Oracle Hospitality RES 3700

Universal Credit Card Driver including Ventiv Version 5.1

July 2016

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

When upgrading the Universal Credit Card Driver including Ventiv to v5.1, 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 5.0 or higher.

****

Installation and Setup

This section contains installation and setup instructions for the Version 5.1 release of the Universal Credit Card Driver (UCCD) including Vantiv. The release version is available on the Oracle web site Product Support page.

Before installing this driver, please familiarize yourself with the changes by reviewing the ReadMe First Section of this document.

This version of the UCCD may be used on RES systems running Version 5.0 or higher.

In This Section...

Installation

Site Requirements

Before installing the Universal Credit Card Driver including Ventiv on the RES system, the following configuration items should be considered:

- The installed version of 3700 POS should be Version 5.0 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 Universal Credit Card Driver 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 V5.0 (or Higher)

1. Make sure all current batches have been settled. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
2. Download the latest Universal Driver from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
   - Universal Credit Card Driver for RES 3700 POS (**UCCDV5.1_MD.pdf**)
   - Oracle RES Universal Credit Card Driver (**CaUCCD(5.1).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(5.1).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 V5.0 (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. Oracle recommends installing a new driver before the site opens for the day. This will ensure that all CA/EDC transactions have been settled to their current version.
3. Download the latest Universal Driver from the Oracle web site. Copy this file to your RES Server's temp folder and unzip the files. The zip file includes the following:
   - Universal Credit Card Driver for RES 3700 POS (**UCCDV5.1_MD.pdf**)
   - Universal Credit Card Driver Software (**CaUCCD(5.1).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(5.1).exe** file to execute the installation program.
7. Double-click on the **CaUCCD(5.1).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

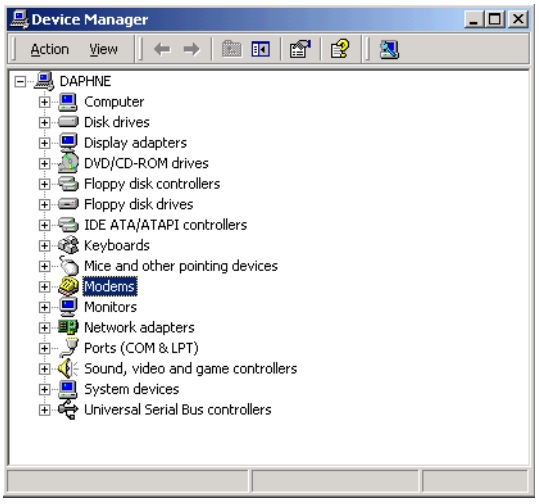
This section is provided as reference when installing the Universal Credit Card Driver. All information listed below has not changed since the initial release of a particular communication channel.

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.

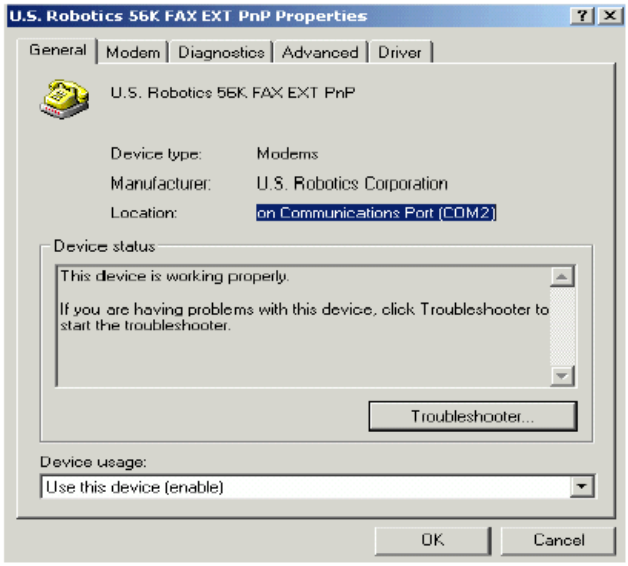
The following setup instructions are for Windows 2000 platforms:

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.

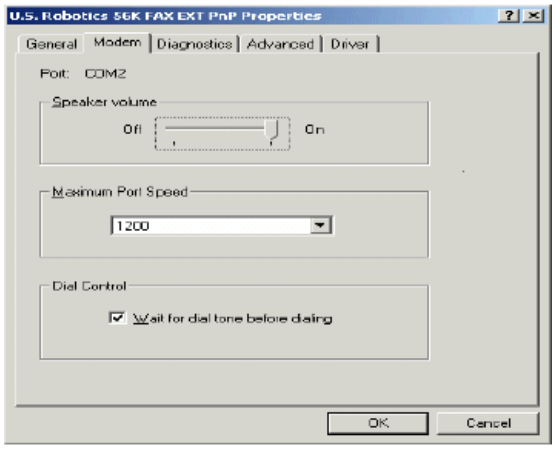


2. Expand the **Modems** entry and double-click on the modem to be used for credit card processing. The properties form will be displayed.

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



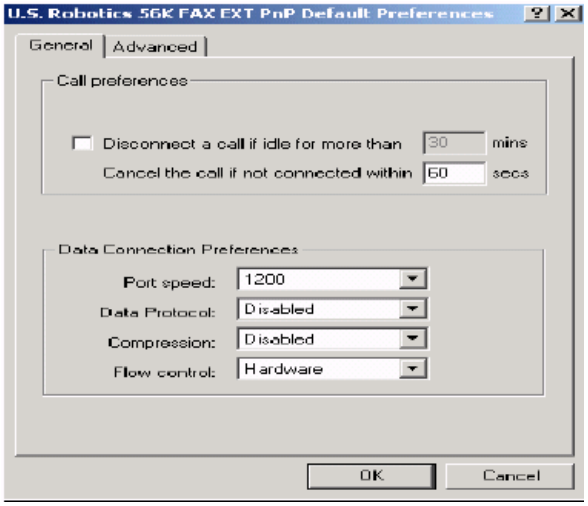
4. Go to the *Modem* tab.



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 Oracle 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, Oracle 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, Oracle 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 Oracle CA/EDC transactions.

2. Internet Connectivity

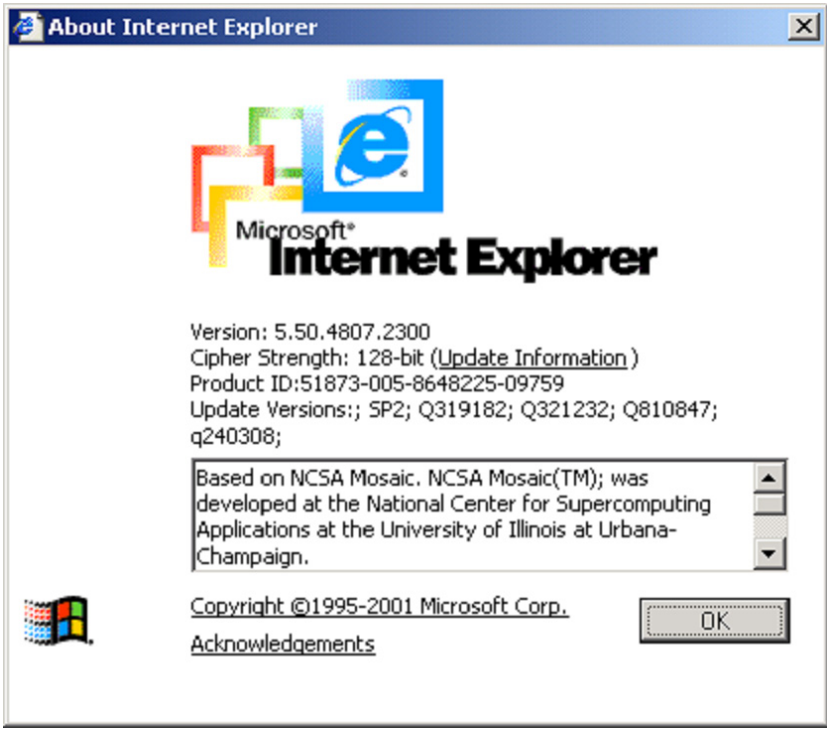
Merchants must have an ISP account that supports DSL, ISDN, or Cable modem connectivity. Connection to the Internet can also be established through a corporate LAN or WAN.

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 Oracle 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 Oracle 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, Oracle 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, Oracle 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 Oracle 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 Oracle network.

The customer is solely and entirely responsible for the security of the Oracle 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 VCC 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:

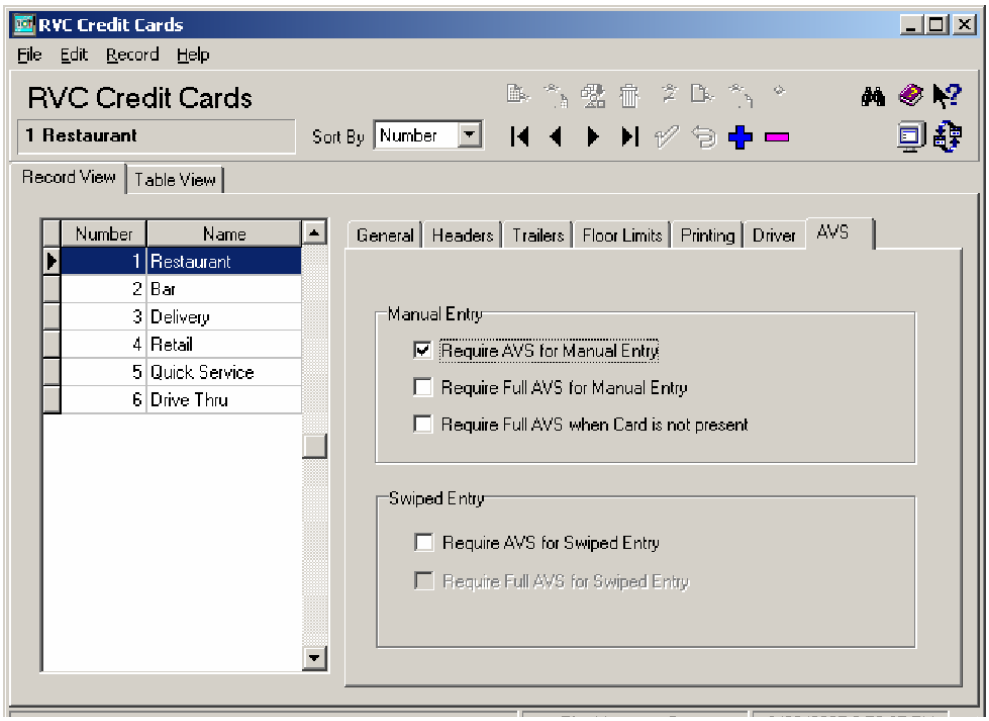
1. Go to the *\Micros\Res\POS\Etc* folder and select the **CaVSST.cfg** file.
2. When the window appears enable the **Select the program from a list** option and click **[Ok]**.
3. Highlight the **NotePad** application and click **[Ok]**.
4. Change the **MaxBatchSize** parameter setting from 300 to the 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.

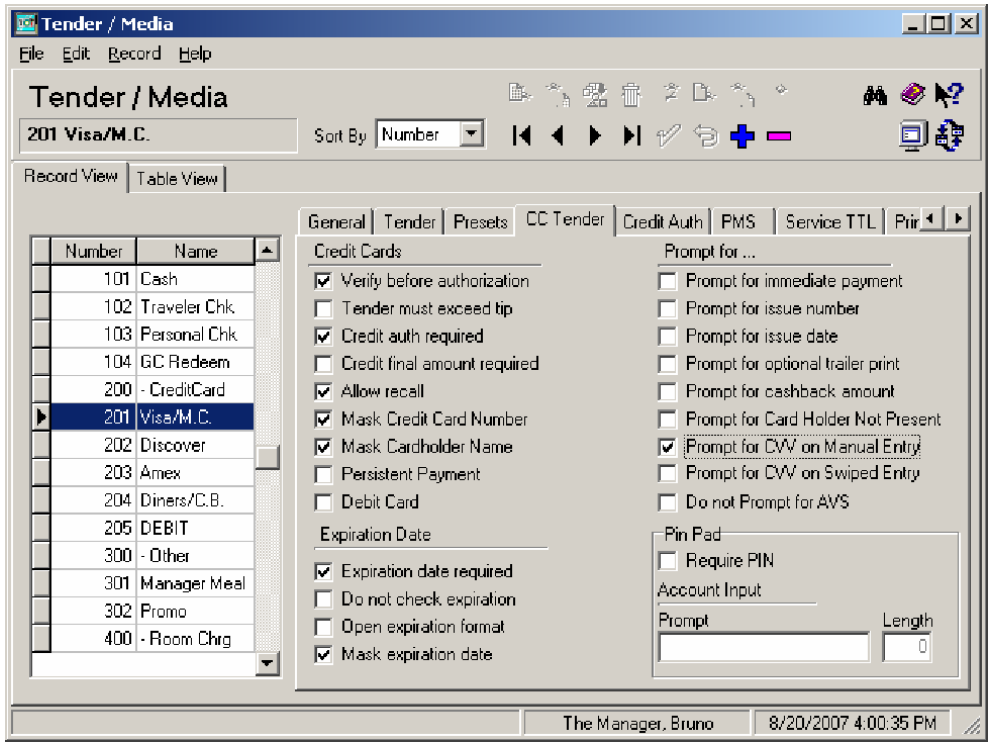
AVS is a system check that matches the address provided in the transaction to the address on file with the bank. CVV is the three or four-digit number listed on the back of the card that provides an additional level of security for the user. AVS and CVV data is transmitted in the Cardholder Identification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

Configuring Intermediate Certificates

To establish a trusted end-to-end Internet connection, you must build and verify a certificate chain by downloading or adding intermediate certificates to the trust list on the credit card server. To enable automatic downloads, open outgoing connections to the URL for each intermediate certificate.
At this time, the URL for the merchant link intermediate certificate is:
http://ss.symcb.com

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 Oracle 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?

Oracle 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. Oracle 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.

Oracle 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, Oracle has added enhancements to the Universal Credit Card Driver 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
V5.1

This section contains a comprehensive guide to the new features, enhancements, and revisions included in the Version 5.1 release of the Universal Credit Card Driver including Vantiv.

In This Section...

What's New

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

New Features Summarized

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

Feature	Page
Added support for Transport Layer Security 1.2 encryption protocol	29
Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols	29

New Features Detailed

Added Support for Transport Layer Security 1.2 Encryption Protocol

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

Removed Support for Non-Transport Layer Security 1.2 Encryption Protocols

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

What's Enhanced

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

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

Enhancements Summarized

There are no enhancements 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.