ORACLE

Oracle Hospitality RES 3700

FDMS North (CaFDMS) Credit Card Driver Version 5.1

July 2016

Installation and Setup

This section contains installation and setup instructions for the Version 5.1 release of the CaFDMS North Credit Card Driver.

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.

In This Section...

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 dial-up 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. For more information see the *Usage* section on page 17.

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_5.1.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 5.1_MD.pdf**).
   - CaFDMS North Driver Executable (**CaFDMS(5.1).exe**).
3. Shutdown all Oracle applications from the MICROS Control Panel and turn the Database to off.
4. Copy the **CaFDMS(5.1).exe** to a TEMP directory on the RES Server.
5. Double-click on the **CaFDMS(5.1).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. Please continue to page 8 for steps on how to configure the credit card driver.

Setup

Communication Channels

Communication Channel can be configured on the *POS Configurator* | *Devices* | *CA/EDC Drivers* | *FDMS North* | *System* form. Communication Channel configuration is explained in the *Configuring the Driver* section of this document on page 8.

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. More information is available on this connection type in the *Datawire Communications Channel* section of this document on page 53.

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.

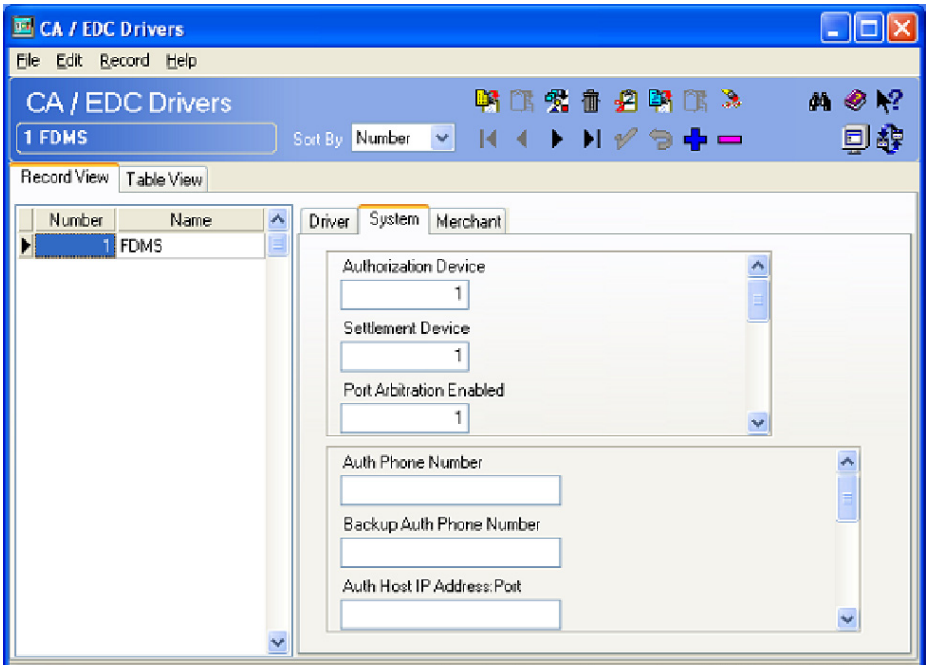
For example, suppose the Mike Rose Cafe is using the CaFDMS North Driver and has configured TCP/IP as their communication channel. Their fallback connection is dial-up. At the end of the night they attempt to settle a batch with the processor. Initially the TCP connection works during the Batch Open 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:

> ***Note*** *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. Select the blue plus sign to add a record.
3. Enter a **Name** for this record and its corresponding code in the **Driver Code** field (e.g., **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.

  Note: 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 (e.g., 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:

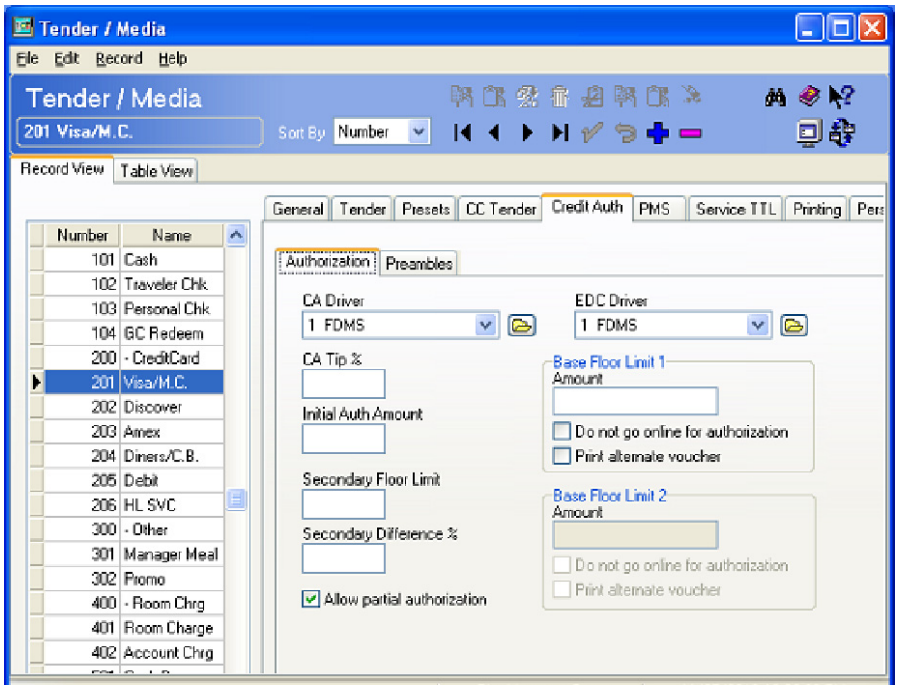
  – Do not include hyphens

  – 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.

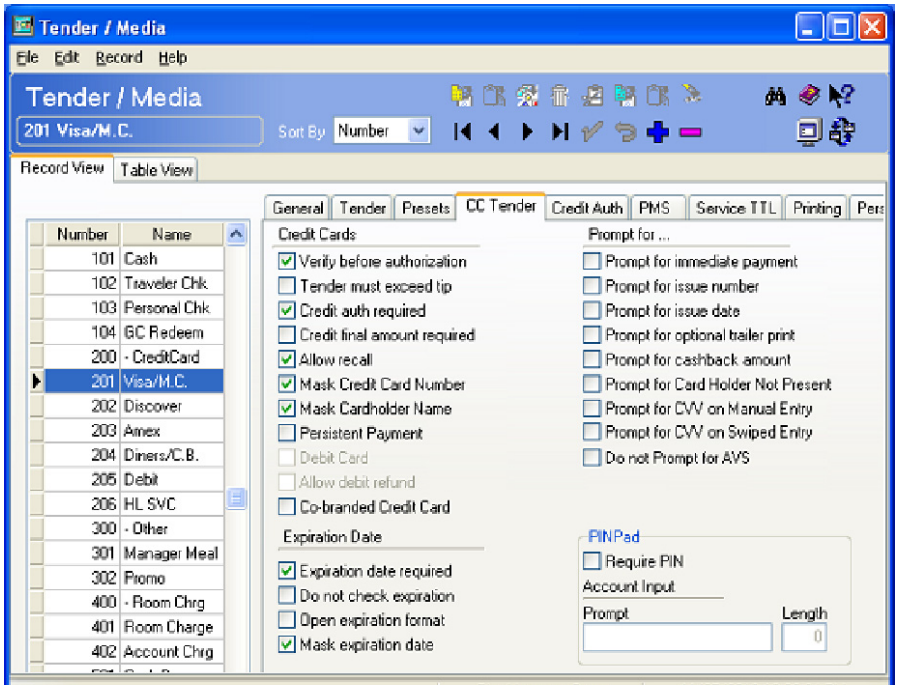


Go to the following fields and select **FDMS** from the drop down box:

- **CA Driver**

- **EDC Driver**

7. Go to the *CC Tender* tab and enable the following options. Configure other CC options as needed:



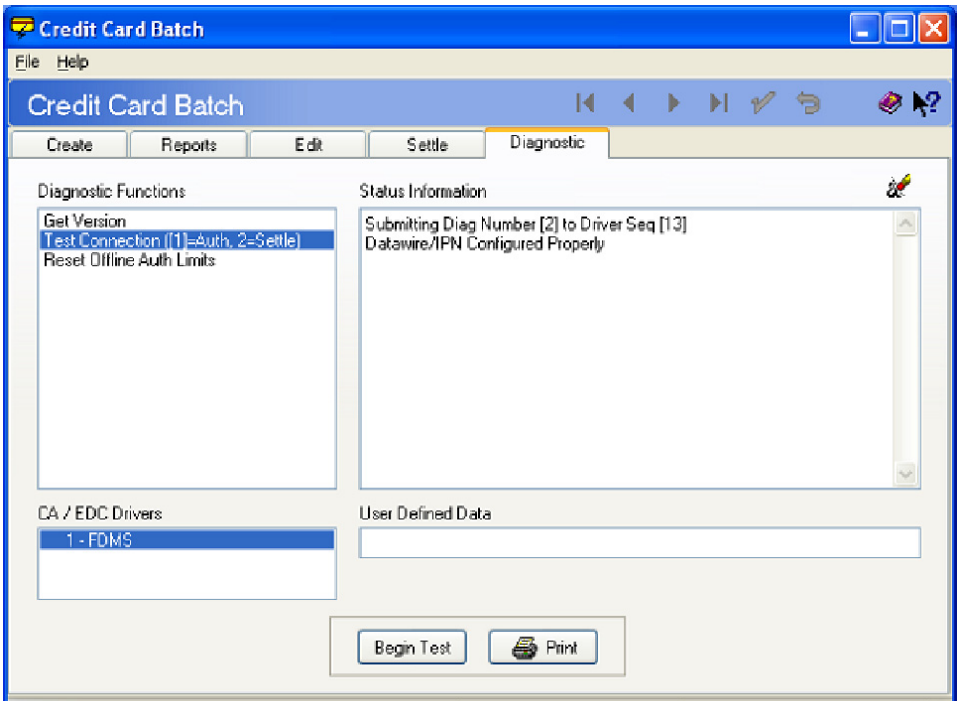
- **Verify Before Authorization**
- **Credit Auth Required**
- **Expiration Date Required**
- **Mask Credit Card Number**
- **Mask Cardholder Name**
- **Mask expiration date**

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:

    - Go to the *MICROS Applications* | *POS* | *Credit Card Batch* | *Diagnostic* tab and select the CaFDMS North driver.



    - Select the **[Test Connection]** button.
    - 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:

    1. On the RES Server select *Start* | *Run* and enter **Regedit**. Click **[Ok]**.
    2. Navigate to the following location of the CaFDMS driver number: *HKLM\Software\MICROS\Common\CCS\DrvrCfg\DrvrX\Support*
    3. Highlight the *Support* folder and select *File* | *Export.*

4. 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.*

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

6. Copy the registry file from the location designated in step 5 to the BSM client's TEMP directory.

7. 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.

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

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

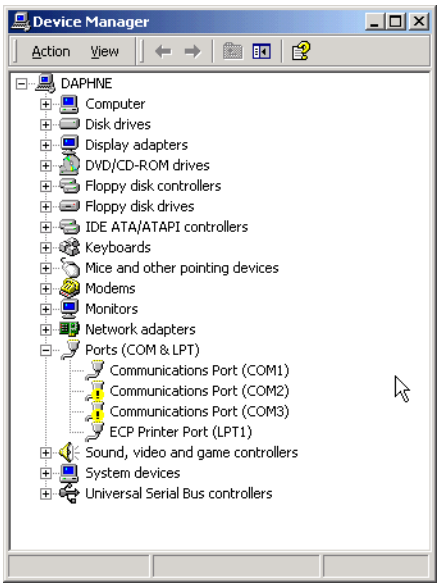
12. Bring the system back to Front-of-House status using the Control Panel.

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 (right).

   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

1. In POS Configurator, select *Devices* | *Devices* | *Network Nodes*. Go to the *Comm Port* tab and set the following options:
   - **Comm 1** — 1200
   - **Parity** — Even
   - **Num Data Bits** — 7
   - **Num Stop Bits** — 1

> ***Note*** *ComPORT 4 or 5 can also be configured on the PINPad using the separate cable.*
>
> *This is only available if the site is running RES 3.2 SP7 HF6 or higher, or RES 4.1 HF2 or higher.*

Confidence Testing

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

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

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

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).

ReadMe First
V. 5.1

This section contains a comprehensive guide to the Version 5.1 release of the CaFDMS North Credit Card 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	19
Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols	19

New Features Detailed

Added Support for Transport Layer Security 1.2 Encryption Protocol

Version 5.1 of the FDMS North Credit (CaFDMS) 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 FDMS North Credit (CaFDMS) 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

The following table summarizes the revisions included in this version.

TPID	CR ID	BUGDB	Revision
110097	36776	22249149	Zero Dollar Account Validation no longer returns the *Declined error.
118971	NA	NA	Keyed transactions now process correctly when the Tender Media/CC Tender option **Prompt for Card Holder Not Present** is enabled and the POS Operations user clicks **Yes** to specify that the card is not physically present. If the option is enabled but the prompt does not appear, make sure you are not overriding the prompt with the Revenue Center/RVC Credit Cards option **Disable Prompt for Card Holder Not Present**.