micros®

Restaurant Enterprise Series

Universal Credit Card Driver for 3700 POS Version 4.15

May 6, 2014

**********************Important**********************

When upgrading the Universal Credit Card Driver to v4.11.21.2408 or higher, the user must go into POS Configurator | Devices | CA / EDC Drivers and select both the VSCA and VSST records. This will update the database with the new configuration file.

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

****

MD0003-070

Declarations

Warranties

Although the best efforts are made to ensure that the information in this document 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 document is subject to change without notice.

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 document.

Trademarks

Installation and Setup

This section contains installation and setup instructions for the Version 4.13 release of the Universal Credit Card Driver (VisaNet). The release version is available on the MICROS 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 UCCD may be used on RES systems running Version 4.3 HF2 or higher.

In This Section...

Installation

Site Requirements

Before installing the Universal Credit Card Driver (UCCD) on the RES system, the following configuration items should be considered:

- The installed version of 3700 POS should be Version 4.3 HF2 or higher.
- To use TCP/IP, a WAN must be configured and working.
- To use Internet Connectivity, an Internet connection must be configured and working. ISP software may be needed to connect to the Internet.
- A dedicated modem and phone line are required for dial-up connectivity or fall-back to dial-up when using TCP/IP or Internet connectivity.
- Security protocols, including firewalls and other protections, should be in place.
- The site's browser software will need to support 128-bit session keys. (See section Internet Explorer Cipher Strength, for a method to check this.)

Files Included

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

Authorization

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

Settlement

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

Installation Instructions

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

- **"[HKEY_LOCAL_MACHINE\SOFTWARE\MICROS\CreditCardDrivers\CaVsCa]"**
- **"[HKEY_LOCAL_MACHINE\SOFTWARE\MICROS\CreditCardDrivers\CaVsSt]"**
- **"InstallationVersion"="4.XX.XX.XXXX"**
  - *The version of the driver being installed*
- **"Installed"="Day MM/DD/YYYY"**
  - *The installation date of the installed driver (for example, 'Thu 01/19/2012')*

Existing Site Running RES V4.3 HF2 (or Higher)

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 latest Universal Driver 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:
   - Universal Credit Card Driver for RES 3700 POS (**UCCDV4.15_MD.pdf**)
   - MICROS RES Universal Credit Card Driver (**CaUCCD(4.15.0.2488).exe**)
3. Please review the ReadMe First for all software changes in the current release.
4. It is not necessary to shut down your RES system during installation. There cannot be any credit card transactions in progress so be cautious and take your RES system to the database level via the **MICROS Control Panel**.
5. Double-click on the **CaUCCD(4.15.0.2488).exe** file to execute the installation program. This will install all of the necessary files on the RES Server and the BSM Client, and the Windows services will be restarted automatically. The credit card service will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started.:

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

File	RES Server	Backup Server Client	RES Server Client Installation Path
CaVsst.cfg	\MICROS\RES\POS\ETC	\MICROS\RES\POS\ETC	\MICROS\RES\CAL\Win32\Files\MICROS\POS\ETC
CaVsca.hlp	\MICROS\RES\POS\BIN	\MICROS\RES\POS\BIN	\MICROS\RES\CAL\Win32\Files\MICROS\POS\BIN
CaVsst.hlp	\MICROS\RES\POS\BIN	\MICROS\RES\POS\BIN	\MICROS\RES\CAL\Win32\Files\MICROS\POS\BIN
CaVsca.cnt	\MICROS\RES\POS\BIN	\MICROS\RES\POS\BIN	\MICROS\RES\CAL\Win32\Files\MICROS\POS\BIN
CaVsst.cnt	\MICROS\RES\POS\BIN	\MICROS\RES\POS\BIN	\MICROS\RES\CAL\Win32\Files\MICROS\POS\BIN

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

New Site Running RES V4.3 HF2 (or Higher)

1. Prior to installation, a new order form (new site) or a change of service form (existing site) must be submitted to Merchant Link, LLC. and you must contact their implementation department.
2. 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.
3. Download the latest Universal Driver 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:
   - Universal Credit Card Driver for RES 3700 POS (**UCCDV4.15_MD.pdf**)
   - Universal Credit Card Driver Software (**CaUCCD(4.15.0.2488).exe**)
4. Please review the ReadMe First for all software changes in the current release.
5. It is not necessary to shut down your RES system during installation. There cannot be any credit card transactions in progress so be cautious and take your RES system to the database level via the **MICROS Control Panel**..
6. Double-click on the **CaUCCD(4.15.0.2488).exe** file to execute the installation program.
7. Double-click on the **CaUCCD(4.15.0.2488).exe** file to execute the installation program. This will install all of the necessary files on the RES Server and the BSM Client, and the Windows services will be restarted automatically. The credit card service will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started

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

File	RES Server	Backup Server Client	RES Server Client Installation Path
CaVsca.cnt	\MICROS\RES\POS\BIN	\MICROS\RES\POS\BIN	\MICROS\RES\CAL\Win32\Files\MICROS\POS\BIN
CaVsst.cnt	\MICROS\RES\POS\BIN	\MICROS\RES\POS\BIN	\MICROS\RES\CAL\Win32\Files\MICROS\POS\BIN

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

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

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

Removing the Software

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

1. Shut down the RES system from the **MICROS Control Panel**.
2. Delete the following files:
   - \Micros\RES\POS\Bin\CaVsca.dll
   - \Micros\RES\POS\etc\CaVsca.cfg
   - \Micros\RES\POS\Bin\CaVsca.hlp
   - \Micros\RES\POS\Bin\CaVsca.cnt
   - \Micros\RES\POS\Bin\CaVsst.dll
   - \Micros\RES\POS\Etc\CaVsst.cfg
   - \Micros\RES\POS\Bin\CaVsst.hlp
   - \Micros\RES\POS\Bin\CaVsst.cnt
3. Shut down the RES System on the Backup Server Client (if applicable).
4. Delete the following files.
   - \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsca.dll
   - \Micros\RES\CAL\Win32\Files\Micros\RES\POS\etc\CaVsca.cfg
   - \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsca.hlp

- \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsca.cnt
- \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsst.dll
- \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Etc\CaVsst.cfg
- \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsst.hlp
- \Micros\RES\CAL\Win32\Files\Micros\RES\POS\Bin\CaVsst.cnt

Setup

Communication Channels Supported

- Dial-Up (Channel 0, system default)
- TCP/IP, Unencrypted via Frame Circuit Connectivity or VSAT Connectivity (Channel 1)
- Internet, Encrypted via Merchant Link's siteNET gateway (Channel 2)

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

Connectivity Considerations

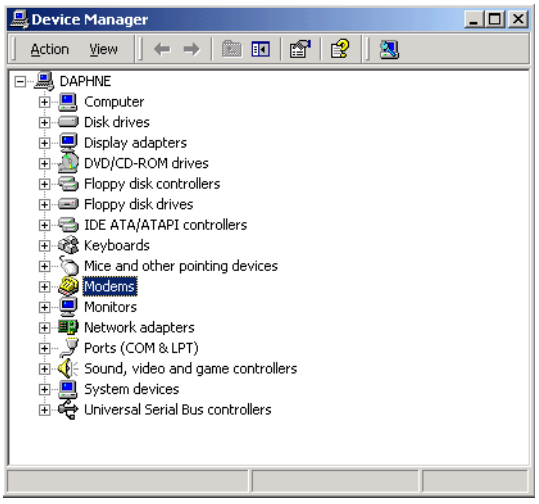
This section is provided as reference when installing the Universal Credit Card Driver. All information listed below has not changed since the initial release of a particular communication channel.

Configuring Dial-Up Connectivity

Before beginning, make sure that the phone line being used is dedicated for credit cards only, and will not be used for other purposes.

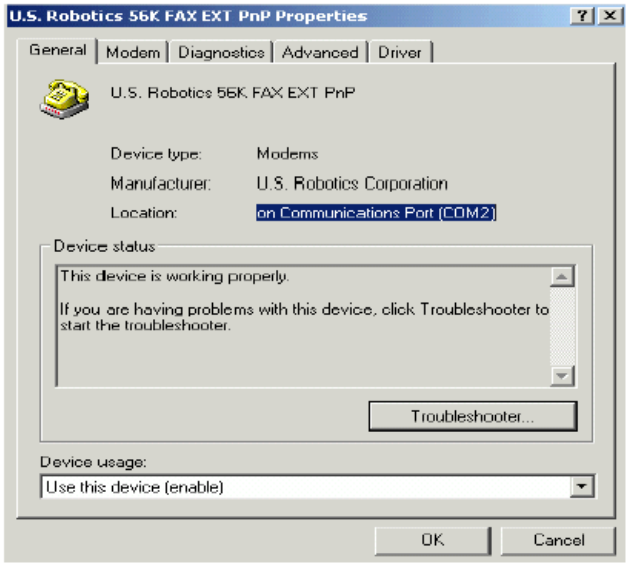
The following setup instructions are for Windows 2000 platforms:

1. From the **Windows Start** menu, select *Settings* | *Control Panel* | *System*. Go to the *Hardware* tab and press the **[Device Manager]** button to open the form.

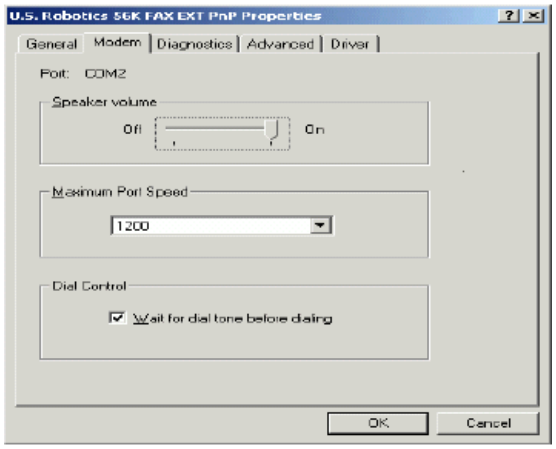


2. Expand the **Modems** entry and double-click on the modem to be used for credit card processing. The properties form will be displayed.

3. From the *General* tab, refer to the **Location** field. Write down the COM Port number, as it will be needed shortly.



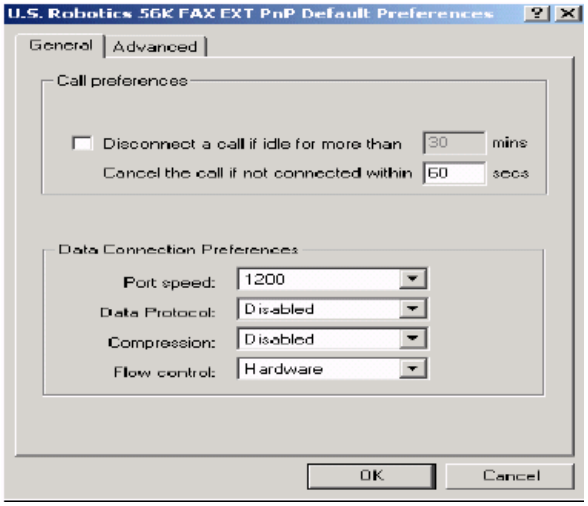
4. Go to the *Modem* tab.



5. Enable the **Dial Control** option and set the **Maximum Port Speed** to *1200*.

   NOTE: In some cases, port speed may need to be set to 2400. If so, this value must be changed to 2400 wherever else it appears in the configuration.

6. Go to the *Advanced* tab and click the **[Change Default Preferences]** button to open the preferences form.



7. On the *General* tab, set the options as follows:
   - **Port speed** — 1200 (or 2400, as discussed in step 4)
   - **Data Protocol** — Disabled
   - **Compression** — Disabled
   - **Flow control** — Hardware
8. Go to the *Advanced* tab and set the options as follows:
   - **Data bits** — 7
   - **Parity** — Even
   - **Stop bits** — 1
   - **Modulation** — Standard
9. Click the **[OK]** button (twice) to accept the changes and return to the Device Manager screen.
10. Expand the **Ports** menu entry and double-click on the COM Port identified in Step 2.
11. Go to the **Port Settings** table and select the following options:
    - **Bits per second** — 1200 (or 2400, as discussed in step 4)
    - **Parity** — Even
    - **Stop bits** — 1
    - **Flow Control** — Hardware

12. Click **[OK**]to save and close the **System** forms.
13. Exit the Control Panel and reboot the PC.

Configuring TCP Connectivity

Merchants can use a private network to process credit card transactions. A secure corporate network is closed to the public and uses security protocols to prevent unauthorized access. Message traffic on a private network is not encrypted. When a private network is used, the 3700 POS can be configured to either connect directly to Merchant Link (ML) or via a corporate WAN connected to Merchant Link.

Network configurations are typically setup one of two ways:

- Satellite connection from each site to ML. This requires contracting with a satellite vendor that has a frame-relay connection from their satellite hub to Merchant Link.
- Connection from each site to a corporate WAN and frame-relay connection from corporate to ML.

1. Host And Backup Host Configuration

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

2. Fallback Configuration

The UCCD has a built-in feature to support failover or “fallback” capability for authorizations using either TCP/IP or Internet Connectivity. This feature enables the driver to automatically switch from a TCP/IP protocol to dial-up if the connection to the ML fails. In other words, fallback is initiated when the MICROS 3700 POS cannot connect to the credit card host.

Fallback is **not** initiated if the POS makes the connection but then an error occurs (i.e., the connection is lost). In this case, the user receives an error and can try the transaction again. If the system consistently connects and then errors out, MICROS recommends the following:

1. Place a call to your support desk.
2. Change the **Communication Channel** option to Dial-up (0) until the situation is resolved.

For this functionality to work, a modem must be installed on the RES Server. The device number and network phone numbers must also be entered into the driver configuration.

As a first step in setting up **Fallback** mode, MICROS recommends testing the UCCD with a communications channel configured for Dial-up (0). Once the system can process credit card transactions in this mode, the communications channel can be changed and the modem can be configured in *POS Configurator* | *Devices* | *CA/EDC Drivers*. This includes specifying the **Authorization** and **Backup Authorization Phone Numbers**.

3. Confirmation Of Connectivity With Network Default Gateway

Most networks have specified gateway routers where connections need to be routed before they can get to the "outside world." To confirm a connection is getting through the merchant's network, ping the address of the Default Gateway router. If the address is unknown, follow these steps to determine the default gateway's IP address:

1. Go to a command prompt.
2. Type **ipconfig /all**
3. Find the line that reads default gateway.
4. Type **ping**, then the **IP address** from Step 3.

If pings to the Default Gateway are unsuccessful, then the Merchant's IT group will need to troubleshoot and fix the issue within their network.

4. Confirmation Of Connectivity With The Merchant Link Network

The easiest way to test the connection from the RES Server to the Merchant Link Network through a frame circuit is by pinging from a command line on the RES Server. This can be done in conjunction with Merchant Link. For more information, contact ML for connection information.

5. Test TCP/IP Connectivity via Credit Card Utility

Another way to test the connection (from the RES Server to the Merchant Link Network through a frame circuit) is to use the diagnostic tools in the Credit Card Batch Utility. This can be done as follows:

1. Open the **Credit Card Batch Program** on the RES Server.
2. Go to the *Diagnostics* tab.
3. In the **CA/EDC Drivers list** box, select one of the UCCD's authorization or settlement drivers.
4. From the *Diagnostic Functions* window, highlight the **Test Settle Connection** option.
5. Click the **[Begin Test]** button to run the test.

If all is configured correctly, a **Connection Successful** message will display. If no connection is made, an error message will be shown.

In the event of a problem, Merchant Link support personnel should provide assistance in discussing the issue with their IT Group.

Configuring Internet Connectivity

The following are considerations when configuring a system to use Internet Connectivity as the communications channel.

1. Internet Configuration

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

2. Internet Connectivity

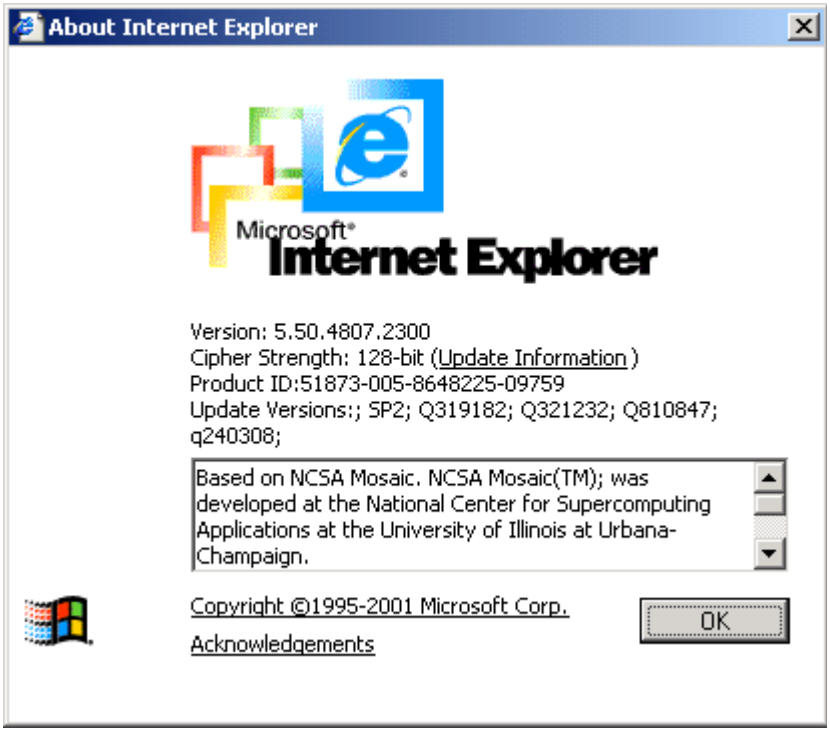
Merchants must have an ISP account that supports DSL, ISDN, or Cable modem connectivity. Connection to the Internet can also be established through a corporate LAN or WAN.

3. Internet Explorer Cipher Strength

In order for the 3700 POS CA/EDC software to properly make connections with **g1.merchantlink.com** and **g2.merchantlink.com**, the encryption strength (or Cipher Strength) of the MICROS RES Server must be 128-bit. The Cipher strength on a given server can be easily checked as follows:

1. Open Internet Explorer
2. Click on the **Help** menu.

3. Select the **About Internet Explorer** option. The following window will display:



The second line is the Cipher Strength. If that is anything less than 128-bit, the server will need to be updated. The specifics on what is needed for the update is dependent upon the RES Server's Operating System and/or Internet Explorer version. The URL for the Microsoft High Encryption Pack update page is:

http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp

4. Test Internet Connectivity

The site must be able to connect to ML's siteNET gateway through port 443. To create a successful round trip test to the siteNET Gateway, open Internet Explorer on the RES Server and attempt to access the following URL from the browser:

https://g1.merchantlink.com/Micros/process_transaction.cgi

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

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

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

- **403 - Forbidden Error** — Indicates that something is blocking the connection.
- **404 - Forbidden Error** — Indicates that the site's network configuration is not resolving the URL correctly.

Should either of these errors occur, a trained network person may be required to configure the site's network for access to the siteNET gateway.

5. Host and Backup Host Configuration

To process via a high-speed internet connection, the site must be able to connect to ML's siteNET gateway through port 443. This requires configuring the following fields on the *System* tab (*POS Configurator* | *Devices* | *CA/EDC Drivers*) for both the authorization and settlement drivers :

- **Host IP Address: Port** — g1.merchantlink.com:443
- **Backup IP Address: Port** — g2.merchantlink.com:443

6. Test Internet Connectivity via Credit Card Utility

If a browser is not available on the RES Server, use the test connection tool in the MICROS Credit Card Batch Utility.

This can be done as follows:

1. Open the **Credit Card Batch** Program on the RES Server.
2. Go to the *Diagnostics* tab.
3. In the **CA/EDC Drivers list** box, select one of the UCCD's authorization or settlement drivers.

4. From the *Diagnostic Functions* window, highlight the **Test Settle Connection** option.
5. Click the **[Begin Test]** button to run the test.

If all is configured correctly, a **Connection Successful** message will display. If no connection is made, an error message will be shown. Problems related to the Internet or ISP will require further investigation from the Merchants ISP. Merchant Link support personnel should provide assistance in discussing these issues with the ISP.

7. Fallback Configuration

The UCCD has a built-in feature to support failover or "fallback" capability for authorizations using either TCP/IP or Internet Connectivity. This feature enables the driver to automatically switch from a TCP/IP protocol to dial-up if the connection to the ML fails. In other words, fallback is initiated when the MICROS 3700 POS cannot connect to the credit card host.

Fallback is **not** initiated if the POS makes the connection but then error out (i.e., the connection is lost). In this case, the user receives an error and can try the transaction again. If the system consistently connects and then errors out, MICROS recommends the following:

1. Place a call to your support desk.
2. Change the **Communication Channel** option to Dial-up (0) until the situation is resolved.

For this functionality to work, a modem must be installed on the RES Server. The device number and network phone numbers must also be entered into the driver configuration.

As a first step in setting up **Fallback** mode, MICROS recommends testing the UCCD with a communications channel configured for Dial-up (0). Once the system can process credit card transactions in this mode, the communications channel can be changed and the modem can be configured in *POS Configurator* | *Devices* | *CA/EDC Drivers*. This includes specifying the **Authorization** and **Backup Authorization Phone Numbers**.

8. Internet Security

The security and protection of the MICROS network, and the data and applications on that network, are solely and entirely the responsibility of the customer. A properly configured firewall is required for each site that uses a persistent connection to the Internet or any private internal network where there is a potential for unauthorized access to the MICROS network.

The customer is solely and entirely responsible for the security of the MICROS network, 3700 POS, and their data against unauthorized access and any damage and support costs incurred as a result of said access.

9. Internet Proxy Considerations

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

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

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

Follow these steps to add the **ProxyName** registry key:

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

In the event that a proxy name is not specified, a new **ProxyAccess** value may be used instead.

Follow these steps to add the **ProxyAccess** registry key:

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

Configuring the Drivers

UCCD setup is not done until the VSCA and VSST driver forms are completed in *POS Configurator* | *Devices* | *CA/EDC Drivers*. An online help file is available to explain the general configuration requirements. However, entries for some options will be provided by the credit card processor. If so, be sure to enter this data exactly as given, as some fields may be case-sensitive. Entering the correct entry in the wrong format may result in communication failure at the Host Processor.

Example:

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

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

Useful Configuration Settings

This section contains a list of several useful configuration settings available for the UCCD.

Change Maximum Batch Size

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

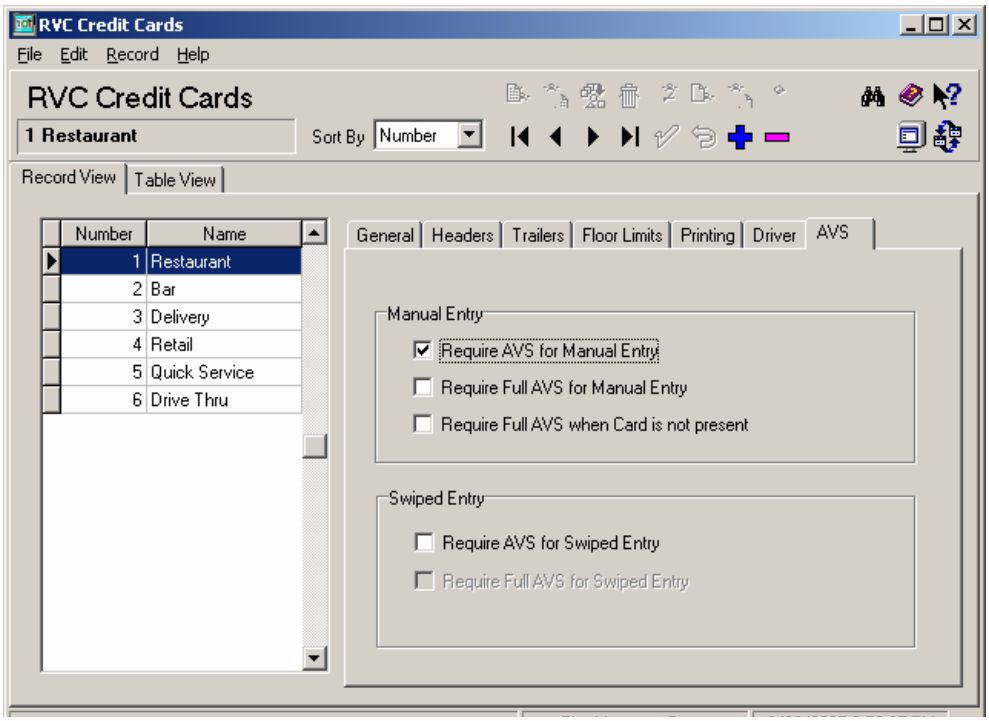
1. Go to the *\Micros\Res\POS\Etc* folder and select the **CaVSST.cfg** file.
2. When the window appears enable the **Select the program from a list** option and click **[Ok]**.
3. Highlight the **NotePad** application and click **[Ok]**.
4. Change the **MaxBatchSize** parameter setting from 300 to the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

AVS and CVV Configuration

The UCCD driver supports the transmission of Address Verification (AVS) and Card Verification Value (CVV) as part of the authorization request.

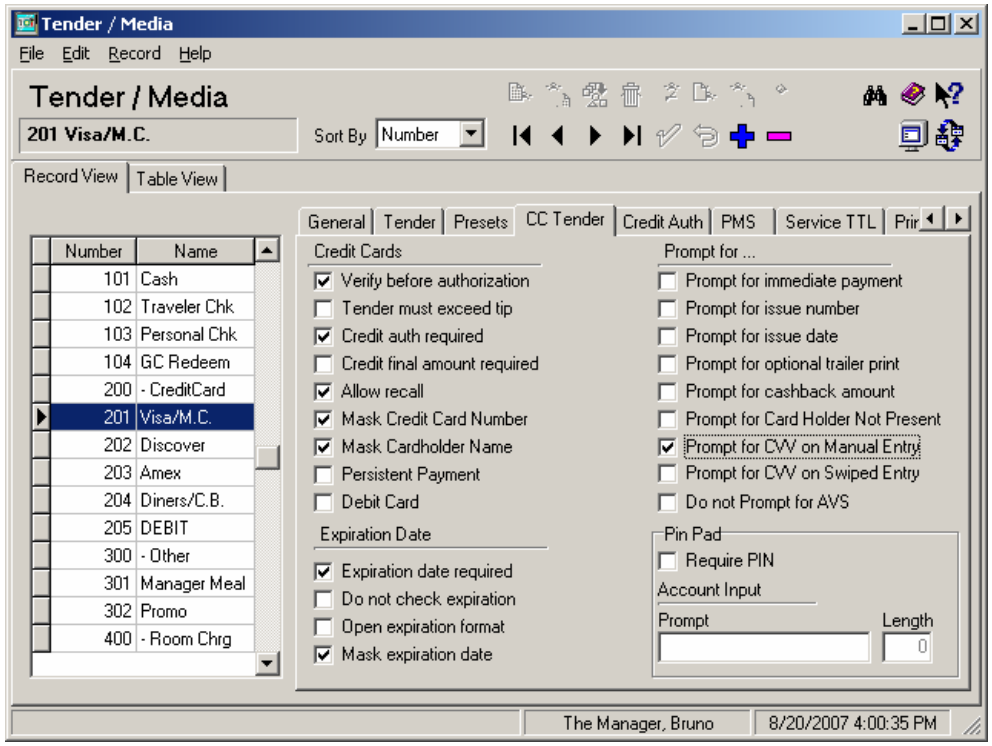
AVS is a system check that matches the address provided in the transaction to the address on file with the bank. CVV is the three or four-digit number listed on the back of the card that provides an additional level of security for the user. AVS and CVV data is transmitted in the Cardholder Identification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

The AVS feature can be enabled by going to the *Revenue Center | RVC Credit Cards | AVS* tab and 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.

Frequently Asked Questions

Why is reading the Credit Card Transfer Report so important?

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

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

What is a credit card batch?

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

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

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

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

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

- Credit card number
- Expiration date

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

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

Terminal-based processing requires that the entire batch be successful for the batch to be closed. Most of the 3700 POS drivers support terminal-based processing. The Universal Credit Card driver uses this type.

Host-based processing requires each transaction to be successful. This means a batch could contain a single card that did not transfer to the credit card host. Once this transaction is adjusted, the batch could be re-sent to the host.

Transfer Status Report

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

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

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

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

How can a duplicate batch occur?

Duplicates occur when the system sends a batch to the credit card host and the host send back a response that does not makes it all the way to the 3700 POS. When this happens, the POS will send the message a second time.

Please note that credit card hosts may have rules in place to catch a second (duplicate) transmission of the batch, using criteria such as transaction amount or card numbers. These rules provide a temporary window for the user to rectify the problem before the batch is submitted again. *The resubmission is not dependent on action by the end-user.* Eventually, if the 3700 POS continues to send the batch, a duplicate will be generated.

To correct this problem, MICROS has added enhancements to the Universal Credit Card Driver (UCCD) for the prevention of duplicate batches. (For more on this topic, refer to the new features section in *ReadMe First - v. 4.1.8.584*).

ReadMe First
V4.15.0.2488

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.13 release of the Universal Credit Card Driver (VisaNet).

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

There are no new features in this release.

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 version:

Feature	CR ID/ SCR #	Page
Authorizations with RES 5.x and 5th3rd mode could take 30 seconds	34037/ 40096	33

Revisions Detailed

Authorizations with RES 5.x and 5th3rd mode could take 30 seconds

CR ID #: 34037

When used in RES 5.x, with 5th3rd mode (the processor now called Vantiv) and communication channel 2 (internet), authorizations would take 30 seconds. This has been corrected.

ReadMe First
V4.13.0.2453

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.13 release of the Universal Credit Card Driver (VisaNet).

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

There are no new features in this release.

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 version:

Feature	CR ID/ SCR #	Page
Driver Locks Up During Settlement	N/A/ 39828	37

Revisions Detailed

Driver Locks Up During Settlement

CR ID #: N/A

Previously, under certain scenarios the driver would lock up during settlement. This has been corrected.

ReadMe First
V4.12.0.2434

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.12 release of the Universal Credit Card Driver (VisaNet).

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

There are no new features in this release.

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 version:

Feature	CR ID/ SCR #	Page
Records Missing Data in Settlement	33060/ 39709	41

Revisions Detailed

Records Missing Data in Settlement

CR ID #: 33060

Previously, some data elements from auth responses were not included in the settlement request. In certain scenarios, the merchant would be charged extra fees. This has been corrected.

ReadMe First
V4.11.21.2408

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.11 release of the Universal Credit Card Driver (VisaNet).

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
Support Added for Timeout Reversals (TOR)	43
Authorization Reversal Support For Fifth Third Mode	43

New Features Detailed

Support Added for Timeout Reversals (TOR)

With this release, Timeout Reversals (TOR) are now supported for Fifth Third Mode.

When a credit authorization does not receive a response from the Host Processor, a TOR will be created. When there is a TOR in progress, no other credit auths will be processed. The number of times a TOR will try to process and how long between tries is configurable. The defaults are five tries, 30 seconds apart. The following *DWORD Value* registry settings can be added in *HKEY_LOCAL_MACHINE* | *SOFTWARE* | *MICROS* | *Common* | *CCS* | *DrvrCfg* | *Drvr#* | *Option* to change from the defaults:

- TORResponseTOut (TCP/IP time period before re-sending)
- TORInternetWaitTime (HTTP time period before re-sending)
- TORAttemptCnt (Number of times to retry)

Authorization Reversal Support For Fifth Third Mode

CR ID #: N/A

With this release, authorization reversals are now supported for Fifth Third Mode. Card associations are now mandating that merchants submit authorization reversals for fully-approved or partially-approved transactions 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 Authorizations, Auto-offline Auths, and Below Floor Limit Offline auths will not be reversed.

There is a limitation that at most two auths can be reversed for each account on a single guest check.

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

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 version:

Feature	CR ID/ SCR #	Page
Cannot Connect to Merchant Link Gateways with RES 5.0	N/A/ 39106	46
Settlement with Dialup Could Fail with a Large Batch	N/A/ 38128	46

Revisions Detailed

Cannot Connect to Merchant Link Gateways with RES 5.0

CR ID #: N/A

Previously, the Credit Card Driver could not connect to the Merchant Link gateways from a RES 5.0. A driver change was needed to accommodate differences with the Windows 7 operating system. This has been corrected.

Settlement with Dialup Could Fail with a Large Batch

CR ID #: N/A

Previously, a large credit card batch could timeout when settling over dialup. In a situation where the Credit Card Host needs additional time to process a settlement request from the driver, the Host will send a message to prevent the driver from timing out while waiting for a response. In the past, the driver would not update the status of the settlement request and would eventually time out. This has been corrected.

ReadMe First
V 4.7.20.2032

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.7 release of the Universal Credit Card Driver (VisaNet).

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

Partial Credit Card Authorization

> ***Note*** *This feature is only supported in Fifth Third Mode (e.g., Custom Mode 3).*

With this release, support has been added for partial authorization, which is a feature that permits a site to accept prepaid credit cards. Unlike traditional gift cards, all prepaid cards issued by credit card companies (e.g., the Visa and American Express) are processed as credit cards.

In a situation where the amount of the check exceeds the balance remaining on the prepaid credit card, or when the balance of the card is unknown, the site can approve the credit card authorization for an amount that is less than the total amount originally requested by the credit card driver.

Additionally, it is possible to perform a balance inquiry on the prepaid credit card, if the credit card host supports a balance inquiry.

Use Cases

This section contains some basic use cases to illustrate the partial authorization feature used in conjunction with a prepaid credit card.

Example 1: Check Total is Less Than Balance on the Card

The Check Total is $35.00 and the Card Balance is $50.00.

1. Employee uses the Credit Authorization key to authorize the prepaid credit card.
2. The credit card processor returns an approval for $35.00 and an available balance of $15.00.
3. POS Operations prints a standard credit card voucher with an additional Available Balance: $15.00 line.
4. When a payment is made using this card (using Credit Final), the charged tip amount will be limited to the available balance, $15.00.

Example 2: Check Total is More Than Balance on the Card

The Check Total is $35.00 and the Card Balance is $25.00.

1. Employee uses the Credit Authorization key to authorize the prepaid credit card.
2. The credit card processor returns a partial approval for $25.00 and an available balance of $0.00.
3. POS Operations prints a standard credit card voucher for $25.00 showing an available balance of $0.00. The voucher will not contain a tip line since the remaining balance is zero.

Example 3: Initial Authorization is More than the Card Balance

The customer wishes to run a bar tab. The Initial Authorization is $50.00 and the card balance is $25.00.

1. Employee uses the Initial Authorization key to request an authorization for $50.00.
2. The credit card processor returns a partial approval for $25.00 and an available balance of $0.00.
3. When the customer is ready to leave, the operator can print a voucher for up to $25.00.

Example 4: Auth N Pay Tender

The Check Total is $35.00 and the Card Balance is $25.00.

1. Employee uses the VISA key to request an authorization for $35.00.

2. The credit card processor returns a partial approval for $25.00 and an available balance of $0.00.
3. POS Operations prints a voucher for $25.00 showing an available balance of $0.00. The normal Auth N Pay trailer is printed. A VISA Payment of $25.00 is posted to the check.

How it Works

When enabled, POS Operations will send a flag to the credit card driver indicating that it supports partial authorizations.

When the transaction has been partially approved, the credit card driver will send a notification to the credit card host, including the amount of the authorization.

If the partial authorization occurred during an Initial Authorization request, then the amount entered cannot exceed the Initial Authorization amount.

Any time a partial authorization occurs, POS Operations will display the following message intended to draw the operator's attention:

Partial Authorization of XX.XX Has Been Applied.

When the driver returns an available balance, POS Operations will store that balance as part of the authorization detail. The remaining balance will print on the credit card voucher.

If the credit card driver does not support partial authorization then it will decline the authorization even if the tender is configured to support partial authorizations.

Configuration

To configure this functionality, the user must enable the **Allow partial authorization** option on the *POS Configurator* | *Sales* | *Tender/Media* | *Credit Auth* form for all applicable tenders.

The user must also configure a merchant and a customer zero balance trailer that will appear when the remaining balance on the card is $0.00. This trailer should be configured to print without a tip line, as a tip does not apply for a zero balance transaction. Use the **Merchant Zero Balance Trailer** and the **Customer Zero Balance Trailer** options on the *POS Configurator* | *Revenue Center* | *RVC Credit Cards* | *Trailers* form to configure these trailers.

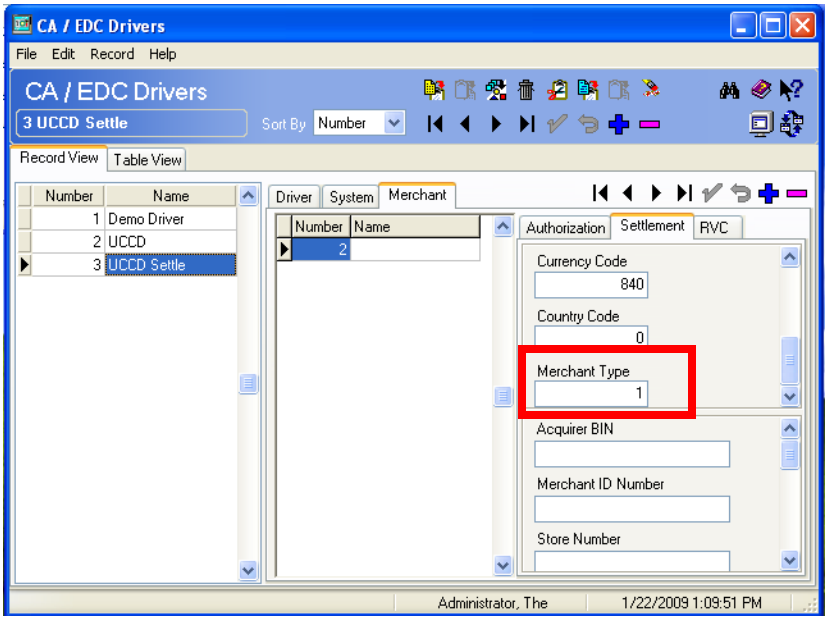
Fifth Third Mode New Feature Support

The Universal Credit Card Driver (UCCD) has been enhanced to support additional new functionality with Fifth Third Mode (e.g., Custom Mode 3). This section outlines this new functionality.

Support for eCommerce Transactions

Support has been added for eCommerce transactions. An eCommerce transaction is one that occurs online. Authorizations for payments submitted online are set with a different set of authorization data.

To support this functionality, the **Merchant Type** field was added to the *POS Configurator* | *Devices* | *CA/EDC Devices* | *Select the CaVSCA/CaVSST Driver* | *Merchant* | *Authorization/Settlement* tab. Enter a 0 in this field to designate restaurant transactions (this is the default setting). Enter a 1 in this field to designate eCommerce transactions. This field must be configured for both the CaVSCA and CaVSST drivers.



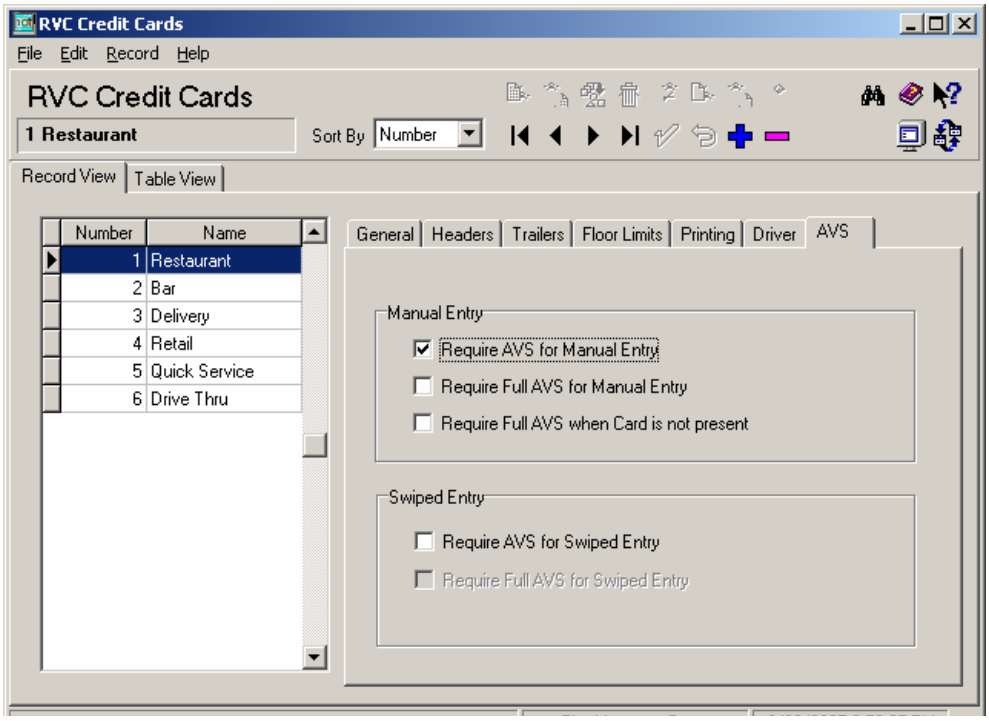
AVS and CVV Support for Fifth Third Mode

The Universal Credit Card Driver (UCCD) has been enhanced to support Address Verification (AVS) and Card Verification Value (CVV) as part of the authorization request for Fifth Third Mode.

> ***Note*** *Partial Authorization is no longer supported with Custom Mode 0. At this time, Partial Authorization is only supported with Custom Mode 3 (Fifth Third Mode).*

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.

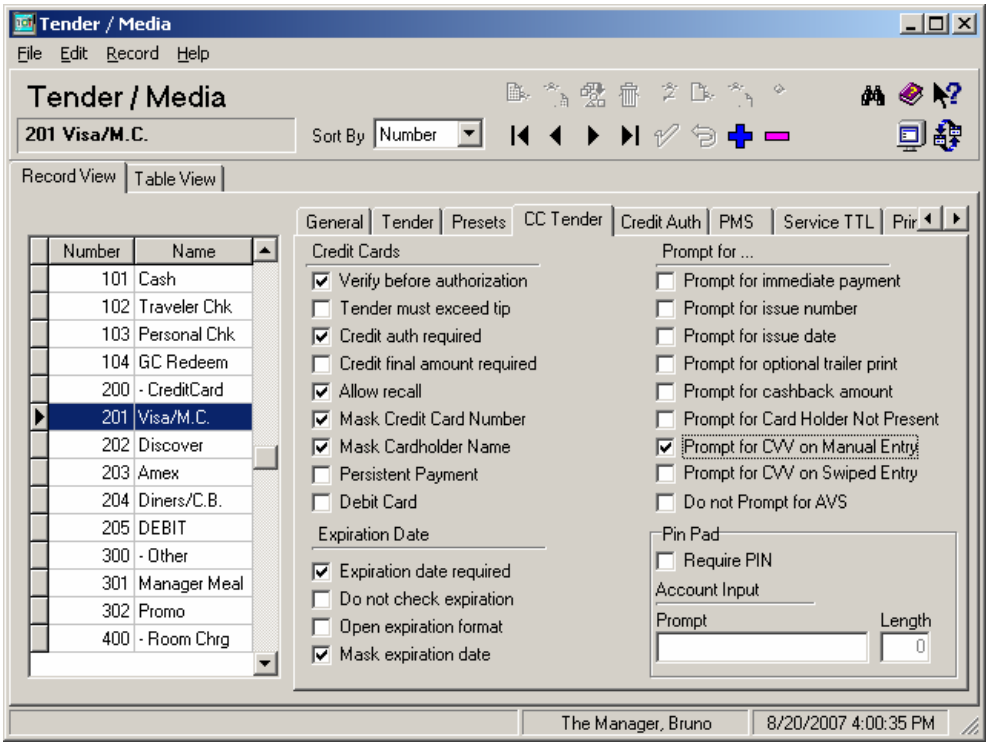


- **Require AVS for Manual Entry**. Select this option to prompt for the cardholder's zip code before submitting a manual credit card authorization,
- **Require Full AVS for Manual Entry**. Select this option to prompt for the cardholder's address AND zip code before submitting a manual credit card authoriza-

tion. 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 either the default VisaD format, or Fifth Third Mode. 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
Driver Uses Swiped Authorization at Settlement	55

Enhancements Detailed

Driver Uses Swiped Authorization at Settlement

When there are multiple authorizations associated with an account the settlement 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.

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:

Feature	CR ID/ SCR #	Page
A Batch Could Timeout During Settlement	N/A/ 33618	57
CaVSST Driver Could Send Incorrect Amounts at Settlement When Check Contained Multiple Authorizations	N/A/ 35668	57
CaVSST Driver Does Not Correctly Quarantine Batch After Local Settlement Failure	N/A/ 35056	57
Driver Would Occasionally Time Out During Authorization or Settlement When Using a Dialup Connection	N/A/ 33797, 33798	57
Timeout Waiting for Batch Response When Settling Large Batches	N/A/ 33881	58

Revisions Detailed

A Batch Could Timeout During Settlement

CR ID #: N/A

Previously, a credit card batch could timeout during settlement. In a situation where the Credit Card Host needs additional time to process a settlement request from the driver, the Host will send a message prevent the driver from timing out while waiting for a response. In the past, the driver would not update the status of the settlement request and would eventually time out. This has been corrected.

CaVSST Driver Could Send Incorrect Amounts at Settlement When Check Contained Multiple Authorizations

CR ID #: N/A

Previously at settlement, the CaVSST Driver would send the authorized amount from the last authorization request. This would not work for checks with multiple authorizations because the authorized amount needs to match the auth code and account data that are located in the first swiped authorization. As a result, the settlement driver could send incorrect data. This has been corrected.

CaVSST Driver Does Not Correctly Quarantine Batch After Local Settlement Failure

CR ID #: N/A

Previously, when a local settlement attempt failed, it was possible for the TransferStatus to inaccurately record the batch status as BatchOpen Submitted. As a result, the credit card application would duplicate the batch thinking that the previous attempt failed when attempting to transmit to Merchant Link.

Now, the driver will always set the TransferStatus to Local Accept for all locally settled batches. In the event of a failure, the batch will be quarantined, until another local settlement attempt is made, rather than try to retransmit the batch to Merchant Link.

Driver Would Occasionally Time Out During Authorization or Settlement When Using a Dialup Connection

CR ID #: N/A

Previously, when a dialup connection was used, the CaVSCA and the CaVSST Drivers could timeout during authorization or settlement. This has been corrected.

Timeout Waiting for Batch Response When Settling Large Batches

CR ID #: N/A

In an effort to make settlement more reliable, the HTTP header has been changed from 'Connection: Keep Alive' to 'Connection: Close.'

ReadMe First
V 4.5.18.1600

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.5.18.1600 release of the Universal Credit Card Driver (VisaNet).

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
CVV and AVS Supported	61
UCCD Supports Visa 62.23 Card Level Results and AMEX CaPN	63

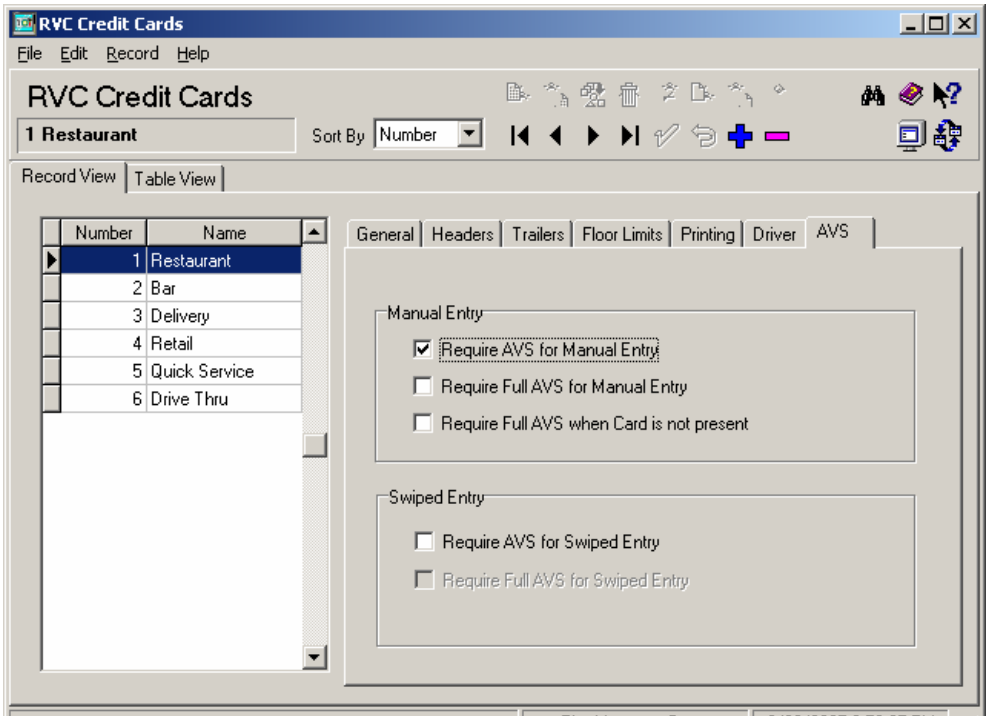
New Features Detailed

AVS and CVV Supported

The Universal Credit Card Driver (UCCD) 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.

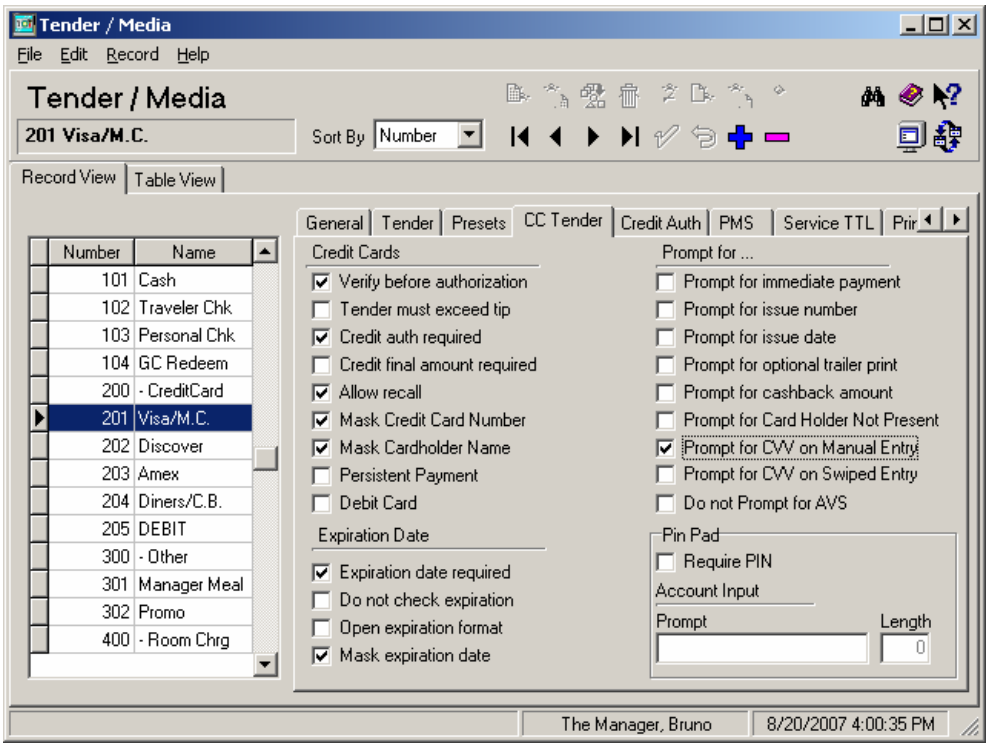
The AVS feature can be enabled by going to the *Revenue Center* | *RVC Credit Cards* | *AVS* tab and enabling the following options. Select the options as they are appropriate for the site.



- **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.

UCCD Supports Visa 62.23 Card Level Results and AMEX CaPN

The Universal Credit Card Driver (UCCD) has been enhanced to support Visa 62.23 (Card-Level Results) and AMEX CaPN which includes support for POS Data Codes. To support the addition of these new fields, the authorization and settlement messages have been changed from the VisaK format to the VisaD format.

These changes do not apply when the driver is operating in custom modes: 1, 2, or 3. Configuring the driver for any of the custom modes disables support for these new features and creates an authorization using the same VisaK format which was used in previous releases.

Configuration Options

To support these new features, two new configuration options have been added to the System tab of the authorization driver (POS Configurator | Devices | CA/EDC Drivers).

- **Enable Card Level Results**. Card-level results are enabled by turning on this option. This option will defaults to 0. The card level results field is a 2 character field sent by the issuer as part of the authorization response and returned as part of the settlement detail record. Enter one of the following options.

  – 0. Option is disabled (default).

  – 1. Option is enabled.

> ***Important!*** *For existing installation upgrades, the card level results option will be 0 and will need to be enabled.*

- **Enable POS Data Code.** Use this field to enable the POS Data Code. This field defaults to 0. The POS Data Code is a fixed 12 character string of data in the authorization message which indicates the condition of the POS Device and transaction at the time of the authorization. Examples of these characteristics are: Amex or non-Amex card; Swipe or Manual entry; card present or not; print and display capabilities; etc. The POS Data Code string will also be sent as part of the Settlement Detail. Enter one of the following values:

  – 0. Option is disabled (default).

  – 1. Option is enabled.

These options will default to the following values for all sites:

- Enable Card Level Results will be disabled.
- Enable POS Data Code will be disabled.

There are no configuration options for the settlement driver. The data in the authorization detail record determines whether or not these fields were enabled at authorization and need to be sent as part of the settlement record.

AMEX Values Below $1.00

In the past the UCCD 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 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
CaVSCA Driver Supports New Discover Credit Card Numbers	66

Enhancements Detailed

CAVSCA Driver Supports New Discover Credit Card Numbers

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

Start	End
62212600	62292599
644000	644999
650000	659999

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:

Feature	CR ID	Page
CaVSCA Driver Causes the Credit Card Server to Fault Unexpectedly When Formatting Long System Error Messages	N/A	68
CaVSCA Driver Encountered Issues with its Security Certificate	23578	68
During Settlement All Offline Transaction Type Detail Records Would Contain the Same Trans Sequence Number of 0001	N/A	68

Revisions Detailed

CaVSCA Driver Causes the Credit Card Server to Fault Unexpectedly When Formatting Long System Error Messages

CR ID #: N/A

When the CaVSCA driver attempted to format an error message that exceeded 100 characters in length, the Credit Card Server would fault unexpectedly. This has been corrected.

CaVSCA Driver Encountered Issues with its Security Certificate

CR ID #: 23578

The CaVSCA driver could have issues with authenticating its security certificate during authorization. This issue has been resolved by adding the WinHTTP interface to the driver. Now, authorization messages will be transmitted using the WinHTTP, and if this interface is unavailable, then the message will be transmitted using WinInet for all transactions processed with communication Channel 2.

During Settlement All Offline Transaction Type Detail Records Would Contain the Same Trans Sequence Number of 0001

CR ID #: N/A

Previously, during settlement all transactions performed offline would contain the Trans Sequence Number of 0001, when the Trans Sequence Number should have been incremented. This has been corrected.

ReadMe First
V 4.4.17.1391

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.4.17.1391 release of the Universal Credit Card Driver (VisaNet).

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

There are no new features in this release.

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 version:

Feature	CR ID	Page
CaVSCA and CaVSST Drivers Logging Improperly	N/A	72
CaVSST Settlement Driver Crashes When a Long System Error Message is Received	N/A	73
Dynamic Batch Numbering Mode Sending Wrong Batch When it Hits Batch #999	N/A	73
Internet Timeout Resulting in Fallback Dialing and a Duplicate Batch	N/A	73

Revisions Detailed

CaVSCA and CaVSST Drivers Logging Improperly

CR ID #: N/A

The Version 4.3 CaVSCA and CaVSST drivers were improperly logging all information about the driver when the verbosity was set to 0. All logging was being sent to the 3700d.log and not to the individual driver logs. This issue has been corrected.

CaVSST Settlement Driver Crashes When a Long System Error Message is Received

CR ID #: N/A

The VSST settlement driver would crash when an error message in excess of 100 characters was received. Now, if an error message is longer than 100 characters, the log message will only copy the first 100 bytes and the user will only see the first 100 characters.

Dynamic Batch Numbering Mode Sending Wrong Batch When it Hits Batch #999

CR ID #: N/A

When the VSST driver was in dynamic batch numbering mode, and the batch number reached 999, the driver would mistakenly send batch number 1. This has been corrected.

Internet Timeout Resulting in Fallback Dialing and a Duplicate Batch

CR ID#: N/A

When the VSST driver would encounter an internet timeout, it would go into Fallback Mode, attempting to redial and send the batch again. This could result in the creation of a duplicate batch. This issue has been corrected.

ReadMe First
V 4.3.16.1057

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.3 release of the Universal Credit Card Driver (VisaNet).

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

There are no new features in this release.

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
Default Name for Host Header is Derived from Configured URL	76

Enhancements Detailed

Default Name for Host Header is Derived from Configured URL

Internet HTTPS communications for the Universal CC drivers (CaVSCA and CaVSST) involve message headers containing certain fields. One example is the **Host Header**, which could change depending upon the specific network or host to be used.

The user has the ability to configure the credit card Host Header message in POS Configurator. Previously, the Universal CC drivers used the default value of **gateway-bmd.nxt.com** for the **Host Header** when this field was left blank.

To prevent confusion, the default Host Header name has been changed to reflect the URL address that is being used.

To configure the URL address go to *Configurator* | *Devices* | *CA/EDC Drivers* | *System* tab and enter the **Host IP Address** (URL) provided by the bank. Enter the **Backup IP Address** (URL) if one is provided.

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

Feature	Page
Account Data Source at Settlement Needs to Match Authorization Data	77
Error Running UCCD Installation Program on a RES v4.0 Server	77
Credit Card Server Fault During Settlement Causing the Next Authorization Attempt to Fail	78
Off-line Authorization Source Code Change	78

Account Data Source at Settlement Needs to Match Authorization Data

Previously, the credit card settlement process was incorrectly concluding that the Account Data Source was Track 2 when it actually came from Track 1. The settlement driver had no way of knowing that the data came from Track 1, since Track 1 data was not being stored in the database. The authorization driver now stores information for settlement to know the account data source.

Error Running UCCD Installation Program on a RES v4.0 Server

Previously, running the UCCD installation on a RES version 4.0 server would produce a Sybase related error condition. The problem was that the installation program file did not reflect the new version 4.0 path, and required modifications to apply the database updates to make it compatible with all versions of RES. This problem has been corrected.

Credit Card Server Fault During Settlement Causing the Next Authorization Attempt to Fail

Previously, the credit card server was faulting intermittently during submission of Batch Close in the settlement process. When performing the first credit card authorization of the business day, the user would receive an error connecting to the credit card server. The problem was due to a timing thread conflict that could intermittently cause the credit card server to fault during batch settlement. This problem has been corrected.

Off-line Authorization Source Code Change

Previously, the Settlement Driver was not properly formatting off-line transactions in the settlement message. When the **Base Floor Limit** *(POS Configurator | Sales | Tender/Media | Credit Auth | Authorization)* and the **Do not go on-line for authorization** options were enabled, the driver would improperly mark the offline transactions with an 'E' at settlement. The 'E' indicated a manual transaction rather than one performed off-line. Now an off-line transaction is marked with a '9' at settlement, indicating that the transaction occurred off-line.

ReadMe First
V 4.2.13.912

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.2 release of the Universal Credit Card Driver (VisaNet).

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

There are no new features in this release.

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
Changed 'Disable Auth Code Limit' Default Setting to 1	81
Added Support for the Internet Communication in Fifth/Third Mode	82

Enhancements Detailed

Changed 'Disable Auth Code Limit' Default Setting to 1

The default value for the settlement driver option **Disable Auth Code Limit** (*POS Configurator* | *Devices* | *CA/EDC Drivers* | *System*) has been changed from 0 to 1. This was done to avoid errors encountered when processing Manual Authorizations that include an Auth Code greater than 6 digits.

During operations, the system does not limit the length of manually entered authorization codes. The problem occurs when the batch is settled. The extra digits can trigger an error message. Changing the default value from 0 to 1avoids unnecessary calls to support by truncating the number to the first 6 digits of the Auth Code which, in turn, allow the batch to be settled.

This change only affects new records added to POS Configurator. Existing installations will not be affected.

Added Support for the Internet Communication in Fifth/Third Mode

Support for the internet HTTPS communications channel has been added for the Universal Credit Card drivers (both authorization and settlement) configured in Fifth/Third Mode. Previously, only TCP/IP and dial-up communications channels were allowed.

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 revision in this release.

ReadMe First
V 4.2.12.766

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.2 release of the Universal Credit Card Driver (VisaNet).

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
Fifth/Third Bank Communication	85

New Features Detailed

Fifth/Third Bank Communication

The Universal Credit Card driver now supports communication to Fifth/Third Bank. Communication can be implemented using either dial-up or TCP/IP methods.

To enable Fifth/Third mode, enter "3" in the **Custom Mode** field (*POS Configurator* | *Devices* | *CA/EDC Drivers* | *System*) for the VSCA Authorization and VSST Settlement drivers.

Refer to the online help for information in setting the rest of the driver options.

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
Added Override Comments to Batch Transfer Status Report	86
Dynamic Batch Numbering Mode	87
Format Change to Help Locate Error Messages in 3700d.log Files	88
Retrieval Reference Number Removed From Voucher Printing	88

Enhancements Detailed

Added Override Comments to Batch Settlement Process

When a settlement ends without receiving a batch close response, that batch is considered unsettled. The CC Driver will not automatically override an unsettled or "quarantined" batch. This must be handled manually by locating the relevant batch history record in the registry, and resetting the **Override** DWORD value at the root of the batch to 1. (For more on this process, refer to the **Duplicate Batch Prevention** feature in the Version 4.1.8.584 release.)

Once a batch was settled, the only way to determine whether the **Override** option had been used, was by reviewing the information in the Registry — a risky and impractical solution. To improve batch auditing capabilities, the settlement process was modified to include override information on the Batch Transfer Status Report. Now, when a batch attempt fails, and the **Override** option is set in the Registry; the word 'Override' is printed, along with the batch information, on the Batch Transfer Status Report.

Dynamic Batch Numbering Mode

With this release, the batch settlement process was enhanced to allow users to determine the circumstances under which a batch number is incremented. This option also determines where the batch number is recorded in the Registry.

New Options

To support this enhancement the following option was added to the settlement driver in POS Configurator (Devices | CA/EDC Drivers | System):

- **Batch Numbering Mode** — Specifies the method used to assign and increment batch numbers during settlement. The options are:

  0 — Static Batch Numbering. Assigns a new number to each batch received by the driver. The number is unique to that particular batch and will be used for all settlements attempts. This method was designed to prevent duplicate batches. It is the default mode.

  1 — Dynamic Batch Numbering Mode. Assigns the next valid number to any batch that is presented for settlement. The number is only incremented when the driver receives a Good Batch (GB) response from the host.

Registry Changes

During batch settlement, the CC Driver records each attempt to settle a batch in the registry. The data are stored in hierarchical format, located at:

HKLM\Software\MICROS\Common\CCS\DrvrCfg\DrvrX\History

A Registry key is created for each credit card batch, consisting of a 9-character string representing the batch number. The number is formatted with leading zeros to allow batches with a variable number of digits to be sorted in the correct order.

In static mode, the batch number is recorded at the History level since the number does not change per attempt.

In dynamic mode, the batch number can change from one attempted settlement to another, provided that a different batch is successfully settled in the interim. To track the assignments, the most recent batch number is stored in its own Attempt subkey beneath the History level.

Format Change to Help Locate Error Messages in 3700d.log Files

When an Internet error occurs and the UCC driver cannot access the Primary Host, it switches to the Backup Host and records the error in the 3700d log. This message is now surrounded by asterisks (*** text ***) to make it easier to locate in the log.

Retrieval Reference Number Removed From Voucher Printing

Due to changes in the requirements, an authorized transaction's Retrieval Reference Number (i.e., the host-generated number used to identify a transaction) will no longer print on the credit card voucher or in the system's Journal file.

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:

Feature	CR ID	Page
Authorization Attempt Fails After Check of Comm Status	N/A	89
Batch Errors Not Processed Immediately If Received Before Batch Close Request	N/A	90
Fallback Mode Results in CCS Assertion Error	20128	90
Faulty Transmit Error Handling	N/A	90
Log Files Not Recording Transaction Detail	N/A	90
Premature Timeouts Cause False Quarantines on WinNT	20126	91
WinInet Does Not Log Correct Error Message	N/A	91

Revisions Detailed

Authorization Attempt Fails After Check of Comm Status

CR ID #: N/A

After using VSST diagnostics to check communications status, a dial-up error would occur when the user initiated an authorization. The problem occurred because VSST was not releasing the comm port and TAPI was not being initialized properly before the AUTH attempt. This has been corrected.

Batch Error Not Processed Immediately If Received Before Batch Close Request

CR ID #: N/A

When settling a batch using TCP/IP mode, the driver would ignore batch error or duplicate batch responses that arrived before the batch close request was sent. This created unnecessary delays in settling credit card records.

To correct this problem, the driver was modified to check for data received from the host. If a message is detected, the driver will stop sending requests and attempt to accumulate and process a host response.

Fallback Mode Results in CCS Assertion Error

CR ID #: 20128

When authorizing a transaction while in fallback mode, the driver would periodically attempt an HTTPS connection which, in turn, would cause an assertion error at the CCS. To correct this problem, the assertion has been replaced with additional logging. Now, if there is a premature attempt to initialize an HTTPS connection, the error "HTTP connection not available" will be recorded.

Faulty Transmit Error Handling

CR ID #: N/A

Previously, if a batch failed during settlement using TCP/IP, the UCC driver did not distinguish between errors recorded during transmission and those that occurred during the receive process. With the introduction of the **Duplicate Batch Prevention** feature, failure to properly identify when the error occurred would cause some batches to be incorrectly marked for quarantined. This problem has been corrected.

Log Files Not Recording Transaction Detail

CR ID #: N/A

When ringing a positive authorization, followed by a void transaction for the same amount, on the same credit card, the settlement driver failed to record the transaction detail in the 3700d.log and the VSST.log files. Instead, the driver would repeat the trailer several times. This problem has been corrected.

Premature Timeouts Cause False Quarantines on WinNT

CR ID #: 20126

When running batch settlement using HTTPS on a Windows NT platform, the connection would prematurely timeout, resulting in a false quarantine. To correct the problem, the ping-timeout value has been increased from 15 to 90 seconds and hard-coded in the driver.

WinInet Does Not Log Correct Error Message

CR ID #: N/A

Previously, if a batch failed during settlement using HTTPS, the UCC driver would return a System Error 183 instead of reporting the correct Internet Error. This problem has been corrected.

ReadMe First
V 4.1.8.584

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.1 release of the Universal Credit Card Driver (VisaNet).

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
Configurable Internet Host Header and Target Name	93
Duplicate Batch Prevention	94

New Features Detailed

Configurable Internet Host Header and Target Name

Internet HTTPS communications for Universal CC drivers (CaVSCA and CaVSST) involve message headers containing certain fields. Among these are the **Host Header** and **Target Name**, which could change depending upon the specific NXT network or host to be used.

Currently, Universal CC drivers use default values of **gateway-bmd.nxt.com** for the **Host Header** and **/Micros/process_transaction.cgi** for the **Target Name**.

During certain test conditions, the defaults may be overridden via **Option** values in the Registry, or they may be changed through the POS Configurator. To make room among the existing fields (*Devices* | *CA/EDC Drivers*), the following changes have been made to the configuration files for the Universal CC drivers:

- The **Currency Code** and the **Country Code** fields have been converted from strings to numbers, and have been moved from the *System* tab to the *Merchant* tab.
- Two new fields — **Internet Host Header** and **Internet Target Name** — have been added to the *System* tab. A maximum of 25 characters is allowed. These fields are required for internet communications to work. They are not required for the configuration of the driver.

Duplicate Batch Prevention

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 transactions. This feature was designed to prevent the creation of duplicate credit card batches.

> ***Note*** *This feature is turned on by default. Refer to Miscellaneous Configuration Options on page 100 for instructions on disabling.*

Causes

The identified causes of a duplicate batch can be divided into two Scenarios:

- **Scenario 1** — For TCP or HTTPS protocols, a timeout or other communication error occurs while waiting for the Batch Close response as described below:
  - The settlement process successfully proceeds to the Batch Close request.
  - The CC Driver submits the batch to the processor.
  - The processor settles the batch and responds to the CC Driver.
  - The good batch (GB) response does not get back to the CC Driver.
- **Scenario 2** — For all protocols, system is unable to get the good batch response from the CC Driver through CCS and CAEDC.dll into the MICROS database.

In both scenarios, the status of the batch is left unsettled in the MICROS database. In either case, a subsequent settlement attempt may or may not be posted as a duplicate by the credit card processor. This depends on the processor's ability to detect the incompletely settled batch.

Solution

To improve the processor's ability to detect (and thus prevent) a duplicate batch, changes were made to the way batch numbers are managed. Now, when an Open Batch request is initiated, a processor batch number (which is different from the MICROS' batch sequence number) is assigned. This number is saved in the registry and re-used for any subsequent settlement attempts of the same batch sequence number.

The change provides the Credit Card Driver with all of the information needed to prevent duplicate batches. By persisting the status of each batch settlement attempt in the registry, the driver can refuse to re-settle a batch that has either ended in a communication error after the batch close request was sent (Scenario 1 above) or was successfully settled but did not receive its good batch confirmation (Scenario 2).

Unsettled Batches

When a settlement ends without receiving a batch close response, that batch is considered unsettled. The driver will not attempt to resubmit an unsettled batch to the processor again.

In addition, any attempt to settle these types of batches (either through the Credit Card Batch Utility or as part of an autosequence) will be prohibited by the driver. The results of each attempt will be duly noted in the registry key history, as described above.

Scenario 1

For Scenario 1 settlement attempts (communication error before GB response), the driver will fail the Batch Open request and provide a descriptive message to be included in the Batch Transfer Status Report. The batch will remain unsettled in the MICROS database. It is the site's responsibility to monitor the failure, contact a support representative, and take the appropriate corrective action.

Overriding Unsettled Batches

The CC Driver does not override an unsettled or "quarantined" batch. This must be handled manually by locating the relevant batch history record in the registry, creating the **Override** DWORD value at the root of the batch, and setting it to 1.

When an override settlement is attempted, the CC Driver resets the data in the **Override** key value to 0. This prevents multiple overrides of the same batch from generating duplicate batches.

Once an attempt fails, the user must reset the value to 1 before trying again. There are exceptions; for example, when the failure results from an inability to connect to the host. In this case, since the batch process was never actually started, the attempt terminates before the **Override** value is changed. The value will still be set at 1 when the next attempt is made.

Finally, the driver determines whether to allow a batch to be settled based on the highest numbered attempt recorded in the registry. In other words, if there are three attempts listed in the registry, the system will use the data in the last entry (Attempt03) to determine whether the settlement process will be allowed.

Scenario 2

For Scenario 2 settlement attempts (batch settled but GB response not sent), the driver will "simulate" a successful settlement. The processor will not actually be contacted, however. Appropriate messages will appear on the Batch Transfer Status Report and the batch will be marked as settled.

Purging

By default, the CC Driver stores the most recent 100 days of batch history or the last 100 batches, whichever is greater. This can be overridden by the DWORD registry entry **HistoryAgePurgeThreshold**, located in the **Option** subkey.

Regardless of the setting, the CC Driver will only execute a purge when the number of batches in the history exceeds 100. In other words, the driver will always keep the most recent 100 batch histories, no matter how old they are. The default of 100 can be changed via the DWORD registry value **HistoryCountPurgeThreshold**, also located in the **Option** subkey.

Note *If the Batch Sequence Number is reset to 1 (e.g., by clearing totals or manually deleting batches from the database), the system will automatically delete the entire Batch History. This prevents new batches from being linked to previous Batch History records.*

Registry Changes

During batch settlement, the CC Driver records each attempt to settle a batch in the registry. The data are stored in a hierarchical format, located at:

HKLM\Software\MICROS\Common\CCS\DrvrCfg\DrvrX\History

Key values are added based on the following:

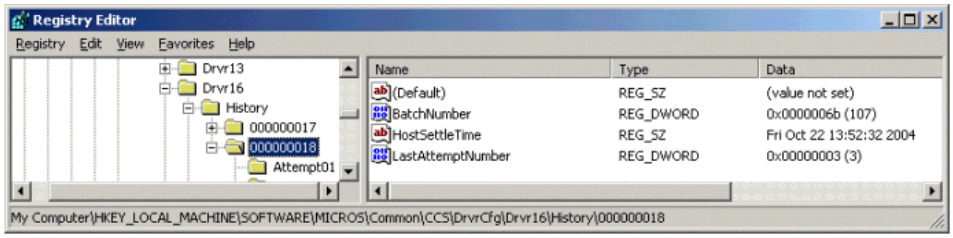
Batches

A registry key is created for each credit card batch. The key consists of a 9-character string representing the batch number. The number is formatted with leading zeros to allow batches with a variable number of digits to be sorted in the correct order.

At this level, the following information is stored:

- **BatchNumber** — DWORD value. Assigned by the driver on the first settlement attempt and re-used for all subsequent settlement attempts.
- **Override** — DWORD value. Created manually and set to 1 to enable the driver to re-settle an otherwise quarantined batch.
- **HostSettleTime** — STRING value. Indicates when the batch was actually settled.
- **LastAttemptNumber** — DWORD value. A convenience for the driver. Assists in creating the next Attempt subkey.

The following illustrates how the open batch request would be saved in the registry:



Settlement Attempt

A registry key is created for each batch settlement attempt. The key name is formatted as **AttemptXX**, where **XX** represents an incrementing count of the number of attempts. The format allows the system to correctly sort up to 99 separate settlement attempts.

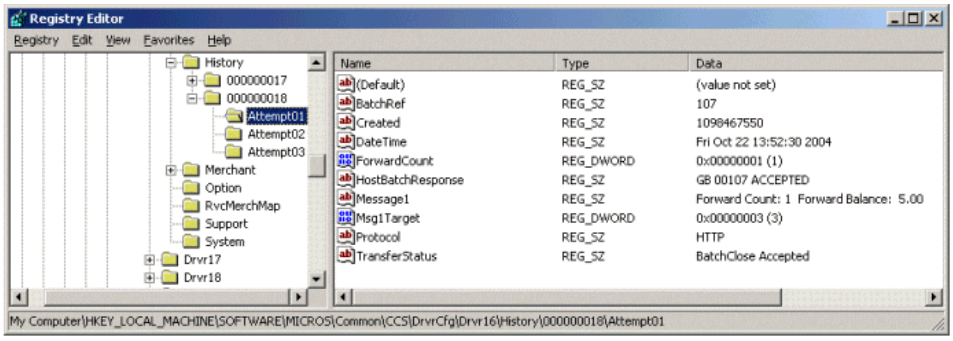
NOTE: Additional attempts are not prohibited; however, the additional digits will be included in the name, which may interfere with the sort order.

At this level, the following information is stored:

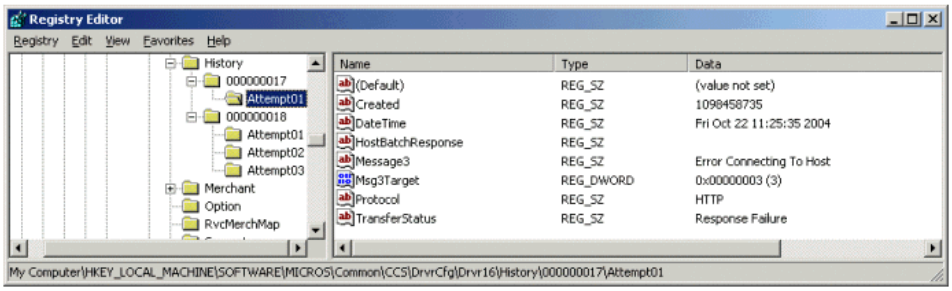
- **DateTime** — STRING value. Formatted as DOW MON HH:MM:SS:YYYY where DOW is Day of Week and MON is the abbreviated Month. For example: Fri Oct 22 13:52:30 2004
- **Created** — DWORD value. Records the system time of the attempt in the numerical format needed for comparison within the driver. Represents the same actual time as the **DateTime** value.
- **Protocol** — STRING value. Indicates the type of interface connection used for this settlement attempt. The value will be one of the following: *DIAL*, *TCP*, or *HTTPS*.

- **HostBatchResponse** — STRING value. Used to store the response from the host (expected to be either a GB, RB, or QD), along with the rest of the response message.
- **TransferStatus** — STRING value. Used by the CC Driver to record (or "remember") how far it made it through a settlement. This value tracks the batch transfer through the various stages of the settlement, recording the progress. (Refer to the TransferStatus table beginning on page 101 for a list of possible notations.)
- **Overridden** — DWORD value. Indicates that this settlement attempt was done as an override. This value is not always present. It is only created if the **Override** value at the root of this batch was set to 1 for this attempt.
- **BatchRef** — STRING value. Needed for Local Accept of a batch. This value is recorded from the update response back to the CCS. It includes the Batch Number.
- **ForwardCount** — STRING value. Needed for Local Accept of a batch. This value is recorded from the update response back to the CCS.
- **MessageX** — STRING value. Needed for Local Accept of a batch. This value is recorded from the update response back to the CCS. Up to four messages may be present, where X represents a numeral from 1 to 4.
- **MsgXTarget** — DWORD value. Needed for Local Accept of a batch. This value is recorded from the update response back to the CCS. Up to four messages may be present, where X represents a numeral from 1 to 4. In this instance, they instruct POS Operations on how to display or print the corresponding messages.

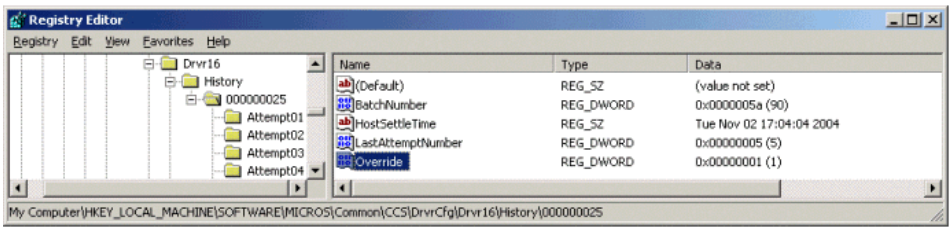
The following illustrates how a **successfully settled batch attempt** would be saved in the registry:



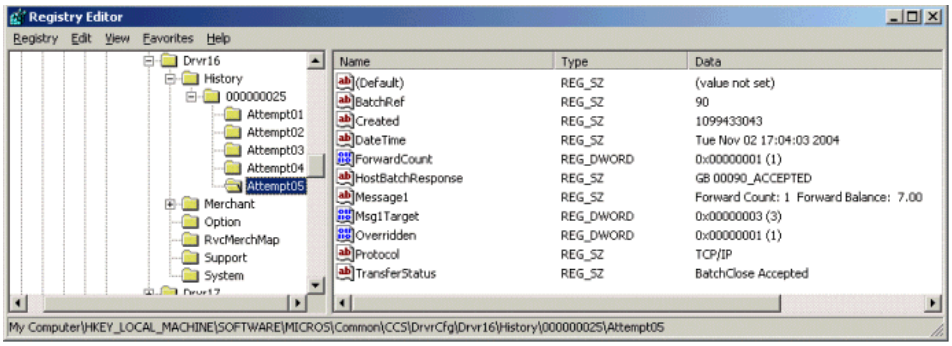
In comparison, if the **settlement timed out** waiting for a batch close response, the attempt would be logged in registry as follows:



To correct the problem, the user could **set the Override value to 1**:



And attempt to settle the batch again.



Miscellaneous Configuration Options

- **DisableDuplicatePrevention —** DWORD Value. Allows the user to disable the duplicate batch prevention function. If activated, the history of each settlement attempt will still be maintained in and purged from the registry. The difference is that the CC Driver will always allow a settlement attempt, regardless of the previous attempt's TransferStatus.

  To control the feature, the DisableDuplicatePrevention is added in the **..\DrvrX\Option** key. A non-zero value will direct the CC Driver to always attempt a settlement. If this value is not present (the default situation) or is present and contains a 0, the function will be disabled.

- **DisableBatch History** — DWORD Value. Disables the storage of Batch History entries in the registry. This can be done to improve system performance or reduce the size of the registry.

  To control the feature, the DisableBatchHistory is added in the **..\DrvrX\Option** key. A non-zero value prevents the CC Driver from adding batch history records to the registry. If this value is not present (the default situation) or is present and contains a 0, the function will add batch history records as described previously.

  If the Batch History function is disabled, the Duplicate Batch Prevention function will also be disabled.

TransferStatus Values

The TransferStatus is stored as a descriptive string to allow support personnel to troubleshoot .

TransferStatus	Description
BatchOpen Submitted	The driver received the Batch Open Request from CCS. A settlement ending in this status indicates that the CC Driver or CCS crashed while processing the request or waiting for the response.
BatchOpen Accepted	The request was accepted by the host.
BatchOpen Rejected	The request was rejected by the host. Driver successfully received a response.
BatchOpen Error	A format or transmission error occurred that prevented the request from being sent.
BatchDetailXXX Submitted	Batch detail number XXX was received from CCS. A settlement ending in this status indicates that the CC Driver or CCS crashed while processing the request.
BatchDetailXXX Accepted	Batch detail number XXX was accepted.
BatchDetailXXX Rejected	The request was rejected by the host. Driver successfully received a response.
BatchDetailXXX Error	A format or transmission error occurred that prevented the request from being sent.
BatchClose Submitted[1]	Batch close request was received from CCS. A settlement ending in this status indicates that the CC Driver or CCS crashed while processing the request.
BatchClose Accepted[2]	The request was accepted by the host.
BatchClose Rejected	The request was rejected by the host. Driver successfully received an RB response.
BatchClose Duplicate[1]	The request was declined by the host. Driver successfully received a QD response.
BatchClose Error	A format or transmission error occurred that prevented the request from being sent.
Response Failure[1]	A timeout, host abort, or I/O error occurred, preventing the reception of a useable response.
Quarantined[1]	The settlement attempt was prevented due to the TransferStatus of the most recent attempt.
Local Accept[2]	The batch had been settled previously. The driver responded with host data from the previous settlement.

[1]CC Driver will prevent another settlement attempt.

[2]CC Driver will auto-settle the batch without contacting the host.

Batch Transfer Status Report Messages

The following table provides examples of the types of error messages that could be included on a Batch Transfer Report when a batch settlement is prevented to avoid duplication. The entries are not definitive, but for illustration purposes only.

Previous Transfer Status	New Transfer Status	Report Messages
None	BatchClose Submitted	Msg1: Error [-2] Waiting for Update From Credit Card Service Msg2: ODBC NOT Initialized
BatchClose Submitted	Quarantined	Msg1: Settlement prevented to avoid duplicate batches. Msg2: Please contact your support personnel for assistance.
None	BatchOpen Error	Msg1: Error Connecting to Host
BatchOpen Error	BatchClose Accepted	Msg1: Forward Count: 1 Forward Balance: 7.00 (After regaining connection.)
None	Response Failure	Msg 1: Socket IO Error
Response Failure	Quarantined	Msg1: Settlement prevented to avoid duplicate batches. Msg2: Please contact your support personnel for assistance.
None	BatchClose Rejected	Msg1: Header Record: Unknown Error Msg2: Batch Error Text from VisaKHost
BatchClose Rejected	BatchClose Rejected	Msg1: Header Record: Unknown Error Msg2: Batch Error Text from VisaKHost
None	BatchClose Duplicate	Msg1: Duplicate Batch [081] detected by Host
BatchClose Duplicate	Quarantined	Msg1: Settlement prevented to avoid duplicate batches. Msg2: Please contact your support personnel for assistance.
Quarantined	Quarantined	Msg1: Settlement prevented to avoid duplicate batches. Msg2: Please contact your support personnel for assistance.

Previous Transfer Status	New Transfer Status	Report Messages
None	BatchClose Accepted	Msg1: Forward Count: 1 Forward Balance: 7.00
BatchClose Accepted	Local Accept	Msg1: Standard Fwd Count and Balance message Msg2: Batch Accepted Locally Msg3: Previously settled by host on Tues Nov 02 15:34:00 2004
Local Accept	Local Accept	Msg1: Standard Fwd Count and Balance message Msg2: Batch Accepted Locally Msg3: Previously settled by host on Tues Nov 02 15:34:00 2004

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
Configuring the CC Driver's COM Port Settings	105
Enhanced Logging at Verbosity Level 0	105
Enhanced Logging for TAPI and Modem Line Error Conditions	105
Increased Internet Connect Timeout Default From 30 to 240 Seconds	106
Support for TAPI Version 2.2	106
'Merchant Info Error' Added to Batch Transfer Status Report	106

Enhancements Detailed

Configuring the CC Drivers Com Port Settings

Due to communications problems involving shared modems in a Win2K environment, the CaVSCA and CaVSST drivers no long contain hard-coded COM port settings.

To ensure that the authorization and settlement processes work properly, users must do one of the following:

1. Manually set the com port settings in the Microsoft Control Panel to:

   Baud Rate = 2400
   Parity Type = Even
   Num Data Bits = 7
   Num Stop Bits = 1

2. Run **settle-c** after installing the drivers and configuring them.

Enhanced Logging at Verbosity Level Zero

The Universal Credit Card driver has been enhanced to log more detailed information when the verbosity level is set at 0. Log files will now include basic and significant information about the batch, including the comm channel, host response, and batch number (which is stored in the registry). Also included are any events linked to the duplicate batch prevention function — such as Local Settle, Overrides, or Quarantines — which may be helpful in diagnosing settlement errors.

Finally, the diagnostic functions which manage the batch number have been enhanced to allow the merchant number to be omitted if only one merchant is configured.

Enhanced Logging for TAPI and Modem Line Error Conditions

The Universal Credit Card driver has been enhanced to log more detailed information when the driver fails to establish a connection with the credit card server. To assist the customer in diagnosing a problem, the log file will note when the failure was caused by the following circumstances:

- No Answer
- Line Busy
- No Dial Tone
- Disconnected.

Increased Internet Connect Timeout Default From 30 to 240 Seconds

When settling a batch using an HTTPS comm link, the connection of the socket, transmission, reception of a response, and closing the connection are all bundled into a single HTTPS function. Initially, the default timeout value was at 30 seconds. This could cause problems when processing a large number of credit card records.

To reduce errors, the default value for the Internet Connection Timeout for the HTTPS functions (connect, receive, and send) were raised from 30 seconds to 4 minutes (240 second).

Support for TAPI Version 2.2

The Universal Credit Card driver has been modified to include support for TAPI Version 2.2 for the Windows 2000 operating system. Previously, the driver only supported Version 1.4.

The change allows for backwards compatibility to RES 3.0, as well as Windows NT. During initialization, the driver will determine the operating system in use and initialize the appropriate TAPI version.

'Merchant Info Error' Added to Batch Transfer Status Report

The UCCD Driver has been modified to handle a new type of HTTPS Rejected Batch response to be in compliance with the VisaK "Vital Residency Requirement Error." The error — which is caused by improper configuration of the Merchant ID or BIN number — will be noted in the Batch Transfer Status Report as a 'Merchant Info Error.'

.

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:

Feature	CR ID	Page
Blank Spaces in Phone Number Configuration Creates Unnecessary Fallback Attempts	N/A	108
Disruption During Fallback Mode Results in False Batch Settlement	N/A	108
Duplicate Batch Open Response Returned To CCS	N/A	108
HTTPS Skips Backup Connection	N/A	109
Incorrect Authorized Amount for Credits/Returns	N/A	109
Missing Asterisk in Error Messages from Host	N/A	109
Multi-Trans Authorizations Persist After 3 NAKs Received	N/A	109
NAK Not Logged After Receiving Bad LRC	N/A	109
No Response to Initial Heartbeats Leads to Disconnection	N/A	110
Settlement Times Out Prematurely	17921	110
Unable to Initialize Universal Driver With 7-Digit RVC Object Number	N/A	110
Unable to Start CC Server with No Modem Configured	N/A	110

Revisions Detailed

Blank Spaces in Phone Number Configuration Creates Unnecessary Fallback Attempts

CR ID #: N/A

When using the Universal Credit Card driver, a failed TCP/IP or Internet connection will automatically revert to a dial-up connection, provided that a Primary and/or Backup Phone Number has been included in the driver configuration. This is referred to as fallback mode. To disable the feature, the phone number fields are simply left blank.

In the past, if a user emptied a field by typing spaces over the number instead of deleting the entry, the driver would read the spaces as an entered value. This resulted in unnecessary attempts (and failures) at fallback mode. To correct the problem, the driver will now consider empty, any phone number field that contains only spaces.

Disruption During Fallback Mode Results in False Batch Settlement

CR ID #: N/A

When settling a batch in fallback mode, if the modem connection was disrupted during the batch close response, the attempt would be recorded in the batch history as an incomplete settlement. That is, the transfer status would indicate Batch Close Accepted but without a corresponding "good batch" response from the host. Because the Credit Card Batch utility looks for open batches based on their transfer status, this prevented the user from attempting to settle this batch again. This problem has been corrected.

Duplicate Batch Open Response Returned To CCS

CR ID #: N/A

A duplicate batch open response was being returned to the Credit Card Server (CCS) by the Universal driver while in dial-up mode. When the second batch open response was returned, the Credit Card Server would receive a response that it believed had already been responded to. This resulted in the "Ignoring driver response..." message being logged. Now a duplicate batch open response is not returned.

HTTPS Skips Backup Connection

CR ID #: N/A

Previously, if the Universal driver failed to establish a connection with the primary URL, it would revert to fallback mode (i.e., dial-up) without first attempting to connect to the backup URL. This has been corrected.

Incorrect Authorized Amount for Credits/Returns

CR ID #: N/A

The **Authorized Amount** field of the batch detail record was incorrectly showing the total credit/return amount. This has been corrected to show a zero in the **Authorized Amount** field for credits/returns.

Missing Asterisk in Error Messages From Host

CR ID #: N/A

During settlement, error messages from a host were not preceded by an asterisk which, by tradition, indicates their point of origin. This has been corrected.

Multi-Trans Authorizations Persist After 3 NAKs Received

CR ID #: N/A

When using a dial-up modem to authorize multiple credit card transactions, the driver would stall if the first transaction failed to establish a viable connection with the processor. This caused the remaining authorization requests to be held up unnecessarily.

To correct the problem, the driver will now hang up and redial the modem for the next request whenever the first request has received 3 NAKs (indicating a communications failure).

NAK Not Logged After Receiving Bad LRC

CR ID #: N/A

Previously, if a bad LRC was detected on an authorization response, a NAK request was not being logged for a re-transmission of the response. This has been corrected.

No Response to Initial Heartbeats Leads to Disconnection

CR ID #: N/A

When using the TCP communications channel, the Universal driver failed to respond to the initial TCP/IP Heartbeats from the host, which in turn, caused the host to disconnect. Once the connection was reestablished, the driver would respond properly. This has been corrected.

Settlement Times Out Prematurely

CR ID #: 17921

When performing credit card settlement over an internet HTTPS comm channel, the communication would occasionally timeout if a 'good batch' response was not received from the credit card processor within 30 seconds of the HTTPS Post being sent. This has been corrected.

Unable to Initialize Universal Driver With 7-Digit RVC Object Number

CR ID #: N/A

Previously, the Universal Authorization and Settlement credit card drivers were unable to initialize when a 7-digit revenue center object number was configured. This has been corrected.

Unable to Start CC Server with No Modem Configured

CR ID #: N/A

If the Universal driver was configured with a telephone number, but no modem was configured on the PC, an Exception error would occur and the Credit Card Server was unable start. This has been corrected.

ReadMe First
V 4.0.2.286C

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 4.0 release of the Universal Credit Card Driver (VisaNet).

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
Disable Authorization Code Limits	112
Edit Batch Numbers	113

New Features Detailed

Disable Authorization Code Limits

In the past, the CaVSST settlement driver would not accept a batch detail record where the manually entered authorization code was longer than 6 digits. When such a record wa located, the batch process would be aborted. this created problems in certain environments, where users had legitimate reasons for entering a fake manual authorization code that exceeded the allowed 6-digit length.

To accommodate these users, a new System-level option was added to the CaVSST driver. The option Disable Auth Code Limit, allows the user to determine whether or not an oversized (i.e., greater than 6 digits) authorization code will be accepted. To set this option, select:

- **0** — (Default Behavior) Aborts a batch settlement if the file contains a detail record with a manually entered code that is longer than 6 digits.
- **1** — Accepts batch files that include detail records with manual authorization codes of more than 6 digits. When an oversized auth code is located, the driver automatically truncates the code to the first 6 digits before continuing to process the batch file.

Edit Batch Numbers

A new diagnostic tool has been added to support the changing of the next batch number. Only a trained MICROS Support person should use this tool.

Users can troubleshoot problems with the CA/EDC driver or with a credit card batch by using one of the diagnostic tests available in the Credit Card Batch Utility. The number and types of tests available will depend on the driver selected. For VISANet drivers, these functions include:

Get Version Number
Test Settlement Connection
Get Batch Number
Set Batch Number

Procedures

To run a test of the installed CA/EDC drivers:

1. Open the Credit Card Batch Utility and select the **[Diagnostics]** button.

2. From the CA/EDC Drivers list, select the CaVSST driver.

3. Select a Diagnostic Function from the list of entries.

4. (Optional) For some drivers, an additional command may be allowed/ required. If necessary, enter this information in the User Defined Data field.

   For example, the CaVSST driver allows the user to view or modify a specific batch number. In this case, the User Defined Data field is used to specify: 1) the desired Merchant for both the Get Batch Number and Set Batch Number commands, and 2) the new Batch Number for the Set Batch Number command.

   The Merchant number must be entered because the Batch Number is kept on a per-merchant basis. In a multi-merchant setup, the Merchant numbers are available to the user through POS Configurator. In a single-merchant setup, the Merchant number should be entered as 0.

   When setting the Batch Number, the new number must be entered after the Merchant number. The two should be separated by a non-numeral such as a comma (e.g., 3, 355). Valid Merchant numbers range from 1 to 999.

5. Press the **[Begin Test]** button to run the test. The results will be posted in the Status Information box on the right.

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
Enhanced Verbosity Control	114
Increased Default Batch Close Response Time-out for TCP/IP Settlement	115

Enhancements Detailed

Enhanced Verbosity Control

With this release, the system was modified to allow for more flexibility in changing the verbosity of the CaVSCA and CaVSST credit card drivers. This is done by recalculating the verbosity level with each new authorization or diagnostic request. To do this, the credit card driver will reread Support information, including the driver's verbosity, from the Registry. It will also read the verbosity setting for the Credit Card Server (CCS)

The driver's verbosity setting will be compared to CCS's verbosity setting. The higher of the two will be compared to the current verbosity setting being used by CaVSCA or CaVSST. If they are different, the newly determined higher setting will be chosen as the new current verbosity setting for the drivers.

Changes to the verbosity will be logged, as will additional information about the verbosity selection process whenever the new verbosity is 3 or higher.

Increased Default Batch Close Response Time-out for TCP/IP Settlement

With this release, the default batch close response timeout parameter was extended from 30 seconds to 90 seconds when using the TCP/IP communications channel. The change only affects TCP/IP settlements. The default timeout for dial-up connections remains 30 seconds and the default timeout for HTTPS remains at 240 seconds.

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:

Feature	CR ID	Page
Credit Card Server Locks Up When Started From Control Panel	16467	117
Driver Fails to Recover TCP/IP Connection After Error	N/A	117
EOT From Host Causes False Settlement	N/A	117
Error During Credit Card Settlement	15389	117
Error Posted When Changing to Internet Communications Channel	N/A	117
Error Reported When a Second Batch is Sent to Settlement Before First is Complete	N/A	118
False Internet Batch Close Response Precedes Failure of Next Batch	N/A	118
Log Entry Incorrect After HTTPS Ping to Host	N/A	118
Modem Required Even When Dial-Up is Not Programmed	N/A	119
Test Connection Diagnostic Not Working Properly for Authorization	N/A	119
Transaction Abort Not Handled Properly	N/A	119
Universal CC Drivers Spontaneously Reconnecting During TCP/IP Communications	16465	119

Revisions Detailed

Credit Card Server Locks Up When Started From Control Panel

CR ID #: 16467

Previously, if the system was configured for KDS or SVS gift cards, any attempt to start the Credit Card Server (CCS) from the Control Panel while using the Universal CC drivers could cause the CCS Service to hang. This problem occurred when a socket connection was established during initialization of the CCS Service instead of waiting until the first authorization request was made. This has been corrected.

Driver Fails to Recover TCP/IP Connection After Error

CR ID #: N/A

While settling credit cards, if the driver receives an error message from the processor, it will fall back to dial-up, without attempting to reestablish the TCP/IP connection. The only way to recover the TCP/IP connection was to restart the Credit Card Server. This has been corrected.

EOT From Host Causes False Settlement

CR ID #: N/A

During a dial-up settlement, if the CaVSST driver received an EOT from the host prior to receiving and responding to the Batch Close Response, the batch would be incorrectly marked as settled, even though the individual transactions were not marked as such and the host had not actually processed the batch to a settlement. This problem has been corrected.

Error During Credit Card Settlement

CR ID #: N/A

Previously, when running a credit card batch settlement, an error was posted while retrieving data from the credit card server. The problem was a synchronization issue between the credit card server and the credit card driver. This has been corrected.

Error Posted When Changing to Internet Communication Channel

CR ID #: N/A

After switching to the Internet Comm channel, every attempt to connect to NXT would result in a Windows System Error 183. The problem was related to the timing of the call to GetLastError( ). which fetches the most recent Windows error code. Instead of making the call immediately, the system would wait until later, including it as part of a common error handling routine. This has been corrected.

Error Reported When a Second Batch is Sent to Settlement Before First is Complete

CR ID #: N/A

For credit card settlements using the HTTPS protocol with a Universal CC driver, an error message would be reported if the user attempted to send a second batch immediately after posting the first batch. The second batch would not be sent.

The problem was related to the way batches were handled by the system. Before a second batch could be started, the first batch had to be gathered, composed, and transferred to the credit card processor. For large batches, this could take some time. To ensure that the batch did not time out, a timer thread was started and updated periodically. Once the batch was transferred, a batch close request would be processed and the timer thread would be closed.

If the second batch arrived before the close request was completed on the first, the system would try to find and terminate the first timer thread before starting a new one. However, if the first timer thread took longer than 20+1 seconds to terminate, it was considered a "zombie thread" and an error message would be generated.

To correct the problem, the programming was changed to allow the batch timer thread to be persistent for the life of the driver. Subsequent batches can now be sent right away without incurring an error.

False Internet Batch Close Response Precedes Failure of Next Batch

CR ID #: N/A

After processing a credit card batch using an Internet communications channel, the system would report the batch file as closed, but without supplying a forward count or balance. The next batch would then fail by exceeding the limit on detail records. This has been corrected.

Log Entry Incorrect After HTTPS Ping to Host

CR ID #: N/A

When issuing an HTTPS ping to the host, the CaVSST driver was posting a log entry that appeared as though a VSST batch close record had been sent with the ping. This has been corrected.

Modem Required Even When Dial-Up is Not Programmed

CR ID #: N/A

After setting the **Communications Channel** (*POS Configurator* | *Devices* | *CA/EDC Drivers* | *System*) to TCP/IP or Internet, the driver was still looking for an **Auth Phone Number** and **Backup Auth Phone Number** and attempting a dial-up connection. When a phone number was not found, a TAPI (dial-up) error message would be displayed.

The problem was caused by a coding error, which required the user to identify a modem in the **Settlement Device** field even for TCP/IP and Internet communications. This has been corrected.

Test Connection Diagnostic Not Working Properly for Authorization

CR ID #: N/A

The test connection diagnostic, which is issued from the Batch Settlement user interface, was reporting a good connection when it hadn't actually checked the status of the internet communications channel. This has been corrected.

Transaction Abort Request Not Handled Properly

CR ID #: N/A

When the Credit Card Server (CCS) times out before receiving authorization from the driver, a transaction abort request is generated by the CSS to terminate the thread.

Previously, when the transaction abort was passed to the CaVSCA driver, the CSS would report back to the POS with the message "No Response From Driver," but the driver would not actually abort the transaction or remove the authorization request from its queue. This problem has been corrected.

Universal CC Drivers Spontaneously Reconnecting During TCP/IP Communications

CR ID #: 16465

When using Universal CC drivers, the system would spontaneously disconnect and then reconnect the TCP/IP connection. To correct the problem, code was added to reset the inactivity count whenever a response is received, a communications error is detected, or a reconnected is commanded.