micros®

Restaurant Enterprise Series

Virtual Net Credit Card Driver for 3700 POS Version 4.12

August 27, 2012

MD0003-092

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.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information recording and retrieval systems, for any purpose other than for personal use, without the express written permission of MICROS Systems, Inc.

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

Trademarks

FrameMaker is a registered trademark of Adobe Corporation.

Microsoft, Microsoft Excel, Win32, Windows, Windows$^{®}$95, Windows 2000 (Win2K), and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

Visio is a registered trademark of Visio Corporation.

All other trademarks are the property of their respective owners.

Installation and Setup

This section contains installation and setup instructions for the Version 4.9 release of the Virtual Net (VN) Credit Card Driver. The VN driver communicates with WorldPay, formerly known as RBS Lynk. 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 VN Driver may be used on RES systems running Version 4.3 HF2 or 4.5 and higher.

In This Section...

Installation

Site Requirements

Before installing the Virtual Net (VN) Credit Card Driver on the RES system, the following configuration items should be considered:

- The installed version of 3700 POS should be Version 4.3 HF2 or 4.5 and 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 fallback to dial-up when using TCP 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 VN Driver is divided into an authorization driver and a settlement driver. The following lists the files installed for each:

Authorization

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

Settlement

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

Additional Files

\Micros\Common\Bin\libeay32.dll
\Micros\Common\Bin\ssleay32.dll
\Micros\Common\Bin\McrsOpenSSLHelper.dll
\WINNT\System32\MSVCR71.dll

Note *The MSVCR71.dll file is installed if it is not found in the \WINNT\System32 directory when the installation program is executed.*

Installation Instructions

The installation of the credit card drivers are separate from the RES software. The Virtual Net driver is an independant install. When upgrading RES, the Virtual Net driver will not be affected.

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. Shutdown the RES system from the **MICROS Control Panel**.

3. Download the latest Virtual Net Credit Card 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:

   - VN Credit Card Driver Installation Documentation (**CaVN_RMF.pdf**).
   - CaVN(4.12.0.2438).exe

4. Double click the CaVN(4.12.0.2438).exe. This will install all the necessary files on the RES Server and on the BSM Client, and Windows Services will be restarted automatically. The MICROS Credit Card Server service will restart automatically during the first Authorization Request or if the Credit Card Batch Utility is started.

5. Go to *POS Configurator* | *Devices* | *CA/EDC Drivers* and configure the following settings for the authorization driver (VNA):

   - 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. VN Auth).
   - Select the ***Driver*** tab and enter VNA as the authorization **Driver Code**.

6. Go to the *System* tab and configure the following settings:

   Authorization Device – Specify the modem to use for authorization requests. Reference the modem using a one-digit number. Use 1 for the first modem listed in Control Panel, 2 for the second, etc. Use 0 for no device.

   To determine the number to enter, type settle -m from a command prompt in the \POS\bin directory. The following sample messages display:

   ```
   Device [1]: Boca 28.8 Kbps V.34 MV.34E
   Device [2]: Standard 1200bps Modem
   Device [3]: Standard 2400 bps Modem
   ```

   Select the appropriate device number.

Note: The modem must be configured in Control Panel before it can be assigned as an authorization device.

Not Used – Leave this field blank.

Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter 1 to enable port arbitration when more than one credit card driver is being used. Enter 0 to disable the option.

Note: Port arbitration is usually enabled.

Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor.
The options are:

- 0 - dial-up
- 1 - Private Network/Unencrypted (Not Used)
- 2 - Public Network/Encrypted

Enable 12-Digit Amount – This field determines whether the credit card processor can accept an amount up to 12-digits long (excluding separator).

The options are:

- 0: Off (not allowed)
- 1: On (allowed)

Auth Phone Number – Enter the telephone number used for authorizations. Your Credit Card Processor will provide this number.

Enter the number as follows:

- Do not include hyphens.
- Include any necessary long distance access code and area code, for example, 14105551212.
- Include any dialing prefix necessary to get an outside line, for example, 914105551212.

Backup Auth Phone Number – Enter the backup authorization phone number provided by your Credit Card Processor. (This field is optional. You may not have a backup number.)

If the system attempts to perform an authorization but cannot get a telephone connection using the Auth Phone Number (for example, if the line is busy or the modem cannot make a connection), the backup number will be used. Enter the number as follows:

- Do not include hyphens.
- Include any necessary long distance access code and area code, for example, 14105551212.
- Include any dialing prefix necessary to get an outside line, for example, 914105551212.

City (Zip) Code – Enter the 3-digit number assigned by the Credit Card Processor to further identify the merchant location within a country. In the USA, the 5- or 9-digit Zip code for the merchant is used. Merchants located outside of the USA will be assigned a number by the Credit Card Processor.

Time Zone – Enter the 3-digit number assigned by the Credit Card Processor used to calculate the local time within the VNANet (i.e., standard local time zone differential from Greenwich Mean Time (GMT).

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

Merchant State - Enter the 2-character state/province code assigned by the Credit Card Processor used to identify the merchant. The 2-characters entered here must correspond to the state/province that prints on the credit card voucher.

Host URL Part 1 – Enter the first part of the URL address of the primary host connection. This consists of the protocol and the site name.

Host URL Part 2:Port – Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.

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

BackUP URL Part 2:Port - Enter the second part of the URL address of the backup host connection. This consists of the domain and the port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

7. Go to the *Merchant* **|** *Authorization* tab and configure the following settings:

   Not Used – Leave this field blank.

   Industry Code – This field is used to identify the type of industry for this merchant.

   - Enter 1 if the merchant business is a retail establishment.
   - Enter 0 if the merchant business is a restaurant.

   Language Code – This field is used to identify the language in which authorization response messages will be returned for display and/ or printing. Select the language code from the following list:

   - 0 (zero) English
   - 1 Spanish
   - 2 Portuguese
   - 3 Irish
   - 4 French
   - 5 German
   - 6 Italian

   Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.

   Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.

   Bin Number – Enter the 6-digit Bank Identification Number assigned by the Credit Card Processor.

   Merchant Number – Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor.

   Store Number – Enter the 4-digit number used to identify the merchant store. This number is assigned by the Credit Card Processor.

   Terminal Number – Enter the 4-digit number used to identify a specific terminal within an establishment.This number is assigned by the Credit Card Processor. Each terminal in the establishment must have a unique number.

Merchant Category – Enter the 4-digit number used to identify the merchant type. This number is assigned by the Credit Card Processor.

Merchant Name – Enter the name of the merchant (up to 25-characters). This name must correspond to the name that prints on the credit card voucher.

8. Go to *POS Configurator* | *Devices* | *CA/EDC Drivers* and configure the following settings for the settlement driver (VNS):
   - 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. VN Settle).
   - Select the *Driver* tab and enter VNS as the settlement **Driver Code**.
9. Go to the *System* tab and configure the following settings:

   Not Used – Leave this field blank.

   Settlement Device – Specify the modem to use for settlement requests. Reference the modem using a one-digit number. Use 1 for the first modem listed in Control Panel, 2 for the second, etc. Use 0 for no device.

   To determine the number to enter, type settle -m from a command prompt in the \POS\bin directory. The following sample message displays:

   Device [1]: Boca 28.8 Kbps V.34 MV.34E
   Device [2]: Standard 1200 bps Modem
   Device {3}: Standard 2400 bps Modem

   Select the appropriate device number.

   Note: The modem must be configured in Control Panel before it can be assigned as settlement device.

   Port Arbitration Enabled – This field prevents errors by checking port availability before attempting an authorization request. Enter 1 to enable port arbitration when more than one credit card driver is being used. Enter 0 to disable the option.

   Note: Port arbitration is usually enabled**.**

Communications Channel – This field specifies the type of interface connection used between the merchant and the credit card processor.

The options are:

- 0 - dial-up
- 1 - Private Network/Unencrypted (Not Used)
- 2 - Public Network/Encrypted

Disable Auth Code Limit– This field determines whether or not the credit card driver will accept a manually entered authorization code that is longer than 6 digits.
The options are:

- 0 - Aborts a batch settlement if the batch file contains a detail record with an authorization code larger than 6 digits.
- 1 - Accepts files for batch settlement that contain oversizes authorization codes in the detail records. When an oversized auth code is found, truncates the number to the first six digits before counting.

Batch Numbering Mode– This field specifies the method to be used when assigning batch numbers during credit card settlement.
The options are:

- 0 - Static Barch Mode. Assigns a new number to each batch recieved 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 vaild 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.

Settle Phone Number - Enter the telephone number used for settlement. Your Credit Card Processor will provide this number.

Enter the number as follows:

- Do not include hyphens.
- Include any necessary long distance access code and area code, for example, 14105551212.
- Include any dialing prefix necessary to get an outside line, for example, 914105551212.

Backup Settle Phone Number - Enter the backup settlement phone number provided by your Credit Card Processor. (This field is optional. You may not have a backup number.)

If the system attempts to perform a settlement but cannot get a telephone connection using the Settle Phone Number (e.g., the line is busy, modem cannot make a connection, etc.), the backup number will be used. Enter the number as follows:

- Do not include hyphens.
- Include any necessary long distance access code and area code, for example, 14105551212.
- Include any dialing prefix necessary to get an outside line, for example, 914105551212.

City (Zip) Code - Enter the 3-digit number assigned by the Credit Card Processor to further identify the merchant location within a country. In the USA, the 5- or 9-digit Zip code for the merchant is used. Merchants located outside of the USA, will be assigned a number by the Credit Card Processor.

Time Zone - Enter the 3-digit number assigned by the Credit Card Processor used to calculate the local time within the VNSNET Settlement System (i.e., standard local time zone differential from Greenwich Mean Time (GMT).

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

Merchant State - Enter the 2-character state/province code assigned by the Credit Card Processor used to identify the merchant. The 2-characters entered here must correspond to the state/province that prints on.

Host URL Part 1 - Enter the first part of the URL address of the primary host connection. This consists of the protocol and the site name.

Host URL Part 2:Port - Enter the second part of the URL address of the primary host connection. This consists of the domain and the port number.

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

BackUP URL Part 2:Port - Enter the second part of the URL address of the backup host connection. This consists of the domain and the port number. Backup connections are triggered when the system cannot establish communication via the primary host address.

8. Go to the *Merchant* **|** *Settlement* tab and configure the following settings:

Not Used – Leave this field blank.

Industry Code - This field is used to identify the type of industry for this merchant.

- Enter 1 if the merchant business is a retail establishment.
- Enter 0 if the merchant business is a restaurant.

Language Code – This field is used to identify the language in which settlement response messages will be returned for display and/ or printing. Select the language code from the following list:

- 0 (zero) English
- 1 Spanish
- 2 Portuguese
- 3 Irish
- 4 French
- 5 German
- 6 Italian

Append Option Data Group – This option determines whether the expiration date and stripe data will be appended to the batch detail record.

Enter 0 to disable the option.

Enter 1 to append the data.

Note: Append Option Data Group should not be enabled when using the Fifth Third Bank Custom Mode. Any settlement records with the optional data appended will be rejected when using the Fifth Third Bank.

Currency Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the type of currency used. In the USA, the code is 840.

Country Code – Enter the 3-digit number assigned by the Credit Card Processor to identify the country in which the merchant is located. In the USA, the code is 840.

Acquirer BIN Number - Enter the 6-digit Bank Identification Number assigned by the Credit Card Processor.

Merchant ID Number - Enter the 12-digit number used to identify the merchant. This number is assigned by the Credit Card Processor.

Store Number - Enter the 4-digit number used to identify the merchant store. This number is assigned by the Credit Card Processor.

Terminal Number - Enter the 4-digit number used to identify a specific terminal within an establishment. This number is assigned by the Credit Card Processor. Each terminal in the establishment must have a unique number.

Merchant Category - Enter the 4-digit number used to identify the merchant type. This number is assigned by the Credit Card Processor.

Merchant Name - Enter the name of the merchant (up to 25-characters). This name must correspond to the name that prints on the credit card voucher.

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

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

Merchant Location Number - Enter the 5-digit number that provides additional information on the location of the merchant. This number is assigned by the Credit Card Processor. Unless specified otherwise by the merchant’s bank or processor, the default for this field should be 00001.

10. Go to *POS Configurator* | *Sales* | *Tender Media* | *Credit Auth* tab. Link all of the appropriate credit card tenders (e.g., Visa/Mastercard) to the NV drivers by configuring the following fields:
    - **CA Driver** – Use the drop down box to select the CaNVA driver.
    - **EDC Driver** – Use the drop down box to select the CaNVS driver.

Setup

Communication Channels Supported

0 - dial-up

1 - Private Network/Unencrypted (Not Used)

2 - Public Network/Encrypted

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 Virtual Net Credit Card Driver.

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 platforms:

1. From the ***Microsoft 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 the **[OK]** button to save and close the **System** forms.

13. Exit the Control Panel and reboot the PC.

Configuring TCP/IP 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 a credit card processor or via a corporate WAN connected to a credit card processor.

Network configurations are typically setup one of two ways:

- Satellite connection from each site to a credit card processor. This requires contracting with a satellite vendor that has a frame-relay connection from their satellite hub to a credit card processor.

- Connection from each site to a corporate WAN and frame-relay connection from corporate to a credit card processor.

1. Host And Backup Host Configuration

In order to process via TCP/IP, contact the credit card processor for Host configuration information.

2. Fallback Configuration

The VN Driver 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 CC processor 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 VN Driver 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 Credit Card Processor’s Network

The easiest way to test the connection from the RES Server to the credit card processor’s network through a frame circuit is by pinging from a command line on the RES Server. For more information, contact the credit card processor for connection information.

5. Test TCP Connectivity via Credit Card Utility

Another way to test the connection (from the RES Server to the credit card processor’s 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 VN’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, the credit card processor’s 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.

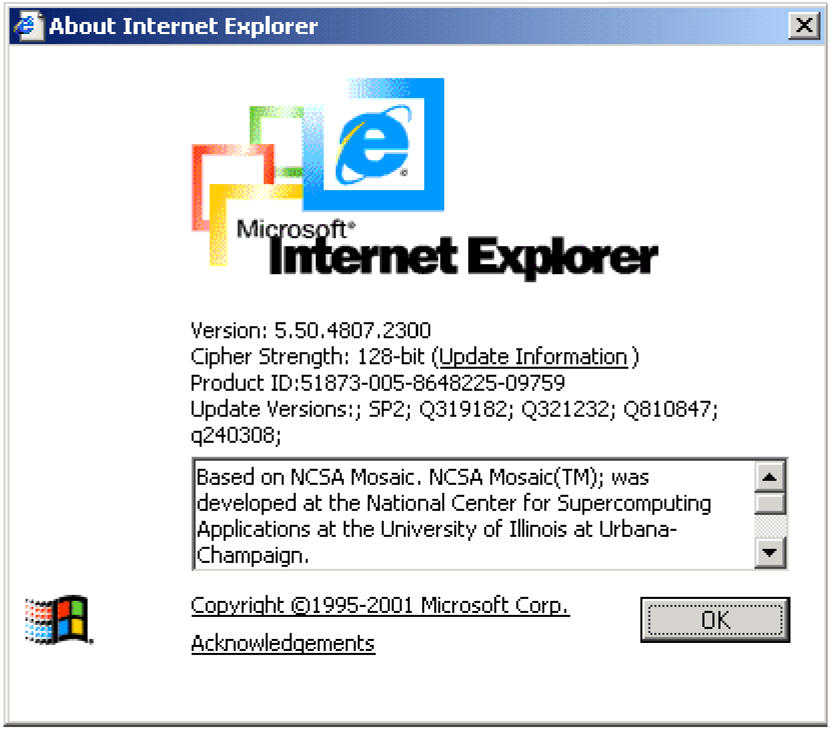
2. Internet Connectivity

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 the credit card processor, 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:



Version: 5.50.4807.2300
Cipher Strength: 128-bit (Update Information)
Product ID:51873-005-8648225-09759
Update Versions:; SP2; Q319182; Q321232; Q810847; q240308;

Based on NCSA Mosaic. NCSA Mosaic(TM); was developed at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.

Copyright ©1995-2001 Microsoft Corp.
Acknowledgements

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. Host and Backup Host Configuration

To process via a high-speed internet connection, the site must be able to connect to the credit card processor. This requires configuring the fields on the *System* tab (*POS Configurator | Devices | CA/EDC Drivers*) for both the authorization and settlement drivers. Contact the credit card processor for primary and backup host port assignments.

5. 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 VN 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.

6. Fallback Configuration

The VN Driver 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 credit card processor 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 VN Driver 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**.

7. 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 their network, 3700 POS, and their data against unauthorized access and any damage and support costs incurred as a result of said access.

8. 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 VN 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

The VN Driver setup is not done until the VNS and VNA 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 with the Host Processor.

Frequently Asked Questions

Why do I have to take down the entire system when loading the new credit card drivers?

When loading any type of software, the standard is to turn off all running applications during installation. MICROS recommends turning off the RES system completely during the installation. The installation program only requires those applications that use the credit card drivers to be turned off (i.e., POS Configurator, Credit Card Server, Credit Card Utility).

What happens if I forget to shut down the Credit Card Server or the system?

If run properly, the VN Driver Installation program does not require a reboot of the RES Server.

However, it is necessary when an application that uses the VN Drivers is left on during the VN Driver Installation. In this case, the program will not overwrite the existing files, but will store the new files in a temporary location. Once the installation is complete, the user will be prompted to reboot the system. Only then will the new driver files be copied from the temp folder to their proper location.

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 Virtual Net 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?

Duplicate batches 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 Virtual Net (VN) Credit Card Driver for the prevention of duplicate batches. 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, or was successfully settled but did not receive a good batch confirmation

ReadMe First V4.12.0.2438

This section contains a comprehensive guide to the Version 4.12 release of the Virtual Net (VN) Credit Card Driver.

In This Section...

What’s New

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

New Features Summarized

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
Open SSL Libraries have been Updated	29

Enhancements Detailed

Open SSL Libraries have been Updated

CR ID #: N/A

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

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	Page
CCS will not start with Auth Phone Number Configured	30

Revisions Detailed

CCS will not start with Auth Phone Number Configured

CR ID #: 32533

Previously, the MICROS Credit Card Service (CCS) would not start if the **Auth Phone Number** or **Backup Auth Phone Number** *(POS Configurator | Devices | CA / EDC | System)* were configured. This has been corrected.

ReadMe First V4.9.21.2351

This section contains a comprehensive guide to the Version 4.9 release of the Virtual Net (VN) Credit Card Driver.

In This Section...

What's New

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

New Features Summarized

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

Feature	Page
Authorization Reversals Are Now Supported	32
Partial Credit Card Authorization	32
Settlement Driver Now Supports AMEX Batch Records	35
Comm Channel 2 Now Supports TCP/IP With Open SSL	35

New Features Detailed

Authorization Reversals Are Now Supported

CR ID #: N/A

With this release, authorization reversals are now supported. Visa is 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.

Partial Credit Card Authorization

CR ID #: N/A

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.

Settlement Driver Now Supports AMEX Batch Records

CR ID #: N/A

With this release, authorizations from the AMEX driver can be settled through the Virtual Net driver.

The support of pre-settle authorization reversals for AMEX batch records have also been added.

Comm Channel 2 Now Supports TCP/IP With Open SSL

CR ID #: N/A

With this release, Comm Channel 2 now supports TCP/IP with Open SSL for authorizations and settlements.

Note *RFID support has been added with 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

There are no revisions in this release.

ReadMe First
V4.3.16.1056

This section contains a comprehensive guide to the Version 4.3 release of the Virtual Net (VN) Credit Card Driver.

In This Section...

What's New

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

New Features Summarized

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

Feature	Page
TCP Communication Mode Option Bit Added	39

New Features Detailed

TCP Communication Mode Option Bit Added

In order to allow a site to communicate through their private network, a Transmission Control Protocol (TCP) option bit has been added to the credit card authorization (VNA) and settlement (VNS) drivers.

The TCP/IP option bit enables a site to transmit data across a network or from one host to another. Customers with multiple store locations can now send credit card authorization data to a central network location before being transmitted to the processor.

To enable the TCP mode option, go to *POS Configurator* | *Devices* | *CA/EDC Drivers* | *System tab* and set the **Communications Channel** to 1.

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

There are no revisions in this release.