micros

Restaurant Enterprise Series

FDMS North (CaFDMS) Credit Card Driver for 3700 POS Version 4.11

February 6, 2013

MD0003-102

Declarations

Warranties

Although the best efforts are made to ensure that the information in this manual is complete and correct, MICROS Systems, Inc. makes no warranty of any kind with regard to this material, including but not limited to the implied warranties of marketability and fitness for a particular purpose. Information in this manual is subject to change without notice. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information recording and retrieval systems, for any purpose other than for personal use, without the express written permission of MICROS Systems, Inc.

MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Trademarks

Adobe FrameMaker is a registered trademark of Adobe Systems Incorporated.

The following are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries;
Operating Systems - Windows® 7, Microsoft Windows Server® 2008 R2, Microsoft Windows Server® 2008, Microsoft Windows Server® 2003 and Windows® XP.
Database Platforms - Microsoft SQL Server® 2008 R, Microsoft SQL Server® 2008 and Microsoft SQL Server® 2005.
Other products - Microsoft Excel, Win32 and Windows® CE.

Visio is a registered trademark of Visio Corporation.

All other trademarks are the property of their respective owners.

.

Installation and Setup

This section contains installation and setup instructions for the Version 4.11.21.2420 release of the CaFDMS North Credit Card Driver.

This version of the driver may be used on RES systems running Version 4.5 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 4.5 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 Micros 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. MICROS 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_4.11.21.2420.zip** file from the MICROS 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 (**CaFDMSV4.11_MD.pdf**).
   - CaFDMS North Driver Executable (**CaFDMS(4.11.21.2420).exe**).
3. Shutdown all MICROS applications from the MICROS Control Panel and turn the Database to off.
4. Copy the **CaFDMS(4.11.21.2420.exe** to a TEMP directory on the RES Server.
5. Double-click on the **CaFDMS(4.11.21.2420).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.

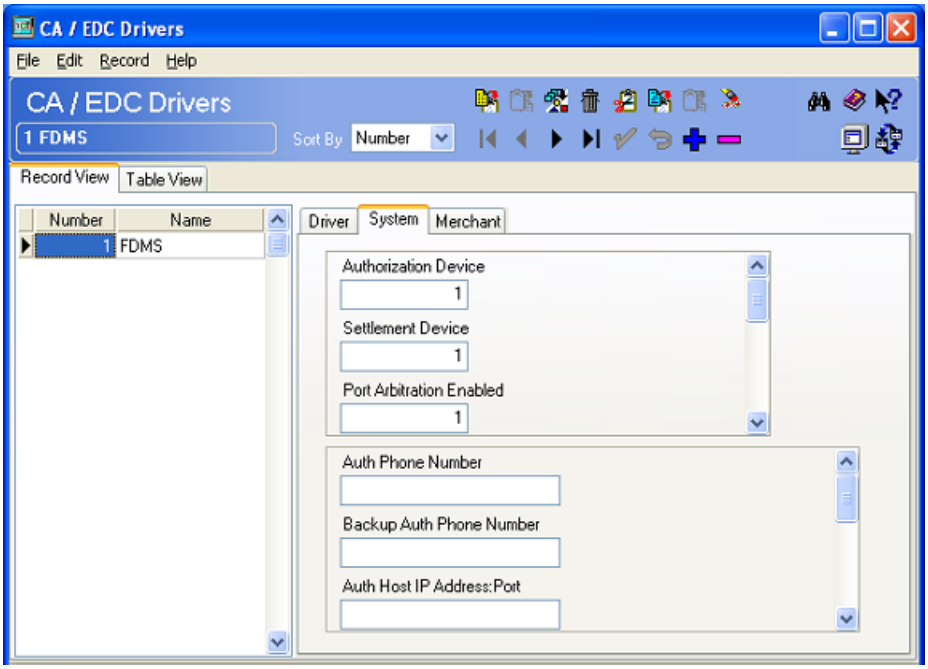
For example, suppose the Mike Rose Cafe is using the CaFDMS North Driver and has configured TCP/IP as their communication channel. Their fallback connection is dial-up. At the end of the night they attempt to settle a batch with the processor. Initially the TCP connection works during the Batch Open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

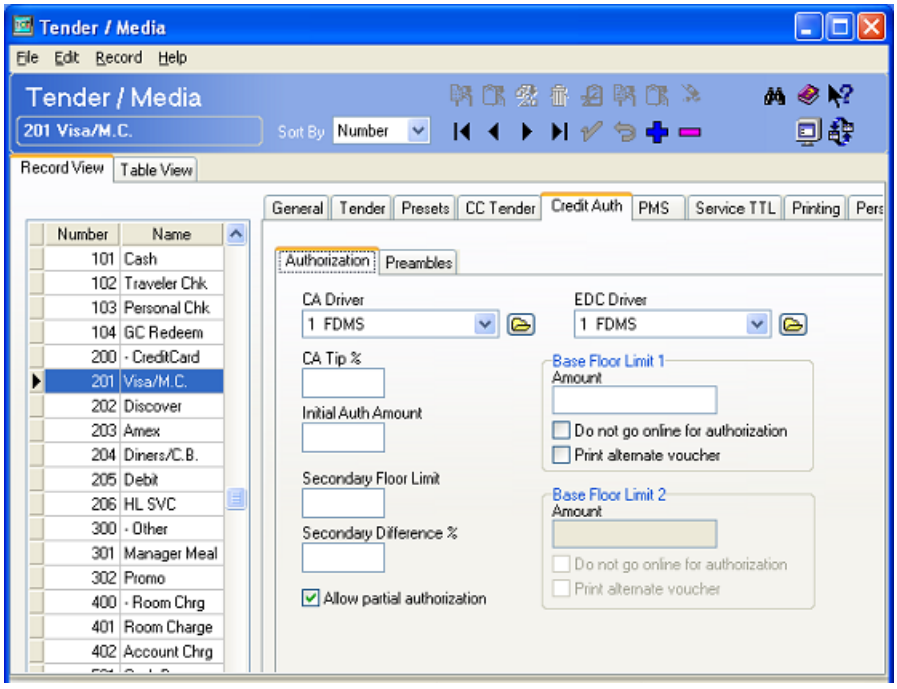
5. Go to the *Merchant* tab. All fields on this tab should be completed using the settings provided by the bank. The following fields must be configured:

   - **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.

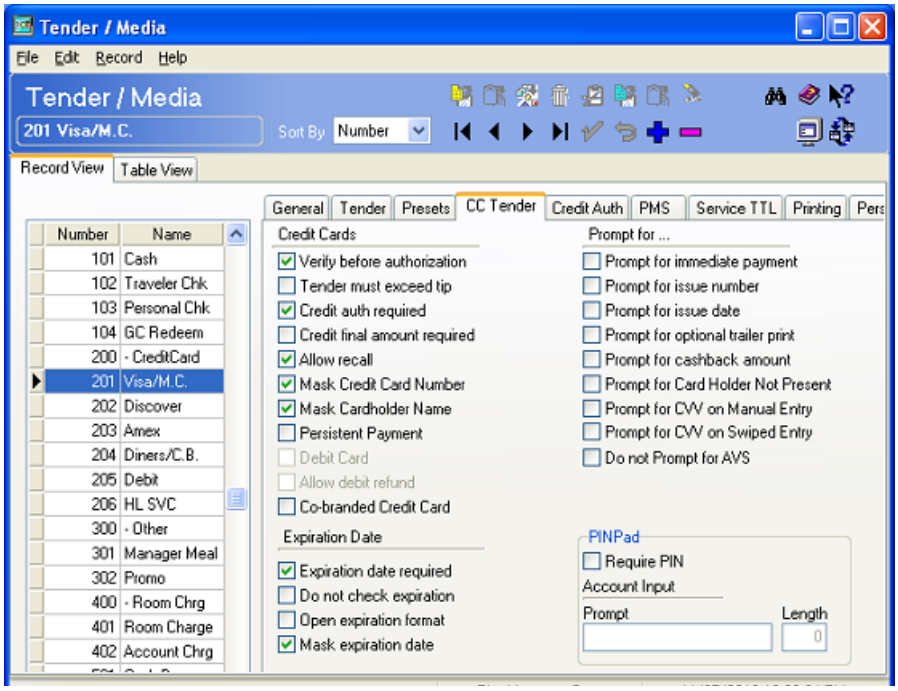


Go to the following fields and select **FDMS** from the drop down box:

- **CA Driver**

- **EDC Driver**

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



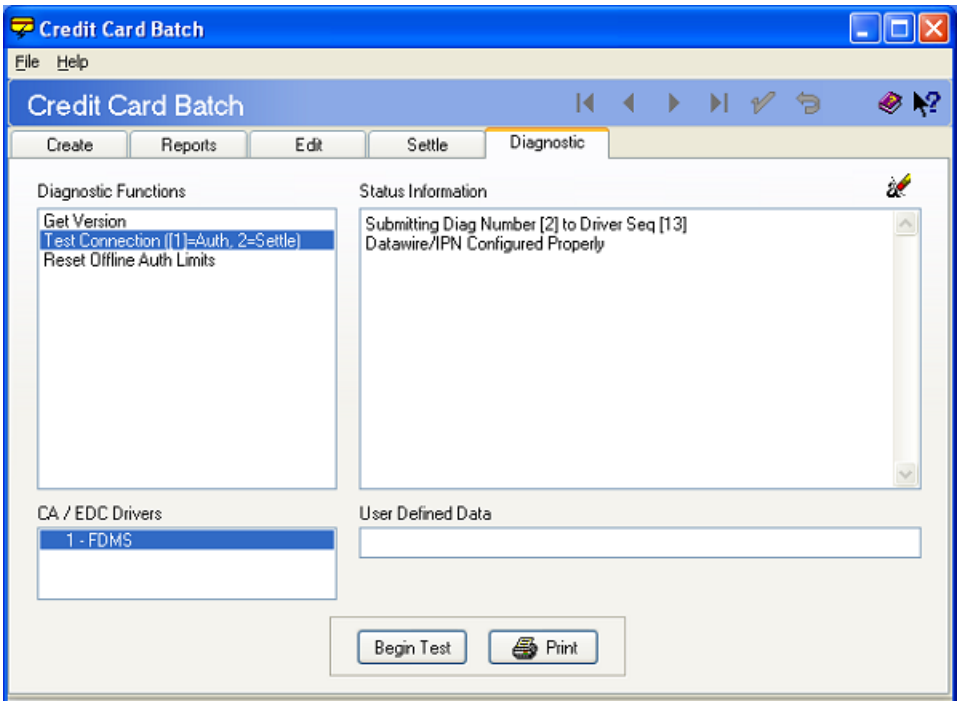
- **Verify Before Authorization**
- **Credit Auth Required**
- **Expiration Date Required**
- **Mask Credit Card Number**
- **Mask Cardholder Name**
- **Mask expiration date**

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 MICROS 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.

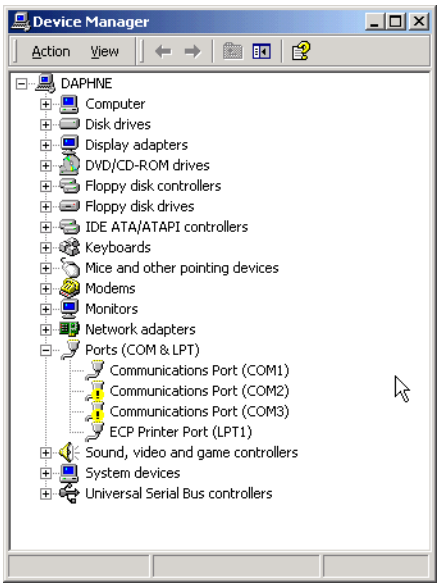
12. Bring the system back to Front-of-House status using the Control Panel.

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.*

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).

Licenses

This driver is subject to the following license agreements:

- OpenSSL License
- SSLeay license

The terms of both licenses are listed below:

OpenSSL License

Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).” The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com).”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

ReadMe First
V. 4.11.21.2420

This section contains a comprehensive guide to the Version 4.11 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

New Features Detailed

FDMS Now Supports eCommerce Transactions

CR ID #: N/A

Support has been added for eCommerce transactions. 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 the ResPosApi, they will have a flag set that distinguishes them as eCommerce.

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

The following table summarizes the enhancements included in this version.

Enhancements Detailed

Open SSL Libraries have been Updated

CR ID #: N/A

With this release, the Secure Sockets Layer (SSL) Libraries (libeay32.dll and ssleay32.dll), which are used when Communication Channel 2 (Internet) is enabled, have been updated to version 1.0.0.4.

Support Updated Datawire DLL

CR ID #: N/A

With this release, the Datawire dll has been updated to version 4.6.0.0. The driver will now support RES installs on Windows 7 Operating Systems.

Support Zero Dollar Account Verification

CR ID #: N/A

With this release, the driver now supports a zero-dollar initial credit card authorization. The use case for initial auths is the bar tab scenario. 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 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.

Authorization Reversal Support Updated

CR ID #: N/A

With this release, authorization reversals are now supported. Card associations are now mandating that merchants submit authorization reversals for fully-approved or partially-approved transaction that will not be settled.

The authorization reversal transaction negates the approved amount that has been 'on hold' on the cardholder's account. It is intended as a clearing transaction that will release the customer's open-to-buy.

For example:

Authorizations on a guest check that receive an Auth Code but are then closed to Cash; will now be reversed at Settlement time. This occurs during the Pre-Settlement Process.

In the case of multiple authorizations for the same account on a single guest check (i.e.-secondary auths), the 'best' authorization is used to settle the transaction and the remaining authorizations on this check will be reversed.

Only authorizations that receive an Auth Code will be reversed. Manual Athorizations, Auto-offline Auths, Below Floor Limit Offline auths, and Zero Dollar Account Verification auths will not be reversed.

Note	*Authorization reversals are only supported in RES Version 4.5 or higher.*

Diners Club International Processes on Discover Network

CR ID #: N/A

With this release, the Diners Club International (DCI) Credit Cards will be active on the Discover Network. With the Credit Card Server verbosity set to 5, the 3700d.log and will show all DCI transactions with a **Card type = [DISCOVER]**.

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 table below lists the revisions included in this release:

Feature	CR ID #	Page
FDMS Driver Does Not Try to Reconnect or Connect to Backup before Using Dial-up During Settlement	28691	26
FDMS Driver Settlement Option Merchant Type Not Used	N/A	26
Credit Card Batch Report Does Not Always Show Reversals	N/A	27

Revisions Detailed

FDMS Driver Does Not Try to Reconnect or Connect to Backup before Using Dial-up During Settlement

CR ID #: 28691

Previously during settlement, if the FDMS North Driver was connected to the primary **(Settle Host IP Address:Port)** and for any reason the connection was lost, the driver would fall back to dial-up instead of using the **Backup Settle IP Address:Port**.

If the driver lost the connection or did not receive a response from the host, the next request receive from the POS would immediately fall back to dial-up instead of re-establishing a TCP connection. This has been corrected.

FDMS Driver Settlement Option Merchant Type Not Used

CR ID #: N/A

The FDMS Settlement Driver has an option called **Merchant Type** *(POS Configurator | Devices | CA / EDC Drivers | Merchant)* that corresponded to

merch_num03 in the CaFDMS.cfg file. This field was not used being used in the driver. Now that the **Merchant Type** option has been changed to correspond to merch_01 in the CaFDMS.cfg file, it is now used by the driver.

Credit Card Batch Report Does Not Always Show Reversals

CR ID #: N/A

Previously, The Credit Card Batch Report would only show the reversal number if there were reversals in the batch. This has been changed to always show the reversal count, even if the count is 0.

ReadMe First
V. 4.8.20.2196

This section contains a comprehensive guide to the Version 4.8 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
FDMS Now Reports Failed Settlement Record Numbers	29

New Features Detailed

FDMS Now Reports Failed Settlement Record Numbers

CR ID #: N/A

When a settlement record is rejected by FDMS, the driver now reports 'Batch detail record [n] rejected' on the batch settlement report. The number reported is the record number in the batch. For example, if records are omitted from the batch and record 5 is the second record transmitted which is rejected, it still reports as 'Batch record 5 rejected', not number 2. This makes it easier to find in the settlement GUI if the record needs to be omitted.

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 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 table below lists the revisions included in this release:

Feature	CR ID #	Page
FDMS Driver Would Send Incorrect PIN Capability Code Causing Debit Transactions To Result in Host Error From A Vx670 Device	N/A	31

Revisions Detailed

FDMS Driver Would Send Incorrect PIN Capability Code Causing Debit Transactions To Result in Host Error From A Vx670 Device

CR ID #: N/A

Previously, the FDMS North Driver would send an incorrect POS Code of 902 instead of 901 when a Vx670 PIN Debit Device was used. The 2 in 902 means that the terminal would not have PIN Capability when sending a PIN Debit.

This was conflicting data and NYCE would return a Format Error response on the PIN debit transactions. This debit request code number was only incorrect from the Vx670. Any transactions performed in POS Operations, from a tethered PIN Pad, were correct. This has been corrected.

ReadMe First
V. 4.7.20.2216

This section contains a comprehensive guide to the Version 4.7 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
Auto Offline Credit Card Authorization Support Introduced	33
Partial Auth Support for Prepaid Credit Cards Introduced	37
FDMS Now Supports Visa 62.23 Card Level Results and AMEX CAPN	38
RFID Transactions Now Supported	38
Duplicate Batch Prevention	38

New Features Detailed

Auto Offline Credit Card Authorization Support Introduced

CR ID #: N/A

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 IP addresses and through dial backup.
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.

6. The **Auth Offline Transactions** option (*Devices* | *CA/EDC Drivers* | *System*) was added to the FDMS settlement driver to control how these transactions are handled at settlement.

   - By default the option is disabled, and the settlement driver will treat these transactions as manually keyed and manually authorized transactions, and will attempt to settle them as though they were regular manual authorizations. ***Note:*** *If these records fail to settle, they will cause the entire batch to fail to settle.*
   - With the option enabled the settlement driver will attempt to obtain a real 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.

7. 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 can not both appear for the same transaction.

8. 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. ***Note:*** *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.

FDMS Driver Configuration

To prevent a restaurant from being offline for an extended period without being aware of the network outage, the following options were added to the FDMS driver.

- **Max offline transactions** (*Devices* | *CA/EDC Drivers* | *System*). This option controls the maximum number of automatic offline transactions that can be processed by the driver.
- **Max offline amount** (*Devices* | *CA/EDC Drivers* | *System*). This option controls the maximum dollar value of automatic offline transactions that can be processed. The maximum cumulative offline amount is entered as dollars (e.g., 2500 is the equivalent of $2500.00).

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.

POS Configuration

To support this functionality, the following options were added 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.

Partial Auth Support for Prepaid Credit Cards Introduced

CR ID #: N/A

With this release, support has been added for the RES partial authorization feature, which permits a site to accept prepaid credit cards more conveniently and reliably

This credit card driver feature is only available when used in conjunction with RES v 4.3 hot fix 2 or RES v 4.5 or greater. For information on how to configure this feature in RES, see the *RES v 4.3 hotfix 2 Documentation*.

FDMS Now Supports Visa 62.23 Card Level Results and AMEX CAPN

CR ID #: N/A

The FDMS credit card driver has been enhanced to support Visa 62.23 (Card-Level Results) and AMEX CAPN which includes support for POS Data Codes.

RFID Transactions Now Supported

CR ID #: N/A

RFID transactions are now supported by the FDMS credit card driver when used in conjunction with RES v 4.5 and the Mx870 device.

An RFID credit card transaction occurs when a credit card authorization is performed by reading the card's data via an RFID chip within the card, as opposed to reading the card's magnetic strip in a magnetic card reader.

Duplicate Batch Prevention

CR ID #: N/A

During credit card settlement, certain events can cause a batch to be duplicated and settled more than once. This, in turn, can result in multiple charges to the customer for the same credit card transaction. This feature was designed to prevent the creation of duplicate credit card batches.

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

Enhancements Detailed

Driver Uses Swiped Authorization at Settlement

When there are multiple authorizations associated with an account the FDMS driver currently selects the most recent authorization to send in the settlement record. In most cases the account data source for this authorization will be keyed rather than swiped.

The driver has been enhanced to always look for an authorization with a swiped account data source flag first. If no swiped authorization is found the driver will now select the oldest authorization (with an auth code) rather than selecting the most recent authorization.

Credit Driver Installation now Enters Information into the Registry

To easily determine the credit driver version, the Credit Driver Installation Package now 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')*

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 table below lists the revisions included in this release:

Feature	CR ID #	Page
FDMS Driver Now Reports Failed Settlement Record Numbers	N/A	40

Revisions Detailed

FDMS Driver Now Reports Failed Settlement Record Numbers

CR ID #: N/A

When a settlement record is rejected by the FDMS host, the driver now reports 'Batch detail record [n] rejected' on the Batch Transfer Status Report. The number reported is the record number in the batch. For example, if records 1-3 are omitted from the batch so record 5 is the second record transmitted which is rejected, it will report as 'Batch record 5 rejected', not number 2. This makes it easier to find the rejected record in the Credit Card application if the record needs to be omitted.

ReadMe First
V. 4.5.19.1665

This section contains a comprehensive guide to the Version 4.5 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
AVS and CVV Supported	42

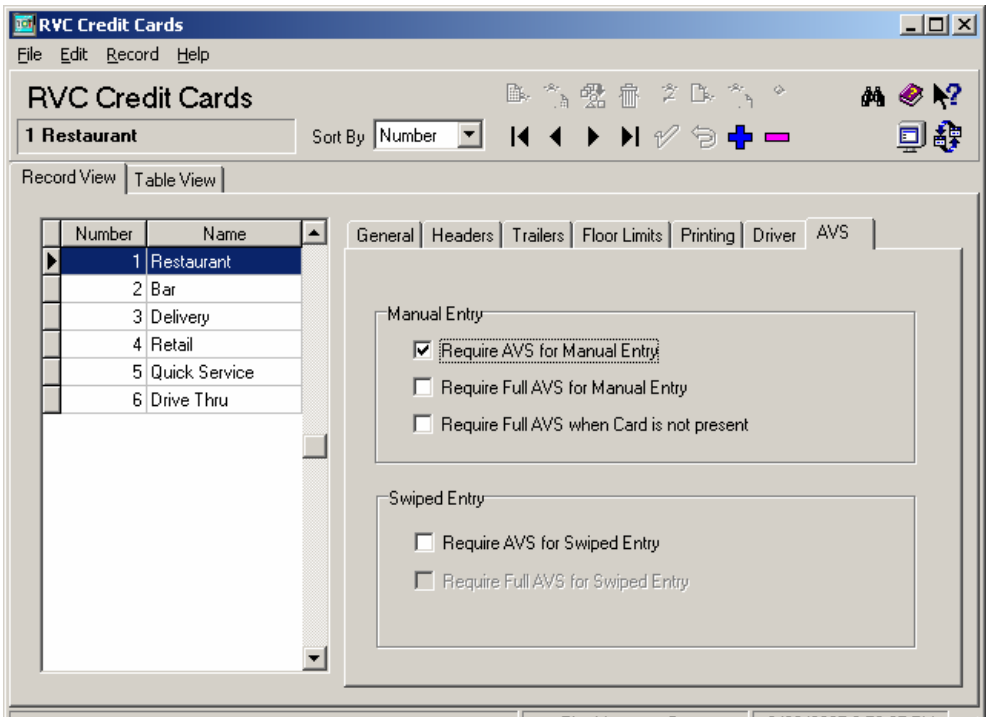
New Features Detailed

AVS and CVV Supported

The CaFDMS has been enhanced to include Address Verification (AVS) and Card Verification Value (CVV) as part of the authorization request.

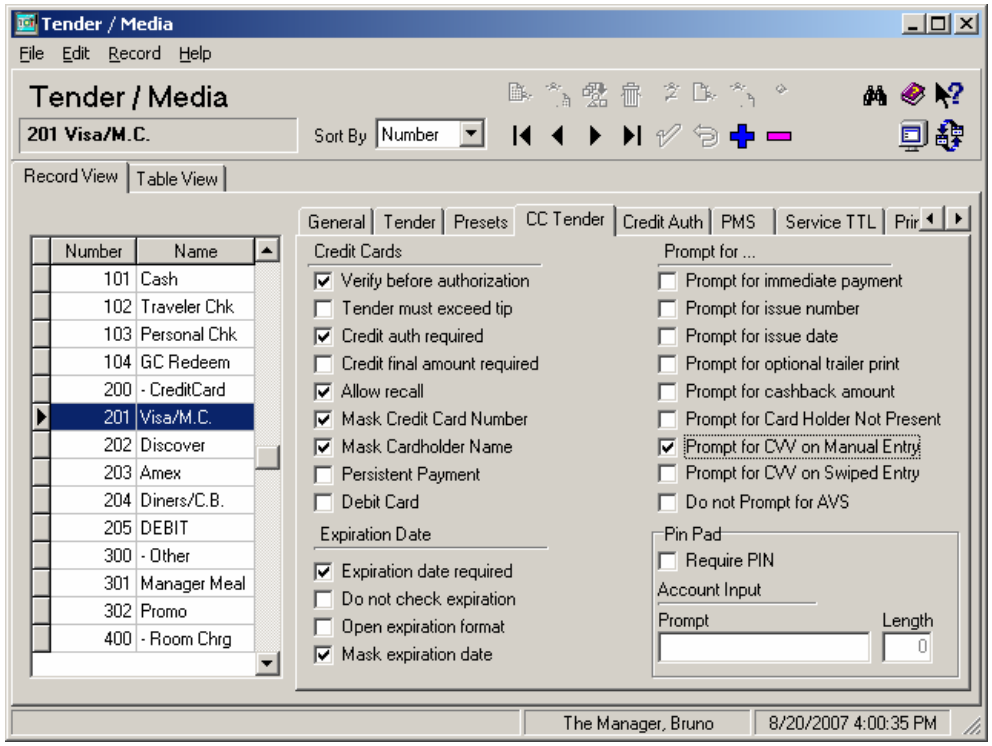
AVS is a system check that matches the address provided in the transaction to the address on file with the bank. CVV is the three or four-digit number listed on the back of the card that provides an additional level of security for the user. AVS and CVV data is transmitted in the Cardholder Identification 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.

This support is only included when the driver is sending authorization requests using the default VisaD format. Custom modes, which use the older VisaK format will ignore CVV and AVS fields.

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

The following table summarizes the enhancements included in this version:

Feature	Page
CaFDMS Driver Supports New Discover Credit Card Numbers	47
Retry Failed Debit Transaction Reversals a Maximum of 3 Times Before Writing to the Text File	47
Support for Authorizations Below $1.00	48

Enhancements Detailed

CAFDMS Driver Supports New Discover Credit Card Numbers

This release of the CaFDMS driver supports the following new Discover credit card number ranges:

Start	End
62212600	62292599
644000	644999
650000	659999

Retry Failed Debit Transaction Reversals a Maximum of 3 Times Before Writing to the Text File

The CaFDMS driver will now retry debit card reversal transactions a maximum of 3 times before writing the transaction data to a text file. Previously, the driver would attempt to re-transmit continuously, interrupting any future transactions.

Now, after the first failure to talk to the host processor occurs, the driver will attempt to re-connect every 20 seconds. After the third try, the driver will cease attempting to connect. At settlement, the reversal information will be written to a text file (e.g., **FDMSFailedReversal.txt)** in the *\Micros\Res\Pos\Etc* directory. If this occurs, the following message will appear at the end of the Batch Transfer Status report:

```
One or more Debit Card Transactions Failed to Process
```

The text file will display the following information about the transaction:

```
An attempt to reverse one or more incomplete debit
transactions has failed. The details of the transaction(s)
are:

Transaction Date and Time: 09/13/07 22:03:49
Account Number: ************1111
Revenue Center: 1
Check Number: 1069
Check Employee: 101 Server 1
Transaction amount: 22.23
```

The user should print out the debit reversal text file. It is the responsibility of the user to contact the bank and have the Debit Amount credited back to the customer's account. This process will NOT occur automatically.

After the bank has been notified, the user must delete the **FDMSFailedReversal.txt** file. Otherwise, the Batch Transfer Status report will continue to reference this file.

Support for Authorizations Below $1.00

In the past the CaFDMS driver would round authorization amounts for less than $1.00 up to the value of $1.00. For example, an authorization for $0.01 would be transmitted as an authorization for $1.00.

Now, if an authorization is submitted for a value below $1.00, the authorization will be transmitted for the exact amount requested.

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 table below lists the revisions included in this release:

Feature	CR ID #	Page
CaFDMS Driver Would Not Record Leading Zeroes When Present in a Zip Code When AVS is Enabled	N/A	50
CaFDMS Driver Returns an Incorrect Error Message During a Debit Reversal	N/A	50
Datawire Registry Setting Information on the Backup Server Is Not Automatically Updating for the CaFDMS Driver	N/A	50
Discover Card Authorization Request Message Would Format CVV Data Incorrectly	N/A	50
Multi-Trans Mode Not Functioning Properly Using Dial-up Communications	N/A	51

Revisions Detailed

CaFDMS Driver Would Not Record Leading Zeroes When Present in a Zip Code When AVS is Enabled

CR ID#: N/A

Previously, if the address verification (AVS) option was enabled, the CaFDMS Driver would not record leading zeroes when they were present as part of a zip code (e.g., 000123 would be recorded as 123). The driver has been corrected to properly format leading zeroes in a zip code.

At this time POS Operations does not support the entry of non-numeric digits as a postal code. For this reason, only US zip codes are supported with the AVS feature.

CaFDMS Driver Returns an Incorrect Error Message During a Debit Reversal

CR ID #: N/A

While processing a debit reversal, the CaFDMS driver will not permit another debit transaction to be submitted by POS Operations. Previously, if another debit transaction was attempted the operator would receive the error message, "Reversal Failure." This message has been changed to, "Reversal in Progress."

Datawire Registry Setting Information on the Backup Server Is Not Automatically Updating for the CaFDMS Driver

CR ID #: N/A

The Datawire registry setting information on the Backup Server is not updating automatically for the CaFDMS driver. The registry update must be performed automatically as part of driver configuration. For complete configuration instructions see the *Setup* section of this document beginning on page 7.

Discover Card Authorization Request Message Would Format CVV Data Incorrectly

CR ID #: N/A

When the CVV option was enabled, the authorization request message for the Discover Card would incorrectly format the CVV data. As a result, the Discover card authorization request was invalid. This has been corrected.

Multi-Trans Mode Not Functioning Properly Using Dial-up Communications

CR ID #: N/A

Performing multiple credit card authorizations simultaneously from more than one workstation when using a dial-up connection would make separate phone calls to the Host; rather than keeping the line open after the first authorization to perform the next. This has been corrected.

ReadMe First
V. 4.3.16.1146

This section contains a comprehensive guide to the Version 4.3 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 release:

Feature	Page
Datawire Communications Channel	53

New Features Detailed

Datawire Communications Channel

The Datawire Communication Channel has been added to the CaFDMS North Driver. Datawire is an HTTP connection that enables communication via the Internet.

The Datawire option does not support persistent connections, and will close at the end of each session. The Datawire Channel will perform the following functions for each authorization:

1. Establish a Datawire connection
2. Send the authorization message(s) to the Host
3. Wait for the Host response(s)
4. Close the Datawire connection

   The user has the ability to configure a fallback connection. Should the Datawire connection fail, the fallback feature will attempt to establish a secondary connection type (e.g., dial-up). Meanwhile, Datawire will try to reconnect (in the background) to the Datawire Host at 30-seconds intervals.

   Once a connection is re-established with the Host, the driver switches back to Datawire mode and will either reconnect during the next authorization attempt, or will return to the beginning of the last batch settled.

Driver Options

To support this feature, the following changes were made to the CaFDMS driver in POS Configurator (*Devices* | *Devices* | *CA/EDC Drivers* | *System)*:

- **Communications Channel** — Addition of the Datawire connection channel (2). The options now are:

  0 – Dial-up (phone/modem)

  1 – TCP/ IP

  2– Datawire/ IPN

> ***Note*** *There are no IP Address:Port settings required for the Datawire connection.*

Testing the Driver

The first time that the driver attempts to connect to the Datawire Host, it will automatically perform a required one-time merchant configuration and registration process. MICROS recommends that the confirmation process occur before the driver has gone live at the site.

This test will only verify the connection settings. It does not verify the communication to and from the Datawire Server. For information on registering the CaFDMS Driver, see step 10 of the *Setup* section on page 13.

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 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 release:

Feature	CR ID #	Page
Driver Incorrectly Showing Batch as Unsuccessful After Settlement is Complete	N/A	56

Revisions Detailed

Driver Incorrectly Showing Batch as Unsuccessful After Settlement is Complete

CR ID #: N/A

Previously, after a batch was sent to the processor and confirmed, the settlement driver incorrectly listed the batch as unsettled. This was due to an error in the **cc_batch_item_dtl** table and was reflected in the Credit Card Batch Detail Report. This has been corrected.