# Using EMV Devices with Shift4 Payments

This document is intended for merchants who have EMV-capable payment devices that have already been configured in the Universal Transaction Gateway® (UTG®) TuneUp. The document outlines the steps needed to enable EMV (after all software and processor updates have been completed).

## *Basic Steps to Use EMV Payment Devices with Shift4 Payments*

**Note:** The following prerequisites must be met before proceeding with the steps listed below:

- Update UTG to the current version.
- Update payment device applications to the current version.
- Update the forms to the current version.

For more information, contact the Shift4 Payments Customer Support team at 702.597.2480, option 2.

### 1. Verify each installed UTG is running the most current version available.

- Our EMV certifications require the current UTG version. Shift4 Payments frequently updates the UTG by adding features and enhancements to improve functionality. You should always try and keep your UTG current. The current version is available at: https://myportal.shift4.com/downloads/utg2setup.exe.

### 2. Verify your Ingenico and Verifone® devices are running the latest firmware.

- It is recommended that you update to the latest application version available for your devices. However, if your devices are not running the firmware versions listed below, you will need to download and push the update to your devices because they are the minimum EMV supported versions. See the *Ingenico Telium Devices RBA Versions Supported and Known Issues* section of the *Using EMV External Devices* guide in MyPortal for more information.
    - If you are using Ingenico Telium devices, they should be as follows:
        - P2PE-enabled
        - RBA version 16.0.2 or higher
    - If you are using Verifone devices, they should be as follows:
        - P2PE-enabled
        - FormAgent version 4.4.1 or higher
        - XPI version 5200p or higher
        - OS version 30145200 or higher for Verifone PCI 3 or PCI 4 devices (unless you are using a serial cable)

**Note:** For a complete list of supported RBA versions for each Shift4 Payments supported device, see the *Ingenico Telium Devices RBA Versions Supported and Known Issues* section of the *Using EMV External Devices* guide in MyPortal.

### 3. Locate and record the API Terminal ID information for each EMV payment device.

**Important:** The API Terminal ID is a value consisting of 1-32 alphanumeric characters. It is specific to each PIN pad, and it is specified by the merchant or point-of-sale (POS) or property management system (PMS) provider. Shift4 Payments suggests a naming convention that keeps the API Terminal ID unique across the merchant's entire enterprise. (For example, 70211 where 702 is the store number and 11 is the lane number where the PIN pad is stationed for use.) The API Terminal ID must be set in the POS/PMS, UTG, and Lighthouse Transaction Manager. The value must match so that those systems can identify the PIN pad being used during the transaction.

- Stop the UTG if it is running as a service, and start the UTG in Standalone mode.
- From the menu, select **Tune Up**.
- Click the **Devices** tab and then click the desired payment device to highlight it. Click **View** under the Device section.
- In the API Terminal ID field, record the API Terminal ID number for the payment device configured.
- If you have multiple EMV devices configured on the Universal Transaction Gateway TuneUp screen, repeat the above steps for all EMV devices.
- Close TuneUp.
- *(If applicable)* Stop UTG Standalone and start the UTG as a service.

**Note:** This information should also be available in the configuration settings of your PMS/POS interface.

**Note:** If you have unique API Terminal IDs, then locating and recording the device serial numbers can be optional.

## 4. Locate and record the Device Serial Number for each payment device configured in UTG TuneUp.

- If your API Terminal IDs are not unique, then the device serial number must be recorded and entered in Lighthouse Transaction Manager.
- Locate and record the Device Serial Number for each EMV payment device.
    - For Ingenico Telium RBA devices, locate the last eight digits of the serial number displayed on the back of the device. See the example below:

- For Verifone MX devices, locate the last nine digits of the serial number (without the dashes) displayed on the back of the device. See the example below:


**Note:** If the labels are not readable, the serial number can be obtained from the device screens. See the *Using EMV External Devices* guide in Lighthouse Transaction Manager Help for directions. If you are using an Ingenico Telium RBA device, look in the *Locating the Ingenico Telium RBA Device Serial Number for Lighthouse Transaction Manager* section. If you are using a Verifone MX device, look in the *Locating the Verifone MX P2PE Device Serial Number for Lighthouse Transaction Manager* section.

## 5. Configure the EMV payment devices in Lighthouse Transaction Manager.

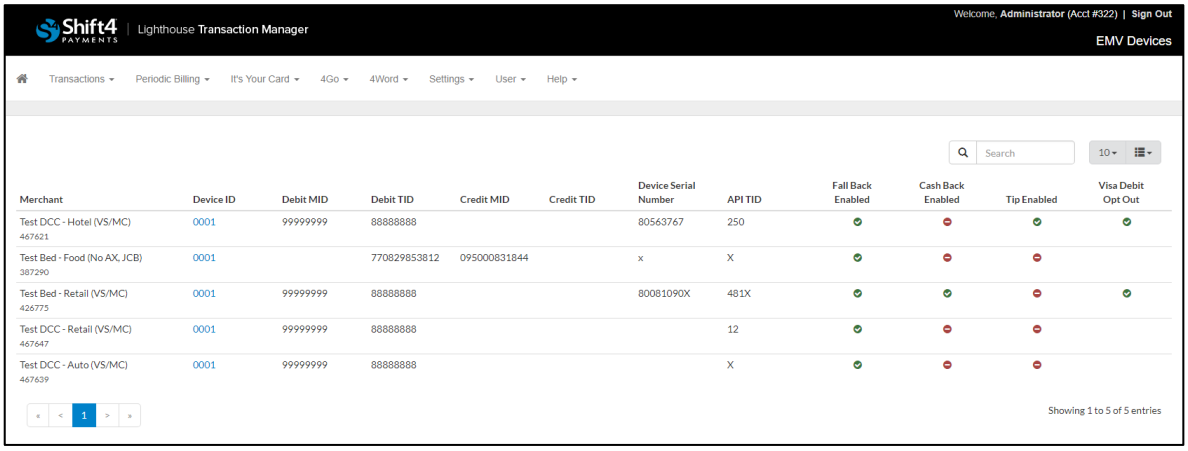
- Log in to Lighthouse Transaction Manager as the Account Administrator and complete the following steps:
  - From the menu, select **Settings > EMV Devices**. By default, the devices are grouped by Merchant Name.

- Under Device ID, click the ID number of the device you would like to configure.

---

**TIP:** You can use the search feature, or one of the column sort options to locate the desired device.

---




---

**Important:** Clicking Reset to Default Settings returns certain EMV device settings, such as Default Tdol, to the default settings. Other settings, such as the EMV Terminal Settings are not affected. It is always advisable to write down the current settings before making changes to be certain you can get back to the previous state if needed.

---

- In the General Settings section, complete the following steps:
  - In the API Terminal field, enter the API Terminal ID that you recorded earlier in the process.

- *(If applicable)* In the Device Serial (Optional) field, enter the serial number that you recorded earlier in the process. (This allows the UTG to validate that the API Terminal ID and device serial number match when downloading any settings configured in Lighthouse Transaction Manager.)


- (*If applicable*) In the EMV Terminal Settings section, select the desired options:
  - **Visa Debit Opt Out** – If selected, Visa debit cards will not be processed through the Visa Debit/Credit AID (A0000000031010). However, they could be processed through other supported AIDs. For additional information, see the *Visa Debit Opt Out Explained* section.

---

**WARNING!** If you enable the Visa Debit Opt Out option, there may be some Visa debit cards that you will not be able to process because there isn't a common AID between the terminal and card. See the *Visa Debit Opt Out Explained* section for more information.

---

  - **Enable Fall Back** – If selected, when the EMV chip card fails, transactions can be processed by swiping the payment card.

---

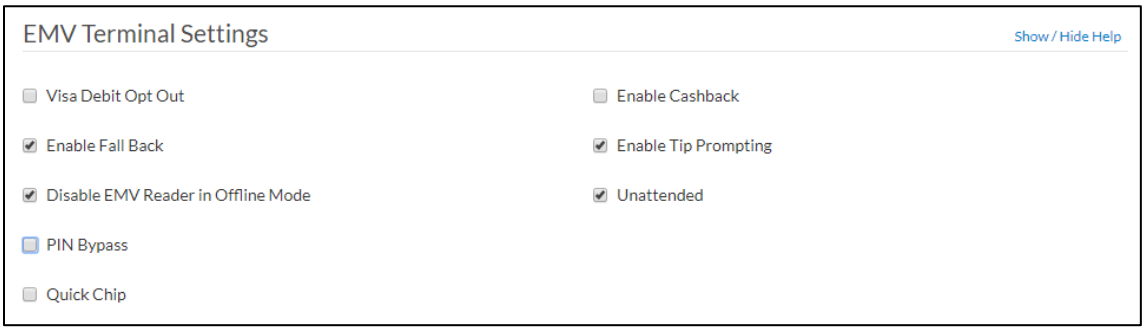
**WARNING!** Selecting Enable Fall Back may affect liability. An alternative would be to ask for another form of payment.

---

  - **Disable EMV Reader in Offline Mode** – If selected, transactions can be processed in offline mode. This allows the payment card to be processed by swiping, tapping, and/or manually entering the number instead of inserting the payment card.
  - **Prefer US Common Debit** – Typically, Visa debit cards support two applications: Global Debit Application ID (labeled VISA DEBIT) and US Common Debit AID (labeled US DEBIT). If selected (and if the card supports the AID and the device is in the United States), the device will automatically process transactions through US

DEBIT. If cleared, the cardholder will have to choose VISA DEBIT or US DEBIT on the device. The latter can be confusing to cardholders, so you may want to keep Prefer US Common Debit selected.

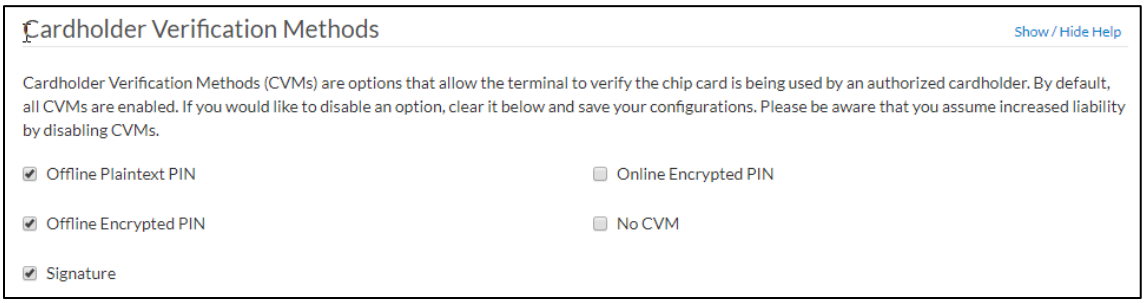
- **Quick Chip** – If selected, the cardholder can remove their card sooner (before the authorization response is received on the device). In addition, the cardholder can insert their card sooner (similar to swipe ahead on non-EMV transactions).
- **Enable Cashback** (Canadian merchants only) – If selected, the device is enabled to prompt for cashback, but you will not be able to enable tip prompting. If cashback is configured differently in the UTG, then the UTG setting will prevail.
- **Enable Tip Prompting** (Canadian merchants only) – If selected, the device is enabled to prompt for tips, but you will not be able to enable cashback. If enable tip is configured differently in the UTG, then the UTG setting will prevail.
- **Unattended** – If selected, your device is configured as being unattended. (If your device is unattended, like a parking garage kiosk or a service station, select this option to properly configure it. For a complete list of supported devices, see www.shift4.com/thirdpartydevices.)
- **PIN Bypass:** If selected, this option will allow the cardholder to bypass entering their PIN on EMV transactions. This option can be used if the merchant is having issues with cardholders not remembering their PIN, or if the merchant wants to allow cardholders to choose not to enter a PIN for any reason. However, there are liability shift implications to enabling this option if the issuer has provided the card a higher level of EMV authentication by enabling PIN. If the merchant allows the cardholder to bypass entering their PIN, then the fraud liability might shift back to the merchant. Selecting this setting can open up a security hole where someone that has stolen another person's card can now easily use the card by bypassing the PIN entry screen. PIN codes are specifically used to prevent lost/stolen card fraud because the card would not be usable unless the unauthorized user also had the cardholder's PIN. Therefore, selecting this option is not recommended by Shift4 Payments.




- (*If applicable*) In the Cardholder Verification Methods section, select or clear the desired options:

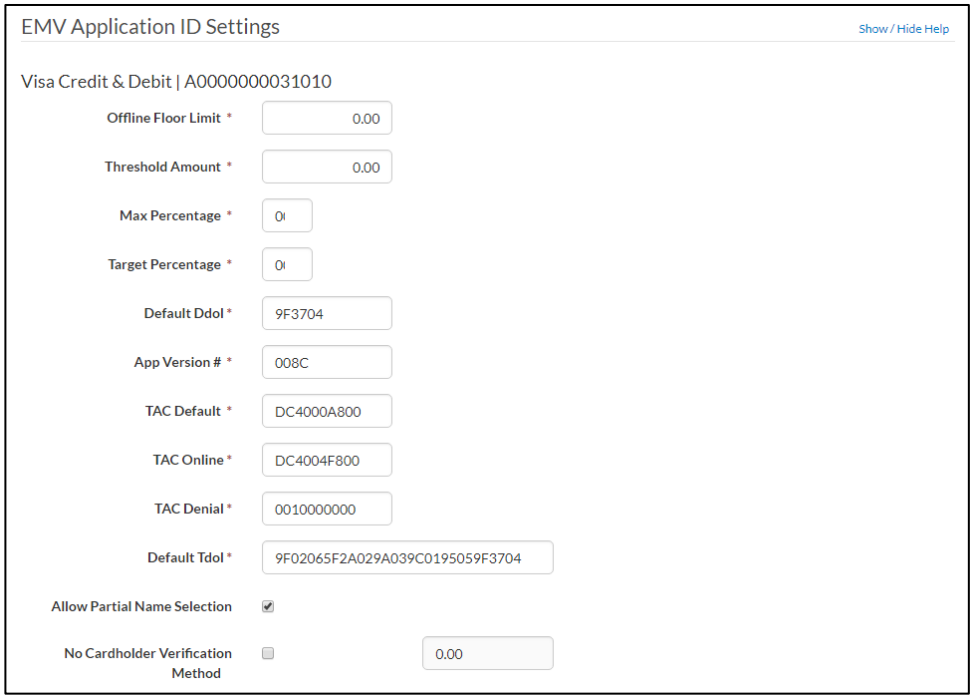
**WARNING!** Changes made in this section may affect EMV liability. If you are unsure of a setting, contact the Shift4 Payments Customer Support team at 702.597.2480, option 2 for further guidance.

- **Offline Plaintext PIN** – A cardholder verification method in which the customer's PIN is entered on the PIN pad and sent unencrypted (in plaintext) to the chip card for verification.
- **Offline Encrypted PIN** – A cardholder verification method in which the customer's PIN is entered on the PIN pad and sent encrypted to the chip card for verification.
- **Signature** – A cardholder verification method in which the customer's signature is signed on the PIN pad. (If the transaction is deemed fraudulent, the signature can be compared to the signature on file with the card issuer.)
- **Online Encrypted PIN** – A cardholder verification method in which the customer's PIN is entered on the PIN pad and sent encrypted to the card issuer for verification.
- **No CVM** – A cardholder verification method in which no cardholder information is required to verify the chip card is being used by an authorized cardholder.




  - Configure EMV Application ID Settings if needed.
- *(If applicable)* In the EMV Application ID Settings section, configure the desired settings for the appropriate application. For most of the settings, you should check with your processor before changing. Two common settings are as follows:
  - Allow Partial Name Selection – Setting this flag allows the payment device to include application IDs that partially match rather than being a full match when building a list of mutually supported applications with the card.

- No Cardholder Verification Method – To not perform a Cardholder Verification Method (CVM), select the option and enter an amount in the field. When the transaction is less than or equal to the amount, a CVM will not be performed (if the card supports not performing a CVM as well). When the field is cleared, a CVM will be performed no matter the amount.




**Tip:** For additional information, click the Show/Hide Help link to the right of each section header. For more information, see the *Account Administrator Guide* in the Lighthouse Transaction Manager Help section.

- When you have configured your EMV Application ID Settings, complete one of the following steps:

  - Click **Save** to save your configuration settings for the current device.
  - Click **Save and Next** to save your configuration settings for the current device and load the next device under the current MID for configuration.

## 6. Configure the Source Serial in the Devices tab in UTG TuneUp.

- In the Source Serial field, enter the account number under which the device is configured in Lighthouse Transaction Manager.
- *(Optional)* Update the EMV Device Configuration Settings in the UTG Standalone if you would like the settings to be reflected immediately. Since the UTG automatically downloads the EMV

Device Configuration Settings every hour (as needed), you may wish to forgo this step. However, if you want to immediately and manually download the updated settings for an EMV device that has already been configured successfully in Lighthouse Transaction Manager and UTG TuneUp, complete the following steps:

- Right-click in the UTG Task Explorer window, and then click **Device Maintenance**.
- In the Device Maintenance window, select the terminal(s) you want to download, and then click **Download Now**.

## 7. Processing EMV Transactions

- At this point, if you have completed the steps listed above along with the prerequisites, you should be able to process EMV transactions. Run a test transaction via your POS/PMS system and ensure that you are able to process the transaction by inserting an EMV card.

**Important:** If you are unable to process EMV transactions after downloading EMV Device Configuration updates, verify the serial number configured in the UTG matches the account number under which the device is configured in Lighthouse Transaction Manager.

# Appendix A: Visa Debit Opt Out Explained

Be prepared because this gets a little confusing…

When an EMV card is inserted into a payment device, the device and card look for common Application Identifiers (AIDs), and they select one or prompt the cardholder to select one.

When Visa implemented EMV, they decided to put both debit and credit on the same AID, called Visa Debit/Credit AID (A0000000031010), which is intended to process Visa debit cards through the Visa debit network. The result was that you could process Visa credit and Visa debit, or neither. This wasn't ideal, so Visa provided the Visa Debit Opt Out option, which allows a merchant to opt out of processing Visa debit cards through the Visa Debit/Credit AID, while still allowing Visa credit cards to process through it. For example, in Canada, this option allowed Visa credit cards to be processed through the Visa Debit/Credit AID and Visa debit cards to be processed through the INTERAC Debit AID.

In addition, Visa developed the Visa Common Debit AID, which is intended to provide a choice of debit networks. So, if you select Visa Debit Opt Out, you may still be able to process Visa debit cards because they may be processed through the Visa Common Debit AID.

To put it simply, if you enable this option, there may be some Visa debit cards that you will not be able to process because there isn't a common AID between the payment device and card.

Below are two examples:

**Example One**: A Canadian merchant who wants to accept Visa credit cards but process all debit cards through INTERAC may want to select Visa Debit Opt Out.

To achieve this, the merchant can take the following steps:

- The merchant verifies their payment devices support the Visa Debit/Credit AID and the INTERAC Debit AID.
- In Lighthouse Transaction Manager, the merchant selects Visa Debit Opt Out for their payment devices.
- Any debit transactions will use the INTERAC Debit AID, as long as no other debit AIDs are supported on the payment devices.

**Example Two**: A United States merchant who wants to accept Visa debit cards but process them through the Visa Common Debit AID may want to select Visa Debit Opt Out.

To achieve this, the merchant can take the following steps:

- The merchant verifies their payment devices support the Visa Common Debit AID.
- In Lighthouse Transaction Manager, the merchant selects Visa Debit Opt Out for their payment devices.
- Visa debit cards will be processed through the Visa Common Debit AID.