ORACLE

Oracle Hospitality RES 3700

Heartland Direct Driver Version 5.1

July 2016

Installation and Setup

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

Before installing this driver, please familiarize yourself with the changes by reviewing the ReadMe First Section of this document.

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

In This Section...

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 independant 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 (5.1).exe
3. Shutdown all Oracle applications from the MICROS Control Panel.
4. Double click the CaHL(5.1).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

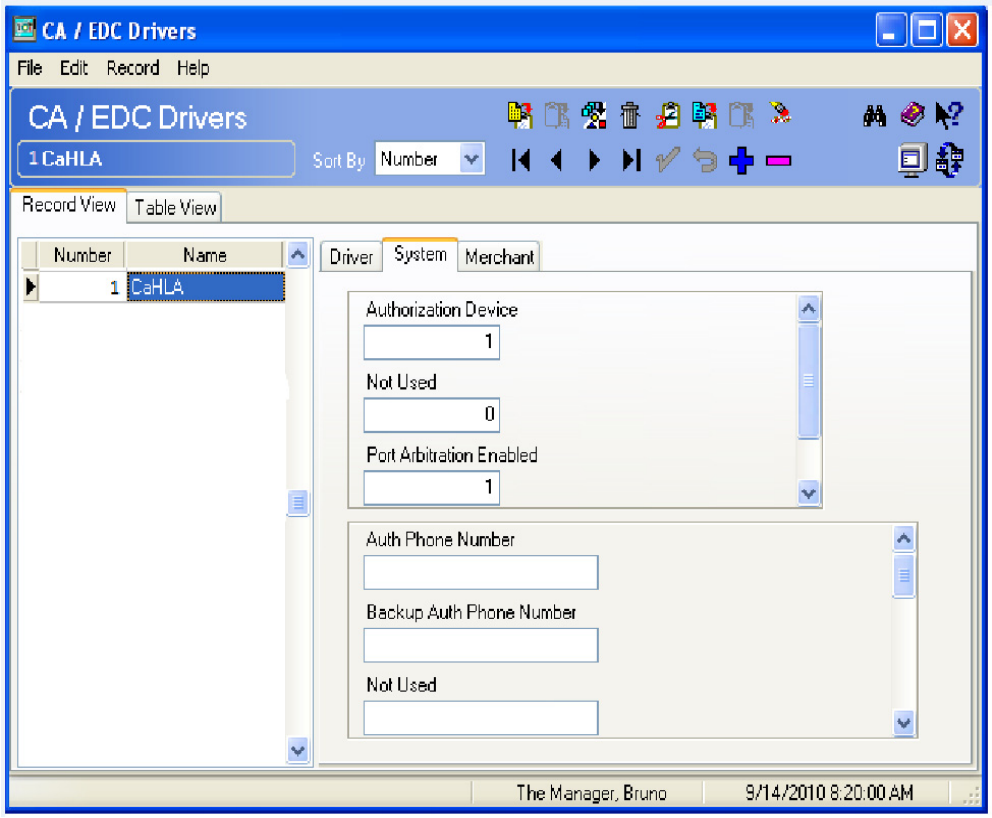
Configuring the Drivers

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.

Note: 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 (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

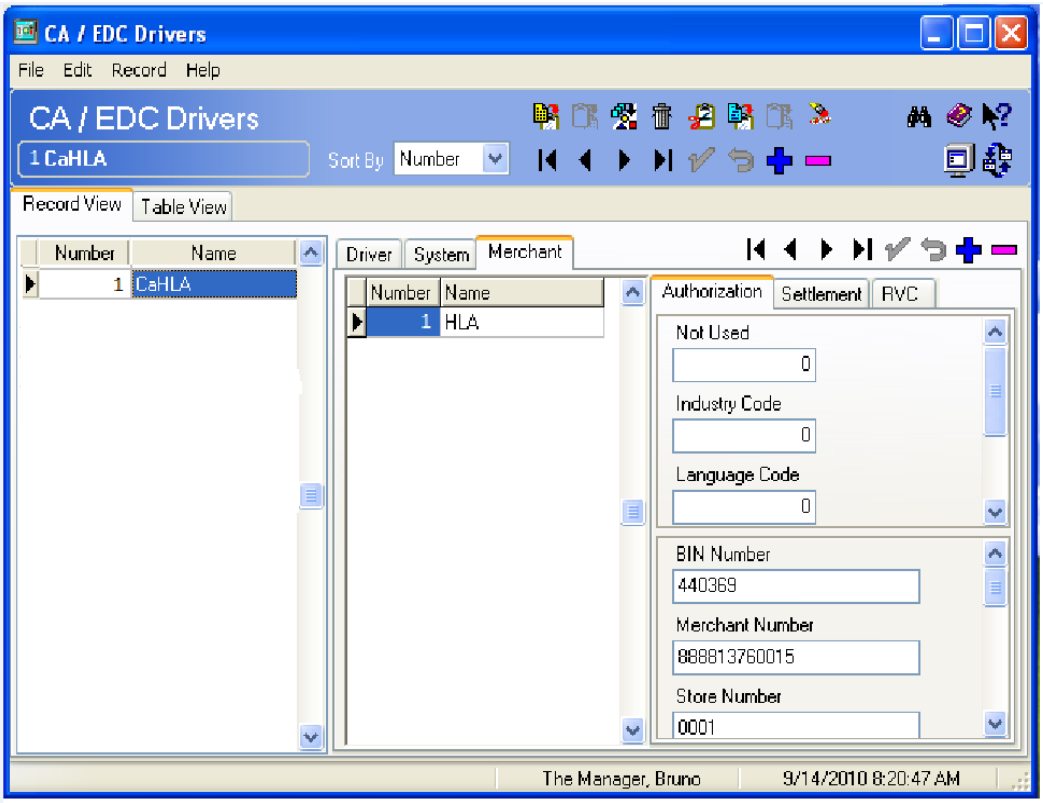
are triggered when the system cannot establish communication via the primary host address.

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.

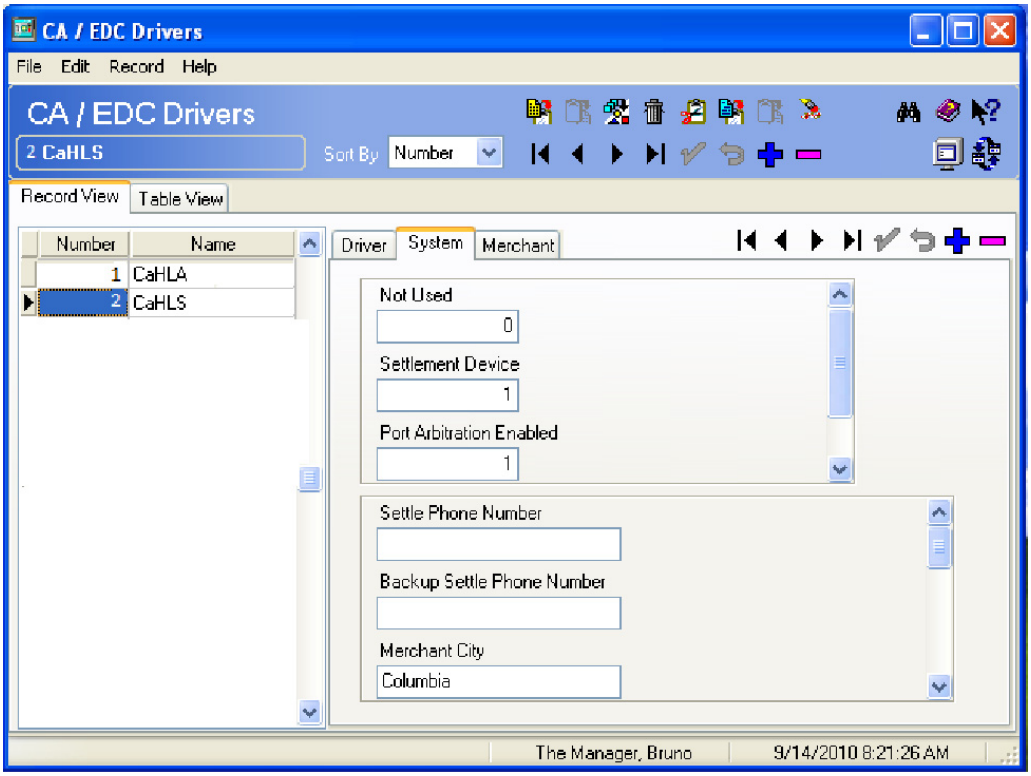
Merchant City - Enter the name of the city where the merchant is located.

***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.

Note: 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.

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 - 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 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 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

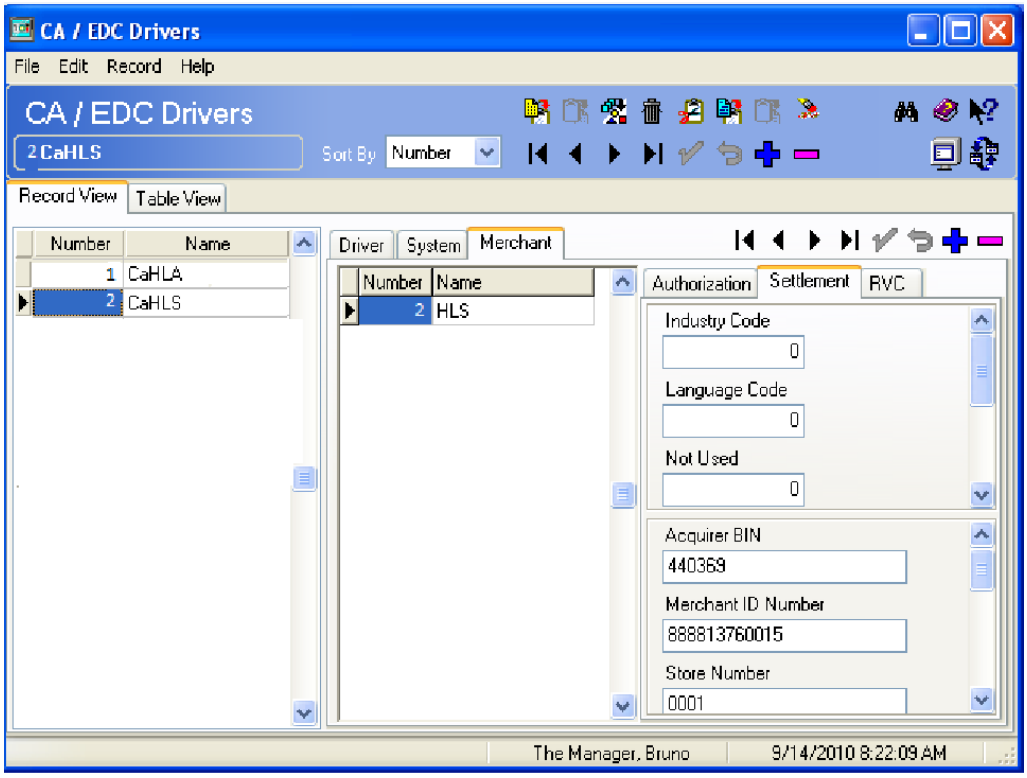
BackUP URL Part 1 - Enter the first part of the URL address of the backup host connection. This consists of the protocol and the site name. Backup connections are triggered when the system cannot establish communication via the primary host address.

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.

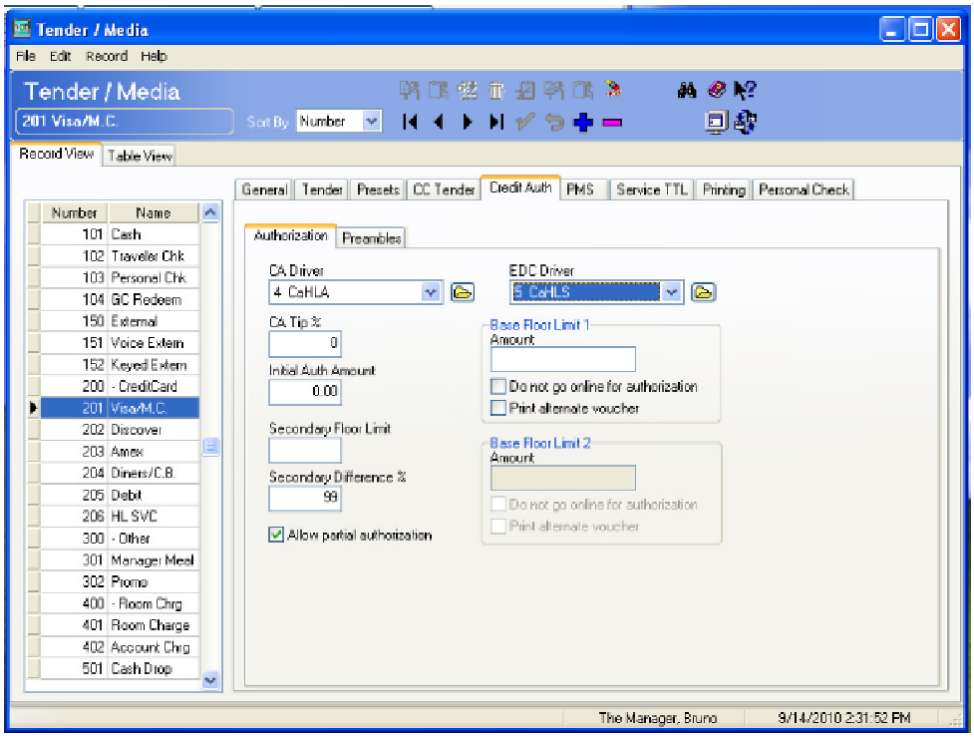
Agent Number - Enter the 6-digit number that identifies the merchant. This number is assigned by the Credit Card Processor.

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

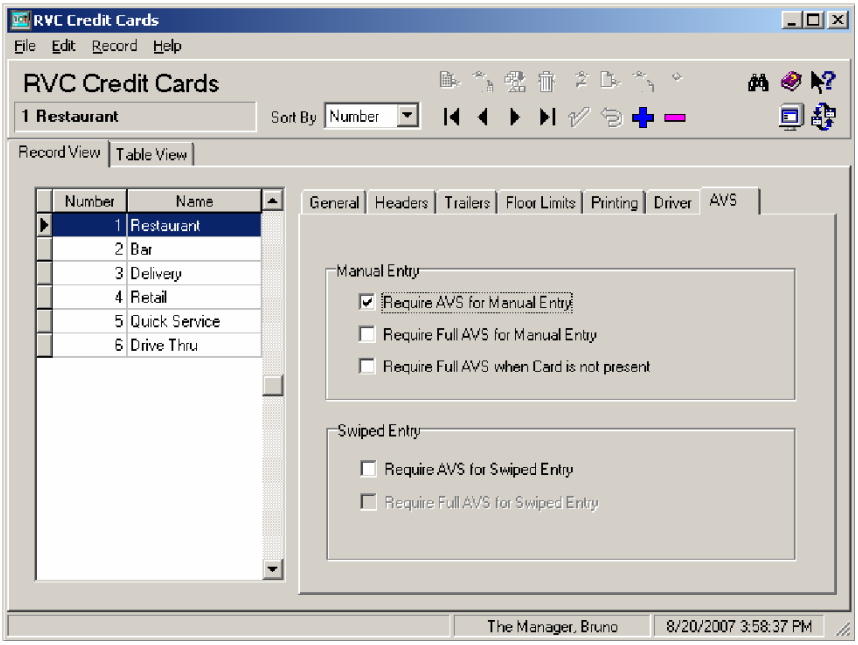
Card Processor. Unless specified otherwise by the merchant's bank or processor, the default for this field should be 00001.

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.

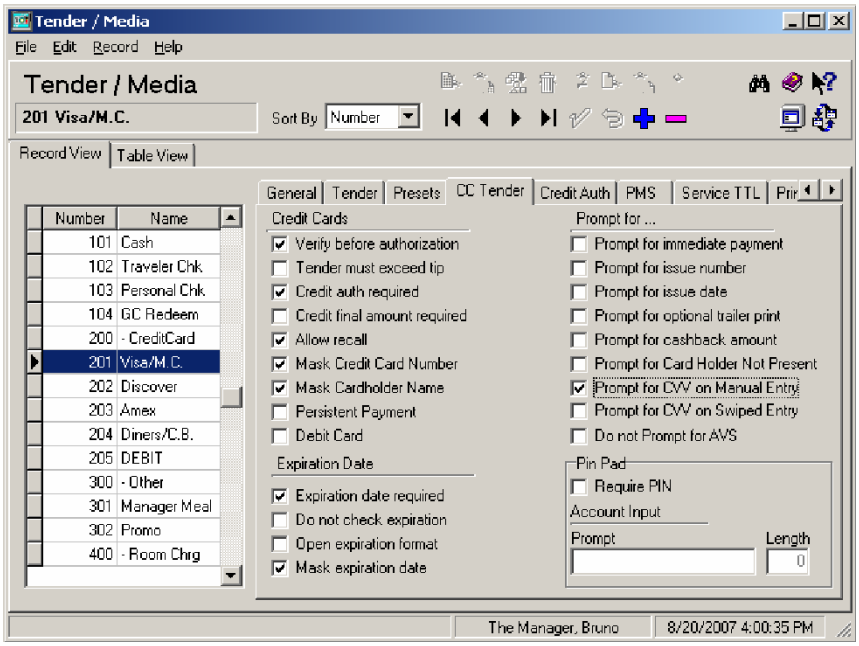
- **Require Full AVS for Manual Entry**. Select this option to prompt for the cardholder's address AND zip code before submitting a manual credit card authorization. This option is only enabled if the **Require AVS for Manual Entry** option is enabled.

- **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.

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.

(1.) Intentionally not provided

(2.) Present and will be provided

(3.) Present but is illegible

(4.) 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.

(1.) Intentionally not provided

(2.) Present and will be provided

(3.) Present but is illegible

(4.) Not present.

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.

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.

ReadMe First
V. 5.1

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 5.1 release of the Heartland Driver.

In This Section...

What's New

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

New Features Summarized

The following table summarizes the new features included in this version:

Feature	Page
Added support for Transport Layer Security 1.2 encryption protocol	21
Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols	21

New Features Detailed

Added Support for Transport Layer Security 1.2 Encryption Protocol

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

Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols

Version 5.1 of the Heartland Driver removes support for all encryption protocols other than TLS 1.2. You must make sure your payment processor accepts TLS 1.2 transactions before upgrading to this version.

What's Enhanced

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

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

Enhancements Summarized

There are no enhancements included in this release.

What's Revised

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

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

Revisions Summarized

There are no revisions included in this release.