Oracle Hospitality RES 3700

American Express Authorization Driver Version 5.1

July 2016

**********IMPORTANT**********

The American Express Credit Card Driver is only for authorization. The site must have a compatible settlement driver installed.

****

Installation and Setup

This section contains installation and setup instructions for the release of the American Express (AMEX) Authorization 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 American Express may be used on RES systems running Version 5.0 or higher.

In This Section...

- Installation 3
  - Site Requirements 3
  - Files Included 3
  - Installation Instructions 4
- Setup. 5
  - Configuring the Drivers. 5
  - Configuring the CaAMEX Driver 5
  - Configuring Intermediate Certificates 8

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 independant 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 (5.1).exe
3. Shutdown all Oracle applications from the MICROS Control Panel.
4. Double click the CaAMEX(5.1).exe.
5. Turn on the RES System from the MICROS Control Panel.
6. Configure the drives. Follow the setup starting on page 5.

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

Setup

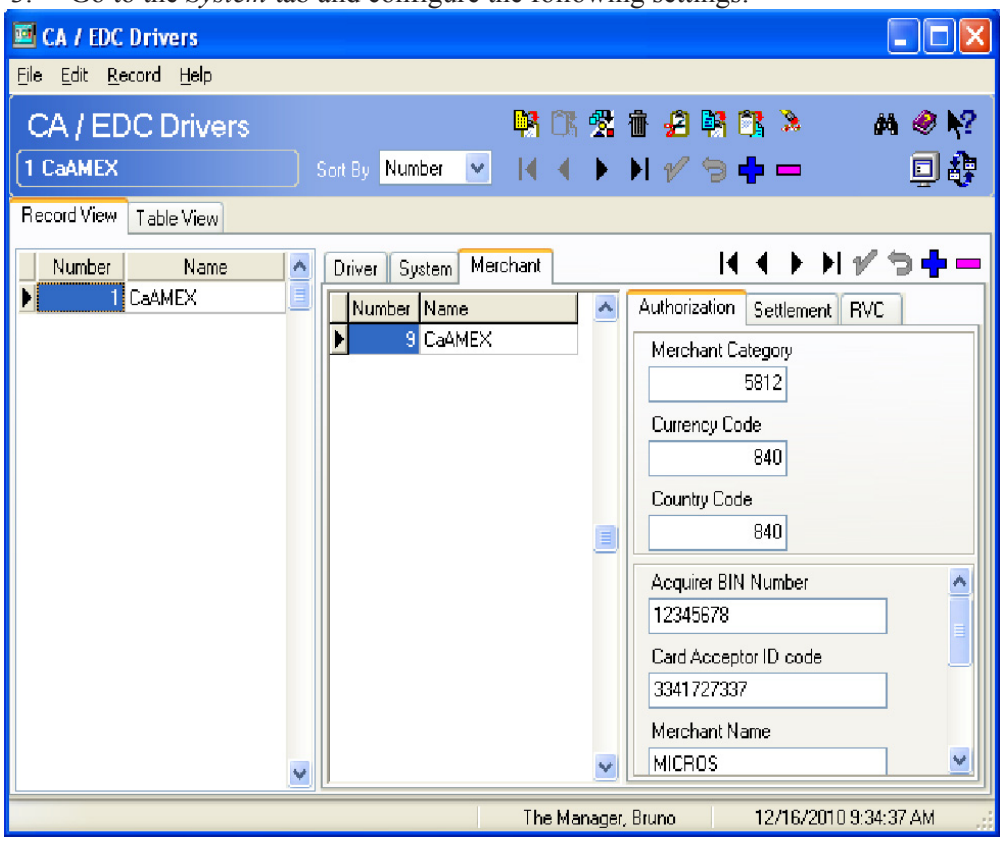
Configuring the Drivers

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**.

- 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.

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:

- 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.

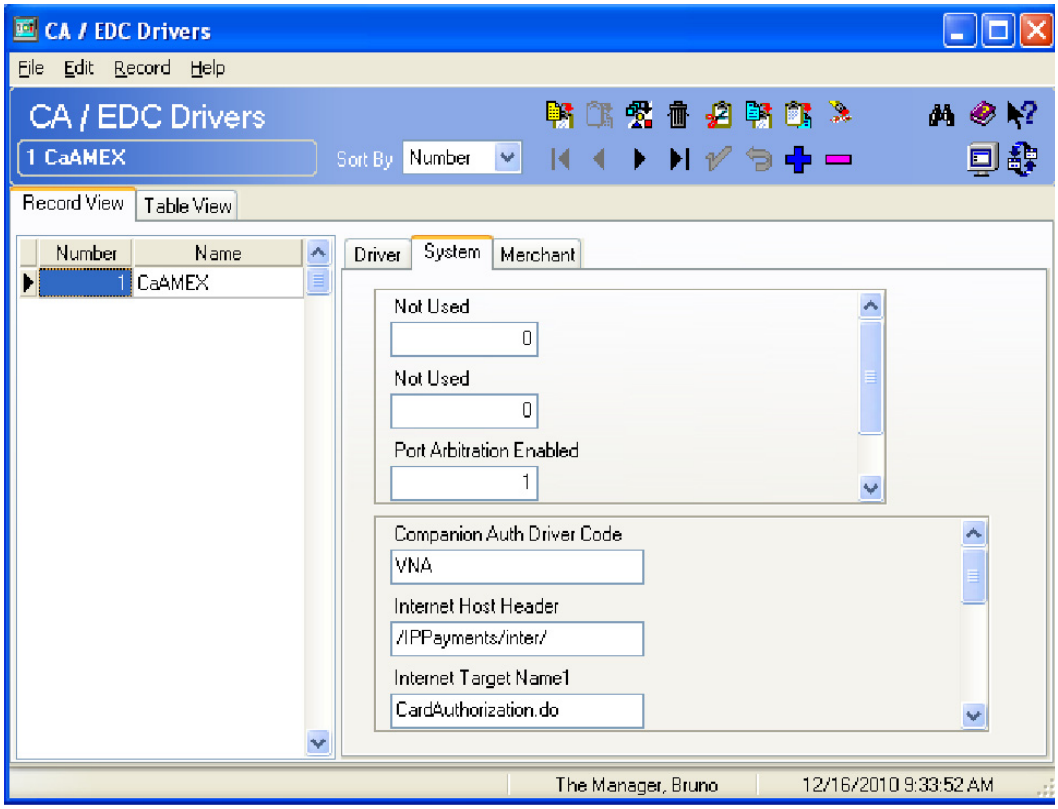
Host URL Part1 – Enter the first part of the URL address of the primary host connection. This consists of the protocol and site name.

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.

ReadMe First
V. 5.1

This section contains a comprehensive guide to the Version 5.1 release of the American Express (AMEX) Authorization Credit Card Driver.

In This Section...

- What's New 10
  - Summarized 10
  - Detailed 10
- What's Enhanced 11
  - Summarized 11
- What's Revised 12
  - Summarized 12

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	10
Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols	10

New Features Detailed

Added Support for Transport Layer Security 1.2 Encryption Protocol

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

Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols

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

What's Enhanced

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

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

Enhancements Summarized

There are no enhancements included in this release.

What's Revised

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

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

Revisions Summarized

There are no revisions included in this release.