OpenEdge
Platform

REMOTE CLIENT MANAGER HELP
VERSION 2.6

MERCHANT SALES: 800-637-8268
- New Merchant Accounts

PARTNER PROGRAMS: 800-637-8268
- New and existing partnerships

CUSTOMER CARE: 800-338-6614
- Existing merchant account support
- Statements and deposits
- Changes to existing merchant accounts
- Technical Support

Copyright Information

TABLE OF CONTENTS

OVERVIEW

The Remote Client Manager (RCM) software is used to handle the communication between PIN Pad devices and OpenEdge payment forms. The RCM supports four PIN Pad devices as of this version, and additional devices and/or functionality may be added in future releases.

RCM Process Flow

1. Partner application requests an OpenEdge payment form.
2. The OpenEdge payment form wakes up the RCM for the desired transaction.
3. The RCM communicates with the configured PIN Pad Device to capture the payment card information.
4. The RCM submits the transaction to the OpenEdge Gateway.
5. The OpenEdge Gateway returns a response to the RCM.
6. The RCM notifies the OpenEdge payment form that the transaction is completed.
7. The partner application retrieves the transaction response from the OpenEdge Gateway.

System Requirements

The RCM uses port 21113 by default, but may be configured for a different port if required. Contact OpenEdge support if a different port is required.

The RCM on Windows supports the following browsers:

- Google Chrome
- Firefox (see **Appendix A** for information on configuring Firefox for use with the RCM)
- Internet Explorer
- Microsoft Edge

The RCM on Windows supports the following Operating Systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

Starting the RCM

After installing the RCM, the RCM application must be started.

1. From the desktop or the "Startup" folder in the Start menu, double-click on the RCM application.
2. The RCM icon displays in the system tray (near the clock).
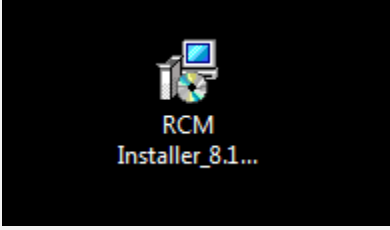
REMOTE CLIENT MANAGER INSTALLATION OVERVIEW
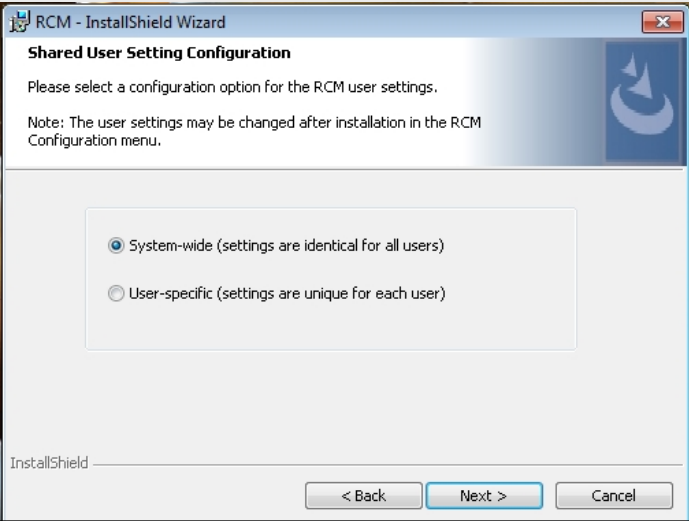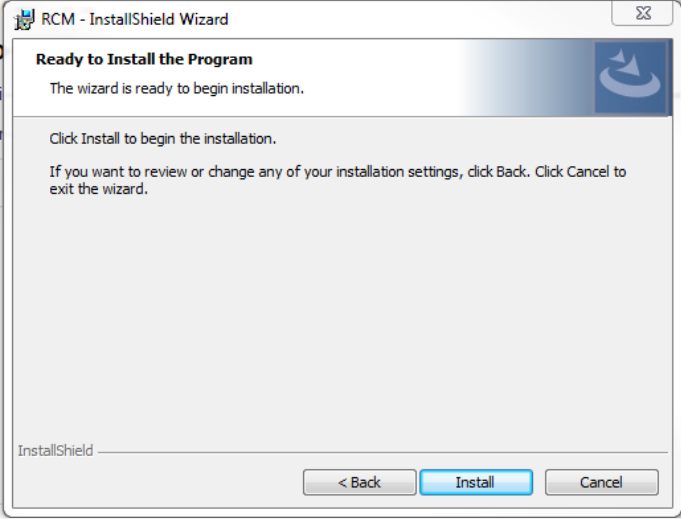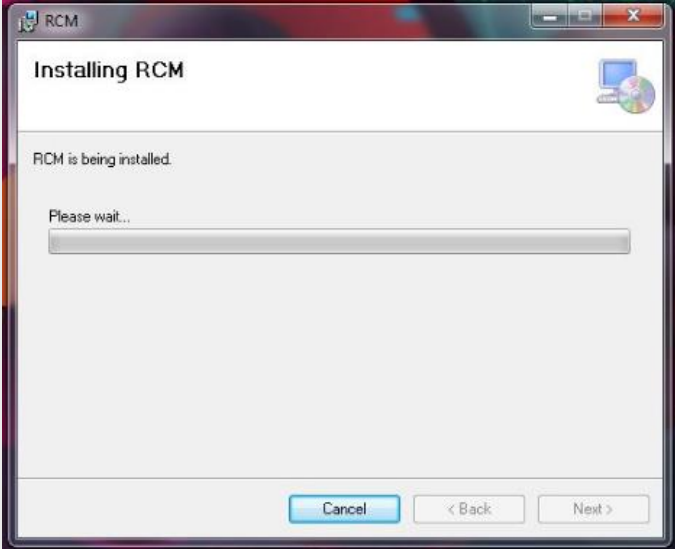
Running the Remote Client Manager (RCM) installation package will install the RCM software to your computer.
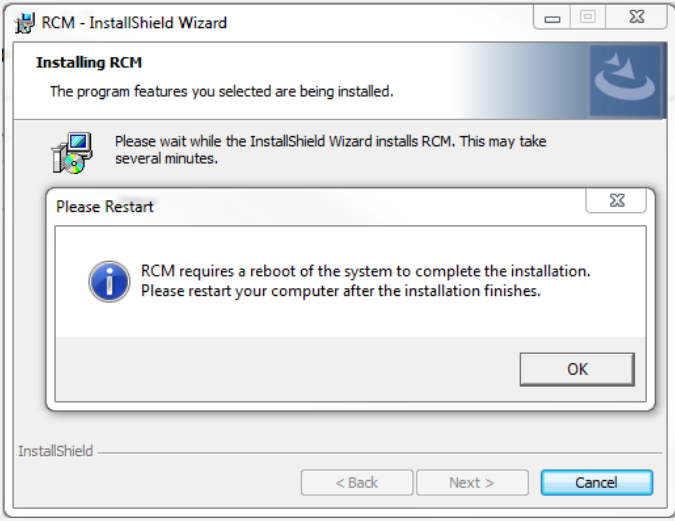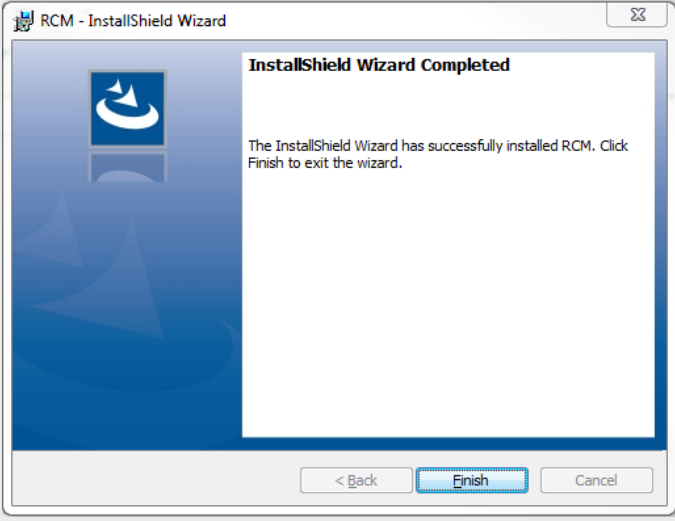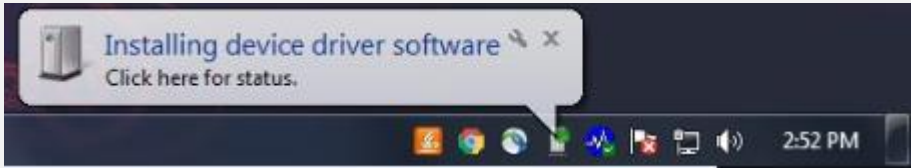
NOTE:
If you are a partner wanting to silently install the RCM alongside your software, please skip to page 8.

Installing the RCM

Instruction	Image
Log into the computer with an Administrator account.	
Double-click on the RCM installation package, to start the installation.	
Select the **Next** button.	

Instruction	Image
On this window you can choose if you would like your settings to be **User Specific** or **System Wide.** (See page 9 for details.) Once you choose, select **Next.**	
Select the **Install** button.	
RCM will begin installing.	

Instruction	Image
A prompt to restart your computer appears shortly before the completion of the installation. Click on **OK.**	
The installation will complete, click on **Finish.**	
NOTE: If a PIN Pad device was plugged into your computer during the installation of the RCM you will see the PIN Pad device drivers being installed as well.	

Uninstalling the RCM

1. Access your **Control Panel** by clicking **Start,** and then **Control Panel.**
2. Locate, and then click on **Programs and Features.**
3. Locate the Programs **RCM, OpenEdge Updater,** and **Ingenico USB Drivers Package (JUNGO v36) 2.60 (remove only).**
4. Uninstall the three applications by clicking the **Uninstall** button, and then clicking the **Next** or **OK** buttons.

RCM SILENT INSTALLATION

OpenEdge provides the option to silently install the RCM, which can be run seamlessly alongside the Partner's product installation. During the silent installation, the RCM will not display any messages, and relies on the Partner product to manage the End User License Agreement. The silent installation can also be used to upgrade the RCM from previous versions.

Silent Installation Steps

NOTE:
To ensure the Silent Installation is successful, you must run the command prompt as an administrator.

Using the Silent Install flag

The RCM supports the "/quiet" flag during installation.

RCM Silent Installation Example

```
"RCM Installer_8.1.1SP6b23_RCM1.14.0023.exe" /S /v/qn
```

Upgrading the RCM using the Silent Install flags

To upgrade the RCM from a previous version, the same "/quiet" flag is used.

RCM Silent Installation Example

```
"RCM Installer_8.1.1SP6b23_RCM1.14.0023.exe" /S /v/qn
```

Optional Parameters for Silent Installation

```
"RCM Installer_8.1.1SP6b23_RCM1.14.0023.exe" /S /v/qn /V"SETTINGSCOPE=User"
```

Using this parameter will implement the **User Specific** setting, rather than the **System Wide** setting, which is the setting by default.

- **User Specific,** will keep any changes you make to the PIN Pad Configuration specific to the Windows user you are logged in under.
- **System Wide,** will apply any changes you make in the PIN Pad Configuration to all Windows users

OpenEdge Platform

> **NOTE:**
>
> During the upgrade, the RCM will check to see if any configured PINPad Devices have an available upgrade. If so, the installer will attempt to upgrade the device. Whether the device upgrade is successful or fails, no messages will be displayed to the user. If the device upgrade fails, the user will be prompted to update when processing the next EMV transaction, or can be manually accessed from the "Device Configure" menu.

SETUP PROCEDURES

RCM Setup - Port Configure

When using the RCM in an environment where multiple users will access the same RCM installation (such as terminal services), the Port range used by the RCM can be configured.
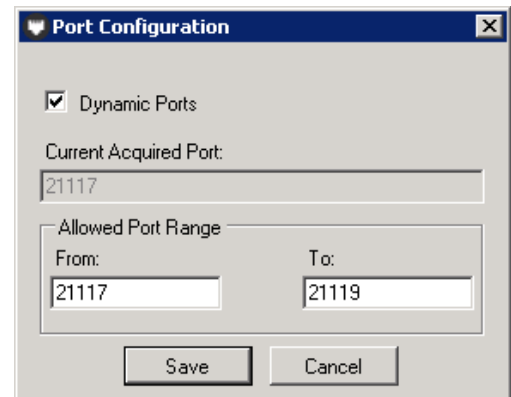
1. Right-click on the RCM tray icon.
2. Select **Port Configure**.
3. Enter the **User Port** for the Port to be used by this user. The **Allowed Port Range** may also be configured, using the **From** and **To** boxes.
4. Select the **Save** button.

RCM Setup – Applying Settings to All Users

When using the RCM in an environment where multiple users will access the same RCM installation, you can enable a feature that applies your settings to all Windows users.
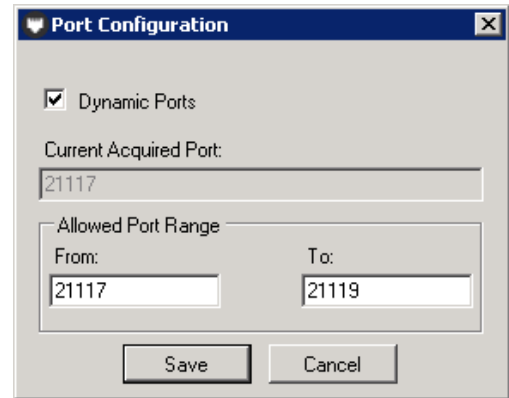
1. Kill the RCM process in the lower right corner of your screen.
2. Once the process is stopped, you will want to **run the RCM as Administrator** by right clicking on the icon and choosing **Run as Administrator.**
3. Right-click on the RCM tray icon.
4. Hover your mouse over **Shared Settings Configuration** and you will see two options: **User Specific**, and **System Wide.**
   - **User Specific**, will keep any changes you make to the PIN Pad Configuration specific to the Windows user you are logged in under.
   - **System Wide**, will apply any changes you make in the PIN Pad Configuration to all Windows users
5. Select your desired setting. (The setting by default is **System Wide.**)

openedge A division of **global**payments

RCM Setup – Dynamic Ports

The Dynamic Ports setting allows RCM to automatically obtain a port in the Allowed Port Range. RCM can use dynamic ports when the **User Specific** Shared Settings Configuration setting is enabled. This functionality does not work if the **System Wide** Shared Settings Configuration setting is enabled.   The Dynamic Ports setting can only be enabled by an Administrator.

1. Right-click on the RCM tray icon .

2. Select **Port Configure**.

3. Check the **Dynamic Ports** box.

4. Select the **Save** button.

RCM Setup - PIN Pad Device Setup

RCM Setup – Device Auto-Detect and Configure

The RCM can automatically detect connected EMV PIN Pad devices and select the appropriate COM port.
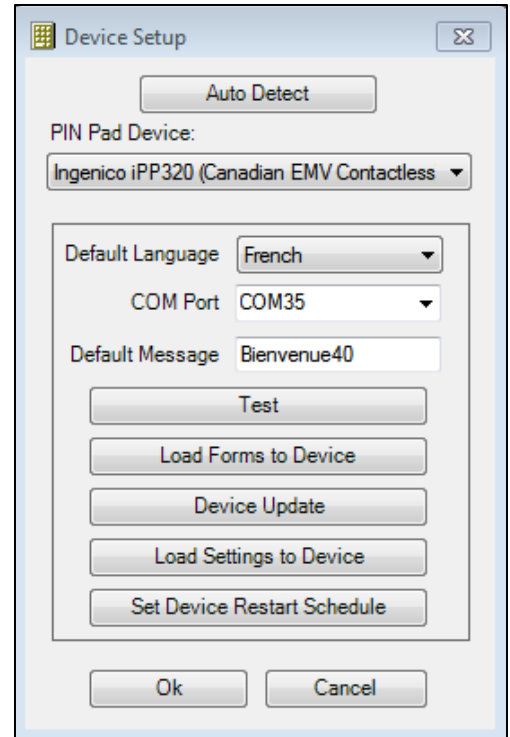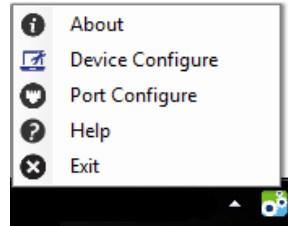
1. Right-click on the RCM tray icon.
2. Select **Device Configure**.
3. Select **Auto Detect**
4. Click **Ok.**

Non-EMV devices need to be manually selected and configured:

1. Right-click on the RCM tray icon.
2. Select **Device Configure**.
3. Choose the desired device from the PIN Pad Device drop down menu.

Ingenico iPP320

The Ingenico iPP320 is a PIN entry **EMV Device** with an integrated Magnetic Stripe Reader, EMV chip card reader, and a monochrome display. See also the **Device Update** section.

NOTE:
If the Auto Detect function detects an Ingenico iPP320 is connected, it will default to the 'Ingenico iPP320 (US EMV)' option. If a different device configuration is desired, change the PIN Pad Device drop-down menu selection.

NOTE:
The Ingenico iPP320 requires unique Credit and Debit Processing Accounts configured per unit when used for Canadian EMV. For assistance with obtaining and configuring your Processing Accounts, please contact OpenEdge.

Ingenico iPP320 (Non-EMV)

1. Plug the Ingenico iPP320 into a USB port and a power outlet.
2. Right-click on the RCM tray icon.
3. Select **Device Configure**.
4. Select the **Ingenico iPP320** from the **PIN Pad Device** drop-down menu.
5. Enter the **COM Port** number used by the device, and the **Default Message** if desired. The **Default Message** must be 30 characters or less.
6. Choose the **Load Forms to Device** button. This may take several minutes, and should not be interrupted.

RCM Setup - PIN Pad Device Setup (CONTINUED)

7. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iPP320 to complete the test.

8. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Ingenico iPP320 (Canadian EMV)

1. Plug the Ingenico iPP320 into a serial port and a power outlet.

2. Right-click on the RCM tray icon .

3. Select **Device Configure**.

4. Select the **Ingenico iPP320 (Canadian EMV)** from the **PIN Pad Device** drop-down menu.

5. Enter the **COM Port** number used by the device.

6. Enter the Processing Account Terminal IDs into the **Debit TID** and **Credit TID** fields.

7. Choose the **Load Settings to Device** button from the **Device Setup** window. This may take several minutes and should not be interrupted.

8. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iPP320 to complete the test.

9. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Ingenico iPP320 (Canadian EMV Contactless)

1. Plug the Ingenico iPP320 into a serial port and a power outlet.

2. Right-click on the RCM tray icon .

3. Select **Device Configure**.

4. Select the **Ingenico iPP320 (Canadian EMV Contactless)** from the **PIN Pad Device** drop-down menu.

5. Select the **Default Language** to be used for transaction forms and prompts.

6. Enter the **COM Port** number used by the device.

7. Enter the Processing Account Terminal IDs into the **Debit TID** and **Credit TID** fields.

8. Choose the **Load Settings to Device** button from the **Device Setup** window. This may take several minutes and should not be interrupted.

9. Choose the **Load Forms to Device** button. This may take several minutes and should not be interrupted.

10. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iPP320 to complete the test.

11. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Ingenico iPP320 (US EMV and EMV Contactless)

1. Plug the Ingenico iPP320 into a USB port and a power outlet.

2. Right-click on the RCM tray icon .

3. Select **Device Configure**.

4. Select the **Ingenico iPP320 (US EMV)** from the **PIN Pad Device** drop-down menu.

5. Enter the **COM Port** number used by the device, and the **Default Message** if desired. The **Default Message** must be 30 characters or less.

6. Choose the **Load Forms to Device** button. This may take several minutes and should not be interrupted.

RCM Setup - PIN Pad Device Setup (CONTINUED)

7. Choose the **Load Settings to Device** button from the **Device Setup** window. This may take several minutes and should not be interrupted.

8. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iPP320 to complete the test.

9. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Ingenico iSC250

The Ingenico iSC250 is a signature capture device equipped to handle all forms of payment including EMV Chip & PIN, Chip & Sign, MagStripe, Signature Capture, and Contactless. The iSC250 has a 480x272 color display, with replaceable logos that display when idle. This device also supports the slide show feature. For additional information, see also the **Device Update**, **Edit Logo**, and **Slide Show** sections.

Ingenico iSC250 (Non-EMV)

1. Plug the Ingenico iSC250 into a USB port and a power outlet.

2. Right-click on the RCM tray icon.

3. Select **Device Configure**.

4. Select the **Ingenico iSC250** from the **PIN Pad Device** drop-down menu.

5. Enter the **COM Port** number used by the device and **Default Message** if desired. The **Default Message** must be 30 characters or less.

6. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iSC250 to complete the test.

7. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Ingenico iSC250 (US EMV and EMV Contactless)

1. Plug the Ingenico iSC250 into a USB port and a power outlet.

2. Right-click on the RCM tray icon.

3. Select **Device Configure**.

4. Select the **Ingenico iSC250 (US EMV)** from the **PIN Pad Device** drop-down menu.

5. Enter the **COM Port** number used by the device and **Default Message** if desired. The **Default Message** must be 30 characters or less.

6. Choose the **Load Forms to Device** button.

7. Choose the **Load Settings to Device** button from the **Device Setup** window. This may take several minutes and should not be interrupted.

8. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iSC250 to complete the test.

9. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

RCM Setup - PIN Pad Device Setup (CONTINUED)

Ingenico iSC480

The Ingenico iSC480 is a signature capture device equipped to handle all forms of payment including EMV Chip & PIN, Chip & Sign, MagStripe, Signature Capture, and Contactless. The iSC480 has a 800x340 color display, with replaceable logos that display when idle. This device also supports the slide show feature. For additional information, see also the **Device Update**, **Edit Logo**, and **Slide Show** sections.

Ingenico iSC480 (Non-EMV)

1. Plug the Ingenico iSC480 into a USB port and a power outlet.
2. Right-click on the RCM tray icon .
3. Select **Device Configure**.
4. Select the **Ingenico iSC480** from the **PIN Pad Device** drop-down menu.
5. Enter the **COM Port** number used by the device, and the **Default Message** if desired. The **Default Message** must be 30 characters or less.
6. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iSC480 to complete the test.
7. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Ingenico iSC480 (US EMV and EMV Contactless)

1. Plug the Ingenico iSC480 into a USB port and a power outlet.
2. Right-click on the RCM tray icon .
3. Select **Device Configure**.
4. Select the **Ingenico iSC480 (US EMV)** from the **PIN Pad Device** drop-down menu.
5. Enter the **COM Port** number used by the device.
6. Choose the **Load Forms to Device** button.
7. Choose the **Load Settings to Device** button from the **Device Setup** window. This may take several minutes and should not be interrupted.
8. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iSC480 to complete the test.
9. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

RCM Setup - PIN Pad Device Setup (CONTINUED)

Ingenico iCMP

The Ingenico iCMP is a Bluetooth PIN entry EMV Device with an integrated Magnetic Stripe Reader, EMV chip card reader, and a monochrome display. See also the Device Update section.

Ingenico iCMP (US EMV and EMV Contactless)

1. Power on and pair the Ingenico iCMP in Windows (see Pairing the iCMP Bluetooth adapter below).

2. Right-click on the RCM tray icon .

3. Select **Device Configure**.

4. Select the **Ingenico iCMP (US EMV)** from the **PIN Pad Device** drop-down menu.

5. Select the **Serial Number used by the device** from the Serial Number drop-down menu, and the Default Message if desired. The Default Message must be 30 characters or less.

6. Choose the **Load Forms to Device** button. This may take several minutes, and should not be interrupted.

7. Choose the **Test** button to initialize the device, then follow the prompts on the screen of the Ingenico iCMP to complete the test.

8. Choose **OK** from the confirmation window, then **OK** on the **Device Setup** window.

Pairing the iCMP Bluetooth Adapter

1. Plug the USB Bluetooth adapter into the USB port on the computer and ensure the device is properly detected by the Windows Device Manager.

2. Power on the iCMP by pressing the power button, next to the charging port.

3. To put the device into pairing mode, the device needs to be at a BT Pairing Required screen.
   - If the device says Welcome instead, rapidly press the F key on the device's keypad, 4 times.

RCM Setup - PIN Pad Device Setup (CONTINUED)

4. On the **BT Pairing Required** screen you should also see **STANDARD**. This should be above the **F2** key.

Press the **F2** key to begin the pairing.

5. Locate the Bluetooth icon in the **System Tray**.

6. Right click the icon and select **Add a Device**.
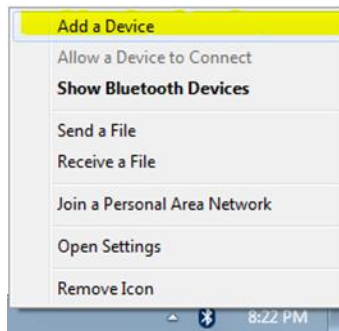
7. Locate and select the device that has **iCMP** next to it. It should match up to what's seen on the Device's screen, for the **BT Name**. Click the **Next** button.
    NOTE: Windows 8 and 10 systems will not have a "Next" button. Instead, once you click on the device, there will be a "Pair" button that appears. Click that instead.

    Example:

iCM122-21038612
Bluetooth
Phone
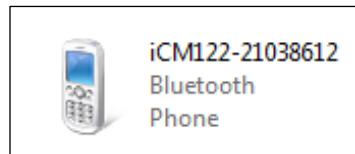
RCM Setup - PIN Pad Device Setup (CONTINUED)

8. On the next screen, it will require a PIN. The PIN it needs can be found on the device screen. Once you enter the PIN into the empty box click the **Next** button.
NOTE: Windows 8 and 10 systems will not move to a different window to enter the pairing PIN, instead a window will pop-up. Enter the PIN in that window, then click the "Next" button.
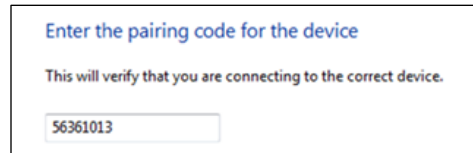
9. The computer and the device will begin/attempt to pair. Once it's done, you should see the following screen.
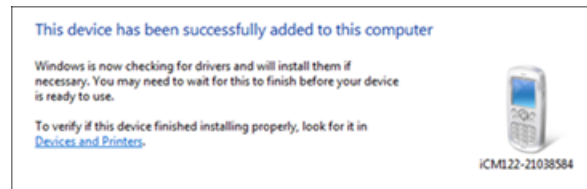
10. *Click* Close.

Ingenico iUC285

The Ingenico iUC285 is a wired Contact and Contactless Device with an integrated Magnetic Stripe Reader, EMV chip card reader, and a monochrome display.

1. Plug the Ingenico iUC285 into a USB port and a power outlet.

2. Right-click on the RCM tray icon.

3. Select Device Configure.

4. Select the **Ingenico iUC285 (US EMV)** from the PIN Pad Device drop-down menu.

5. Enter the COM Port number used by the device, and the **Default Message** if desired. The **Default Message** must be no more than 30 characters in length.

6. Choose the **Test** button to initialize the device, then follow the prompts on the Ingenico iUC285 to complete the test.

7. Choose **OK** from the confirmation window, then OK on the **Device Setup** window.

PIN Pad Functions

PIN Pad Device Update

OpenEdge can provide software updates to certain PIN Pad devices, which may add support for new features or resolve issues. When a new update is available for the configured device, a window will display prompting the user to update the device. The updates usually take 5 to 15 minutes to complete, and the device will automatically restart during the process. If the update is optional, it may be postponed.

Manually checking for PIN Pad Device Updates

1. Right-click on the RCM tray icon .
2. Select **Device Configure**.
3. If the PIN Pad Device is already configured, then proceed to Step 4. Otherwise, see the "RCM Setup - PIN Pad Device Setup" section.
4. Select the **Device Update** button.

Default Language

Some devices support prompts and menus in both French and English. If one of these devices has been set up, follow these steps to set the default language for the device:

Set the Default Language Used by Device

1. Right-click on the RCM tray icon .
2. Select Device Configure
3. Click **Default Language** dropdown
4. Select desired default language
5. Click **Ok**
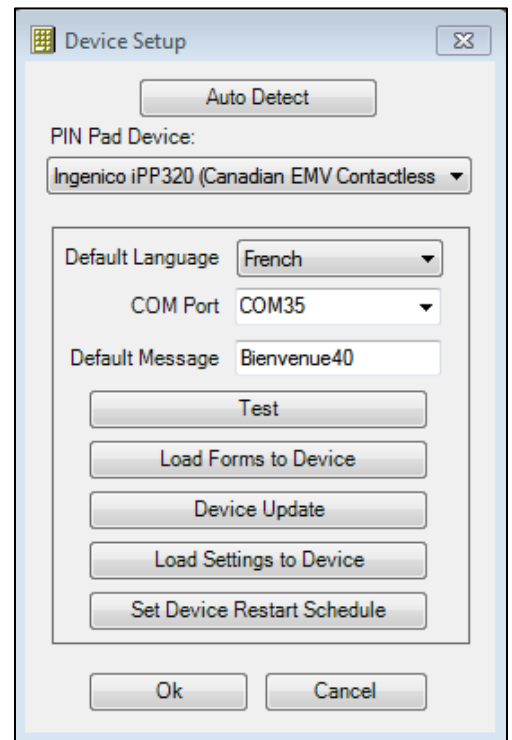
Device Restart Schedule

PCI regulations require that Ingenico V4 devices be rebooted daily. To ensure that this reboot does not interfere with normal business operations, a specific time can be designated for daily restarts. This restart does not need to occur during business hours. The device restart can be scheduled for any time. If restart is not scheduled, the default time is 3:00 AM.

Set the Device Restart Time

1. Right-click on the RCM tray icon.
2. Select Device Configure
3. Click **Set Device Restart Schedule**
4. Enter the desired time for the daily reboot which will not interfere with normal business operations
5. Click **Ok** on **Restart Schedule** window.
6. Click **Ok** on **Device Setup** window.
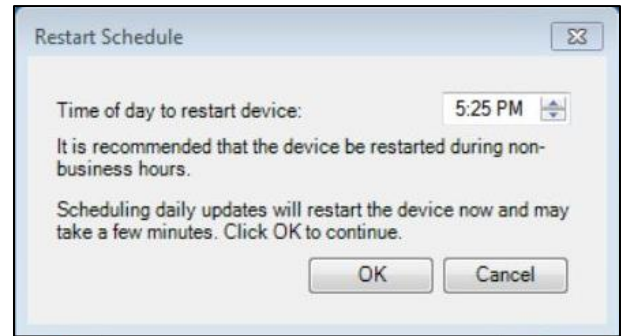
NOTE:

The PIN Pad device will automatically restart during the device update process.

Edit Logo

On supported devices, a single image may be selected to be shown as the default screen. This image will be displayed when the device is idle and a slide show is not running. Images must be of the same resolution as the PIN Pad device's screen and of the format required by the device (typically .jpg or .png).

1. Right-click on the RCM tray icon.
2. Select **Device Configure**.
3. Select the **Edit Logo** button.
4. Browse to the image file. Select **OK**.
5. Select the **Load Forms to Device** button to update the PIN Pad device with any changes.

Slide Show

On supported devices, images may be displayed while the device is idle. Images must be of the PIN Pad device's resolution and of the format required by the device (typically .jpg or .png). To load the images onto the device, use the **Slide Show** feature.

1. Right-click on the RCM tray icon.
2. Select **Device Configure**.
3. Select the **Slide Show** button.
4. The Image Slide Show window displays.

a. Check the **Enable Slide Show** box.

b. Choose the **Wait** and **Pause** times.

c. Select the **Add** button to add images to the slide show.

d. Select the **Delete** button to remove images from the slide show.

e. The **Display** button will show the selected image on the device.

f. The **Test Slide Show** button will initiate a slide show on the device using the images currently loaded to the PIN Pad device.

> **NOTE:**
>
> The **Load Forms to Device** button from the Device Setup window must be used to update the PIN Pad before changes to the slide show will appear.

5. Select the **OK** button to save the changes made.

6. Select the **Load Forms to Device** button to update the PIN Pad device with any changes.

Schedule Device Updates

On supported devices, updates can be scheduled for times that will not disrupt business operations.

1. Right-click on the RCM tray icon .

2. Select **Device Configure**.

3. Select the **Set Device Update Schedule** button. A pop-up window will appear.

4. Select the time of day and days of the week for the device to check for and install updates.

openedge
A division of **globalpayments**

ADDITIONAL INFORMATION

EMV Device Prompts

The following list details all possible prompts that may display on each EMV device, and describes what each prompt means.

Ingenico iPP320

- "READY" is the default idle message. This message can be changed through the PIN Pad device setup configuration. The prompt indicates that the device is functional and ready to use. You may proceed to running your transaction.
- "AMOUNT: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper.
- "REFUND: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper on a refund transaction.
- "AMOUNT: $X.XX TAP OR SWIPE CARD" is the prompt received when the card is ready to be tapped against the NFC sensor, or swiped through the card swiper.
- "DO NOT REMOVE CARD" displays when an EMV transaction is in progress. Do not remove your card from the EMV reader.
- "ENTER PIN" is prompting you to enter in the PIN associated with your card.
- "TRANSACTION CANCELLED REMOVE CARD" appears when a transaction is cancelled either intentionally or otherwise. Remove your card from the EMV reader.
- "AUTHORIZING DO NOT REMOVE CARD" displays while your card is being authorized. Do not remove your card.
- "APPROVED REMOVE CARD" displays after your card has been approved. Remove your card from the EMV reader.
- "APPROVED" displays after you have completed your transaction successfully and removed your card from the EMV reader.
- "DECLINED REMOVE CARD" indicates that the card was not approved. Remove your card from the EMV Reader.
- "ENTRY TIMEOUT TRANSACTION CANCELLED REMOVE CARD" displays when the device has been left idle for too long after beginning a transaction. Remove your card from the EMV reader and retry your transaction.
- "ENTER CARD NUMBER" prompts you to manually input the EMV card number, rather than swiping, tapping, or inserting the card.
- "ENTER EXPIRATION DATE" prompts you to enter the expiration date of the card for keyed in processing.
- "ENTER CVV OR CID FROM CARD" prompts you to enter the CVV or CID from the card for keyed in processing.
- "AMOUNT $X.XX ADD TIP?" displays the amount of your transaction, and asks if you would like to add a tip. SELECT "YES" or "NO".
- "ENTER TIP:" prompts you to enter in the amount you would like to add as a tip.

Ingenico iSC250

- "READY" is the default idle message. This message can be changed through the PIN Pad device setup configuration. The prompt indicates that the device is functional and ready to use. You may proceed to running your transaction.
- "AMOUNT: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper.
- "REFUND: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper on a refund transaction.
- "AMOUNT: $X.XX TAP OR SWIPE CARD" is the prompt received when the card is ready to be tapped against the NFC sensor, or swiped through the card swiper.
- "ENTER PIN" is prompting you to enter in the PIN associated with your card.
- "PROCESSING" is displayed while the non-EMV transaction is being processed.
- "AUTHORIZING DO NOT REMOVE CARD" displays while your card is being authorized. Do not remove your card.
- "APPROVED REMOVE CARD" displays after your card has been approved. Remove your card from the EMV reader.
- "APPROVED" displays after you have completed your transaction successfully and removed your card from the EMV reader.
- "DECLINED REMOVE CARD" indicates that the card was not approved. Remove your card from the EMV Reader.
- "ENTER CARD NUMBER" prompts you to manually input the EMV card number, rather than swiping, tapping, or inserting the card.
- "ENTER EXPIRATION DATE" prompts you to enter the expiration date of the card for keyed in processing.
- "ENTER CVV OR CID FROM CARD" prompts you to enter the CVV or CID from the card for keyed in processing.
- "PROCESSING" is displayed while the transaction is being processed.
- "TRANSACTION CANCELLED REMOVE CARD" appears when a transaction is cancelled either intentionally or otherwise. Remove your card from the EMV reader.
- "AMOUNT $X.XX ADD TIP?" displays the amount of your transaction, and asks if you would like to add a tip. Select "YES" or "NO".
- "ENTER TIP:" prompts you to enter in the amount you would like to add as a tip.
- "PLEASE ENTER SIGNATURE" prompts you to sign for your purchase. Select "Accept" or the green button after signing.
- "SIGNATURE ACCEPTED" displays after you accept your signature on the PIN pad.

Ingenico iSC480

- "READY" is the default idle message. This message can be changed through the PIN Pad device setup configuration. The prompt indicates that the device is functional and ready to use. You may proceed to running your transaction.
- "AMOUNT: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper.
- "AMOUNT: $X.XX TAP OR SWIPE CARD" is the prompt received when the card is ready to be tapped against the NFC sensor, or swiped through the card swiper.

Ingenico iSC480 (Continued)

- "REFUND: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper on a refund transaction.
- "ENTER PIN" is prompting you to enter in the PIN associated with your card.
- "PROCESSING" is displayed while the non-EMV transaction is being processed.
- "AUTHORIZING DO NOT REMOVE CARD" displays while your card is being authorized. Do not remove your card.
- "APPROVED REMOVE CARD" displays after your card has been approved. Remove your card from the EMV reader.
- "APPROVED" displays after you have completed your transaction successfully and removed your card from the EMV reader.
- "DECLINED REMOVE CARD" indicates that the card was not approved. Remove your card from the EMV Reader.
- "ENTER CARD NUMBER" prompts you to manually input the EMV card number, rather than swiping, tapping, or inserting the card.
- "ENTER EXPIRATION DATE" prompts you to enter the expiration date of the card for keyed in processing.
- "ENTER CVV OR CID FROM CARD" prompts you to enter the CVV or CID from the card for keyed in processing.
- "TRANSACTION CANCELLED REMOVE CARD" appears when a transaction is cancelled either intentionally or otherwise. Remove your card from the EMV reader.
- "AMOUNT $X.XX ADD TIP?" displays the amount of your transaction, and asks if you would like to add a tip. SELECT "YES" or "NO".
- "ENTER TIP:" prompts you to enter in the amount you would like to add as a tip.
- "PLEASE ENTER SIGNATURE" prompts you to sign for your purchase. SELECT "ACCEPT" or the green button after signing.
- "SIGNATURE ACCEPTED" displays after you accept your signature on the PIN pad.

Ingenico iCMP

- "READY" is the default idle message. This message can be changed through the PIN Pad device setup configuration. The prompt indicates that the device is functional and ready to use. You may proceed to running your transaction.
- "AMOUNT: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper.
- "AMOUNT: $X.XX SWIPE OR TAP CARD" is the prompt received when the card is ready to be tapped against the NFC sensor or swiped through the card swiper.
- "REFUND: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper on a refund transaction.
- "ENTER PIN" is prompting you to enter in the PIN associated with your card.
- "PROCESSING" is displayed while the non-EMV transaction is being processed.
- "AUTHORIZING DO NOT REMOVE CARD" displays while your card is being authorized. Do not remove your card.

Ingenico iCMP (Continued)

- "APPROVED REMOVE CARD" displays after your card has been approved. Remove your card from the EMV reader.
- "APPROVED" displays after you have completed your transaction successfully and removed your card from the EMV reader.
- "DECLINED REMOVE CARD" indicates that the card was not approved. Remove your card from the EMV Reader.
- "ENTER CARD NUMBER" prompts you to manually input the EMV card number, rather than swiping, tapping, or inserting the card.
- "ENTER EXPIRATION DATE" prompts you to enter the expiration date of the card for keyed in processing.
- "ENTER CVV OR CID FROM CARD" prompts you to enter the CVV or CID from the card for keyed in processing.
- "TRANSACTION CANCELLED REMOVE CARD" appears when a transaction is cancelled either intentionally or otherwise. Remove your card from the EMV reader.
- "AMOUNT $X.XX ADD TIP?" displays the amount of your transaction, and asks if you would like to add a tip. Select "YES" or "NO".
- "ENTER TIP:" prompts you to enter in the amount you would like to add as a tip.
- "PLEASE ENTER SIGNATURE" prompts you to sign for your purchase. Select "ACCEPT" or the green button after signing.
- "SIGNATURE ACCEPTED" displays after you accept your signature on the PIN pad.

Ingenico iUC285

- "READY" is the default idle message. This message can be changed through the PIN Pad device setup configuration. The prompt indicates that the device is functional and ready to use. You may proceed to running your transaction.
- "AMOUNT: $X.XX INSERT, SWIPE OR TAP CARD" is the prompt received when the card is ready to be inserted into the EMV reader, tapped against the NFC sensor, or swiped through the card swiper.
- "PROCESSING" is displayed while the non-EMV transaction is being processed.
- "AUTHORIZING DO NOT REMOVE CARD" displays while your card is being authorized. Do not remove your card.
- "APPROVED REMOVE CARD" displays after your card has been approved. Remove your card from the EMV reader.
- "APPROVED" displays after you have completed your transaction successfully and removed your card from the EMV reader.
- "DECLINED REMOVE CARD" indicates that the card was not approved. Remove your card from the EMV Reader.
- "TRANSACTION CANCELLED REMOVE CARD" appears when a transaction is cancelled either intentionally or otherwise. Remove your card from the EMV reader.

OpenEdge Gateway Response Codes

These tables list the Response Codes that may be returned when processing with the Credit Card Processor configured to XWeb.

OpenEdge Gateway Response Codes		
Code	**Verbiage**	**Description**
000	Approval	The transaction was approved.
001	Decline	The transaction was declined, no specific decline reason was given.
002	Call	A Voice Authorization is requested. For more information on Voice Auths see **Additional Information - Frequently Asked Questions**.
003	Success	Batch settled successfully.
004	Inquiry	Batch inquiry successful.
005	Alias Success	A payment account (e.g. credit card) Alias was created successfully and the number has been stored on the gateway for future use.
007	Partial Approval	Transaction was approved, but not for the entire amount. This response is only possible with "Partial Approval Support" is enabled, which is mandated in many circumstances. The "Approved Amount" should be returned with the response, and the balance may need to be paid with another card or other form of tender.
008	Report Complete	This is the standard response for a successful report retrieval from the XWeb gateway.
009	Auto Decline	The transaction was declined due to an AVS or CSC mismatch. The AVS (Address Verification System, house number and/or ZIP code verification for keyed transactions) or CSC (Card Security Code, also known as the CVV, CVC or CID) is set to "required" for keyed transactions at the XWeb gateway, but the value(s) entered did not match the value(s) on file. The reason for the decline may be specified.
010	Invalid Expiration Date	Expiration date entered is incorrect.
011	Check Submitted	This is the standard response for a successful Check Sale or Check Credit transaction.
012	Check Approval	This is the standard response for an approved Check Verification transaction.
013	Check Decline	This is the standard response for a declined Check Verification transaction.
014	Check Warning	This message can indicate that the Check Verification service is currently unavailable for the configured OpenEdge Check Processing Account. The reason for the warning may be specified.

OpenEdge Gateway Response Codes

Code	Verbiage	Description
015	Check Error	This occurs when there is a physical problem with the check and the check cannot be read.
016	Check Transaction Amount Limit Exceeded	The amount attempted on the Check Sale or Check Credit transaction exceeds the maximum amount configured on the OpenEdge Check Processing Account. This does not pertain to the "Maximum Charge Amount" setting in the XCharge Server Setup.
017	Check Daily Amount Limit Exceeded	The total amount of all the transactions for that day has exceeded the pre-set limit configured on the OpenEdge Check Processing Account. The amount limit can be adjusted via the DCS ACHeck21 Global Gateway.
018	Check Monthly Amount Limit Exceeded	The total amount of all the transactions for that month has exceeded the pre-set limit configured on the OpenEdge Check Processing Account. The amount limit can be adjusted via the DCS ACHeck21 Global Gateway.
019	RDFI Not Qualified To Participate	The bank on which the check was written (as indicated by the Routing Number) cannot participate in the ACH system. The most common reasons for this response are: using a test check, or the check is from an institution that is no longer in business.
020	Corporate Customer Advises Not Authorized	This response code indicates that the check is written on a corporate account and is therefore not eligible to be processed via ACH. Note that this is an ACH-only error - if an image is available, the item could be processed via Check21.
021	Check Not Previously Authorized	Indicates that the attempted check transaction cannot be completed until a successful Check Verification transaction is completed first.
022	Ineligible Transaction For ACH Network	The check that was entered cannot be processed through the ACH network.
031	Preverification Failure	The value Address, CVV, or ZIP code submitted with the Pre-Transaction Verification transaction did not match the value on file.
025	BIN Lookup Success	Standard response for a successful BIN Lookup transaction.
800	Parsing Error	Unable to parse the XML request sent.
801	Maximum Request Data Exceeded Error	The XML request exceeds the 2048-byte maximum size.
802	Duplicate Field Error	The XML request had more than one copy of a particular field. The field causing the error may be specified.
803	Improper DLL Error	Unrecognized DLL name. This can be caused by a wrong URL entered into the "Server Location" setting under XCharge Server Setup, Credit Cards, Connection.

OpenEdge Gateway Response Codes

Code	Verbiage	Description
804	Specification Version Error	XML error, the Specification Version field is set incorrectly.
805	Authentication Error	The XWeb ID, Auth Key or Terminal ID fields are incorrect (check for leading and trailing spaces if they appear to match those on file). The field causing the error may be specified.
806	Production Merchant Set Up Error	The Mode was incorrectly sent. This can happen when trying to process on the Production server with a Development or Test Mode Processing Account.
807	Test Merchant Set Up Error	The Mode was incorrectly sent. This can happen when trying to process on the Test server with a Development or Production Mode Processing Account.
808	Development Merchant Set Up Error	The Mode was incorrectly sent. This can happen when trying to process on the Development server with a Production or Test Mode Processing Account.
809	Required Field Not Sent Error	A field that is required for this transaction type was not sent. The field causing the error may be specified.
810	Inconsistent Conditional Field Error	A field that does not have to be sent was sent in the wrong context. The field causing the error may be specified.
811	Improper Field Data Error	A field sent to the XWeb gateway was not formatted correctly. This could pertain to Processing Account Information configured in XCharge or BMS, or card information. The field causing the error may be specified.
812	Unrecognized Name / Tag Error	The XML tag sent is not in the API.
813	Duplicate Transaction Error	A transaction was run for the same amount on the same card within a certain time limit. The duplicate checking time is set on the XWeb gateway, usually between 1 and 60 minutes.
814	Invalid Reference Error	The Transaction ID used for a Void, Return, etc. is invalid.
815	Transaction Already Voided	The Transaction ID used for a Void was already voided.
816	Transaction Already Captured	The Transaction ID used for a Capture of an Authorized charge was already used and the transaction has been Captured.
817	Empty Batch	The batch is empty and cannot settle. You cannot settle an empty batch.
818	Merchant Locked For Settlement	The Processing Account is in the process of being settled/batched. Wait a moment and try again.

OpenEdge Gateway Response Codes

Code	Verbiage	Description
819	Merchant Locked for Maintenance	The Processing Account is locked for database or server maintenance. Wait a moment and try again.
820	Temporary Service Outage - Retry Transaction	The XWeb gateway itself may be down. Wait a moment and try again.
823	Invalid Account Data	A field sent to the XWeb gateway appears invalid (correctly formatted but not on file). This could pertain to Processing Account Information configured in XCharge or BMS, or card information. The field causing the response may be specified.
824	Industry Mismatch Error	The Processing Account is configured with the incorrect Market Type. This can occur if XCharge or BMS is not configured with the same Market Type as the XWeb gateway.
828	Card Type Not Supported	The card type (Visa, MasterCard, American Express, etc.) for the attempted transaction is not enabled at the XWeb gateway.
829	Card Code Required	The Card Security Code (CSC, also known as the CVV, CVC or CID) is set to "required" for keyed transactions at the XWeb gateway, but was not sent.
830	Address Required	The address (house number, part of the Address Verification System) is set to "required" for keyed transactions at the XWeb gateway, but was not sent.
831	ZIP Code Required	The ZIP code (part of the Address Verification System) is set to "required" for keyed transactions at the XWeb gateway, but was not sent.
832	Encoded Data Format Error	Encoded format of check image file could not be read or was not submitted when expected.
833	Check Services Image Error - MICR and Amount cannot be read	The attempted paper check scan failed. When this occurs you should have the option to manually enter the check information or rescan the check.
834	Check Services Image Error - MICR cannot be read	The attempted paper check scan failed. When this occurs you should have the option to manually enter the check information or rescan the check.
835	Check Services Image Error - Amount cannot be read	The attempted paper check scan failed. When this occurs you should have the option to manually enter the check information or rescan the check.
900	TSYS Error	Error thrown by Processor TSYS: XWeb is setup correctly, but the card or other value submitted is incorrect. SERV NOT ALLOWED usually indicates a Decline, Failure CV indicates the Card Type is not supported (e.g. AMEX needs to be enabled), and Failure HV indicates an error on the account setup in XWeb.

OpenEdge Gateway Response Codes		
Code	**Verbiage**	**Description**
901	Processor Error	Can be Global or TSYS errors (900 Global Payments Error: or 900 TSYS Error:) are returned on transactions if a processor setting is not configured correctly. This can occur if the card or transaction type is not enabled on the Processing Account at the processor end.
903	DCS Error	These errors are returned on transactions if a processor setting is not configured correctly. This can occur if the transaction type is not enabled on the OpenEdge Check Processing Account at the processor end. The reason for the error may be specified (e.g. NoValidationActionsSetup for Check Verification).

OpenEdge Host Pay Specific Response Codes

This table lists the Response Codes that may be returned when processing with the Credit Card Processor configured with OpenEdge Host Pay.

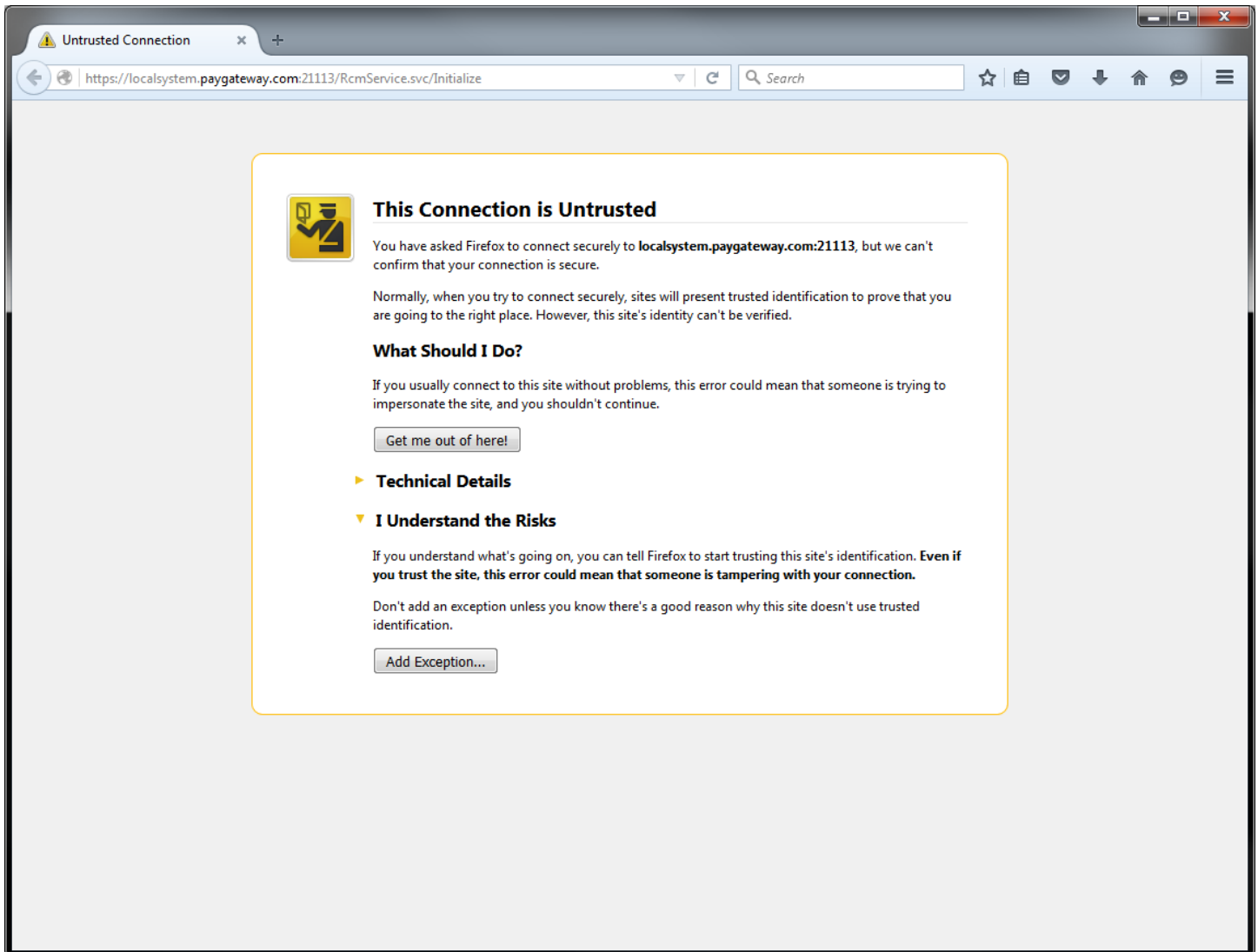| Response Codes	
Response Code	**Description**
1	SUCCESSFUL TRANSACTION: Response code indicating the transaction was successfully processed.
2	MISSING REQUIRED REQUEST FIELD: Response code indicating that a required request field was not provided with the request. The required field will be identified in the response code text.
3	INVALID REQUEST FIELD: Response code indicating that one of the values provided was not valid. The field will be identified in the response code text.
4	ILLEGAL TRANSACTION REQUEST: Response code indicating the transaction request was illegal. This can happen if a transaction is sent for an account that does not exist or if the account has not been configured to perform the requested transaction type.
5	TRANSACTION SERVER ERROR: Response code indicating that an error occurred within the transaction server. This type of error is temporary. If one occurs, the gateway maintenance staff are immediately signaled to investigate the problem.
6	TRANSACTION NOT POSSIBLE: Response code indicating that the requested transaction is not possible. This can occur if the transaction request refers to a previous transaction that does not exist. For example, one possible request is to perform a capture of funds previously authorized from a customer's credit card. If a capture request is sent that refers to an authorization that does not exist, this response code will be returned. This can also occur if you perform a card authorization using an existing order ID, whether approved or declined.
100	CREDIT CARD DECLINED: Response code indicating the transaction request was declined.
101	ACQUIRER GATEWAY ERROR: Response code indicating that the acquirer processor encountered an error. This is software that handles financial transactions and communicates with the private banking network.
102	PAYMENT ENGINE ERROR: Response indicating that the payment service encountered an error.

RCM Response Codes

RCM Response Codes	
rcm_response_code	rcm_response_description
0	Success
1	NotSupportedByDevice
2	CommError
3	Canceled
4	Fail
5	NoDeviceConfigured
6	DeviceNotConfigured
7	DeviceInitError
8	InvalidCardType
9	InvalidCcNumber
10	InvalidAmount
11	InvalidTrack2
12	Declined
100	MissingRequiredField
101	ImproperDataFormat

OpenEdge Platform

Appendix A - Using the RCM with Firefox

If you intend to use the Remote Client Manager (RCM) with Firefox, please follow the instructions below to properly configure Firefox.

Step 1:

Open Firefox and browse to: https://localsystem.paygateway.com:21113/RcmService.svc/Initialize
Expand the 'I Understand the Risks' section. Click the Add Exception button.

openedge
A division of globalpayments

Appendix A - Using the RCM with Firefox (Continued)

Step 2:

Check the '**Permanently store this exception**' checkbox. Click the **Confirm Security Exception** button.
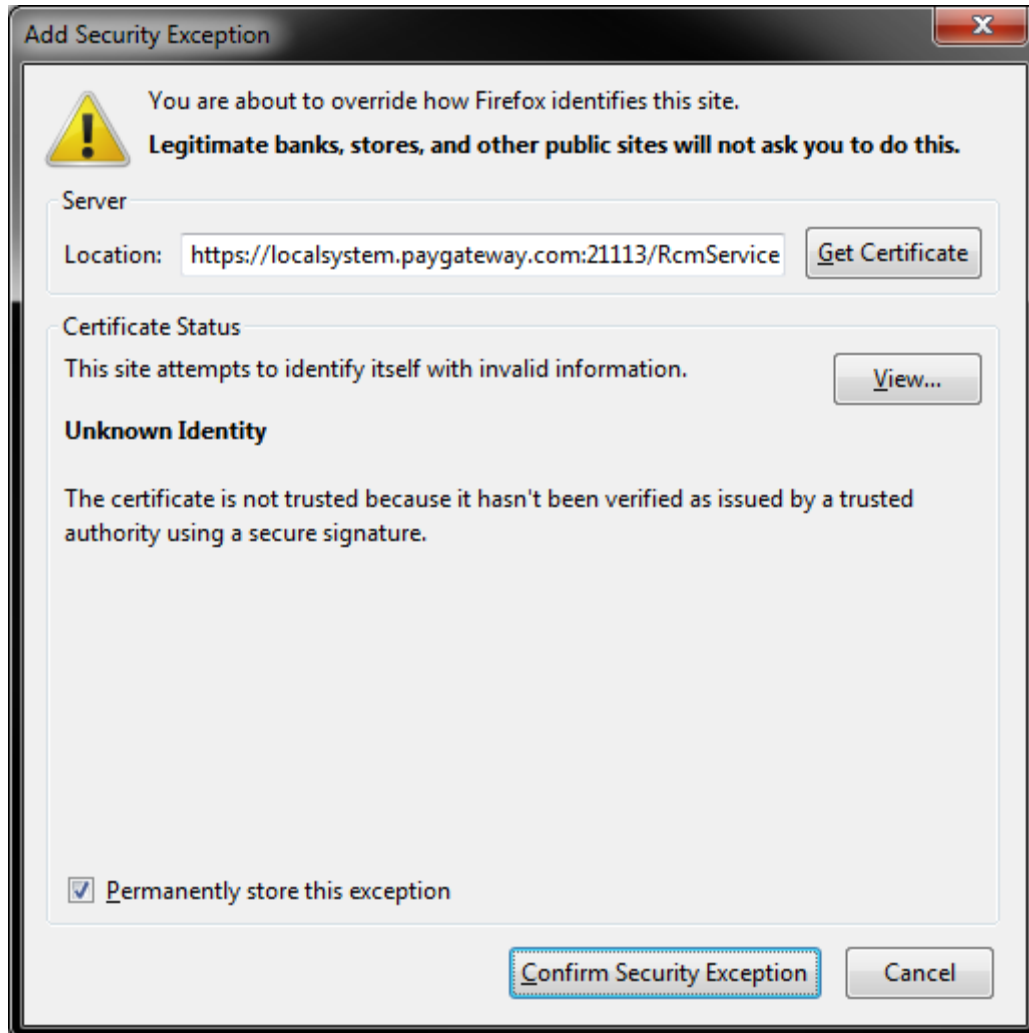
Done!

Firefox is now properly configured for use with the RCM.

RCM Release Notes

- = Issue, Enhancement
- o = Resolution

January 2020	Version 2.6.2
Area	**Description**
EdgeExpress Cloud, Enhancement	• Updated RBAUpdate URL to go through secure HTTPS protocol. • Improved transaction time when using iCMP devices.

EdgeExpress Cloud, Bug Fix	• CardholderName is not returned in transaction response for CONTACT/CONTACTLESS transactions.
	  o Fixed by obtaining cardholder name for Quick Chip transactions.
	• VISA ZDAs are reversed by the RCM after being approved by the processor for EMV transactions.
	  o Updated EMVIssuerResponse calculation at the gateway level to support Visa ZDA for EMV transactions.
	• Tip amount is not summed up properly.
	  o Fixed by adding tip amount on follow-on transactions.
	• Error Updating Device SlideShow settings.
	  o Removed Clear message when updating slideshow.
	• Remove Card while Transaction is in progress is behaving differently between 2.6.0 Alpha and Beta.
	  o Reverted code that was causing the undesired behavior in Beta.
	• Generic "814; Invalid Reference Error" is returned instead of a specific error message.
	  o Changed code to restrict CreditUpdateTransaction to show relevant error message.
	• The Hardware Device Failure message is not suppressed on Silent Installs.
	  o Added SUPPRESSUI validation in the code.
	• PINPad Device upgrade process is not entirely silent when the device is configured to a bad COM port.
	  o Added SUPPRESSUI validation in the code.
	• PINPad Device Updates - Exclusive Access to Firmware Not Obtained.
	  o Protected against "Time of Check-Time of Use" vulnerability.
	• Incorrect PPDGETCONFIGUREDDEVICE result for CAN RBA EMV PIN Pad
	  o Located and corrected issue in code.
	• Signature fails when the card is removed at initial card removal prompt.
	  o Set signature to prompt after card has been removed.

October 2019	Version 2.6.0
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added support for Quick Chip for all card brands on US EMV Ingenico iPP320, iSC250, iSC480, and iCMP devices.

	• Added support for card pre-insertion functionality on US EMV Ingenico iPP320, iSC250, iSC480, and iCMP devices, allowing cardholders to insert their card before the transaction is started. • Removed Magstripe Contactless support for Discover to comply with card-brand regulations. • Updated the Terminal Configurations for Mastercard AIDs. • Added PROMPTCASHBACK, CASHBACKLIMIT, CASHBACKOPTION1, CASHBACKOPTION2, and CASHBACKOPTION3 to EdgeExpress API V2. • Updated EBTTYPE to not have a default value and also be required in EdgeExpress API V2.

EdgeExpress Cloud, Bug Fix	• A CASHBACKAMOUNT of "0" was returned in the EdgeExpress response on EBTSALETRANSACTIONs when CASHBACKAMOUNT was not sent in the request.
	  o EdgeExpress returns CASHBACKAMOUNT only if it is sent or the result is greater than 0.
	• Contactless DebitSale and EBTSale transactions including a CASHBACKAMOUNT are declined.
	  o Removed tap option for DebitSale and EBTSale transactions that include Cashback, entered as CASHBACKAMOUNT or chosen using PROMPTCASHBACK.
	• "Unable to update device form" on the iUC285 device.
	  o Resolved issue causing forms to not be loaded to the iUC285 device.
	• Non-EMV transactions including a Tip are not generating a correct total amount properly.
	  o Resolved issue causing total amounts not being added correctly.
	• Transactions are partially approved even when sending PARTIALAPPROVALSUPPORT as False.
	  o Issue fixed by validating the value sent with the PARTIALAPPROVALSUPPORT parameter.
	• EMV zero dollar authorizations get stuck on 'Please Wait' screen.
	  o Fixed issue causing the device to freeze on a zero dollar authorization.
	• Transactions process when PROMPTCASHBACK is sent along with an empty CASHBACKAMOUNT value.
	  o Added validation so that PROMPTCASHBACK and CASHBACKAMOUNT cannot be sent in the same transaction request.
	• The transaction contactless limit in Canada was set to $100.
	  o Updated the contactless limit in Canada to $999,999.99.

June 2019	Version 2.5.0
Area	**Description**
EdgeExpress Cloud, Enhancement	• Upgraded Ingenico devices to use RBA 23.0.26. • Added support for US EMV and US non-EMV Ingenico V4 devices. • Added functionality to schedule device reboot for Ingenico V4 devices. • Removed Magstripe Contactless support for Visa and Mastercard to comply with card-brand regulations. • Added APIVERSION and CREATEALIAS to EdgeExpress API.

	• For Canadian Contactlesss tranasactions, increased CVM Required Limit from $50 to $999,999.99.

EdgeExpress Cloud, Bug Fix	• Expected RBA rollback warning is not displayed when the device RBA version does not match the current EEPC/EEC supported RBA version. (TRIAGE-1064)
	   o Updated to display expected RBA rollback warning.
	   o Removed non-EMV fallback support when device RBA version does not match the EdgeExpress Cloud supported version.
	• In some cases, Force and Adjustment transaction amounts are rounded to the nearest whole dollar.
	   o Fixed error by validating decimal-point lengths on submitted amounts.
	• For systems with the Windows language set to French Canadian, transactions fail with an Invalid Amount error.
	   o Updated EdgeExpress Cloud to gracefully handle amount conversions to support Windows regional settings with French (Canada).
	• For silent installations (or upgrades) of EdgeExpress Cloud 2.5.0, the PPD Update functions fails when the device does not need an RBA update.
	   o Updated to correctly handle silent installations and upgrades to EdgeExpress Cloud 2.5.0.
	• Tapping specific Discover Debit cards puts the device in a bad state causing the device to freeze on Insert.
	   o Updated so the device no longer freezes on Insert after tapped with specific Discover Debit cards.

March 2019	**Version 2.4.1**
Area	**Description**

EdgeExpress Cloud, Bug Fix	• US Contact Discover Debit transactions fail with error, "Function Failed. No US Debit PIN Data."
	   o Fixed error by ensuring prompt for PIN entry when performing Discover Debit.
	• Debit EMV transactions attempted with CIBC Bank Cards fail with error, "PIN Pad Device Failed. Transaction cancelled. Please try again." (TRIAGE-1067)
	   o Fixed error by removing the requirement for cardholder name with transactions on CPX devices.

January 2019	**Version 2.4.0**
Area	**Description**

EdgeExpress Cloud, Enhancement	• Added support for Ingenico iPP320 (Canadian EMV Contactless) device using RBA 23.
	   o Added support for single TID processing in Canada.
	   o Added support for EMV Contactless transactions in Canada.
	   o Added support for Interac void transactions.
	   o Disabled fallback support for Canadian EMV transactions.
	   o Updated currency format for French language transactions.
	   o Added French language support for PinPadDevice functions.
	   o Added "Set Device Restart Schedule" option to Device Setup screen.

	○ Added "Default Language" dropdown menu with options "French" and "English" to Device Setup screen.

EdgeExpress Cloud, Bug Fix	• When setting up a new EMV device, JUNGO drivers are not automatically loaded. (TRIAGE-1021)
	  ○ Updated to automatically load drivers.
	• After installing and attempting to run EdgeExpress Cloud 2.4.0, an "Access to the registry key" error may display. (TRIAGE-1022)
	  ○ Ensured required registry settings are set during EdgeExpress Cloud installation.
	• For Remote Desktop Protocol installations of RCM, after selecting User Specific option during installation, RCM is configured for System Wide Settings instead.
	  ○ Ensured required registry settings are set during EdgeExpress Cloud installation.

October 2018	Version 2.3.1
Area	**Description**
EdgeExpress Cloud, Enhancement	• Updated to process EMV zero dollar authorizations as MSR transactions. • Updated to not return receipt data for zero dollar authorizations. • Added End User License Agreement to the Remote Client Manager "About" window. • Enhanced EdgeExpress PC and EdgeExpress Cloud/RCM logging.

EdgeExpress Cloud, Bug Fix	• Devices intermittently fail to initialize.
	  ○ Fixed error by closing PIN Pad device connection after device functions.
	• Attempting transactions using parameter <SUPPRESSUI /> and the iUC285 device returns an exception error.
	  ○ Fixed error by ensuring that <SUPPRESSUI /> is only submitted once per request.

August 2018	Version 2.3.0
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added EMV Contactless support for Ingenico iPP320, iSC250, iSC480 and iCMP. • Added functionality to download Help document instead of including with installation package. • Added End User License Agreement to installation package. • Removed application selection screen on device for Debit transactions. • Updated to include EBT card balance with EBT transaction results. • Removed tap option for EBT transactions.
EdgeExpress Cloud, Bug Fix	• Using both <SUPPRESSUI> and <TIPSUPPORT> parameters causes "Transaction Cancelled" result with US devices.

August 2018	Version 2.3.0
Area	**Description**
	o Fixed error to allow both <SUPPRESSUI> and <TIPSUPPORT> parameters with US devices.

March 2019	Version 2.2.3
Area	**Description**
EdgeExpress Cloud, Enhancement	• Updated root certificate to allow for RCM communication. • Refactored EdgeExpress Cloud to run requests in a thread object with a single-threaded apartment state (STA), allowing COM objects created within EdgeExpress Cloud to be private in their own threads.

June 2018	Version 2.2.2
Area	**Description**

EdgeExpress Cloud, Enhancement	• Reduced transaction-processing time with the following changes:
	   o Reduced approval notification display-time.
	   o Reduced device reset time after gateway responses.
	• Enhanced transaction status response to include PromptingforCard and PromptingForCardRemoval states so partner applications can display prompts.

EdgeExpress Cloud, Bug Fix	• When attempting Alias Create, the Ingenico iUC285 device prompts for "Insert, Swipe, or Tap" when insert is not supported. o Changed the device prompt to "Swipe or Tap."

May 2018	Version 2.2.1
Area	**Description**
EdgeExpress Cloud, Bug Fix	• When attempting a Contactless General Sale Debit Transaction, the cardholder is prompted twice to enter PIN. o Disabled Contactless and Manual Entry for General Sale Debit transactions pending full resolution in future Contactless EMV release.

April 2018	Version 2.2.0
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added support for Ingenico iUC285.

April 2018	Version 2.2.0
	- Leveraged Microsoft functionality to allow for enhanced logging during installation. - Added option to automatically detect connected EMV devices. - Updated API to allow "True" and "False" for the following parameters: - SUPPRESSUI - RECURRING - RECEIPTPRINTTIPLINE - ALLOWDUPLICATES - SUPPRESSUIPROMPTS - PARTIALAPPROVALSUPPORT - CHECKVERIFY - CREATECHECKALIAS - PURCHASECARD - Updated root certificate to allow for gateway communications after updating to Google Chrome release #66.
EdgeExpress Cloud, Bug Fix	- Parameter "SUPPRESSUI" does not function with the iCMP device. - Fixed bug to allow parameter "SUPPRESSUI" to function with the iCMP device.

June 2018	Version 2.1.3
Area	**Description**
EdgeExpress Cloud, Bug Fix	- Processing a Debit transaction using an invalid PIN results in an approval and some EMV PIN Debit transactions are declined incorrectly. - Updated logic to include encrypted PIN data for EMV debit transactions on cards that require Online PIN CVM.

April 2018	Version 2.1.2
Area	**Description**
EdgeExpress Cloud, Bug Fix	- When performing a Debit transaction, a network selection prompt is given on the device. - Fixed error to remove network selection prompt on the device when performing a Debit transaction.

March 2018	Version 2.1.1
Area	**Description**
Remote Client Manager, Enhancement	• Added EMV PIN Debit Purchase support on Ingenico iPP320, iSC250, iSC480 and iCMP.
EdgeExpress Cloud, Enhancement	• Debit (Sale, Return), EBT (Sale, Return, Voucher Clear), and Check (Sale, Credit, Verification) transactions now support the ORDERID parameter for tracking transactions and processing follow-on transactions. • In the case of fallback procedure from Current Phone Home Server to Legacy Phone Home Server, added support for TLS 1.2 and a restricted cipher suite.
Remote Client Manager, Bug Fix	• GETRCMCURRENTUSERPORT is not working due to files not being registered when installing the RCM. (TRIAGE-560) o Updated installation to register COM libraries.
EdgeExpress Cloud, Bug Fix	• When submitting to EdgeExpress Cloud and another transaction is already running, no <RESULT> tag is returned. o Added "Another transaction is already in process" <RESULT> tag when another transaction is already running.

March 2018	Version 2.0.6
Area	**Description**
Remote Client Manager, Enhancement	• Updated root certificate to allow for gateway communications after updating to Google Chrome release #66.

January 2018	Version 2.0.5
Area	**Description**
EdgeExpress Cloud, Enhancement	• Updated OpenEdge Updater.

December 2017	Version 2.0.3
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added support for TLS 1.2 and Ciphers.

October 2017	Version 2.0.2
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added new DISABLEDEVICEMANUALENTRY parameter that disables the option to manually enter card information through the PINPad Device. • The ORDERID and REFERENCEORDERID parameters have been added for tracking Credit transactions and processing follow-on transactions.

August 2017	Version 2.0.1
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added support for iCMP Bluetooth device. • Added new parameter BATTERYSTATUS to check the battery life on the iCMP device. • Ability to obtain BIN lookup with an alias.

EdgeExpress Cloud, Bug Fix	• Transaction Builder does not have IIAS/FSA parameters.
	    o Updated Transaction Builder to include IIAS/FSA parameters
	• CREDIT_DEBIT_CARD selection is not suppressed when OpenEdge Host Pay submits suppress_rcm_window=true.
	    o Added SUPPRESSUIPROMPTS parameter.

April 2017	Version 1.18
Area	**Description**
EdgeExpress Cloud, Enhancement	• Added support for Check Sale, Credit, Verification and Alias processing. • Added support for EBT processing. • Added support for FSA, HSA, and IIAS processing. • Added functionality to specify XML return format. • Transaction Builder, JavaScript, and ASP.NET sample code now includes XML responses in addition to JSON responses. • Added support for AVS and CV Results.
Remote Client Manager, Bug Fix	• Inserting a chip card before the transaction launches freezes RCM. (SF#023351) o Updated code to allow chip card to be removed after prompting to remove card without RCM freezing.

March 2017	Version 1.16
Area	**Description**
Remote Client Manager, Enhancement	• When a dynamic port is selected, RCM selects the next available port each time the RCM is restarted. • XpressLink2 logs are enhanced to include the product name, product version, integration entry point, and operating system. (SF#023107) • RCM now prompts to retry the card swipe or EMV insert if the initial card read was unsuccessful.

Remote Client Manager, Bug Fix	• CreditReturn transactions decline if TransactionID is passed in the same request with DeviceType=EMV. (SF#023228)
	    ○ Updated code to accept CreditReturn transactions with TransactionID and DeviceType=EMV.
	 • Exception error occurs after the prompt to update PIN Pad portion of an RCM 1.14 installation on Windows 7 Pro 64-bit. (SF#023246)
	    ○ Implemented a backup alternative method of port and certificate binding if the initial method fails to eliminate the exception error.
	 • Unable to perform an AliasCreate transaction with HPF when ZipCode or Address is passed with DeviceType=EMV. (SF#023240)
	    ○ Updated code to accept AliasCreate HPF transactions when ZipCode or Address is sent with DeviceType=EMV.
	 • ISC250 PIN Pad randomly gets stuck on "Remove Card" prompt after an EMV card has been removed from the device. (SF#023213)
	    ○ Improved EMV Fallback/Chip Error logic.

December 2016	Version 1.15b
Area	**Description**
XpressLink2, Enhancement	• Added ability to lookup the RCM port of the current user using the GETRCMCURRENTUSERPORT transaction type.

November 2016	Version 1.15
Area	**Description**
Remote Client Manager, Enhancement	• The CA Key file update is no longer required to occur during payment processing. The update can be scheduled for a specific time and date to prevent business disruption. • RCM is enabled to accept a script from the payment form that can set up or change device configurations. Changes to the default PIN Pad message will take effect the next time RCM communicates with the PIN Pad. (SF#023125) • "Amount OK" screen is removed from the PIN Pad devices to optimize transaction process. The transaction amount displays on the PIN Pad screen when the user is asked to insert the card. • RCM is enabled to accept a cancelation request from the payment form. (SF#023176) • RCM returns CARDHOLDERNAME for EMV Transactions. (SF#023160) • EMV device configuration refreshes with every RCM installation.

Remote Client Manager, Bug Fix	• "Parsing Error: Whitespace embedded in open tag" message displays on random Canadian EMV transactions. (SF#023179)
	    ○ Updated code to prevent empty XML elements from being sent to the gateway.
	• If attempting to swipe a chip card on an EMV transaction, an incorrect error message "Closing" appears. (SF#023177)
	    ○ Updated the message text to "Cancel".
	• "Declined by Device – Reason Code 4002" message displays on random EMV transactions in an RDP environment. (SF#023198)
	    ○ Updated logic to properly handle null messages received from the device communication layer.
	• Device update is forced on the first transaction after installation of 1.15, if the maximum amount of update postponements was met on the previous version before the upgrade.
	    ○ Implemented a reset of all device prompt values during installation of 1.15.

July 2016	Version 1.14
Area	**Description**
Remote Client Manager, Enhancement	• When using OpenEdge Host Pay, card holder names are now returned on EMV transactions with QUERY_PAYMENT. • The OpenEdge Updater application will now be installed with RCM, which will update itself silently, and alert the user of an available update for RCM.

July 2016	Version 1.14
Area	**Description**

Remote Client Manager, Bug Fix	• Device update feature fails for the iSC250 over a Remote Desktop connection. (SF# 023074)
	     ○ Device update feature works properly for iSC250 over a Remote Desktop Connection.
	 • HR Result error "Specified logon session does not exist. It may already been terminated." occurs during RCM installation. (SF# 023101)
	     ○ Removed error message that occurs during RCM installation.
	 • POS Sequence Numbers are not shared between Windows users. (SF#023023)
	     ○ POS Sequence Numbers can be shared between Windows users.
	 • Invalid ZIP Code error occurs on EMV transactions when the ZIP code contains the hyphen symbol. (SF#023087)
	     ○ Hyphen symbol can be sent with ZIP codes on EMV transactions without an error being returned.
	 • Error message "Connecting Remote Client Manager Timeout" appears after installing RCM.
	     ○ Updated RCM certificate when using InstallShield.

April 2016	Version 1.13
Area	**Description**
PINPad, Bug Fix	• The ISC250 briefly showed the idle screen before asking for a signature. • Canadian IPP320 was not able to have settings loaded to it. • Added keyboard focus to the signature accept window. • RBA update occasionally failed. • RBA update displayed an error when Dynapro SC was configured. • Occasionally unable to test PINPad devices.
EMV Cards, Bug Fix	• MasterCard transactions were being declined. • Canadian Return transactions froze on "Please Wait". • Canadian Debit transactions are inconsistently reversed after receiving error "Transaction Result Declined by Device".

April 2016	Version 1.13
Area	**Description**
Remote Client Manager, Enhancement	- Created function to alert the RCM user that a duplicate card has been detected within their Point of Sale. - Added function to allow Xpresslink2 to send the status update message directly to OEHP. - Added function to alert user that the incorrect device was configured at the configuration screen. - Added feature to apply settings to all users. - During the installation the Firefox setup instructions randomly appeared behind the RCM install progress window. - Application is auto starting without showing the icon in the system tray. - Added function to install the current CA key with RCM. - Improved serial device communication layer. - Changed the Incorrect Device Selected message to appear when the device is first selected. - COM port would increase after each upgrade.

April 2016	Version 1.13
Area	**Description**
Remote Client Manager, Bug Fix	• RCM would fail when you "Switch Users" on Windows, rather than completely logging off, and back into Windows as a different user. • After confirming Duplicate Checking Prompt, an error would occur. • An error would occur when special characters were sent from the address field. • A security alert message would pop up on every first transaction after RCM is initiated. • Eliminated reboot prompt each time computer restarts. • Tab order is incorrect after loading forms to a device. • An error occurred if CountryCode 840 was not sent with transaction. • Improved serial device communication layer. • Device Configure window quickly appeared, then disappeared. • iSC250 did not have biometric abilities. • Application did not prompt for signature when using OpenEdge Host Pay. • Icon in the task bar for the card validation window is missing. • Swiped card transactions are prompting for signature when not necessary. • Error displayed during RSA key generation. • Duplicate Card Validation window is appearing behind the browser screen on Windows 8.1. • RCM window still appears when it is supposed to be suppressed. • Slideshow test did not cycle through every image. • Application crashed upon a transaction attempt when using Win Server Standard 2008/R2. • Upon the exit of the PINPad Device configure window, "Incorrect Device Selected" error message displayed, and the application froze. • An error displayed when trying to update the CAkey.

February 2016	Version 1.12a
Area	**Description**
Remote Client Manager, Enhancement	• Added setting to apply the PIN Pad configuration to all Windows users.
EMV Cards, Bug Fix	• Fixed issue causing an error if CountryCode 840 is not sent with transaction.

January 2016	Version 1.12
Area	**Description**
Remote Client Manager, Enhancement	• Added the option to configure the port that the RCM listens on for each user.

January 2016	Version 1.12
Area	**Description**
Remote Client Manager, Bug Fix	• Fixed issue causing the Duplicate Card Check window to not gain focus when opening.
Installation, Enhancement	• The RCM installation now no longer creates a desktop shortcut, and instead puts a Start menu shortcut under the "OpenEdge" folder. • During the RCM installation, if the user's account is detected to not be an Administrator, a message displays instructing the user to install the program as an administrator. • During an upgrade of the RCM from a previous version, if a configured PINPad Device has an update available, the installer will attempt to automatically update the device.
Installation, Bug Fix	• Fixed issue causing the RCM installation to fail due to a previously installed version of the RCM or XCharge that was locking the Hosts file.
PINPad, Enhancement	• Updated Ingenico devices to use RBA 15.04 for EMV transactions.
Documentation, Enhancement	• Added the "RCM Setup - Port Configure" section. • Added note that the "Default Message" must be 30 characters or less.

November 2015	Version 1.11
Area	**Description**
EMV Cards, Bug Fix	• Fixed issue causing some EMV transactions to be voided due to a Credit Update failing.

November 2015	Version 1.10
Area	**Description**
Remote Client Manager, Enhancement	• Updated the RCM to use a fully qualified domain name in order to support Google Chrome 45 and Microsoft Edge. • The RCM now allows multiple users in a Terminal Server environment to use the same instance of the RCM. • Added the ability to use one EMV device for multiple processing accounts. • Added a duplicate card check and warning message to validate the final four digits of the card to be processed.

November 2015	Version 1.10
Area	**Description**
Remote Client Manager, Bug Fix	• Rebranded the "Security Update" window with the title of "OpenEdge EMV". • Fixed an issue causing automatic updates from the Phone Home Server to not download and start. • Void transactions no longer fail to process.
Installation, Bug Fix	• When updating the RCM from a previous version, the desktop shortcuts are no longer removed.
Security, Enhancement	• Updated the RCM to only communicate using TLS 1.2.
EMV Cards, Bug Fix	• Offline Force EMV transactions no longer fail when prompting for a signature. • Interac Application Identifiers (AID) are no longer used on US EMV transactions. • Issues affecting certain Wells Fargo EMV cards to decline were resolved by updating the PINPad RBA version.
PINPad, Enhancement	• Updated Ingenico devices to use RBA 14.06 for EMV transactions. • EMV transactions no longer request a signature when the prompt signature is set to false by the integrator.
PINPad, Bug Fix	• Fixed issue causing PINPad devices to not initialize if a different device had been previously configured in the Device Setup.
Documentation, Enhancement	• Added the "Installing the RCM" section.

September 2015	Version 1.09
Area	**Description**
Remote Client Manager, Enhancement	• Added the RCM Help and Release Notes to the RCM menu. • Debit Sale transactions will no longer prompt to process using an EMV chip.
Remote Client Manager, Bug Fix	• Fixed issue causing an "Approval" message to display on OpenEdge payment forms on reversed transactions.
EMV Cards, Enhancement	• Added support for the Ingenico iSC480 PIN Pad for Global US EMV processing.
PINPad, Enhancement	• Added support for the Ingenico iSC480 device.
PINPad, Bug Fix	• Fixed issue causing HSM errors on Ingenico devices due to KSID padding.

July 2015	Version 1.08
Area	**Description**
Remote Client Manager, Enhancement	• Added an "About" menu to the RCM system tray icon. • Updated the RCM logo and branding. • Added "Firefox Instructions" menu to the RCM system tray icon.
Installation, Enhancement	• During installation, the RCM handles security and certificate generation, making the RCM not need to be started as an administrator after each restart. • Added instructions to the installation on configuring Firefox for use with the RCM. • Added functionality to remove previously used certificates that have been replaced.
Installation, Bug Fix	• Fixed issue causing the RCM installation to fail on Windows 8.1 when editing the Host file. • Updated the URL used to direct users to install .NET 4.5 if not installed.
Credit Cards, Enhancement	• Added support for FSA (Flexible Spending Account) cards.
EBT Cards, Enhancement	• Added support for EBT transaction types.
PINPad, Bug Fix	• Fixed issue causing MagTek devices to stop responding after going into sleep mode.
Documentation, Enhancement	• Added "RCM Process Flow" and "System Requirements" sections. • Added "Appendix A - Using the RCM with Firefox".

May 2015	Version 1.07
Area	**Description**
EMV Cards, Enhancement	• Added support for EMV processing (Europay MasterCard Visa, also referred to as "Chip and PIN" or "chip cards") for Global US merchants through the Ingenico iPP320 and iSC250.
Credit Cards, Enhancement	• Added support for zero dollar authorizations.

April 2015	Version 1.06
Area	**Description**
Credit Cards, Enhancement	• Added support for encrypted swipe transactions.
PINPad, Enhancement	• Added functionality to check for and download updated RBA (Retail Base Application) files for Ingenico PIN Pad devices. • Updated the devices drop down menu with all available devices.
PINPad, Bug Fix	• Fixed issue causing keyed transactions on the Ingenico iSC250 to process slowly. • Fixed issue allowing Debit cards to be manually keyed on Ingenico iPP320 devices.

2015	Version 1.0
Area	**Description**
Remote Client Manager	• Initial Release.