OpenEdge SecurePlus Manual

1. User Guide 4
1.1 Requirements 5
1.2 Pre-Installation Check List 6
1.3 Upgrade Notes 8
1.4 Installation Process 9
1.5 Remote Client Manager (RCM) Configuration 13
1.6 SecurePlus Configuration 17
1.7 Configure Tenders 20
1.8 Configure Gift Cards 22
1.9 Configure EdgeLink 24
1.10 Configure MISC 26
1.11 Configure Store and Forward 28
1.12 Configure Advanced 30
1.13 Process Credit/Debit/Manual Entry 31
1.14 Process Returns and Voids 35
1.15 Processing Tips 37
1.16 Gift Card Console 39
1.17 Receipt 43
1.18 Appendix 45
1.19 Contact Information 47

User Guide

Requirements

WELCOME
Thank you for purchasing the RMS OpenEdge SecurePlus add-on. The focus of the OpenEdge SecurePlus add-on is to provide a means of processing secure tokenized transactions through RMS.

INSTALLATION

The installation will need to be performed on all point of sale stations you wish to use the OpenEdge SecurePlus functionality.

REQUIREMENTS

The following prerequisites must be met prior to installing and running the application:

Supported Operating Systems

- Windows 7 (32-bit/64-bit) Windows 8 (32-bit/64-bit) Windows 8.1 (32-bit/64-bit) Windows 10 (64-bit)

Software

- Microsoft Retail Management System (v2.0.0105 and above)
- Microsoft .NET Framework v4.5.1

Hardware

- Ingenico ISC250 PIN Pad
- Ingenico ICMP 122 PIN Pad

Other

- Connection to Microsoft SQL Server:
    - SQL 2008 (Express), SQL 2008 R2 (Express), SQL 2012 (Express)* or SQL 2014 (Express)*

      *Requires SQL Browser service to be running
- ISP (Internet Service Provider)
- OpenEdge SecurePlus Account
- Make sure your firewall allows access to the following:

  URL's:
    - https://gw.t3secure.net/x-chargeweb.dll
    - https://online.t3secure.net/Dashboard/default.aspx?cid=xweb

  IP Addresses:
    - 216.7.182.196
    - 63.240.140.198
    - 63.240.140.205

  Ports:
    - 443: SSL (External)
    - 29716: Used for Manual/Batch settling (External)
    - 49201: (Internal)
    - 26: (Internal)

Pre-Installation Check List

1) What operating system are you running on the POS client stations?

- Confirm the operating system is supported.Refer to Requirements – Supported Operating System.
- Steps to determine the operating system used:

  Click on the Windows Start Menu o Choose Run
  Type “winver"

  Press Ok

2) What version of Microsoft RMS are you running?

- Confirm that RMS version meets the supported version.Refer to Requirements - Other.
- Steps to determine the RMS version:

  Run Store Operations Administrator or Manager o Choose Help
  Choose About.

3) Do you have the SQL Database credentials available? You will need the following at the time of installation:

- SQL Server Computer Name
- SQL Database Name
- SQL Server Login ID
- SQL Server Password

4) What version of SQL Server are you running?

- Confirm the SQL Server version meets supported version.Refer to Requirements– Software.
- Steps to determine the version of SQL Server using a SQL script ran against the RMS database:

  Run Store Operations Administrator o Choose File
  Choose Connect
  Enter the SQL password and Press OK o Choose Query and New

  Enter the following SQL script in the query window and Press F5 SELECT@@VERSIONAS SQL_Version

5) Was SQL Server installed with the RMS Installation Disc or as a separate instance?

- If installed separately, the SQL client components required for our integration to connect to the RMS

  SQL database may be missing. If this is the case.Refer to Appendix II – SQL Configuration

6) Is the SQL Instance listening on Port 1433?

- To check the SQL Server port. Refer to Appendix II – SQL Configuration

7) Is Microsoft.NET framework v3.5 installed on the POS client stations?

- If not, please download from:

http://www.microsoft.com/downloads/details.aspx?FamilyId=333325FD-AE52-4E35-B531-508D977D32A6&displaylang=en

8) Are you running any other RMS Add-ins?

- If the answer is yes, you will want to confirm that all add-ons are checked and updated appropriately with any updated information from our OpenE dgeSecurePlus add-on. Such as new tender types for accounting programs, SQL credentials required for connectivity, etc.

Upgrade Notes

If you are upgrading **SecurePlus** from either **SecurePlus Version 2** or **SecurePlus Version 3** then please review the following information:

Upgrading from SecurePlus Version 2:

- You can upgrade SecurePlus version 2 directly to version 4 without having to install version 3 first.
- Your settings and password for the SecurePlus Configuration software should carry over to the new version. The Merchant Token you used in version 2 is now located in the Gift tab of the Configuration software. However, this new software will require certain account information that did not exist in version 2.
  This includes:

  a. **Web ID**
  b. **Terminal ID**
  c. **Auth Key**
  d. **HostPay Merchant Token**

- SecurePlus version 4 will install software called the Remote Client Manager (RCM). This software needs to be configured before launching Microsoft RMS
- When testing the connection to your pin pad via the RCM software, be sure to click the Load Settings and Load Forms buttons before attempting any transactions.

Upgrading from SecurePlus Version 3:

- During the installation of this software you will find that the ELPC X-Charge program has been uninstalled and replaced by the Remote Client Manager (RCM) software. RCM functions in a similar fashion but is simplified and easy to configure.
- Your settings and password for the SecurePlus Configuration software should carry over to the new version. However the new software also requires the **HostPay Merchant Token**.
- When testing the connection to your pin pad via the RCM software, be sure to click the Load Settings and Load Forms buttons before using Microsoft RMS.

Installation Process

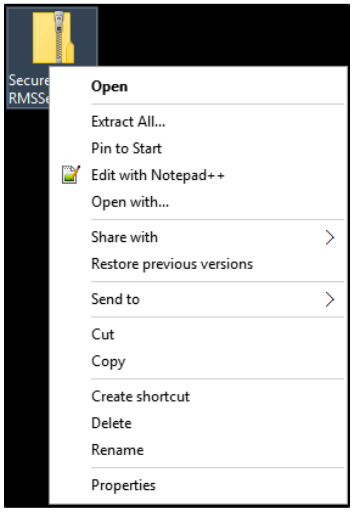
SECURE PLUS ONLY INSTALLATION WALKTHROUGH

Step #1

If the software arrived as a compressed ZIP package, or archive, (denoted by the Zipper on the folder)

extract the files by right-clicking on the archive and selecting Extract All. If the software arrived as

an executable, please continue to step #3.

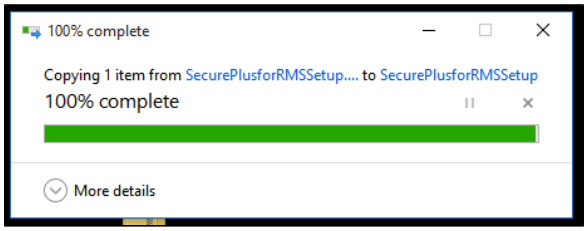


Step #2

Click **Browse** to select a folder into which the files will be extracted. By default, a new folder will be created in the same place as the archive with the same name (in this case, OpenEdgeSecurePlusSetup).

Check **Show extracted files when complete** and the folder with the new files will automatically open.

Select **Extract** and wait for the progress bar to fill, indicating that the file extraction has completed.



Step #3

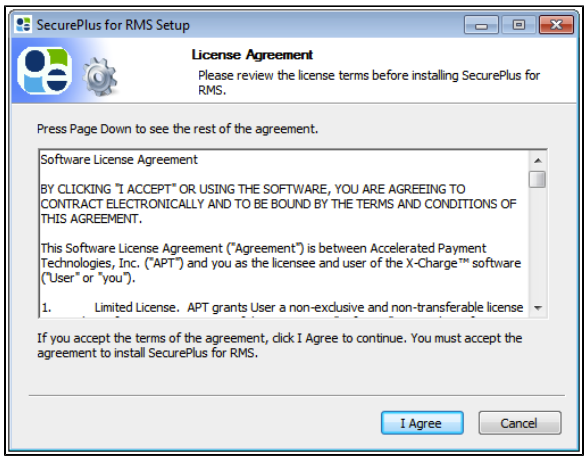
Locate the installation icon labeled **OpenEdgeSecurePlusSetup**. Right click the icon and select Open to begin installation.



Step #4

Please review the license terms before installing OpenEdge SecurePlus.

Click **I Agree** to continue.



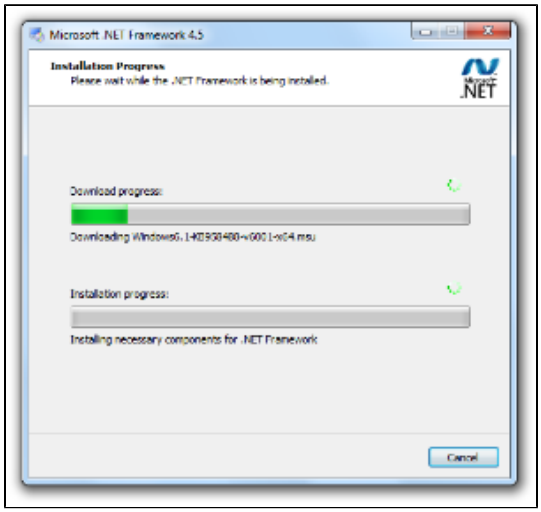
Step #5

Please review the welcome screen and perform any recommended tasks.

Click **Next** to continue.



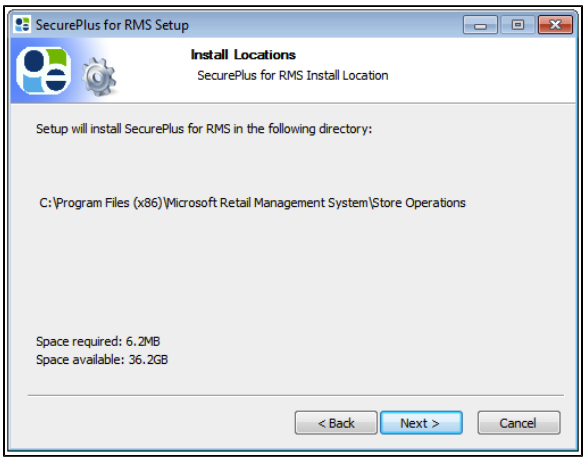
Step #6
If your computer does not have Microsoft .Net 4.5.1 currently installed then the SecurePlus installation wizard will automatically install it for you. Otherwise the installation wizard will continue on Step #7.



Step #7

Setup will install SecurePlus for RMS in the default directory.

Click **Next** to continue.



Step #8

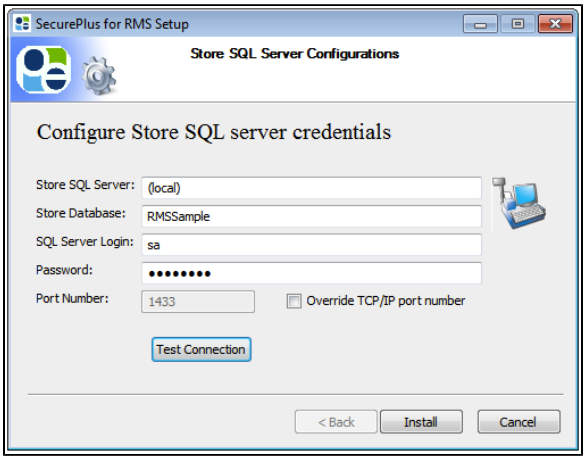
Enter the Store SQL server credentials. The settings used during installation will create any required components which need to be applied to the RMS

database.

The database settings can be found in Store Operations Administrator > File > Configuration.

Contact your system administrator to obtain SQL password authentication.

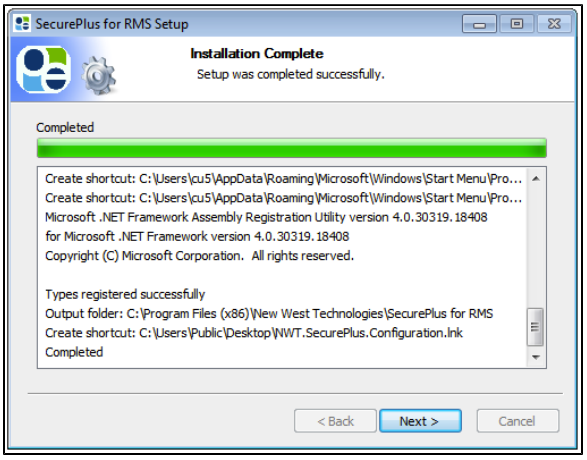
Click **Install** to continue.



Step #9

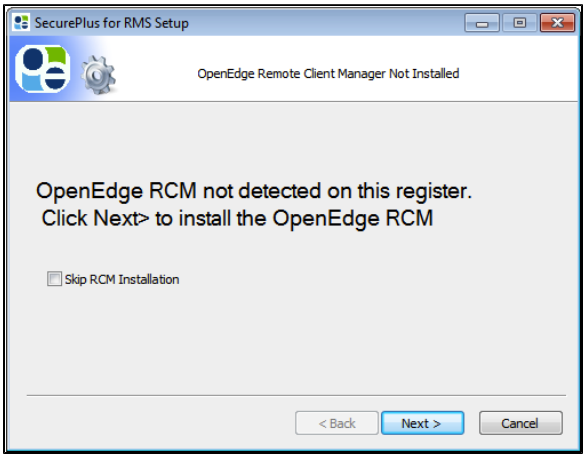
Review the installation progress and confirm successful installation.

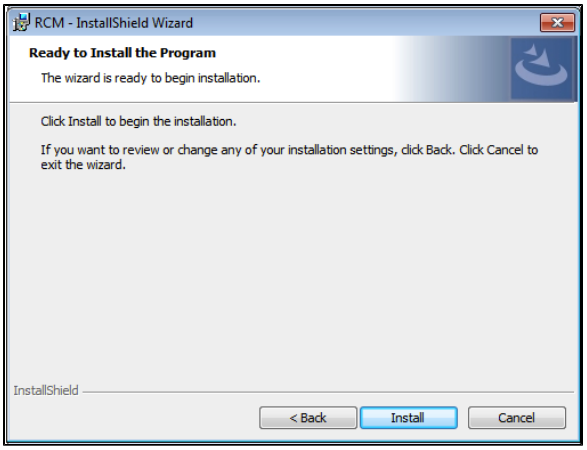
Click **Next** to continue.



Step #10

The SecurePlus installation wizard will check to see if the **OpenEdge Remote Client Manager** application is installed. If the Remote Client Manager application is not installed then simply press **Next** and it will be installed at that time.

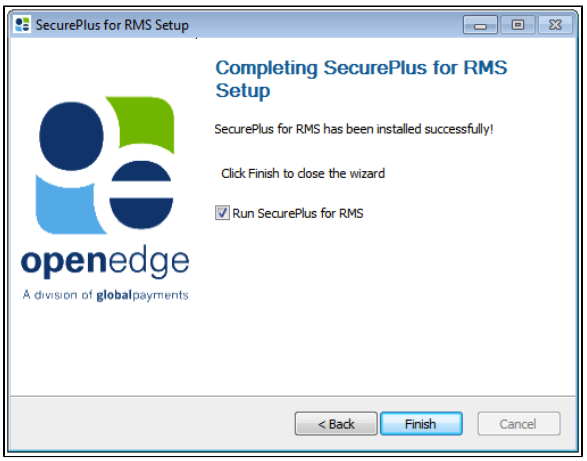




Step #11

The SecurePlus installation process should now be complete. Leave the check box marked in this window if you would like to run the SecurePlus Configuration Utility.

Otherwise click on **Finish** to close the installation wizard window.



Remote Client Manager (RCM) Configuration

Important: If you plan on using the mobile **Ingenico ICMP** PIN-Pad you will need to connect it to the POS computer via bluetooth before configuring **RCM**. If you are not using the ICMP mobile device then you can skip to Step #1 below.

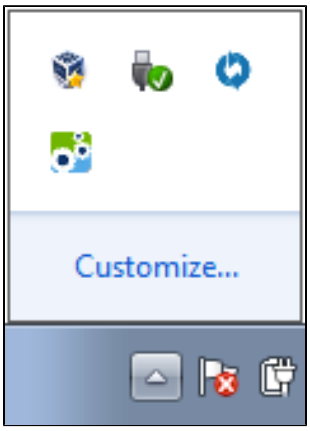
Bluetooth pairing directions for Ingenico ICMP device:

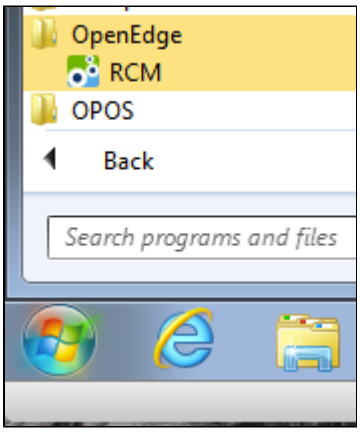
- Power on the ICMP device
- Screen will say BT Pairing Required and show options for IOS and Standard
- Press F2 button on device to select Standard
- Display will then show:
    a. BT Name
    b. PIN Number
- Enable Bluetooth on Windows computer and scan for available devices
- Select the ICMP device from the list and enter the PIN to complete pairing process.

Step #1

After SecurePlus version 4 has been installed you will need to configure the Remote Client Manager program, also called **RCM**. To open **RCM** locate the icon in your Windows Task Tray - Notification Area.

If you do not see the **RCM** icon in the Task Tray then open the Windows Start Menu, locate the OpenEdge folder and double click on the icon inside to launch **RCM**. Now it should show up in the Task Tray.



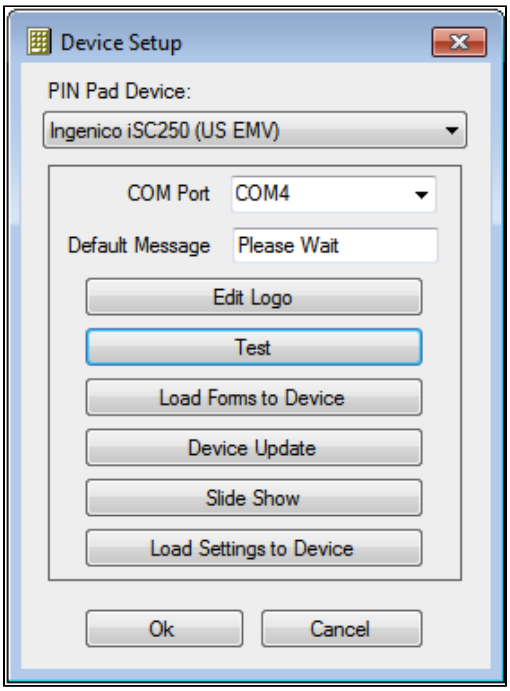


Step #2

Right click on the RCM icon in your task tray and then select **Device Setup**.

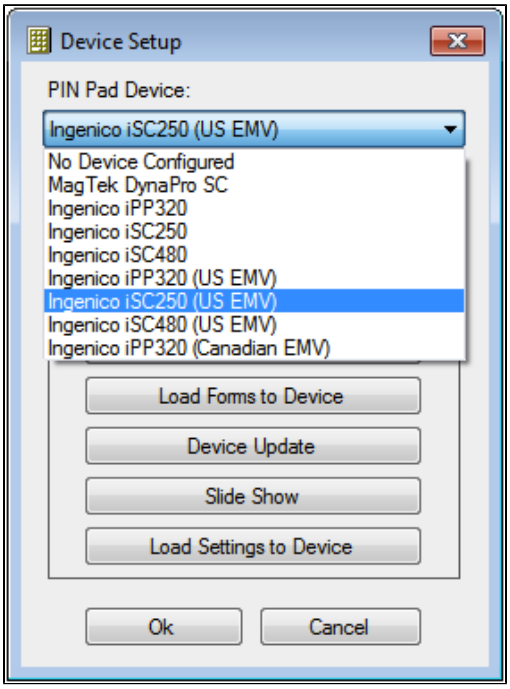
In this Device Setup window you have the following options:

- Pin Pad Device
- COM Port
- Default Message
- Edit Logo
- Test
- Load Forms To Device
- Device Update
- Slide Show



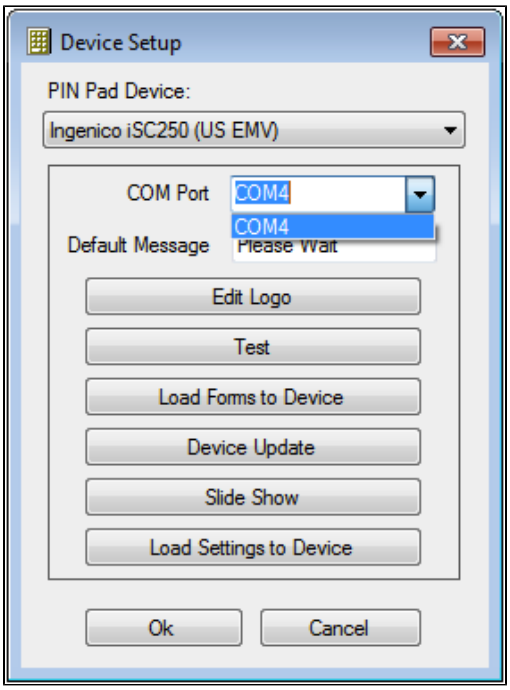
Step #3

From the drop down menul labeled PIN Pad Device select the pin pad device you will be using at this register. In this example the Ingenico ISC250 (US EMV) is selected.



Step #4

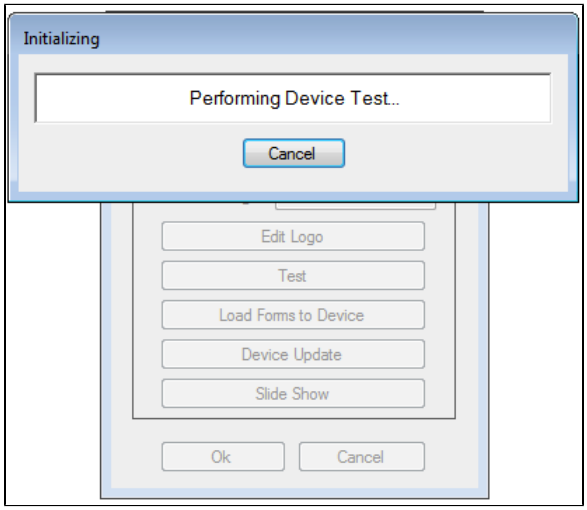
Now select the COM port. In most cases when click the down arrow in the drop down menu it will show the COM port your pin pad is using. However you may need to reference the Windows Device Manager to see what COM port the pin pad has been assigned.



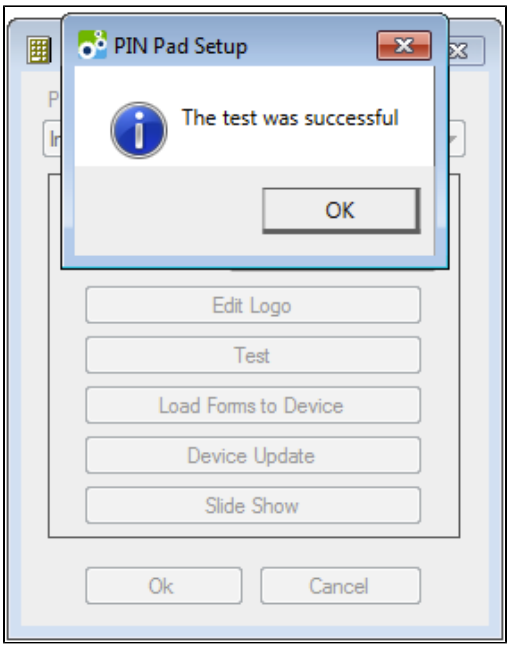
Step #5

Once the pin pad and COM port have been selected you should now be able to click the TEST button in the menu.

When you click on the TEST button you will be prompted with two buttons on the pin pad's LCD screen. Click either one to complete the test. Now you have verified the software can successfully communicate with the hardware.



Click OK to return to the main RCM window.

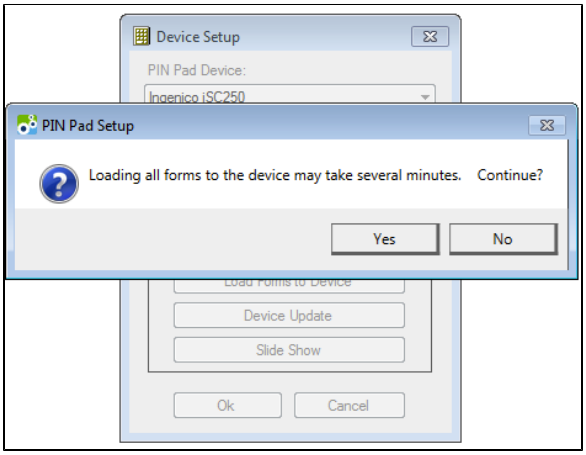


Step #6

Before closing out of the RCM window click on the Load Forms To Device button.

This is required in order to process transactions with the pin pad and will take a few minutes to complete.

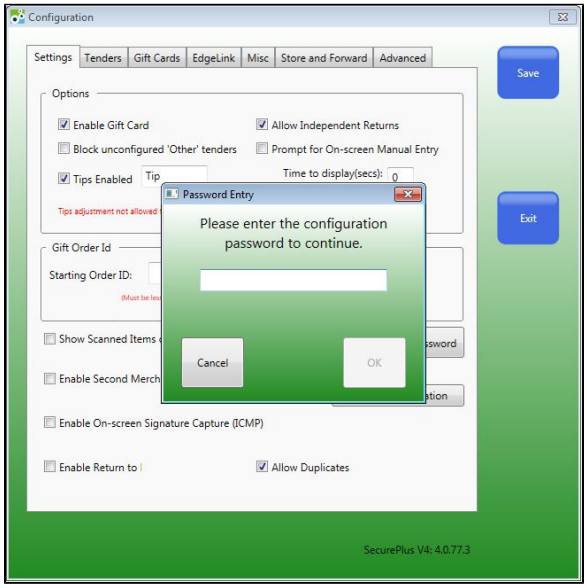
Once it has finished the process you can now click OK to close the RCM Device Setup Window.



SecurePlus Configuration

Configure Settings

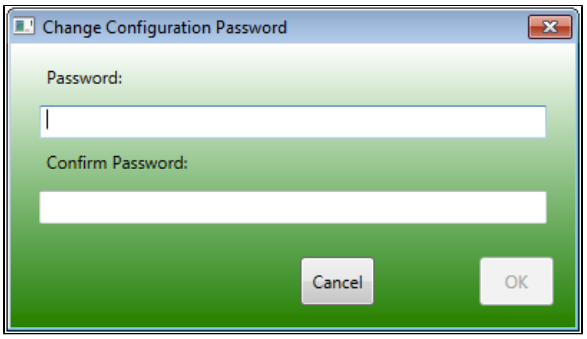
This page covers the different functions and features of the Settings tab in the SecurePlus Configuration application.



Set Password:

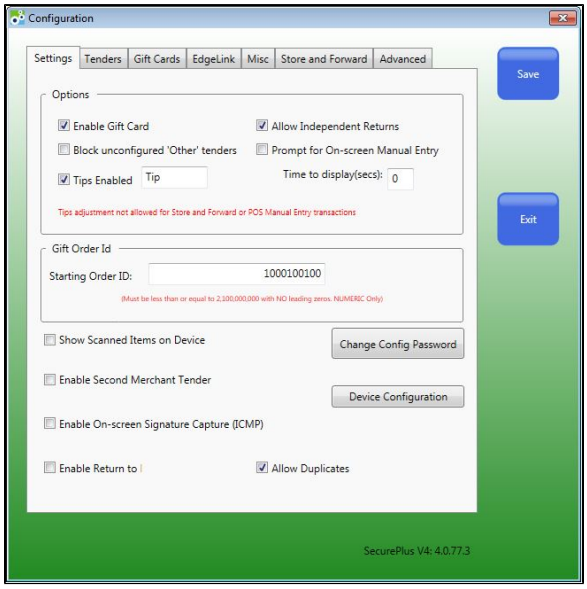
When you first open the SecurePlus Configuration utility you will be prompted to log in with the default password. The default password is: SPv4P@$$!

After you have entered that password you will be able to click on the **Change Config Password** button. You then have the ability to change the password to what ever you would like.



Options:

Enabled Gift Cards: Check this option to enable the gift card tender processing. This option will also create the gift cards console button when selected or remove the custom button when deselected. Refer to G ift Card Console for more information.



- Important: If this software is deployed in an HQ environment, it is recommended to manage item changes from HQ and push the item changes to the store(s).
- Important: Each point of sale station will need to be restarted to reflect the changes made. If you do not restart, the button may be visible but un-usable.

Block Unconfigured 'Other' tenders: Check this option to prevent tendering of unsupported tender types configured as 'Other' and where the tender type is not configured for use in the OpenEdge SecurePlus tender configuration.

Allow Independent Returns: Checking this option will allow cashiers to accept returns on both dependent and independent transactions.

- Dependent returns requires recall of the original transaction, recalling all transactional data (e.g. cashier must recall the transaction for return via RMS return process).
- Independent returns are not dependent on an existing transaction where the item was sold allowing the cashier to create a new transaction and return the item by entering a (negative) quantity.

Prompt for On-Screen Manual Entry: Checking this option will enable the ability to manually process Credit Cards and Gift Cards through a screen on your RMS POS window. When this option is checked the cashier will have a certain amount of time to select the manual entry option or the usual swipe option. The specific amount of time can be configured by entering the amount of seconds you prefer in the: Time To Display(secs) field.

- This option was created for situations where a register does not have access to customer's physical credit cards. A good example would be a register set up to process sales from a website.
- Additionally, this is separate from the manual entry option that a customer can use with the pin-pad in situations where their credit card won't successfully swipe.

Tips Enabled: Applying tips to a transaction will require a few transaction details. This information is commonly found on the printed receipt or in the RMS journal logs. Enter the required information and select Process when complete. The OpenEdgeSecurePlus add-on will then confirm the original transaction and add the additional tip amount.

After enabling Tips you have the option to change the label of the custom button viewed in the RMS POS screen. The default label is "Tip".

- Important: Please note that enabling **Tips** will in turn disable the ability to process **Debit** transactions. This is due to the inability to apply **Tips** to **Debit** transactions.

Gift Order ID: The starting order ID is a unique identifier assigned to each tender that gets processed with OpenEdge.

- Important: **Starting Order ID** should not be altered after initial configuration.

Show Scanned Items on Device:

Select this option to show line items on the device as they are scanned into, modified or removed from RMS Point of Sale.

- Important: This option can only be selected when using Ingenico ISC250 pin-pad.

Enable Second Merchant Tender:

SecurePlus has the ability to utilize two Processor Accounts on the same register. Click the **Enable Second Merchant Tender** check box to enable the use of a secondary processor account. Once enabled you will find a secondary account section in the **EdgeLink tab** of the Configuration Management software.

Enable On-Screen Signature Capture (ICMP):

Select this option to enable on-screen signature capture when using the bluetooth enabled ICMP pin-pad device.

Device Configuration:

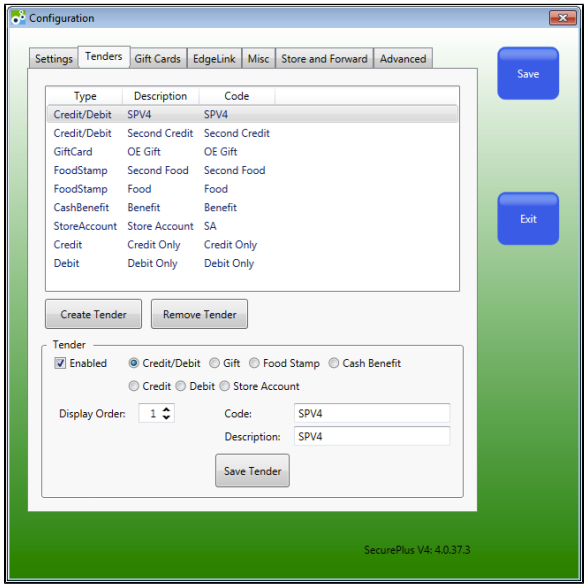
This button provides an easy way to launch the RCM (Remote Client Manager) if you need to change or verify pin-pad hardware settings.

Allow Duplicates:

This option is enabled by default. When the Allow Duplicates option is enabled the SPV4 software will allow a customer to make a duplicate purchase (same payment card, same price).

Configure Tenders

This page covers the different functions and features of the Tenders tab in the SecurePlus Configuration application.



Create Tender:

Select Create Tender to add a new tender type. Enter the required information, select the appropriate tender type from the list of tender options, and use the drop down menu to select/change the Merchant Token.

Remove Tender:

Highlight the tender you wish to remove and use the remove tender option to delete the tender from the RMS database.

- Important: If this software is deployed in an HQ environment, it is recommended to complete all tender changes from HQ and push the changes to the store(s).
- Important: In order for your existing RMS tenders to appear in this window they must be configured with a tender type of "Other" in RMS Store Operations Manager. Refer to Store Operations Manager > Help > Contents > Search > Tender Type.

Tender:

Enabled:

Check the enabled option to enable the selected tender type or de-select this option to disable.

- Important: Enabling the tender is required for use with the OpenEdge SecurePlus add-on.

Credit/Debit:

Check the Credit/Debit option to select a tender that can be used with used with Credit OR Debit. Both the cashier and customer will be prompted to select one of the two options during the tender process.

Credit:

Check the credit option to configure the selected tender as credit.

Display Order:

Set the display order of the selected tender so the cashiers will have easy access to those they use most often.

Code:

The tender code is a unique tender ID for each tender type created. The code may consist of no more than 17 alphanumeric characters and must be unique.

Description:

The tender description is a description of the tender type and will be displayed from the RMS tender window. The description may consist of no more than 25 alphanumeric characters.

Debit:

Check the debit option to configure the selected tender as debit.

Gift:

Check the gift option to configure the selected tender as gift.

Food Stamp:

Check the food stamp option to configure the selected tender as food stamp.

- Important: Before you use the Food Stamp tender in SecurePlus you must first enable the "Accept food stamps for this item" option for each corresponding food item in your RMS database.

Cash Benefit:

Check the cash benefit option to configure the selected tender as cash benefit.

Save Tender:

Selecting save tender will save the current tender configuration.

- Important: If you edit a tender, you will need to close the register batch by performing a Z report to display tender changes. Refer to Store Operations Manager > Help > Contents > Search > Printing a Z report.
- Important: If using accounting software, you may need to configure any new tender type with the accounting integration. Refer to Store Operations Manager > Help > Contents > Search >Assign GL Accounts option or Interfacing with accounting overview.

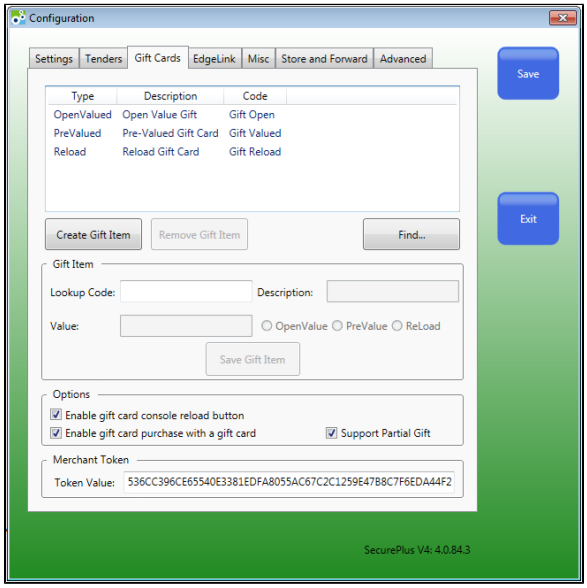
Store Account:

Check the store account option to configure the selected tender as store account.

- Important: When using this tender it will not process the sale through OpenEdge but it will prompt the customer to sign using the pin-pad.

Configure Gift Cards

This page covers the different functions and features of the Gift Card tab in the SecurePlus Configuration application.



Create Gift Item:

Select Create Gift Item to add a new item to the RMS database. Enter the required information and select the appropriate gift item type from the list of options.

- Important: If this software is deployed in an HQ environment, it is recommended to manage item changes from HQ and push the item changes to the store(s). Refer to Appendix I - New Item.

Remove Gift Item:

Highlight the item to be removed. Once you have selected the item, press the Remove Gift Item option to remove the item from the database and the item list.

- Important: If this software is deployed in an HQ environment, it is recommended to manage item changes from HQ and push the item changes to the store(s). Refer to Appendix I - New Item.

Find:

The Find option will retrieve the gift card item details. Enter the item lookup code of the gift card item into the Lookup Code field, press Find t o add the item to the list.

Gift Item

Lookup Code:

The item lookup code is a unique item ID often set to the manufacturing barcode to enable scanning of item during transaction. The code may consist of no more than 25 alphanumeric characters and must be unique.

Description:

The item description is a short description of the item created and is displayed when purchasing gift card item. The description may consist of no more than 30 alphanumeric characters.

Open Value:

Setting the item as open valued will configure the item to prompt for card value during purchase of item. Item price may not exceed $500.00.

Pre Value:

Setting the item to pre valued will configure the item to the value determined in the value field.

Reload:

Setting the item as reload will configure the item to allow adding value to a gift card. Cashier will receive prompt to enter value to be added.

Value:

This option is used with thePre Valued option. Set the item value to update the selected item price.

Save Gift Item:

Select save item to save the current item configuration.

User Interface:

Enable gift card console reload button:

When this box is checked you will be able to see the Reload button in the Gift Card console in RMS POS.

Enable gift card purchase with a gift card:

When this box is checked you are allowed to to purchase or reload a gift card and pay for it using an existing gift card.

Support Partial Gift:

If the customer has a current balance on their gift card that is below the tender amount they are attempting to use, SecurePlus has the ability treat this scenario just like a normal partial authorization scenario.

If this option is enabled then the customer will be notified of the partially approved amount and then be prompted to select a different tender to pay the remainder of the total due.

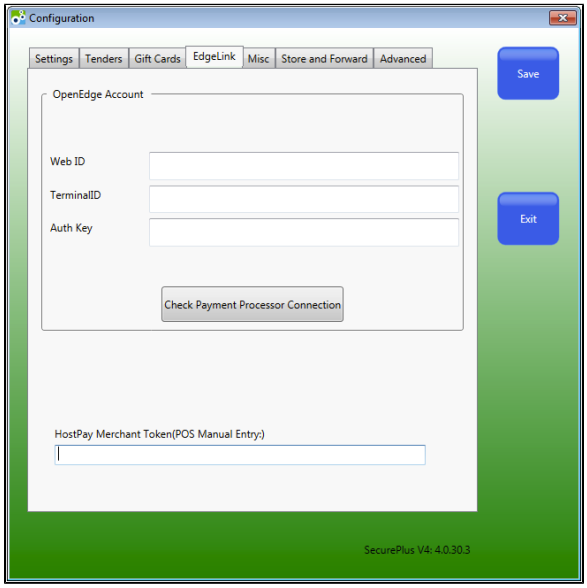
Merchant Token:

At the bottom of the window is a section dedicated to the Merchant Token. If SecurePlus has been installed on top of a previous version then the Marchant Token should already appear in this screen. Though SecurePlus does not use this token for Credit or Debit sales, it is required for Gift Card transactions as well as performing Returns from sales that were tendered using the previous SecurePlus version software.

- Important: If you have installed SecurePlus on a register that did not previously have SecurePlus installed and you do need to use Gift Cards then OpenEdge Support will need to provide a new Merchant Token that will be manually added to this software.
- Important: If you do not require the use of Gift Cards and never had a previous SecurePlus version installed on your register then you can skip over this section as you will not be configuring it.

Configure EdgeLink

This page covers the different functions and features of the EdgeLink tab in the SecurePlus Configuration application.



EdgeLink:

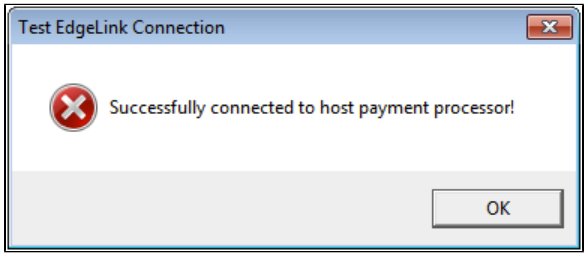
The function of this tab is to configure SecurePlus with the settings it will need to properly communicate with the **Remote Client Manager (RCM)**.

The **WebID, TerminalID, Auth Key and HostPay Merchant Token** are all settings that should be provided by your OpenEdge representative.

- Important: You will not be able to process transactions through SecurePlus unless the information required in this tab is filled out and saved.

Test Connectivity URL:

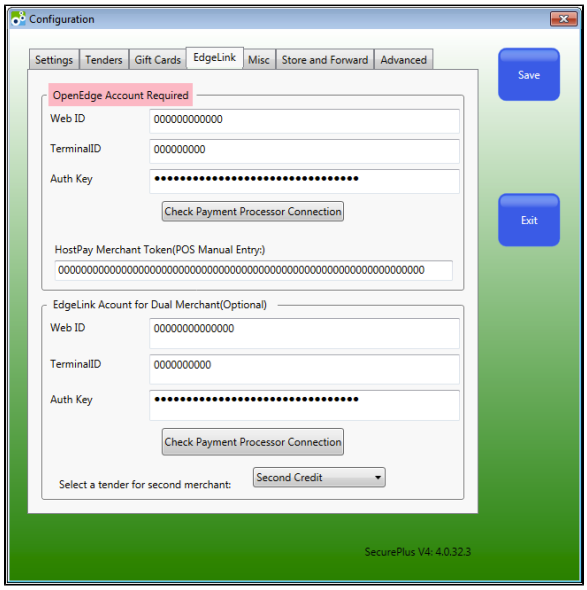
SecurePlus provides the ability to test the computer's connection to the **OpenEdge payment gateway** by clicking on the **Check Host Payment Processor Connection** button. When the button is pressed the software will try to connect to the payment processor.



Optional:

If the Enable Second Merchant Tender box has been enabled under the **Settings tab** then the **EdgeLink tab** will show **EdgeLink Account For Dual Merchant** on the lower half of the window. This section will require the following:

- **Web ID**
- **Terminal ID**
- **Auth Key**
- **Tender for Second Merchant** (account). Here you would select from a drop down list and choose the tender that will be specifically assigned to purchases for this second account.

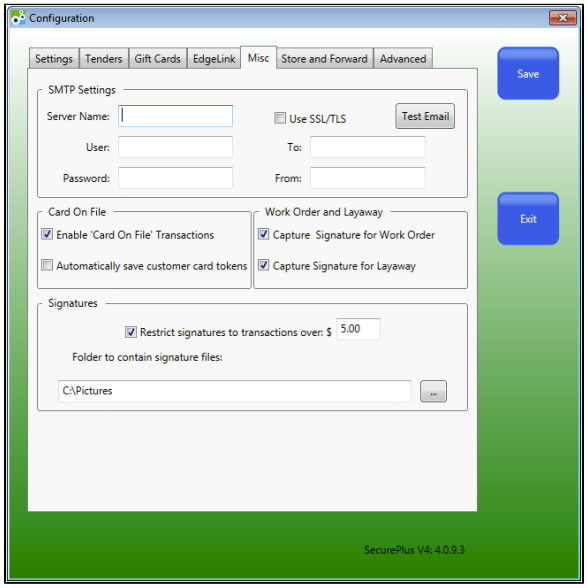


Important: Split tender transactions using tenders from both primary and secondary merchant accounts at the same time are not allowed.

Important: On-Screen Manual Entry is not available when using the secondary merchant account.

Configure MISC

This page covers the different functions and features of the **Misc** tab in the SecurePlus Configuration application.



SMTP Settings:

The simple mail transfer protocol (SMTP) is an internet standard for electronic mail transmission across internet

protocol networks. Enter the SMTP server information to receive notification via e-mail when offline transactions fail to receive authorization.

- Important: Contact your system administrator to determine the required settings.

Server Name: Enter the SMTP server name of the server you will connect to.

Use SSL/TLS: Check this option to enable SSL/TLS connectivity with the email server.

- Important: Provides additional security and may be required with the email service provider.

User: Enter the user name used when accessing email.

Password: Enter the password used when accessing email.

To: Enter the email address you wish to have all messages sent to.

From: Enter the email address you wish to display all messages received from.

Test SMTP Settings: Use the test button to confirm connection with the SMTP server.

Card On File:

Enable 'Card On File' Transactions: Check this option to prompt the cashier to use the assigned payer token on file. A customer must be assigned during the transaction. The prompt takes place at the end of the tender process. The next time a transaction occurs while that same customer is assigned the SecurePlus software will ask you if the customer would like to use the credit card they already have on file.

Automatically Save Customer Tokens: With this option enabled the SecurePlus software will automatically record the customer's credit card using 'Card On File'. A customer must be assigned during the transaction process for this to take place.

Work Order and Layaway:

Capture Signature For Work Order: Enable this option to require the customer to sign when tendering a Work Order transaction using the pin-pad device.

Capture Signature For Layaway: Enable this option to require the customer to sign when tendering a Layaway transaction using the pin-pad device.

Signatures:

Each transaction will create and store an image file to the directory specified. The signature file created for each transaction will include the register and transaction number in the signature file name.The signature is also captured and printed to the transaction receipt.

Restrict signature to transaction over: Checking this option will prompt for a signature on all transactions equal to or greater than the specified

dollar amount.Set the dollar amount you wish to require a signature.

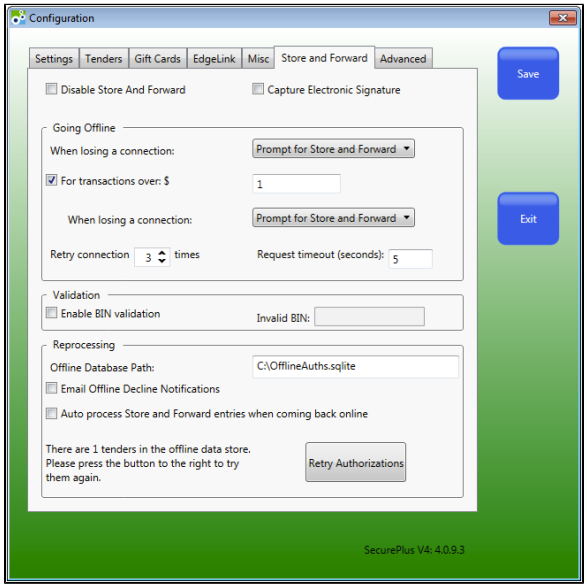
- Min: = [Any Number]
- Max: = [Any Number]

Folder to contain signature files: Enter or browse to the directory source you wish to save the signature files to.

- Important: Supports local directories (recommended) and mapped network directories.

Configure Store and Forward

This page covers the different functions and features of the Store and Forward tab in the SecurePlus Configuration application.



- **Important:** Only the ISC250 pin-pad supports Store and Forward functionality

- **Disable Store and Forward:**
  If you do not wish to use any of the Store and Forward offline capabilities in SecurePlus then you can check this box to completely disable it.
- **Capture Electronic Signature:**
  Check this box to prompt customers to sign the pin-pad when running transaction in Store and Forward mode.

Going Offline:

When in store and forward mode is enabled each transaction will attempt to confirm connectivity to the merchant pay services. If connection is unsuccessful the software will request the cashier to swipe the credit card so the encrypted data can be stored on the computer. When the connection to the merchant pay services is restored then the stored transaction data will be processed following the very next successful online transaction.

- Important: This feature is available to prevent loss of payment when performing transactions offline. The user is assuming full responsibility for failure to receive payment.

- Important: Tips adjustment not allowed for Store and Forward transactions.

When Losing a Connection: This will determine the behavior of the Store and Forward process once the loss of connection has been detected. The drown menu provides three different options:

- Prompt For Store and Forward
- Always Store and Forward
- Always Decline.

For Transactions Over $: This option gives you the ability to choose a Store and Forward function depending on the dollar amount selected. To enable this option you must click on the check box, determine the dollar amount and then select the desired behavior from the drop down menu.

- For example lets say you wanted to use Store and Forward for most transactions but wanted to disable the option for purchases above $100.00. First you would need to select either Prompt for Store and Forward or Always Store and Forward from the previous drop down menu at the top of the screen. Next you would need to check the box For Transactions Over: $. Then select the dollar amount in the field to the right. Finally, select Always Decline from the lower drop down menu.

Retry Count: Set the number of retries the application will attempt to access the payment server.

Validation:

While in Store and Forward mode you have the option to screen and disable certain cards by their BIN (card) number. For example: American Express or Gift/Loyalty cards. Enter the first digit(s) of a card number that you would like to prevent from being used while in Store and Forward mode.

- If you enter **6** into the Invalid BIN field then any card starting with **6** would be blocked.
- If you enter **6050** then any card starting with **6050** would be blocked, etc.
- You can enter up to 20 digits in the Invalid BIN field.

Reprocessing:

Offline Database Path: The offline database will be installed to a default directory (C:\OfflineAuths.sqlite). This database may be relocated to an alternative directory location. If relocated, use the browse button to locate and reconfigure the database location.

Important: No tenders are present in the offline data store.

Auto Process Store and Forward entries when coming back online: Check this option to enable SecurePlus to automatically process any pending Store and Forward transactions following the next successful online transaction.

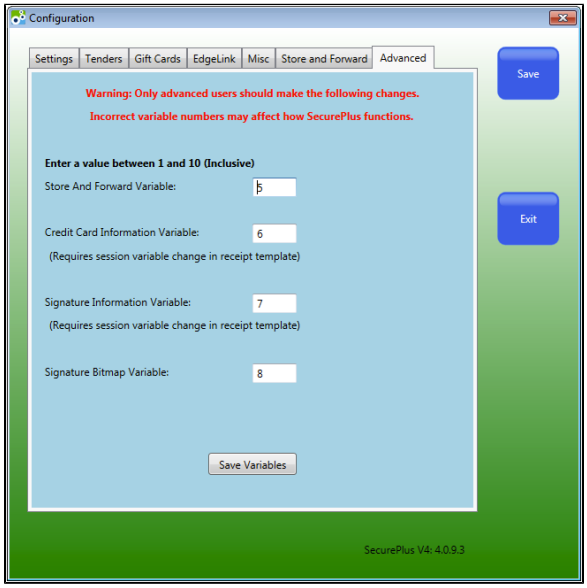
Email Offline Decline Notifications: Checking this option allows you to receive notification via email when offline transactions fail to receive authorization. You can configure the e-mail settings under the MISC tab of the SecurePlus Configuration program.

Retry Authorization: Use the retry authorization option to manually sync the offline database with the payment gateway services and authorize any offline stored transactions.

Configure Advanced

This page covers the different functions and features of the Advanced tab in the SecurePlus Configuration application.

Please NOTE: Only advanced user should make changes to the session variables. Incorrect settings may affect how SecurePlus works.



Store and Forward Variable:

- Default Value: 5

Credit Card Information Variable:

- Default Value: 6
- Important: Changing this value requires changes to the receipt template!

Signature Information Variable:

- Default Value: 7
- Important: Changing this value requires changes to the receipt template!

Signature Bitmap Variable:

- Default Value: 8

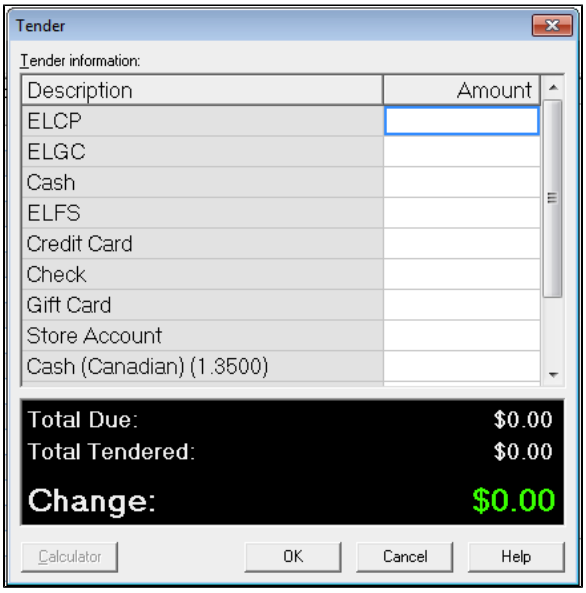
Process Credit/Debit/Manual Entry



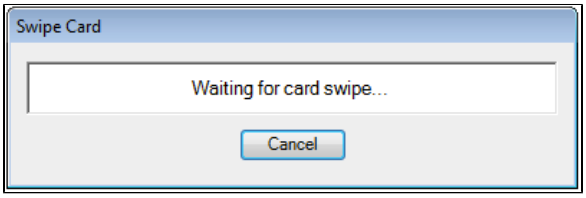
Tender Begin:

Once you have rung up all the items for the current transaction you will press the **Tender** button on the RMS POS screen. Next enter the dollar value into the tender type that the customer chooses to use. If the customer chooses **Credit** or **Debit** then the dollar amount will be entered into the corresponding tender field and then you press **OK**.

- Important: Tips adjustment not allowed for POS Manual Entry transactions.



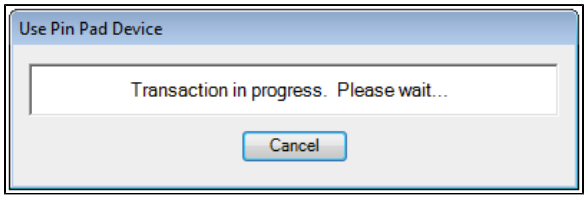
Credit Transaction Walkthrough



Swipe Credit Card:

You will be prompted to select **Credit** or **Debit** from both the SecurePlus software as well as the pin-pad device. Click **Credit** and you will be prompted to **Insert**, **Swipe** or **Tap Card**

Processing Credit:



The SecurePlus software will ask the cashier to wait while the customer follows the prompts from the pin-pad device.

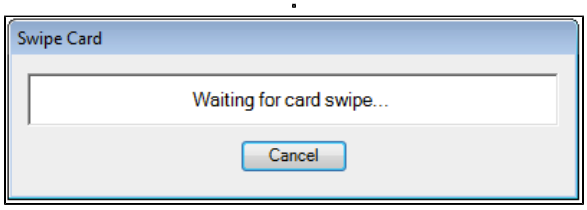
Once you swipe the card the pin-pad will ask the customer to approve the dollar amount to be charged from the card. Once they tap **Yes** on the screen the transaction will continue to process until it returns with a response.

Customer signature:

Finally the customer will be prompted to **sign** on the pin-pad screen using the stylus. After signing press the **OK** button. The pin-pad screen will return to the default message and RMS POS will be ready to start the next transaction.

Debit Transaction Walkthrough

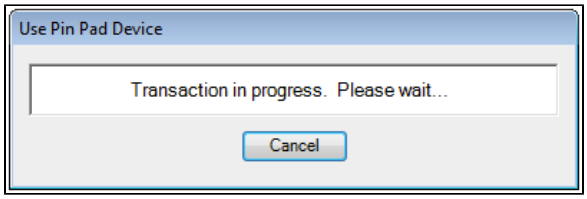
- Important: Please note that enabling **Tips** will in turn disable the ability to process **Debit** transactions. This is due to the inability to apply **Tips** to **Debit** transactions.



Swipe Debit Card:

You will be prompted to select **Credit** or **Debit** from both the SecurePlus software as well as the pin-pad device. Click **Debit** and you will be prompted to **Insert**, **Swipe** or **Tap Card**. The customer will be prompted to approve the dollar amount by pressing **OK** on the pin-pad.

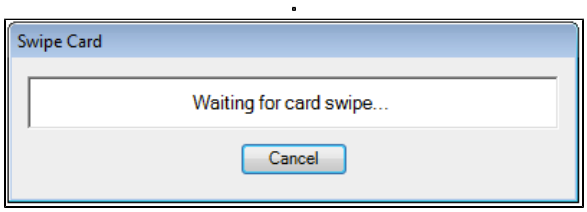
Processing Debit:



The SecurePlus software will ask the cashier to wait while the customer follows the prompts from the pin-pad device.

The customer will be prompted on the pin-pad to enter their **PIN** number and press **OK**. Once the transaction completes the pin-pad screen show the confirmation message and the return to the default screen.

EMV Transaction Walkthrough



Insert EMV card:

You will be prompted to select **Credit** or **Debit** from both the SecurePlus software as well as the pin-pad device. Click **Credit** and you will be prompted to swipe or insert the credit card.

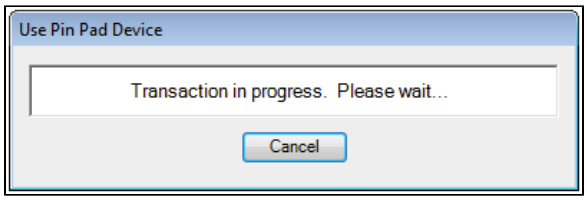
Insert the EMV card and continue to follow the prompt on the pin-pad screen.

Processing EMV:

The SecurePlus software will ask the cashier to wait while the customer follows the prompts from the pin-pad device.

Next the customer will be prompted to approve the dollar amount that will be charged to the EMV card by pressing **OK**. After that they will be prompted to enter their security **PIN** number.

Once the transaction completes the pin-pad screen show the confirmation message and the return to the default screen.



Manual Entry Walkthrough

There are two kinds of manual entry possible with SecurePlus.

- Manual entry via the **Pin-Pad Device**: An example where you would use this option is if the customer's credit card is worn and won't swipe properly.
- Manual entry via O**n-Screen Prompts**: An example where you would use this option is if your register is used to process web orders and never have the customer's physical credit card on hand.

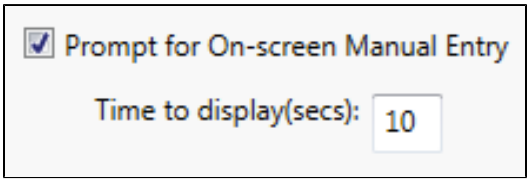
Manual entry via the Pin-Pad:

This process is made possible once you are prompted to **Insert**, **Swipe** or **Tap** the card. On the pin-pad device press the **Manual Entry** button at the bottom right corner of the screen.

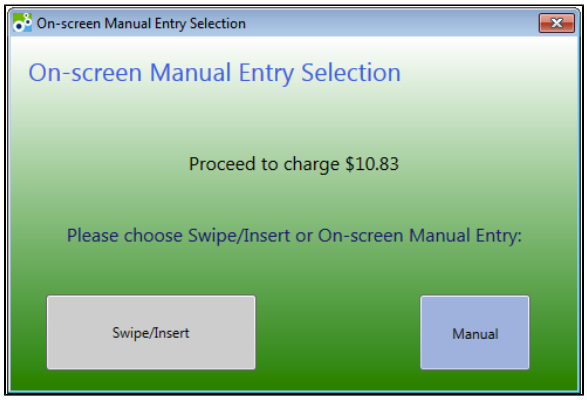
You will then be prompted to **Enter Card Number**, **Expiration Date** and **CVV/CID** security code from the back of the card.

Next you will be prompted to confirm the amount you want to charge to the card by pressing **OK**. Finally you will receive the authorization from the processor.

Manual entry using the On-Screen Prompts:



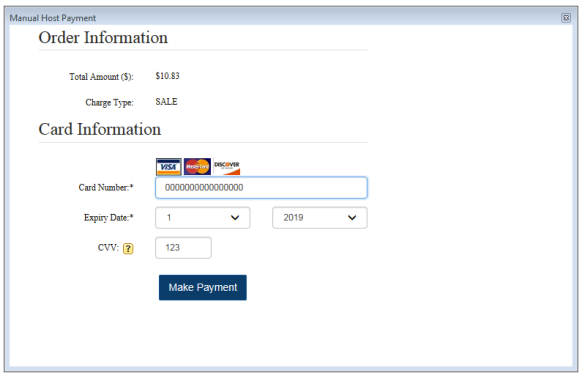
Before you can use this feature you must first enable it in the Settings Tab of the **SecurePlus Configuration** program. Please reference: SecurePlus Configuration



After you have pressed the Tender button in RMS POS to begin the tender process you will see a prompt window asking if you would like to swipe the credit card or manually enter.

If you click on the Manual Entry option a separate window will appear prompting you to enter the credit card number, expiration date, card security code, home address and postal code. The total amount in this window cannot be changed.

Once the required information has been entered you can press Submit. You will receive a response from the processor and the transaction will be completed.



Process Returns and Voids

DEPENDENT RETURNS

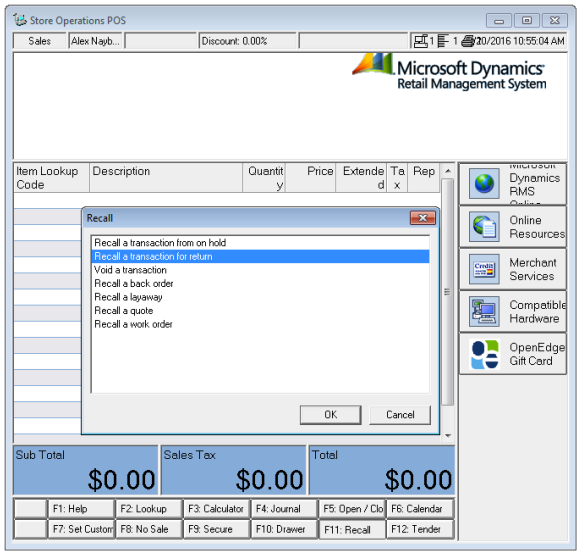
A dependent return is performed when the cashier can recall the original transaction. This is often done when the customer has proof of purchase or the cashier can look up the transaction based on customer information, or time and date of purchase.

Performing a dependent return

Press F11 to open the Recall window. Click on Recall a transaction for return. Select the date or date range and finally select the specific transaction the customer wishes to return.

Refer to Store Operations Manager > Help > Contents > Search > Type ‘Processing Returns’ > Select ‘Processing Returns’ for more information.

- Important: Performing a return of items sold prior to use of the OpenEdge SecurePlus add-on will need to be performed as an independent return.
- Important: Performing a return of items sold on the same day when configured to limit dependent returns is enabled will need to be performed as an independent return.
- Though RMS natively allows consecutive returns of the same transaction SecurePlus prevents such action.



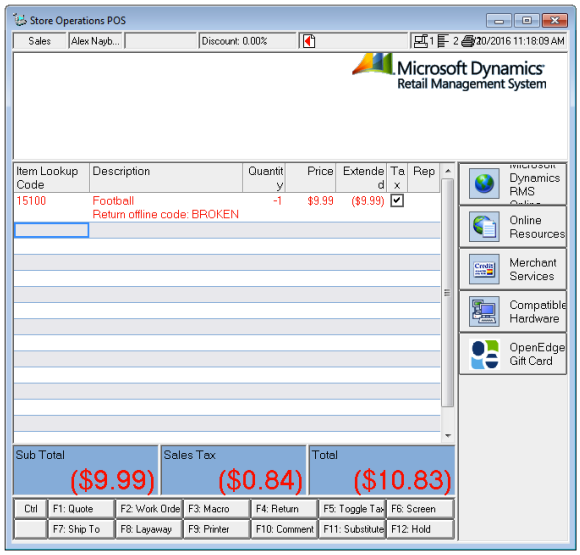
INDEPENDENT RETURNS

An independent return is performed when the cashier returns an item without record of the original transaction. This is often done when the customer does not have proof of purchase or the cashier cannot look up the transaction based on customer information, time and date of purchase or if the item was received as a gift.

Performing an independent return

Press Control+F4 to enter "Return Mode" in the Point of Sale software. You may be asked to select a reason code depending on your RMS configuration. Ring up the appropriate items and then select the required tender.

Refer to Store Operations Manager > Help > Contents > Search > Type ‘Processing Returns’ > Select ‘Processing Returns’ for more information.



Voids

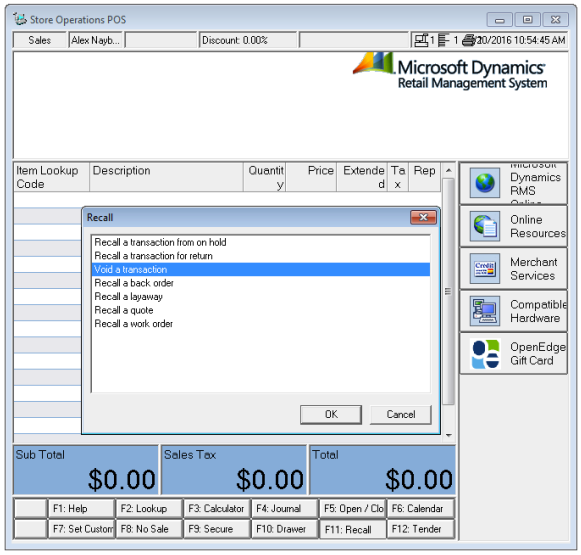
Performing a void will allow you to cancel a transaction that occurred earlier in the day. In order to return funds on a transaction from an earlier date you must complete a return instead of a void.

Performing a void

Press F11 to open the Recall window. Click on Recall a transaction for return. Select today's date and finally select the specific transaction the customer wishes to void.

Refer to Store Operations Manager > Help > Contents > Search > Type ‘void’ > Select ‘voiding transactions’ for more information.

- Important: Voided debit card transactions are processed as returns. The funds have already been deducted from the customer’s bank account and cannot be voided.



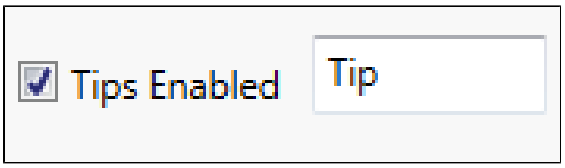
Processing Tips

Processing tips with SecurePlus

In order to use Tips with SecurePlus you must first enable the Tips option under Settings tab, Options in the SecurePlus Configuration utility.

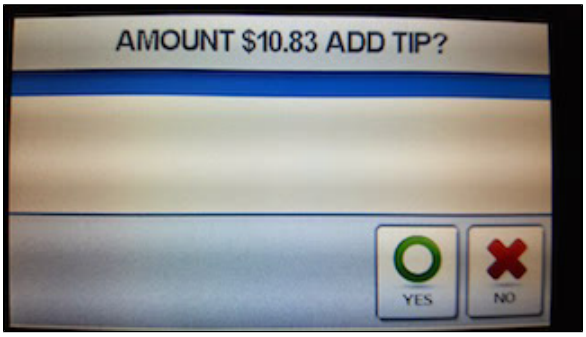
There are two ways to apply a tip to a credit transaction.

- The customer is prompted by the pin-pad during a credit transaction to apply a tip before they complete the tender process.
- The cashier uses a custom POS button to use the Tips Adjustment Console.



Processing a Tip using the Pin-Pad:

When performing a Credit transaction the pin-pad will prompt the customer if they would like to add a tip to the current tender total. Click Yes and proceed to enter the dollar amount to be added. Finally you will Insert, Swipe or Tap to complete the Credit transaction as normal.



Processing a Tip using the Custom POS button:

Locate the Tip custom button on the right hand side of the Microsoft RMS Point of Sale screen. This will launch the Tips Adjustment console.

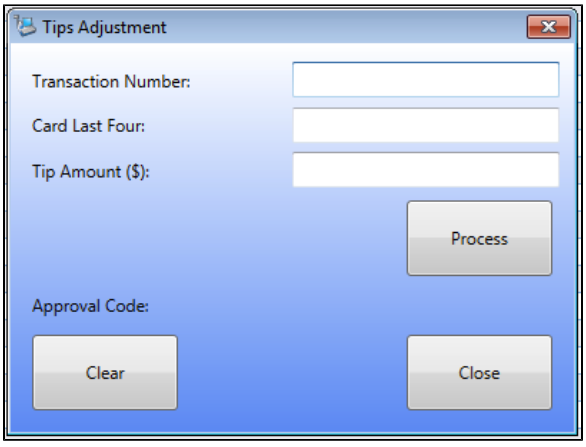


The following information is required in the Tips Adjustment console:

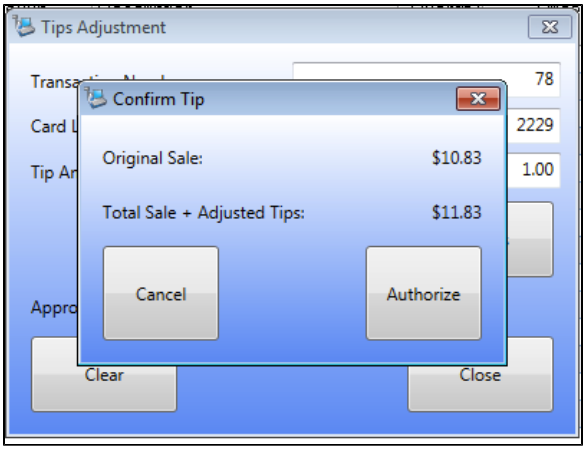
Transaction Number -
The RMS transaction number assigned during sale. This information is commonly found on the printed receipt or in the RMS journal logs.

Card Last Four Digits -
The last 4 digits of the card number used during sale. This information is commonly found on the printed receipt or in the RMS journal logs.

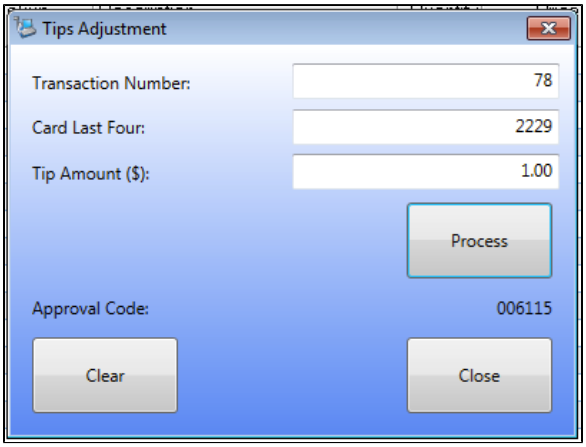
Tip Amount ($)
The dollar amount to be added to sale as a tip.



Once you have entered the required transaction information you can click on the **Process** button. A small prompt window will appear showing you the updated dollar total for the transaction after the tip is added. You will then be asked to **Authorize** or **Cancel** the Tip.



If the Tip adjustment is successfully authorized then you will receive an authorization code below the **Process** button. At this point you can either click **Clear** so you can add a tip to a different transaction or else click **Close** to return to the RMS Point of Sale screen.



- **Important**: Tips adjustment are not allowed for Debit, EBT (Food Stamps), Gift, Store and Forward or POS Manual Entry transactions.

If you receive an **Invalid Transaction** error:

There are two main reasons you may receive this error.

- You are attempting to use a transaction number that does not exist in your database.
- You are attempting to add a tip to a Non-Credit transaction. It is not possible to add a tip to Debit, Gift or EBT (Food Stamps), Store and Forward or POS Manual Entry transactions.

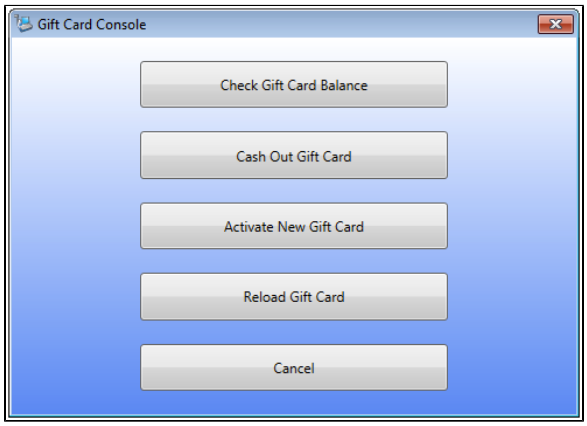
Gift Card Console

Before you can utilize gift cards in SecurePlus you will need to have configured the Gift Card Items and Gift Card Tenders in the SecurePlus Configuration utility.

GIFT CARD CONSOLE WALKTHROUGH

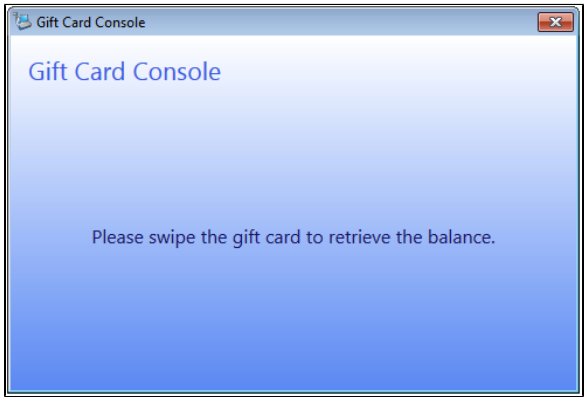


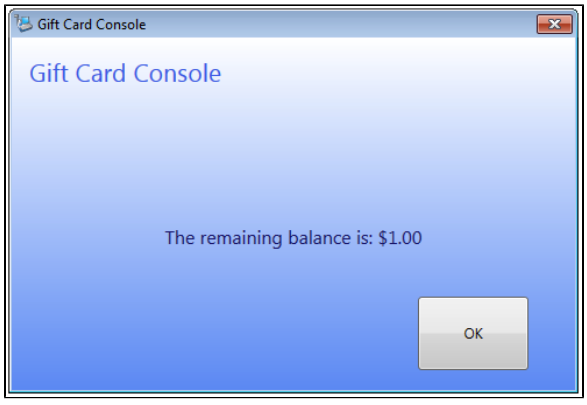
To access the Gift Card Console simply launch Microsoft Retail Management System POS. On the right hand side of the POS screen you will find your custom buttons. One of these buttons should be labeled **OpenEdge Gift Card**. Clicking on this button will open a sub-window that gives you several options to choose from including: **Check Gift Card Balance**, **Cash Out Gift Card**, **Activate New Gift Card**, **Reload Gift Card and Cancel**. Below we will go over the function of each of these buttons.



Check Gift Card Balance:

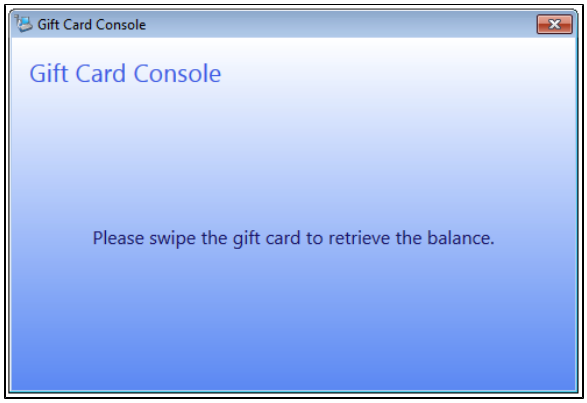
When you click on this button you will see a small window that prompts you to swipe your gift card to retrieve the current card balance.Once you have given the customer the card balance you can click **OK** close the window and return to the RMS POS screen.

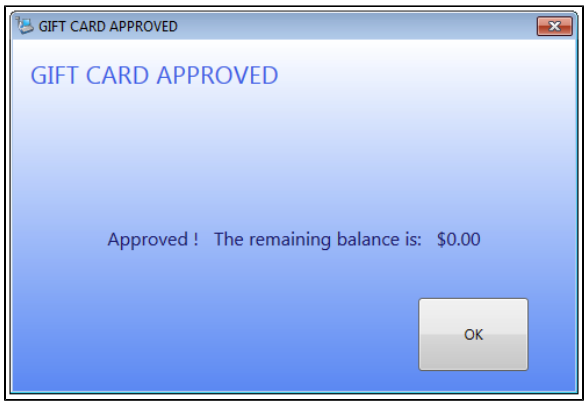




Cash Out Gift Card:

When you click on this button you will see a small window that prompts you to swipe the gift card in order to determine the amount the customer will be about to transfer into cash. Once you swipe the card a line item on your POS screen will appear and the price will automatically be set to match the balance of the gift card. You can then tender the transaction to your Cash Tender and you will be prompted to swipe the card one more time. Once you receive a message saying the gift card was approved our software will remove the balance from the gift card. If the customer chooses not to cash out the gift card then you could simply cancel the transaction in POS.

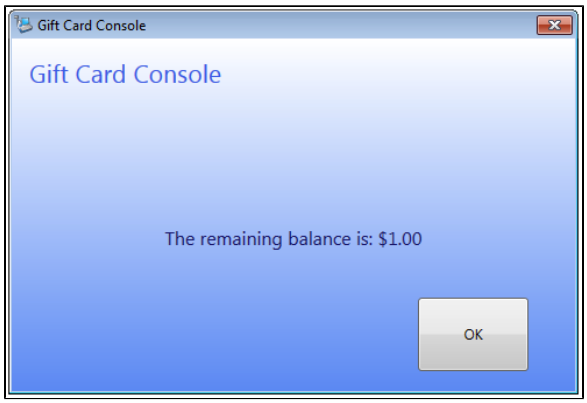




Activate New Gift Card:

When you click on this button you will see a small window asking you to enter an amount to add to the new gift card. After entering the amount the customer wants you can either click on **Activate** or **Cancel**. If you click on **Activate** you will then have a line item added to your POS and the price will be set to the amount you previously chose. When tendering the transaction you will be prompted to swipe the new gift card from the pin-pad device. Finally you will be shown a small window indicating the new gift card balance.

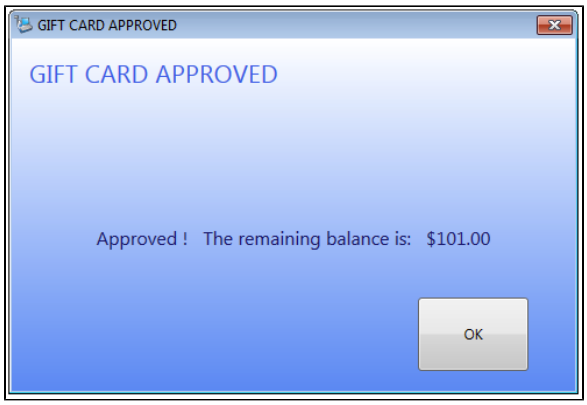




Reload Gift Card:

When you click on this button you will see a small window asking you the amount you would like to add to the previously activated gift card. After you have entered the desired amount you can either click **Reload Value** or **Cancel**. If you click on **Reload Value** the software will add a line item in the POS transaction screen along with the price you chose in the previous screen. Once the tender process is completed you will be prompted to swipe the gift card and the new updated balance will appear on the screen.



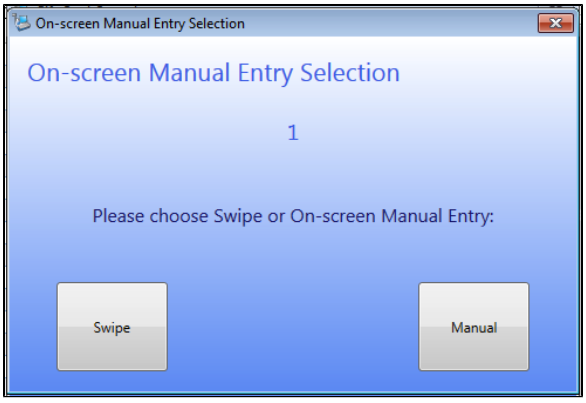


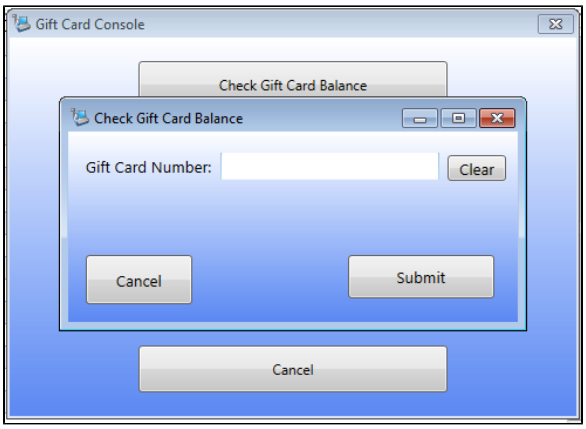
Cancel:

When you click on this button the Gift Card Console will disappear and you will be returned to the RMS POS screen.

Manual Entry:

To enable On-Screen Manual Entry for Gift Cards you must check the Prompt for On-Screen Manual Entry option in the Settings tab of the SecurePlus Configuration software. Please reference: SecurePlus Configuration




Gift Card Console
Check Gift Card Balance
Check Gift Card Balance
Gift Card Number:
Clear
Cancel
Submit
Cancel

Receipt

Receipt Configuration:

Receipt configuration is done from Store Operations Manager. Refer to Receipt Formats below or Store Operations Manager > Help > Contents > Search and type Creating receipt formats for more information.

Important: The receipt template included is based on the default RMS receipt template. If you are using a customized receipt template, any customizations will need to be merged.

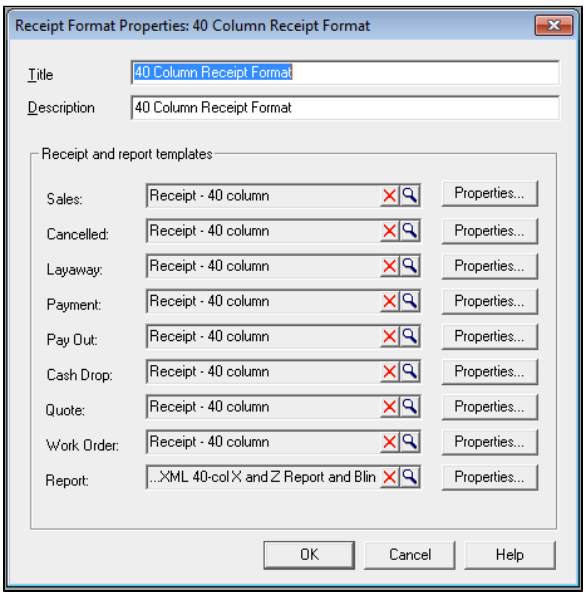
Receipt Formats:

From the **Database** menu, click **Registers**, and then click **Receipt Formats**. Select the receipt format you wish to modify. Such as **Sales**.

Next select the magnifying glass icon from the Sales row, browse to the directory (default: C:\Program Files\Microsoft Retail Management System\Store Operations\ReceiptTemplates) and select a template file, then press Yes to apply to all transactions types. Press OK from the receipt format properties window to save changes.

There are four templates available by default:

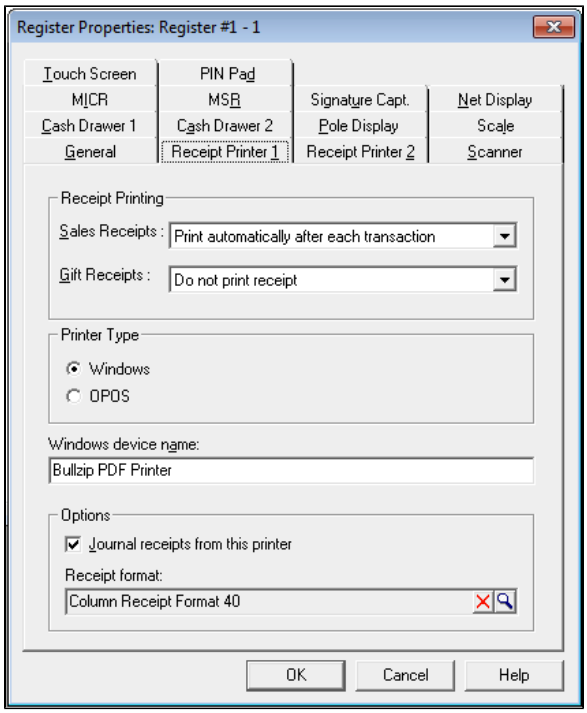
- **SPv4FullPage.xml**
  (Full Page Receipt)
- **SPv4FullPage-RMS2.0.1xxx.xml**
  (Full Page Recipt for newer RMS versions)
- **SPv4Receipt-RMS2.0.2-SigCap.xxx.xml**
  (40 column receipt with Signature Capture for newer RMS versions)
- **SPv4Receipt-RMSSigCap.xml**
  (40 column receipt with Signature capture)



Assigning Receipt Formats To Registers:

Refer to Store Operations Manager > Help > Contents > Search and type Assigning receipt formats to register for more information.

Important: The RMS point of sale software will need to be restarted on each POS station for changes to take effect.



Information displayed on the receipt:

The Secure Plus Receipt contains specific transaction data such as **XCT ransaction ID (ELPC)**, **Approval code**, **Last four digits** of the card number and the **Card type**.

Important: The Card Holder is not displayed at this time.

Appendix

Pairing Ingenico iCMP Bluetooth device with a Windows computer:

- Power on the iCMP unit using the power button on the right side. The reader should display **'BT Pairing Required'**.
  If the screen displays a 'Welcome' message, tap the 'F' key 4 times rapidly.
- Tap the F2 key for Standard on the iCMP. Now the LCD display should show the Bluetooth name of the iCMP device as well as the PIN: code to use in the pairing process.
- From Windows open the Control Panel and then open Devices and Printers. Click on Add a Device at the top left corner of the screen. If the Bluetooth radio is enabled on you Windows device then it should search for available devices and locate the nearby iCMP.
- Click on the iCMP device once it is found and then proceed to enter the Bluetooth pairing code presently located on the iCMP LCD screen. The pairing process should now be complete.



Confirm you have a successful connection to the database from Store Operations Administrator:

Click >File>Connect and test connection.

- Important: It is important to perform this test from File > Connect vs File > Configuration, which uses a different connection method.

If connection fails and you are running SQL 2005 – 2008 on the server hosting the RMS database, install the SQL backward compatibility tools http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=16177

Microsoft SQL Server 2005 Backward Compatibility Components
The SQL Server Backward Compatibility package includes the latest versions of Data Transformation Services 2000 runtime (DTS), SQL Distributed Management Objects (SQL-DMO), Decision Support Objects (DSO), and SQL Virtual Device Interface (SQLVDI). These versions have been updated for compatibility with both SQL Server 2005 and SQL Server 2008 and include all fixes shipped through SQL Server 2000 SP4 and SQL Server 2005 SP2.

Audience(s): Customer, Partner, Developer

X86 Package (SQLServer2005_BC.msi) - 11273 KB X64 Package (SQLServer2005_BC.msi) - 18569 KB IA64 Package (SQLServer2005_BC.msi) - 23510 KB

Confirm the database settings entered match the database settings used in Store Operations Administrator.

If using the Servers PC name, try using the Servers IP address instead. The network may not be configured to convert the PC host name to the proper IP.

Try running a Telnet test from a PC on the network connecting to the server... Telnet [IP Address of server] [SQLport] (e.g. Telnet 192.168.1.111 1433).

If failed, confirm the server has the required port open to allow connection in the firewall.

- Important: Some operating systems do not have the telnet command enabled by default. If you are unable to complete this test, move on to the next or contact your system administrator for assistance. (search keywords - Enable Telnet)

In some cases the server may have multiple Instances of SQL installed. If this is the case, you will need to confirm which instance the RMS database resides on and add this information to the server name (e.g. Server\MSSQLEXPRESS or 192.168.1.111\MSSQLEXPRESS).

Confirm the SQL instance is configured to the default port 1433.

If not, enter the assigned port number in the port over ride field or add the port number to the end of the server field (e.g. server,1320).

In some cases it may be required to combine steps 6-7 (e.g. Server\MSSQLEXPRESS,1320)

OSQL Test

Run an OSQL connection test to ensure database connection via OSQL (enter information specific to clients environment determined from above steps).
Expected Format:

- OSQL

- –Stcp: = Enter server details (this may include SQL Instance and port number)
- –U = SQL user login credentials
- –P = SQL password login credentials
- –d = Database name

(e.g. OSQL –Stcp:192.168.1.1\SQLinstance,1433 –U sa –P password –d database)

How to determine SQL Instance

When installing SQL server you may be prompted to provide an Instance name. This is important when multiple versions of SQL are installed on the server. There are many ways to determine the SQL Instance name.

In this example we will be running a SQL script against our current RMS database.

From the server, run Store Operations Administrator > File > Connect >Enter the SQL settings and confirm connection, next select Query > New.

Copy the below SQL script to the query window and run the SQL script. If the result returns NULL, it's likely the database resides on the default SQL Instance.

```
SelectSERVERPROPERTY('InstanceName')AS SQL_Instance
```

In this example we will reference the list of known services running. From Start > Run > Type "Services.msc"

Scroll through the list of services and note all services with a name of SQL Server(Instance Name). Also note, whether the service is running (Status field will read Started). If found to have more than 1 SQL Server service running (e.g. SQL Server (MSSQLSERVER) or SQL Server (MSSQLEXPRESS)), you will need to stop the SQL service, then attempt to connect to the database. If you cannot connect to the database, you have found the SQL service which the RMS database resides on. Restart the service and confirm database connectivity.

Note: Login to RMS to confirm database connection.

How to enable transaction logs for troubleshooting:

1. Launch Windows application **Notepad** with **Admin** rights.
    a. Click **Start,** in search field type **Notepad** and once you see the application icon appear right click on it and select **Run As Administrator**.
2. In Notepad open file: NWT_RMSPaymentsIntegration.xml located in path: C:\ProgramData\New West Technologies\RMSPaymentsIntegration.
3. Locate line: <ApplicationLoggingEnabled>False</ApplicationLoggingEnabled> and change it to <ApplicationLoggingEnabled>True</ApplicationLoggingEnabled>.
4. In **Notepad** click **File**, **Save**.
5. Relaunch **SecurePlus for RMS** and complete a credit transaction.
6. Next, browse to Windows User account **Documents** folder: Libraries\Documents. Locate file named SecurePlusRMS.TXT and open it.
7. This document will contain historical data involving the requests made to the credit card processor and their responses.

Contact Information

Corporate Headquarters:

OpenEdge, A division of Global Payments 8200 Central Ave.
Newark, CA 94560 U. S. A. www.openedgepay.com

Voice: 1.800.774.6462 or 510.795.2290 Fax: 1.800.900.7487 or 510.795.2299
Email:
Technical support - support@openedgepay.com (For fastest service, please contact us by phone.)
General Information - information@openedgepay.com
Sales Information - sales@openedgepay.com

