS driver.
10. If AVS and CVV are configured at the site complete step 10. If not go to step 12. Go to the **Revenue Center** | **RVC Credit Cards** | **AVS** tab and enable the following options. Select the options as they are appropriate for the site.
    - Require AVS for Manual Entry. Select this option to prompt for the cardholder's zip code before submitting a manual credit card authorization.
    - Require Full AVS for Manual Entry. Select this option to prompt for the cardholder's address AND zip code before submitting a manual credit card authorization. This option is only enabled if the **Require AVS for Manual Entry** option is enabled.
    - Require Full AVS when Card is not Present. Select this option to determine whether the credit card is present before proceeding. If it is, the system will prompt for the zip code only. If it is not, the system will

prompt for the cardholder's complete address and zip code. This option is only enabled with the **Require AVS for Manual Entry** option is also enabled.

- Require AVS for Swiped Entry. Select this option to prompt for the cardholder's zip code before proceeding with a swiped credit card transaction.
- Require Full AVS for Swiped Entry. Select this option to prompt for the cardholder's address AND zip code before proceeding with a swiped credit card authorization. This option is only enabled with the **Require AVS for Swiped Entry** option is also enabled.

11. Go to the **Sales** | **Tender/Media** | **CC Tender** tab and select the options as they are appropriate for the site.
    - Prompt for CVV on Manual Entry. Select this option to display the following menu of options when a credit card is manually entered. To proceed, the user must select one of these options and respond accordingly.
        - Intentionally not provided
        - Present and will be provided
        - Present but is illegible
        - Not present
    - Prompt for CVV on Swiped Entry. Select this option to display the following menu of options when a credit card is swiped. To proceed, the user must select one of these options and respond accordingly.
        - Intentionally not provided
        - Present and will be provided
        - Present but is illegible
        - Not present
12. Reload the database from the MICROS Control Panel.
13. 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.

6 TSYS Acquiring Solutions

This version of the TSYS Acquiring Solutions Credit Card Driver only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

This driver supports the following functionality:

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

Installation

Pre Installation Requirements

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

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

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

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

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

See Password Handling Process before installing the TSYS Credit Card Driver.

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

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

Site Requirements

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

The installed version of 3700 POS should be Version RES 5.0 or higher.

To use Internet Connectivity, an Internet connection must be configured and working. ISP software is needed to connect to the Internet.

Security protocols, including firewalls and other protections, should be in place.

The site's browser software will need to support 128-bit session keys.

Files Included

The following list the files installed for the driver:

```
\MICROS\Res\Pos\Bin\CaTSYS.dll
\MICROS\Res\Pos\Etc\CaTSYS.cfg
\MICROS\Res\Pos\Bin\CaTSYS.hlp
\MICROS\Res\Pos\Bin\CaTSYS.cnt
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.dll
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTSYS.cfg
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.hlp
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.cnt
\WINDOWS\system32\MSVCR71.dll
```

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

Installation Instructions for a Site Running RES 5.0 or Higher

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

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

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the latest TSYS Credit Card Driver from the Oracle web site. Copy this file to your RES Server's temp folder.
3. Double click on the `CaTSYS(5.2).exe` file. This will install of the necessary files on RES Server and the BSM Client, and Windows Services will be restarted automatically.
4. Reboot the RES Server.

Configuration Instructions

Follow these steps to complete the configuration for the driver:

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

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

2. Go to the **System** tab and configure the following settings:
   - Not Used – Leave this field blank.
   - Not Used – Leave this field blank.
   - Not Used – Leave this field blank.
   - Communication Channel – This field specifies the type of interface connection used between the merchant and the credit card processor. This field will default to 2 for an internet connection.
   - Max Offline Transaction – This option controls the maximum number of automatic offline transactions that can be processed by the driver. When this limit is exceeded, the "`Manual Auth Required`" error message will be returned to POS Operations. This value will accumulate until the time that a batch is successfully settled by the settlement driver. At that time, the value is re-set.
   - Max Offline Amount (Dollars) – This option controls the maximum dollar value of automatic offline transactions that can be processed. The maximum offline amount is entered as dollars and cents with no decimal (e.g., 2500 is the equivalent of $25.00). When this limit is exceeded, the "`Manual Auth Required`" error message will be returned to POS Operations. This value will accumulate until the time that a batch is successfully settled by the settlement driver. At that time, the value is re-set.

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

     The total count and dollar value of the offline authorizations is reset any time a batch is successfully settled by the settlement driver. In addition a new driver diagnostic has been added which will reset the totals to zero.

This diagnostic is available through both the credit card GUI and the command line settlement application.

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

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

  See Auto Offline Credit Card Authorization Support for further information.
- Internet Host Header – Enter the HTTP host name to be included in every outgoing authorization request. Up to 25 characters is allowed.
- Internet Target Name1 – Enter the HTTP target name to be included in every outgoing authorization request. Up to 25 characters is allowed. If no existing data exists, it will default to: `/servlets/`
- Internet Target Name2 – Enter the remaining target name if longer than 25 characters from the previous field. If no existing data exists, it will default to: `TransNox_API_Server`
- Host URL Part1 – Enter the first part of the URL address of the primary host connection. This consists of the protocol and site name. If no existing data exists, it will default to the following: `gateway.transit-pass.com`
- Host URL Part2:Port – Enter the second part of the URL address of the primary host connection. This consists of the domain and port number. Leave this field blank.
- BackUP URL Part1 – Enter the first part of the URL address of the backup host connection. This consists of the protocol and site name. Backup connections are triggered when the system cannot establish communication via the primary host address.
- BackUP URL Part2:Port – Enter the second part of the URL address of the backup host connection. This consists of the domain and port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

3. Go to the **Merchant** | **Authorization** tab and configure the following settings:
   - Merchant ID – Enter the number used to identify the merchant. This number is assigned by the Credit Card Processor (bank). The valid range is 3-20 digits.
   - Operator – Enter the Operator User ID added to the TSYS Merchant Center chosen for this site. The valid range is 6-20 alphanumeric characters. This is the **Operator** name that is used to identify this store. For example, `Store1234` and the second site to be rolled out might be `Store5678`. Each site that the driver is installed in requires its own Operator name. Per the Pre Installation Requirements, your TSYS

representative will provide instructions on how to access the TSYS Website and obtain a temporary password for each installation.

4. Go to the **Merchant** | **RVC** tab and configure the following settings:
    - Merchant Name/Number – Lists the names of each merchant associated with the POS System. This option allows a user to establish multiple merchant ID's for accounting and reporting purposes.
    - RVC Name – Lists the name of the revenue centers linked to the highlighted Merchant ID. When adding a new record, right click in the Name field to open the drop-down list of all the revenue centers configured across the POS System.

      A revenue center may only be linked to one Merchant at a time. Attempts to link to more than one will result in an error message.
    - For Single Merchant Sites: If only one Merchant ID is issued by the bank for this site, then in **Credit Card Batch** | **Diagnostics** | **Set Host Password** only use the first Revenue Center number to enter the Password.
    - For Multiple Merchant Sites: If there are two or more Merchant ID's issued by the bank for this site, then add Merchant 2 and link the appropriate RVC's to each Merchant IFD. For example, above there are six RVC's. If RVC 6 (Drive Thru) is assigned Merchant ID 2, then in **Credit Card Batch** | **Diagnostics** | **Set Host Password**, enter Merchant ID 2's Operator ID and Password,
    - Merchant ID 1 = 1|Password@123 (this will cover RVC's 1-5)
    - Merchant ID 2 = 6|Password@123 (this will cover RVC 6)
5. Go to **POS Configurator** | **Sales** | **Tender / Media** | **Credit Auth** form. Link all of the appropriate credit card tenders (e.g., Visa/Mastercard) to the TSYS driver by configuring the following fields for each card type:
    - CA Driver – Use the drop down box to select the CaTSYS driver.
    - EDC Driver – Use the drop down box to select the CaTSYS driver.
6. Go to **POS Configurator** | **Sales** | **Tender / Media** | **CC Tender**. Configure these options to mask the Card Number, Customer Name, and Expiration Date on all credit card transactions. This is required for Credit Card Security (PCI Compliance).
7. If AVS and CVV are configured at the site complete step 7. If not go to step 10. Go to the **Revenue Center** | **RVC Credit Cards** | **AVS** tab and select the options as they are appropriate for the site.
    - Require AVS for Manual Entry - Select this option to prompt for the cardholder's zip code before submitting a manual credit card authorization.
    - Require Full AVS for Manual Entry - Select this option to prompt for the cardholder's address AND zip code before submitting a manual credit card authorization. This option is only enabled if the **Require AVS for Manual Entry** option is enabled.

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

8. Go to the **Sales** | **Tender / Media** | **CC Tender** tab and enable the following options. Select the options as they are appropriate for the site.
    - **Prompt for CVV on Manual Entry**. Select this option to display the following menu of options when a credit card is manually entered. To proceed, the user must select one of these options and respond accordingly.
    - Intentionally not provided.
    - Present and will be provided.
    - Present but is illegible.
    - Not present.
    - **Prompt for CVV on Swiped Entry**. Select this option to display the following menu of options when a credit card is swiped. To proceed, the user must select one of these options and respond accordingly.
    - Intentionally not provided.
    - Present and will be provided.
9. Go to the **Sales** | **Tender / Media** | **CC Tender** tab and enable the following options for all credit cards configured as they are appropriate for the site.
    - Verify before authorization - Select this option to test for a valid credit card number before processing.

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

      This option works with the following setting:

      Disable Prompt for Card Holder Not Present (RVC Credit Cards)

10. Go to the **Sales** | **Tender / Media** | **Credit Auth** tab and enable the following option for all credit cards configured as they are appropriate for the site.
    - Allow partial authorization- Enable this option to allow this credit card tender to preform partial authorizations. A partial amount is any amount less than the amount required by the credit card driver.
11. Reload the database from the MICROS Control Panel.
12. Go to **Start** | **Programs** | **MICROS Applications** | **POS** | **Credit Card Batch**. Click on the **Diagnostic** tab and select the **Test Auth Connection** and the **Test Settlement Connection** buttons to verify that the drivers are up and running. A few test transactions can also be done to ensure all is working correctly.

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

Configuring Intermediate Certificates

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

Features Supported

Auto Offline Credit Card Authorization Support

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

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

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

Basic Use Cases

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

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

How It Works

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

Authorization:

1. The driver is unable to contact the credit card host through the primary and backup Host URL's.
2. The driver will generate a random 6-digit authorization code and return an approval to POS Operations (Approval is dependent upon whether floor limits are used, continue reading for more information).

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

   POS Operations pauses before responding so that it is not obvious that no attempt was made to contact the host. Only the random 6-digit auth code appears on the credit voucher.
3. The transaction is flagged as having been automatically approved.
4. POS Operations will mark the authorization detail as having been auto approved but will not indicate that the auth code was manually generated on either the voucher or the display.

Settlement:

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

   The settlement driver will attempt to obtain an online authorization from the issuing bank to replace the authorization generated by the credit driver. These authorizations will occur before the actual settlement in an operation known as pre-settlement. The authorization request in pre-settlement will treat the authorization as a card present / manually keyed transaction.
6. The batch settlement report will show an L flag next to transactions where an auto offline auth was generated. The "L" flag has been added to the Credit Card Batch Detail report, in the flags column, to indicate an Auto Offline Authorization. This occurs if the Host Processor is down and the transaction amount is below the designated floor limit. An auto offline auth transaction was obtained rather than an actual authorization. The L flag will appear in the same column as the manual authorization flag since the two flags cannot both appear for the same transaction.
7. If an authorization request is declined in pre-settlement, the settlement driver will change the authorization code on the record to '**DECLINED'** and mark the

record as omitted by the driver (a 'D' flag on the batch detail report). These transactions will also be shown in the omitted record summary of the batch transfer report.

Omitted by the driver (Dflag) will only occur if the driver option 'Auth Offline Transactions' is set to one '1' (enabled).

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

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

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

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

POS Configuration

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

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

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

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

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

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

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

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

Support Zero Dollar Account Verification

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

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

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

eCommerce Transactions Support

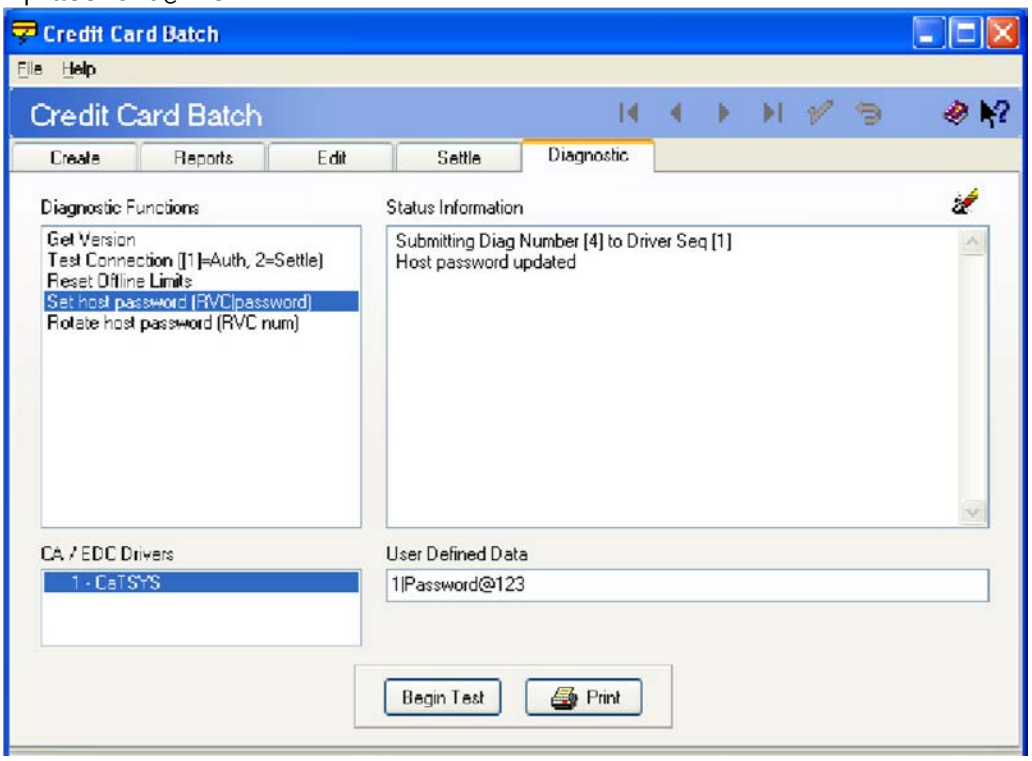
An eCommerce transaction is one that occurs online. Authorization for payments submitted online are sent with a different set of authorization data. When transactions come through Transaction Services will have a flag set that distinguishes them as eCommerce.

Password Support

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

1. Go to Start | Programs | MICROS Applications | POS | Credit Card Batch and click on the Diagnostic tab.
2. Select Set host password (RVC|password).

3. In the **User Defined Data** field, enter the Revenue Center number followed by a pipe then the password. Click on the **Begin Test** button. For example:
`1|Password@123`



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

   The TSYS Administrator password will expire every 45 days.

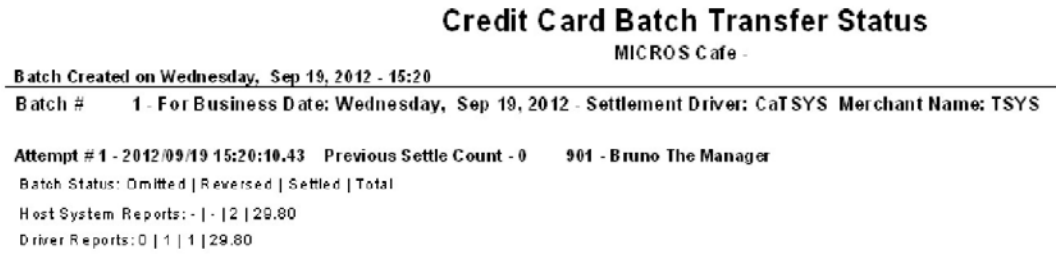
   The TSYS Store Operator password, used for credit transactions, will automatically update every seven days once the initial password has been entered in **Credit Card Batch** | **Diagnostic** and used for the first week.

End of Day Procedures

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

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

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



Sample Credit Card Voucher

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

```
Date:       Sep18'12 01:47PM
Card Type:  Visa/M.C.
Acct #:     XXXXXXXXXXXX1111*
Card Entry: KEYED
Trans Type: PURCHASE
Auth Code:  836248
Check:      8
Table:      61/1
Server:     101 Sally S
Reference:  2543375

Subtotal:           18.88
Date:       Sep18'12 01:47PM
Card Type:  Visa/M.C.
Acct #:     XXXXXXXXXXXX1111*
Card Entry: KEYED
Trans Type: PURCHASE
Auth Code:  836248
Check:      8
Table:      61/1
Server:     101 Sally S
Reference:  2543375 <-------- Transaction ID

Subtotal:           18.88
```

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

Removing the Software

Removing Software From a Site Running RES 4.5 or Higher

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

1. Shut down the RES system from the MICROS Control Panel.
2. Delete the following files:
   `\MICROS\Res\Pos\Bin\CaTSYS.dll`
   `\MICROS\Res\Pos\Etc\CaTSYS.cfg`
   `\MICROS\Res\Pos\Bin\CaTSYS.hlp`

```
\MICROS\Res\Pos\Bin\CaTSYS.cnt
```

3. Delete the following files on the server:
```
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.dll
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Etc\CaTSYS.cfg
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.hlp
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bin\CaTSYS.cnt
```
4. Shut down the RES System on the Backup Server Client (if applicable). Also on the BSM Client, delete the following driver files:
```
\MICROS\Res\Pos\Bin\CaTSYS.dll
\MICROS\Res\Pos\Etc\CaTSYS.cfg
\MICROS\Res\Pos\Bin\CaTSYS.hlp
\MICROS\Res\Pos\Bin\CaTSYS.cnt
```

Password Handling Process

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

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

   Warning: The Administrator password, received via e-mail from the TSYS Merchant Center when first setting up the driver, cannot be used for credit transactions in RES. The Administrator password is to be used only for management purposes (i.e. - checking on Pending Batches, Settled Batches, or possible adjustments).
2. A separate store 'Operator' password needs to be created, using the TSYS Merchant Center Web Site, for daily credit transactions. This is the only password that is automatically updated after the initial password is entered via Credit Card Batch | Diagnostics.
   - Choose a password that is at least eight (8) characters long, it must have numbers (0-9), upper, lowercase letters (A-Z, a-z) and special character (!,@,$,^,*,-,_.) but no spaces. You are not allowed to reuse any of the last 6 Passwords used. (It is recommended doubling this to the last 12 passwords, to be extra secure).
   - The 'Operator' password will be automatically rotated every 7 days (default), by sending a change password request to the host. This can be changed (See #3 below).
3. What Password Information is stored in the registry?
   - The encrypted password, represented in ASCII HEX.
   - The last time the password was updated - formatted as mm-dd-yyyy.

- Optional DWORD value to configure how often to update the password (indicating number of days). Registry name = RotatePasswordEveryXDays.
- This parameter will default to 7 days if not configured in the registry.

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

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

Troubleshooting Tips

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

Verbosity = 5 in the MICROS Control Panel

This will log extra information in the 3700d.log.

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

`HKEY_LOCAL_MACHINE\SOFTWARE\MICROS\Common\CCS\DrvrCfg\Drvr#\Support`

The following keys can be created as DWORD Value:

- DiskLog = 1
- LogCaMsgs = 1
- LogSettleMsgs = 1

  These will create a TSYS.log file in the \MICROS\Res\Pos\Etc folder.
- LogXMLMsgs = 1

  This will log each XML message in a separate XML file in the \MICROS\Res\Pos\Etc\TSYS folder.

Frequently Asked Questions

Why is reading the Credit Card Transfer Report so important?

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

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

What is a credit card batch?

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

At the end of the day, a process is run to combine all the credit card transactions into a batch. This groups all of these types of transactions into a single message that will be sent

to the credit card host (during the transfer process). A batch report can also be run listing each individual credit card transaction, sorted by credit card type.

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

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

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

- Credit card number
- Expiration date

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

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

- Terminal-based processing requires that the entire batch be successful for the batch to be closed. Most of the 3700 POS drivers support terminal-based processing.
- Host-based processing requires each transaction to be successful. This means a batch could contain a single card that did not transfer to the credit card host. Once this transaction is adjusted, the batch could be re-sent to the host. The TSYS Credit Card Driver is host-based.

Transfer Status Report

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

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

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

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

7 American Express Authorization

This version of the American Express Authorization Credit Card Driver only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

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

Installation

Site Requirements

Before installing the AMEX Authorization Credit Card 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.

Files Included

The AMEX driver includes the following files:

```
\Micros\RES\POS\Bin\CaAMEX.dll
\Micros\RES\POS\etc\CaAMEX.cfg
\Micros\RES\POS\Bin\CaAMEX.hlp
\Micros\RES\POS\Bin\CaAMEX.cnt
```

Installation Instructions

The installation of the credit card drivers are separate from the RES software. The American Express driver is an independent install. When upgrading RES, the American Express driver will not be affected.

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the latest American Express Authorization Credit Card Driver from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
    - AMEX Authorization Credit Card Driver Installation Documentation (`CaAMEX_MD.pdf`).
    - CaAMEX (5.2).exe
3. Shutdown all Oracle applications from the MICROS Control Panel.
4. Double click the `CaAMEX(5.2).exe`.
5. Turn on the RES System from the MICROS Control Panel.
6. Configure the driver.

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

Setup

Configuring the Drivers

Credit card drivers are setup through the **POS Configurator** | **Devices** | **CA/EDC Drivers**. A separate record should be added for each of the following, using the specified **Driver Code**: AMEX - `CaAMEX Authorizations`

Configuring the CaAMEX Driver

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., CaAMEX) and a value of the **Driver Code** field (e.g., AMEX) and save the record.
3. Go to the **System** tab and configure the following settings:
    - Not Used 1 – Leave this field blank.
    - Not Used 2 – Leave this field blank.
    - Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter 1 to enable port arbitration when more than one credit card driver is being used. Enter 0 to disable the option.

      Port arbitration is usually enabled.
    - Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor. The options are:
        - 2: internet
    - Companion Auth Driver Code– This field specifies the name of the auth driver in correspondence to the settlement driver that AMEX will use.
    - Internet Host Header – Enter the HTTP host name to be included in every outgoing authorization request. Up to 25 characters is allowed.
    - Internet Target Name1– Enter the HTTP target name to be included in every outgoing authorization request. Up to 25 characters is allowed.
    - Internet Target Name2 – Enter the remaining internet target name if longer than 25 characters from previous field.
    - Host URL Part1 – Enter the first part of the URL address of the primary host connection. This consists of the protocol and site name.
    - Host URL Part2: Port– Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.
    - BackUP URL Part1 – Enter the first part of the URL address of the backup host connection. This consists of the protocol and the site name. Backup connections are triggered when the system cannot establish communication via the primary host address.

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

4. Go to the **Merchant** | **Authorization** tab and configure the following settings:
    - Merchant Category – Enter the 4-digit number used to identify the merchant type. The number is assigned by the Credit Card Processor.
    - Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.
    - Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.
    - Card not present enabled – This field specifies if telephone orders are accepted without the credit card present.
    - Acquirer BIN Number – Enter the Bank Identification Number assigned by the Credit Card Processor. This field allows up to 11 digits.
    - Card Acceptor ID code – Enter the number used to identify the merchant. This field allows up to 15 digits. This number is assigned by the Credit Card Processor.
    - Merchant Name – Enter the name of the merchant (up to 25 - characters). This name must correspond to the name that prints on the credit card voucher.
    - Merchant Street – Enter the name of the street where the merchant is located.
    - Merchant City – Enter the name of the city where the merchant is located.
    - Merchant Postal Code– Enter the 3-digit number assigned by the Credit Card Processor to futher identify the merchant location within a country. In the USA, the 5- or 9-digit postal code for the merchant is used. Merchants located outside of the USA, will be assigned a number by the Credit Card Processor.

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.

8 Universal Credit Card Driver (UCCD) including Ventiv

This version of the Universal Credit Card Driver (UCCD) including Ventiv only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

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

Installation

When upgrading the Universal Credit Card Driver including Ventiv to v5.2, the user must go into **POS Configurator** | **Devices** | **CA / EDC Drivers** and select both the VSCA and VSST records. This will update the database with the new configuration file.

Authorization reversals are only supported in RES Version 5.0 or higher.

Site Requirements

Before installing the Universal Credit Card Driver including Ventiv 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 TCP/IP, a WAN must be configured and working.
- 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.

Files Included

The Universal Credit Card Driver is divided into an authorization driver and a settlement driver. The following lists the files installed for each:

Authorization:

```
\Micros\RES\POS\Bin\CaVsca.dll
\Micros\RES\POS\etc\CaVsca.cfg
\Micros\RES\POS\Bin\CaVsca.hlp
\Micros\RES\POS\Bin\CaVsca.cnt
```

Settlement"

```
\Micros\RES\POS\Bin\CaVsst.dll
\Micros\RES\POS\Etc\CaVsst.cfg
\Micros\RES\POS\Bin\CaVsst.hlp
\Micros\RES\POS\Bin\CaVsst.cnt
```

Installation Instructions

This Credit Driver Installation Package enters the following driver related information to Windows Registry:

`"[HKEY_LOCAL_MACHINE\SOFTWARE\MICROS\CreditCardDrivers\CaVsCa]"`

`"[HKEY_LOCAL_MACHINE\SOFTWARE\MICROS\CreditCardDrivers\CaVsSt]"`

`"InstallationVersion"="4.XX.XX.XXXX"`

The version of the driver being installed.

`"Installed"="Day MM/DD/YYYY"`

The installation date of the installed driver (for example, 'Thu 01/19/2012').

Existing Site Running RES V5.0 (or Higher)

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the latest Universal Driver from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
    - Universal Credit Card Driver for RES 3700 POS (`UCCDV5.2_MD.pdf`)
    - Oracle RES Universal Credit Card Driver (`CaUCCD(5.2).exe`)
3. Review the ReadMe First for all software changes in the current release.
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 MICROS Control Panel.
5. Double-click on the `CaUCCD(5.2).exe` file to execute the installation program. This will install all of the necessary files on the RES Server and the BSM Client, and the Windows services will be restarted automatically. The credit card service will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started:

File	RES Server	Backup Server Client
CaVsca.dll	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsst.dll	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsca.cfg	\MICROS\RES\POS\ ETC	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC
CaVsst.cfg	\MICROS\RES\POS\ ETC	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC
CaVsca.hlp	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsst.hlp	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN

CaVsca.cnt	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsst.cnt	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN

6. Take the RES system to **Front Of House** from the MICROS Control Panel.
7. Open **POS Configurator** | **Devices** | **CA / EDC Drivers** and select both the VSCA and VSST records. This will update the database with the new configuration file.
8. CA/EDC should be operational. A few test transactions should be done to ensure all is working correctly.

New Site Running RES V5.0 (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.
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 Universal Driver from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
    - Universal Credit Card Driver for RES 3700 POS (`UCCDV5.2_MD.pdf`)
    - Universal Credit Card Driver Software (`CaUCCD(5.2).exe`)
4. Review the ReadMe First for all software changes in the current release.
5. 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 MICROS Control Panel.
6. Double-click on the `CaUCCD(5.2)`.exe file to execute the installation program. This will install all of the necessary files on the RES Server and the BSM Client, and the Windows services will be restarted automatically. The credit card service will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started

File	RES Server	Backup Server Client
CaVsca.dll	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsst.dll	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsca.cfg	\MICROS\RES\POS\ ETC	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC
CaVsst.cfg	\MICROS\RES\POS\ ETC	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\ETC

CaVsca.hlp	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsst.hlp	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsca.cnt	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN
CaVsst.cnt	\MICROS\RES\POS\ BIN	\Micros\RES\CAL\Win32\Files\MICROS\RES\POS\BIN

7. Take the RES system to **Front Of House** from the MICROS Control Panel.
8. Configure the driver using the site information provided by MerchantLink.
9. Go to **POS Configurator** | **Devices** | **CA/EDC Drivers** and configure the following settings for the authorization driver (VSCA):
    - Click on the blue plus button to add a new driver.
    - Click on the **Name** cell of the new row and give the driver an appropriate name (e.g. VSCA Auth).
    - Select the **Driver** tab and enter VSCA as the **Driver Code**.
    - Select the **System** tab.
    - Set the **Port Arbitration Enabled** field to `1` to enable this driver.
    - Set the **Communication Channel** to the communication type enabled at the store (0= dial-up, 1 = TCP/IP, 2= HTTPS).
    - Use the **Enable Card Level Results** option to indicate whether card level results will be transmitted as part of the authorization message. This option will be disabled by default as well as when Custom Mode is used. Enter one of the following values:
        - 0. Option is disabled (default).
        - 1. Option is enabled.
    - Use the **Enable POS Data Code** option to indicate whether the POS data code will be transmitted during authorization. Enter one of the following values:
        - 0. Option is disabled.
        - 1. Option is enabled.
    - Enter a URL address in the **Host IP Address: Port** field. The URL can be obtained from the bank.
    - Enter a secondary URL in the **Backup IP Address: Port** field. This URL will be used in the event that the primary URL fails. The URL can be obtained from the bank.
    - All settings under the **Merchant** tab should be completed using the instructions provided by the bank.
10. Go to **POS Configurator** | **Devices** | **CA/EDC Drivers** and configure the following settings for the settlement driver (VSST):
    - Click on the blue plus button to add a new driver.

- Click on the **Name** cell of the new row and give the driver an appropriate name (e.g. VSST Settle).
- Select the **Driver** tab and enter VSST as the **Driver Code**.
- Select the **System** tab.
- Set the **Port Arbitration Enabled** field to `1` to enable this driver.
- Set the **Communication Channel** to the communication type enabled at the store (0= dial-up, 1 = TCP/IP, 2= HTTPS).
- Enter a URL address in the **Host IP Address: Port** field. The URL can be obtained from the bank.
- Enter a secondary URL in the **Backup IP Address: Port** field. This URL will be used in the event that the primary URL fails. The URL can be obtained from the bank.
- All settings under the **Merchant** tab should be completed using the instructions provided by the bank.

11. CA/EDC should be operational. A few test transactions should be done to ensure all is working correctly.

Removing the Software

Follow these steps to remove the UCCD 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\CaVsca.dll
   \Micros\RES\POS\etc\CaVsca.cfg
   \Micros\RES\POS\Bin\CaVsca.hlp
   \Micros\RES\POS\Bin\CaVsca.cnt
   \Micros\RES\POS\Bin\CaVsst.dll
   \Micros\RES\POS\Etc\CaVsst.cfg
   \Micros\RES\POS\Bin\CaVsst.hlp
   \Micros\RES\POS\Bin\CaVsst.cnt
   ```
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\CaVsca.dll
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\etc\CaVsca.cfg
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsca.hlp
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsca.cnt
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsst.dll
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Etc\CaVsst.cfg
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsst.hlp
   \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsst.cnt
   ```

Setup

Communication Channels Supported

- Dial-Up (Channel 0, system default)
- TCP/IP, Unencrypted via Frame Circuit Connectivity or VSAT Connectivity (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

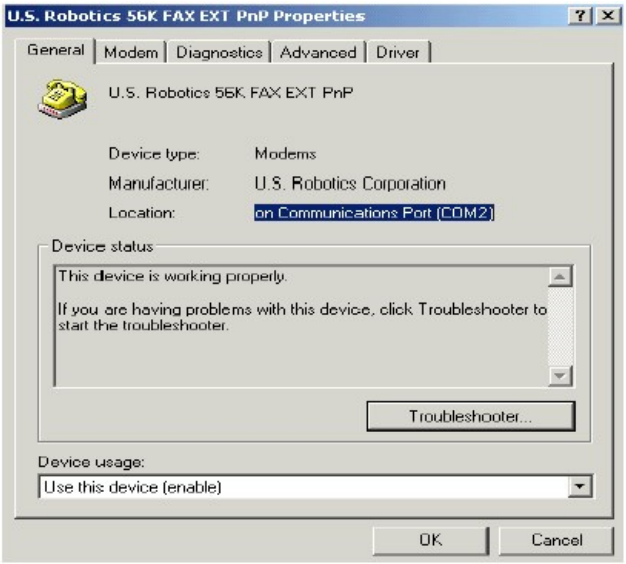
This section is provided as reference when installing the Universal Credit Card Driver. All information listed below has not changed since the initial release of a particular communication channel.

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:

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`.

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 3.
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 frame-relay connection from their satellite hub to Merchant Link.
- Connection from each site to a corporate WAN and frame-relay connection from corporate to ML.

Host And Backup Host Configuration

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

Fallback Configuration

The UCCD 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 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 UCCD 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**.

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.

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.

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 UCCD'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.

Internet Configuration

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

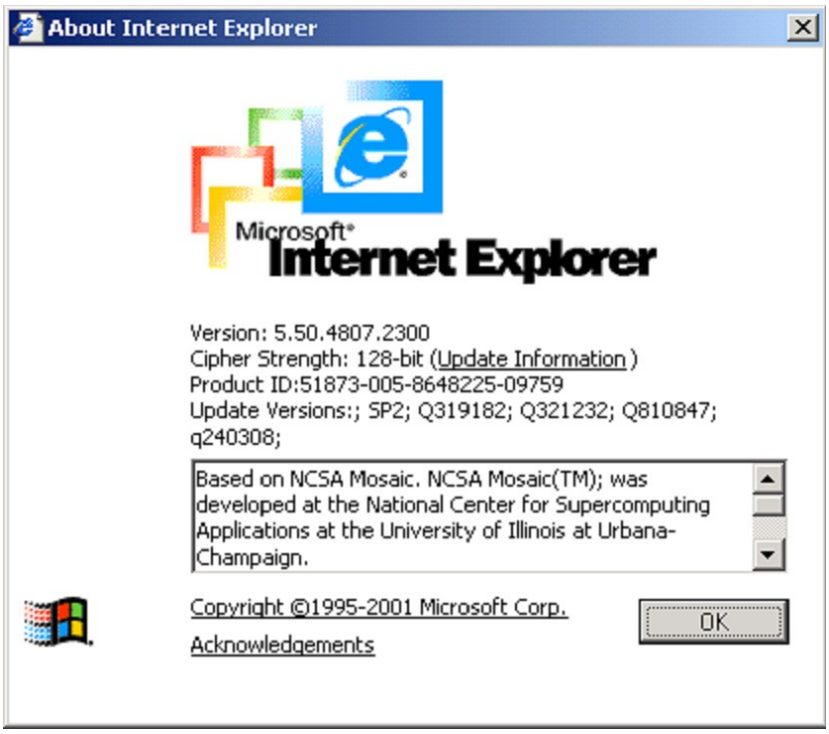
Internet Connectivity

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.

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 Oracle 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

Test Internet Connectivity

The site must be able to connect to ML's siteNET gateway through port 443. 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/Micros/process_transaction.cgi`

This does an HTTPS GET request to the siteNET Gateway. Internet Explorer responds with a File Download request. Select **Open this file from the current location** and use Notepad as the text viewer.

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

If a problem is encountered, one of two error messages will be displayed:

- 403 - Forbidden Error — Indicates that something is blocking the connection.
- 404 - Forbidden Error — Indicates that 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.

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 443. 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:443
- Backup IP Address: Port — g2.merchantlink.com:443

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 UCCD'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.

Fallback Configuration

The UCCD 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 UCCD 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**.

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.

Internet Proxy Considerations

In the past, Internet communications used WinInet proxy settings configured through the Internet Explorer. Due to changes in the Microsoft operating systems, Internet communications are now handled through the WinHTTPS protocol.

To configure the settings for WinHTTPS, Microsoft provides a utility program, `proxycfg.exe`. However, at this time, the program is only available for the Windows XP operating system. This means that anyone running in a Windows 2000 or higher operating system — and using a proxy server — will need to manually configure the proxy server information.

To accommodate RES customers, a new **ProxyName** value is available in the Registry. The current release of the VCC Driver will use proxy settings from this location.

Follow these steps to add the ProxyName registry key:

1. Open Regedit to \HKLM\SOFTWARE\MICROS\Common\CCS\DrvrCfg\.
2. Under the Authorization Driver (i.e., Drvr1), make sure that you have a key called **[Option]**. If not, create one.
3. Under the Settlement Driver (i.e., Drvr2), make sure that you have a key called **[Option]**. If not, create one.
4. Under the **[Option]** key for each driver, create a STRING value called **ProxyName**.
5. Right-click on **ProxyName** and select **Modify**.
6. Enter the name of your Proxy Server. This can be either a domain name or URL, followed by a colon, then the SSL listening port of the proxy (e.g., `micros1:8443` or `172.28.213.212:8443`).

In the event that a proxy name is not specified, a new ProxyAccess value may be used instead. Follow these steps to add the ProxyAccess registry key:

1. Repeat Steps 1-3, as described in the ProxyName directions above.
2. Under the **[Option]** key for each driver, create a DWORD value called **ProxyAccess**.
3. Right-click on **ProxyAccess** and select **Modify**.
4. Enter one of the following values:
    - 1 (direct access to internet)
    - 4 (no autoproxy, startup, or Internet Setup (INS) file)

Configuring the Drivers

UCCD setup is not done until the VSCA and VSST 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.

Example:

For the **Internet Target Name** field (**System** tab),

`/USB/Gateway` does not equal `/usb/gateway`.

Change Maximum Batch Size

Follow these steps to edit the maximum batch size value in the Credit Card Batch Utility:

1. Go to the `\Micros\Res\POS\Etc` folder and select the `CaVSST.cfg` file.
2. When the window appears enable the **Select the program from a list** option and click **[Ok]**.
3. Highlight the NotePad application and click **[Ok]**.
4. Change the **MaxBatchSize** parameter setting from 300 to the desired value (i.e., `500`).
5. Save the record.
6. In POS Configurator, go to the **Devices** | **CA/EDC Drivers** | **CaVsST** | **Table View** tab.
7. Select the **Driver Object Number** row on this form. This updates the **New Max Batch Size** value; which will update the **caedc_driver_def** table in the database to the new configured value (i.e., 500 records).

AVS and CVV Configuration

The UCCD driver supports the transmission of 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 selecting 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.

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.

At this time, the URL for the merchant link intermediate certificate is:

http://ss.symcb.com

Frequently Asked Questions

Why is reading the Credit Card Transfer Report so important?

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

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

What is a credit card batch?

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

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

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

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

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

- Credit card number
- Expiration date

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

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

- Terminal-based processing requires that the entire batch be successful for the batch to be closed. Most of the 3700 POS drivers support terminal-based processing. The Universal 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 Universal Credit Card Driver for the prevention of duplicate batches. (For more on this topic, refer to the new features section in ReadMe First - v. 4.1.8.584)

9 Worldpay

This version of the Worldpay Credit Card Driver only supports 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. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

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

Installation

Site Requirements

Before installing the Worldpay Credit Card 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 TCP/IP, a WAN must be configured and working.
- 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 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.

Files Included

The Worldpay Driver is divided into an authorization driver and a settlement driver. The following lists the files installed for each:

Authorization:

```
\Micros\RES\POS\Bin\CaVNA.dll
\Micros\RES\POS\etc\CaVNA.cfg
\Micros\RES\POS\Bin\CaVNA.hlp
\Micros\RES\POS\Bin\CaVNA.cnt
```

Settlement:

```
\Micros\RES\POS\Bin\CaVNS.dll
\Micros\RES\POS\Etc\CaVNS.cfg
\Micros\RES\POS\Bin\CaVNS.hlp
\Micros\RES\POS\Bin\CaVNS.cnt
```

Additional Files:

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

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

Installation Instructions

The installation of the credit card drivers are separate from the RES software. The Worldpay driver is an independant install. When upgrading RES, the Worldpay driver will not be affected.

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Shutdown the RES system from the MICROS Control Panel.
3. Download the latest Worldpay Credit Card Driver from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
    - Worldpay Card Driver Installation Documentation (`CaVN_RMF.pdf`)
    - `CaVN(5.2).exe`
4. Double click the `CaVN(5.2).exe`. This will install all the necessary files on the RES Server and on the BSM Client, and Windows Services will be restarted automatically. The Oracle Credit Card Server service will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started.
5. Go to **POS Configurator** | **Devices** | **CA/EDC Drivers** and configure the following settings for the authorization driver (Worldpay):
    a. Click on the blue plus button to add a new driver.
    b. Click on the Name cell of the new row and give the driver an appropriate name (e.g. Worldpay Auth).
    c. Select the Driver tab and enter VNA as the authorization Driver Code.
6. Go to the **System** tab and configure the following settings:
    - Authorization Device – Specify the modem to use for authorization requests. Reference the modem using a one-digit number. Use `1` for the first modem listed in Control Panel, 2 for the second, etc. Use `0` for no device.
    - To determine the number to enter, type settle -m from a command prompt in the `\POS\bin` directory. The following sample messages 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.
      ```

      The modem must be configured in Control Panel before it can be assigned as an authorization device.
    - Not Used – Leave this field blank.
    - Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter `1` to enable

port arbitration when more than one credit card driver is being used. Enter `0` to disable the option.

Note: Port arbitration is usually enabled.

- Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor. The options are:
    - 0 - dial-up
    - 1 - Private Network/Unencrypted (Not Used)
    - 2 - Public Network/Encrypted
- Enable 12-Digit Amount – This field determines whether the credit card processor can accept an amount up to 12-digits long (excluding separator). The options are:
    - 0: Off (not allowed)
    - 1: On (allowed)
- Auth Phone Number – Enter the telephone number used for authorizations. Your Credit Card Processor will provide this number. Enter the number as follows:
    - Do not include hyphens.
    - Include any necessary long distance access code and area code, for example, 14105551212.
    - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- Backup Auth Phone Number – Enter the backup authorization phone number provided by your Credit Card Processor. (This field is optional. You may not have a backup number.)

  If the system attempts to perform an authorization but cannot get a telephone connection using the Auth Phone Number (for example, if the line is busy or the modem cannot make a connection), the backup number will be used. Enter the number as follows:
    - Do not include hyphens.
    - Include any necessary long distance access code and area code, for example, 14105551212.
    - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- City (Zip) Code – Enter the 3-digit number assigned by the Credit Card Processor to further identify the merchant location within a country. In the USA, the 5- or 9-digit Zip code for the merchant is used. Merchants located outside of the USA will be assigned a number by the Credit Card Processor.
- Time Zone – Enter the 3-digit number assigned by the Credit Card Processor used to calculate the local time within the VNANet (i.e., standard local time zone differential from Greenwich Mean Time (GMT).
- Merchant City - Enter the name of the city where the merchant is located.

- Merchant State - Enter the 2-character state/province code assigned by the Credit Card Processor used to identify the merchant. The 2-characters entered here must correspond to the state/province that prints on the credit card voucher.
- Host URL Part 1 – Enter the first part of the URL address of the primary host connection. This consists of the protocol and the site name.
- Host URL Part 2:Port – Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.
- BackUP URL Part 1 – Enter the first part of the URL address of the backup host connection. This consists of the protocol and the site name. Backup connections are triggered when the system cannot establish communication via the primary host address.
- BackUP URL Part 2:Port - Enter the second part of the URL address of the backup host connection. This consists of the domain and the port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

7. Go to the **Merchant** | **Authorization** tab and configure the following settings:
    - Not Used – Leave this field blank.
    - Industry Code – This field is used to identify the type of industry for this merchant.
        - Enter 1 if the merchant business is a retail establishment.
        - Enter 0 if the merchant business is a restaurant.
    - Language Code – This field is used to identify the language in which authorization response messages will be returned for display and/ or printing. Select the language code from the following list:
        - 0 (zero) English
        - 1 Spanish
        - 2 Portuguese
        - 3 Irish
        - 4 French
        - 5 German
        - 6 Italian
    - Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.
    - Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.
    - Bin Number – Enter the 6-digit Bank Identification Number assigned by the Credit Card Processor.
    - Merchant Number – Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor.

- Store Number – Enter the 4-digit number used to identify the merchant store. This number is assigned by the Credit Card Processor.
- Terminal Number – Enter the 4-digit number used to identify a specific terminal within an establishment.This number is assigned by the Credit Card Processor. Each terminal in the establishment must have a unique number.
- Merchant Category – Enter the 4-digit number used to identify the merchant type. This number is assigned by the Credit Card Processor.
- Merchant Name – Enter the name of the merchant (up to 25-characters). This name must correspond to the name that prints on the credit card voucher.

8. Go to **POS Configurator | Devices | CA/EDC Drivers** and configure the following settings for the settlement driver (VNS):
    a. Click on the blue plus button to add a new driver.
    b. Click on the **Name** cell of the new row and give the driver an appropriate name (e.g. Worldpay Settle).
    c. Select the **Driver** tab and enter VNS as the settlement **Driver Code**.
9. Go to the **System** tab and configure the following settings:
    - Not Used – Leave this field blank.
    - Settlement Device – Specify the modem to use for settlement requests. Reference the modem using a one-digit number. Use `1` for the first modem listed in Control Panel, `2` for the second, etc. Use 0 for no device.

      To determine the number to enter, type settle -m from a command prompt in the `\POS\bin` directory. The following sample message displays:

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

      The modem must be configured in Control Panel before it can be assigned as settlement device.
    - Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter `1` to enable port arbitration when more than one credit card driver is being used. Enter `0` to disable the option.

      Port arbitration is usually enabled.
    - Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor. The options are:
        - 0 - dial-up
        - 1 - Private Network/Unencrypted (Not Used)
        - 2 - Public Network/Encrypted

- Disable Auth Code Limit– This field determines whether or not the credit card driver will accept a manually entered authorization code that is longer than 6 digits. The options are:
    - 0 - Aborts a batch settlement if the batch file contains a detail record with an authorization code larger than 6 digits.
    - 1 - Accepts files for batch settlement that contain oversizes authorization codes in the detail records. When an oversized auth code is found, truncates the number to the first six digits before counting.
- Batch Numbering Mode– This field specifies the method to be used when assigning batch numbers during credit card settlement. The options are:
    - 0 - Static Barch Mode. Assigns a new number to each batch recieved by the driver. The number is unique to that particular batch and will be used for all settlements attempts. This method was designed to prevent duplicate batches. It is the default mode.
    - 1 - Dynamic Batch Numbering Mode. Assigns the next vaild number to any batch that is presented for settlement. The number is only incremented when the driver receives a Good Batch (GB) response from the host.
- Settle Phone Number - Enter the telephone number used for settlement. Your Credit Card Processor will provide this number. Enter the number as follows:
    - Do not include hyphens.
    - Include any necessary long distance access code and area code, for example, 14105551212.
    - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- Backup Settle Phone Number - Enter the backup settlement phone number provided by your Credit Card Processor. (This field is optional. You may not have a backup number.)

  If the system attempts to perform a settlement but cannot get a telephone connection using the Settle Phone Number (e.g., the line is busy, modem cannot make a connection, etc.), the backup number will be used. Enter the number as follows:
    - Do not include hyphens.
    - Include any necessary long distance access code and area code, for example, 14105551212.
    - Include any dialing prefix necessary to get an outside line, for example, 914105551212.
- City (Zip) Code - Enter the 3-digit number assigned by the Credit Card Processor to further identify the merchant location within a country. In the USA, the 5- or 9digit Zip code for the merchant is used. Merchants

located outside of the USA, will be assigned a number by the Credit Card Processor.

- Time Zone - Enter the 3-digit number assigned by the Credit Card Processor used to calculate the local time within the VNSNET Settlement System (i.e., standard local time zone differential from Greenwich Mean Time (GMT).
- Merchant City - Enter the name of the city where the merchant is located.
- Merchant State - Enter the 2-character state/province code assigned by the Credit Card Processor used to identify the merchant. The 2-characters entered here must correspond to the state/province that prints on.
- Host URL Part 1 - Enter the first part of the URL address of the primary host connection. This consists of the protocol and the site name.
- Host URL Part 2:Port - Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.
- BackUP URL Part 1 - Enter the first part of the URL address of the backup host connection. This consists of the protocol and the site name. Backup connections are triggered when the system cannot establish communication via the primary host address.
- BackUP URL Part 2:Port - Enter the second part of the URL address of the backup host connection. This consists of the domain and the port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

10. Go to the **Merchant | Settlement** tab and configure the following settings:
    - Not Used – Leave this field blank.
    - Industry Code - This field is used to identify the type of industry for this merchant.
        - Enter 1 if the merchant business is a retail establishment.
        - Enter 0 if the merchant business is a restaurant.
    - Language Code – This field is used to identify the language in which settlement response messages will be returned for display and/ or printing. Select the language code from the following list:
        - 0 (zero) English
        - 1 Spanish
        - 2 Portuguese
        - 3 Irish
        - 4 French
        - 5 German
        - 6 Italian
    - Append Option Data Group – This option determines whether the expiration date and stripe data will be appended to the batch detail record.

- Enter 0 to disable the option.
- Enter 1 to append the data.

Append Option Data Group should not be enabled when using the Fifth Third Bank Custom Mode. Any settlement records with the optional data appended will be rejected when using the Fifth Third Bank.

- Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.
- Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.
- Acquirer BIN Number - Enter the 6-digit Bank Identification Number assigned by the Credit Card Processor.
- Merchant ID Number - Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor.
- Store Number - Enter the 4-digit number used to identify the merchant store. This number is assigned by the Credit Card Processor.
- Terminal Number - Enter the 4-digit number used to identify a specific terminal within an establishment. This number is assigned by the Credit Card Processor. Each terminal in the establishment must have a unique number.
- Merchant Category - Enter the 4-digit number used to identify the merchant type. This number is assigned by the Credit Card Processor.
- Merchant Name - Enter the name of the merchant (up to 25-characters). This name must correspond to the name that prints on the credit card voucher.
- Agent Number - Enter the 6-digit number that identifies the merchant. This number is assigned by the Credit Card Processor.
- Chain Number - Enter the 6-digit number that identifies the merchant chain. This number is assigned by the Credit Card Processor.
- Merchant Location Number - Enter the 5-digit number that provides additional information on the location of the merchant. This number is assigned by the Credit Card Processor. Unless specified otherwise by the merchant's bank or processor, the default for this field should be 00001.

11. Go to **POS Configurator** | **Sales** | **Tender Media** | **Credit Auth** tab. Link all of the appropriate credit card tenders (e.g., Visa/Mastercard) to the NV drivers by configuring the following fields:
    - CA Driver – Use the drop down box to select the CaNVA driver.
    - EDC Driver – Use the drop down box to select the CaNVS driver.

Setup

Communication Channels Supported

- Dial-Up (Channel 0, system default)
- Private Network/Unencrypted (Not Used) (Channel 1)
- Public Network/Encrypted (Channel 2)

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

Connectivity Considerations

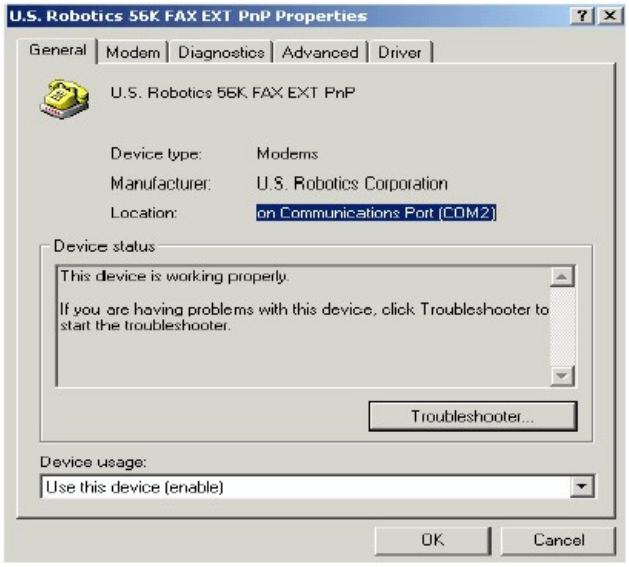
This section is provided as reference when installing the Universal Credit Card Driver. All information listed below has not changed since the initial release of a particular communication channel.

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:

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`.

   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 3.
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 frame-relay connection from their satellite hub to Merchant Link.
- Connection from each site to a corporate WAN and frame-relay connection from corporate to ML.

Host And Backup Host Configuration

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

Fallback Configuration

The UCCD 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 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 UCCD 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**.

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.

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.

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 UCCD'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.

Internet Configuration

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

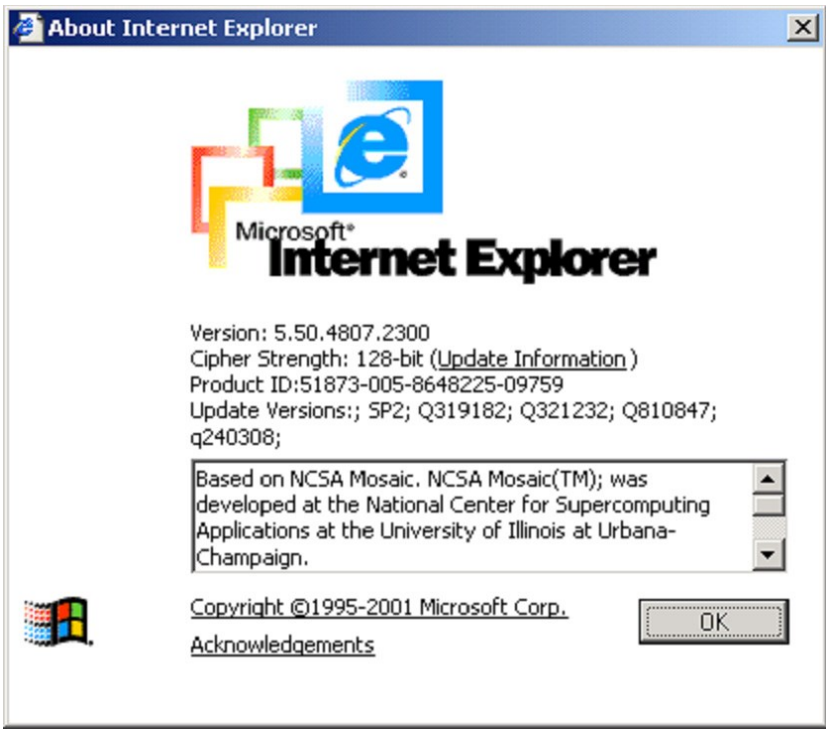
Internet Connectivity

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.

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 Oracle 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

Test Internet Connectivity

The site must be able to connect to ML's siteNET gateway through port 443. 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/Micros/process_transaction.cgi`

This does an HTTPS GET request to the siteNET Gateway. Internet Explorer responds with a File Download request. Select **Open this file from the current location** and use Notepad as the text viewer.

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

If a problem is encountered, one of two error messages will be displayed:

- 403 - Forbidden Error — Indicates that something is blocking the connection.
- 404 - Forbidden Error — Indicates that 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.

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 443. 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:443
- Backup IP Address: Port — g2.merchantlink.com:443

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 UCCD'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.

Fallback Configuration

The UCCD 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 UCCD 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**.

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.

Internet Proxy Considerations

In the past, Internet communications used WinInet proxy settings configured through the Internet Explorer. Due to changes in the Microsoft operating systems, Internet communications are now handled through the WinHTTPS protocol.

To configure the settings for WinHTTPS, Microsoft provides a utility program, `proxycfg.exe`. However, at this time, the program is only available for the Windows XP operating system. This means that anyone running in a Windows 2000 or higher operating system — and using a proxy server — will need to manually configure the proxy server information.

To accommodate RES customers, a new **ProxyName** value is available in the Registry. The current release of the VCC Driver will use proxy settings from this location.

Follow these steps to add the ProxyName registry key:

1. Open Regedit to `\HKLM\SOFTWARE\MICROS\Common\CCS\DrvrCfg\`.
2. Under the Authorization Driver (i.e., Drvr1), make sure that you have a key called **[Option]**. If not, create one.
3. Under the Settlement Driver (i.e., Drvr2), make sure that you have a key called **[Option]**. If not, create one.
4. Under the **[Option]** key for each driver, create a STRING value called **ProxyName**.
5. Right-click on **ProxyName** and select **Modify**.
6. Enter the name of your Proxy Server. This can be either a domain name or URL, followed by a colon, then the SSL listening port of the proxy (e.g., `micros1:8443` or `172.28.213.212:8443`).

In the event that a proxy name is not specified, a new ProxyAccess value may be used instead. Follow these steps to add the ProxyAccess registry key:

1. Repeat Steps 1-3, as described in the ProxyName directions above.
2. Under the **[Option]** key for each driver, create a DWORD value called **ProxyAccess**.
3. Right-click on **ProxyAccess** and select **Modify**.
4. Enter one of the following values:
    - 1 (direct access to internet)
    - 4 (no autoproxy, startup, or Internet Setup (INS) file)

Configuring the Drivers

The Worldpay Driver setup is not done until the VNS and VNA 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 with the Host Processor.

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.

Frequently Asked Questions

Why do I have to take down the entire system when loading the new credit card drivers?

When loading any type of software, the standard is to turn off all running applications during installation. Oracle recommends turning off the RES system completely during the installation. The installation program only requires those applications that use the credit card drivers to be turned off (i.e., POS Configurator, Credit Card Server, Credit Card Utility).

What happens if I forget to shut down the Credit Card Server or the system?

If run properly, the Worldpay Driver Installation program does not require a reboot of the RES Server.

However, it is necessary when an application that uses the Worldpay Drivers is left on during the Worldpay Driver Installation. In this case, the program will not overwrite the existing files, but will store the new files in a temporary location. Once the installation is complete, the user will be prompted to reboot the system. Only then will the new driver files be copied from the temp folder to their proper location.

Why is reading the Credit Card Transfer Report so important?

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

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

What is a credit card batch?

Oracle 3700 POS allows credit cards to be authorized throughout the day. This authorization process is done when a guest asks to pay his transaction with his credit

card. The POS then stores that credit card information along with the transaction in the RES database.

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

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

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

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

- Credit card number
- Expiration date

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

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

Terminal-based processing requires that the entire batch be successful for the batch to be closed. Most of the 3700 POS drivers support terminal-based processing. The Worldpay 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?

Duplicate batches 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 Worldpay Credit Card Driver for the prevention of duplicate batches. Now, when an Open Batch request is initiated, a processor batch number (which is different from the Oracle batch sequence number) is assigned. This number is saved in the registry and reused for any subsequent settlement attempts of the same batch sequence number.

The change provides the Credit Card Driver with all of the information needed to prevent duplicate batches. By persisting the status of each batch settlement attempt in the registry, the driver can refuse to re-settle a batch that has either ended in a communication error after the batch close request was sent, or was successfully settled but did not receive a good batch confirmation.