4Go®

Technical Installation Guide

Shift4® PAYMENTS

Copyright Notice

Shift4 Payments
1491 Center Crossing Road
Las Vegas, NV 89144
702.597.2480

www.shift4.com | info@shift4.com
Document Title: 4Go® Technical Installation Guide
Publication Date: 01/14/2019

Using the 4Go Technical Installation Guide

The *4Go Technical Installation Guide* provides detailed information on configuring Shift4 Payments' Universal Transaction Gateway® (UTG®) and Lighthouse Transaction Manager, followed by installing and configuring 4Go®.

It is important to note that this document was created using the Windows XP operating system – if a different Windows operating system is in use, screen shots and path directories may vary.

Security and 4Go

To ensure 4Go is installed, configured, and securely operated in an environment that is compliant with Payment Card Industry Data Security Standard (PCI DSS) standards, you must read the following documents:

- *4Go PA-DSS Implementation Guide*
- *4Go Technical Installation Guide*
- *4Go Reference Guide*
- The latest version of the PCI DSS documentation at www.pcisecuritystandards.org

WARNING! For security implementation and best practices, see the *4Go PA-DSS Implementation Guide*.

Use of a Payment Application Data Security Standard (PA-DSS) compliant application by itself does not make an entity PCI DSS compliant since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS implementation guide provided by the payment application vendor.

All applications that store, process, or transmit cardholder data (CHD) are in scope for an entity's PCI DSS assessment, including applications that have been validated to PA-DSS. The PCI DSS assessment should verify the PA-DSS validated payment application is properly configured and securely implemented per PCI DSS requirements and the vendor's PA-DSS implementation guide. If the payment application has undergone any customization, a more in-depth review will be required during the PCI DSS assessment, as the application may no longer be representative of the version that was validated to PA-DSS.

The PA-DSS requirements are derived from the *PCI DSS Requirements and Security Assessment Procedures*. The PA-DSS details the requirements a payment application must meet in order to facilitate a customer's PCI DSS compliance. As security threats are constantly evolving, applications that are no longer supported by the vendor (e.g., identified by the vendor as "end of life") may not offer the same level of security as supported versions.

Prior to Installation and Configuration Checklist

Use this checklist prior to installing and configuring any Shift4 Payments products for use with 4Go to ensure the following requirements are met:

- ☐ Certification and testing of the interface must be completed with Shift4 Payments.
- ☐ The most current UTG must be installed.
- ☐ Account Administrator access in Lighthouse Transaction Manager is required.
- ☐ Any device that will be running 4Go must use a 32-bit or 64-bit Windows operating system:
  - Microsoft® Windows Vista
  - Microsoft® Windows 7
  - Microsoft® Windows 8
  - Microsoft® Windows 2012
- ☐ Access to the Windows operating system must be by a Windows administrator account (if available) during the installation and configuration of 4Go. Once complete, 4Go must be run from a Windows account with minimal privileges to comply with PCI DSS and PA-DSS requirements and guidelines.

Installation and Configuration Checklist

Print and use this checklist throughout the installation and configuration process to ensure the UTG, Lighthouse Transaction Manager, and 4Go are properly installed and configured. Contact Shift4 Payments' Installations team with any questions at 702.597.2480, option 4.

1. Reviewing the UTG Installation Method

   ☐ UTG Installation Method 1 – A UTG Installed on Each Terminal

   ☐ UTG Installation Method 2 – A UTG Installed on the Server

   ☐ UTG Installation Method 3 – A UTG Installed on a Terminal

2. Configuring the UTG to Communicate

   ☐ *(If applicable)* TCP/IP – Configuring the UTG to Communicate with the POS/PMS and 4Go

   ☐ *(If applicable)* HTTP – Configuring the UTG to Communicate with the POS/PMS and 4Go

   ☐ Enabling 4Go in the UTG

3. Configuring 4Go Settings in Lighthouse Transaction Manager

   ☐ Configuring Terminal Settings

   ☐ Configuring Bin Ranges

4. Installing and Configuring 4Go

   ☐ Installing 4Go

   ☐ Configuring 4Go to Communicate with the UTG

5. Post-Installation Process

   ☐ Verifying File Placement

   ☐ Verifying the 4Go Invocation Methods

   ☐ Processing a Test Transaction

Reviewing the UTG Installation Method

The three most common UTG installation methods are reviewed in the following three sections:

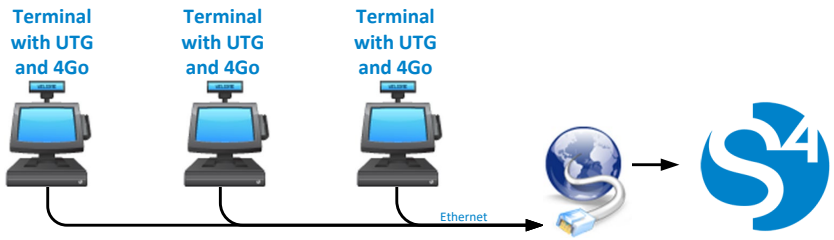
- *UTG Installation Method 1 – A UTG Installed on Each Terminal*
- *UTG Installation Method 2 – A UTG Installed on the Server*
- *UTG Installation Method 3 – A UTG Installed on a Terminal*

Before proceeding, the POS/PMS communication method with the UTG (either TCP/IP or HTTP) must be determined as it will affect the manner in which the UTG is configured to communicate with the POS/PMS and 4Go.

When the POS/PMS communication method with the UTG has been determined, review the section that corresponds to how your UTG was installed.

UTG Installation Method 1 – A UTG Installed on Each Terminal

The first most common and preferred UTG installation method is to install a UTG on each POS/PMS terminal.

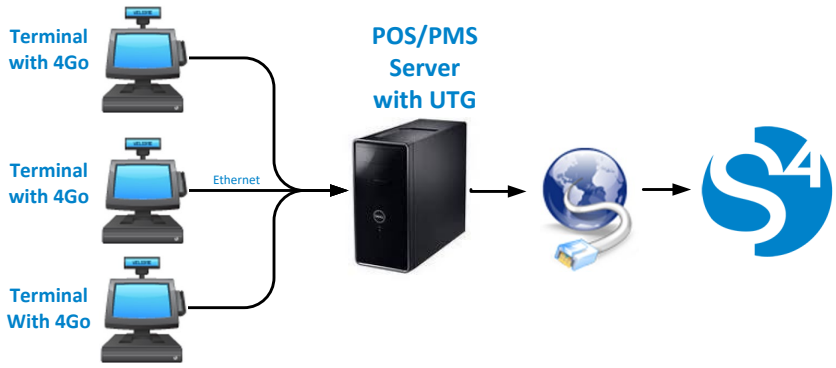


If this is how your UTG was installed, depending on your POS/PMS communication method with the UTG, you will be required to complete the following in each UTG.

POS/PMS Communicates with UTG via TCP/IP	POS/PMS Communicates with UTG via HTTP
1) Add one TCP/IP interface.	1) Add one HTTP interface.
2) Add the terminal the UTG is installed on as a client of the TCP/IP interface with an interface type of 4Go and Secure POS.	2) Add the terminal the UTG is installed on as a client of the HTTP interface with an interface type of Secure POS Only.
3) Enable 4Go.	3) Add one TCP/IP interface.
	4) Add the terminal the UTG is installed on as a client of the TCP/IP interface with an interface type of 4Go.
	5) Enable 4Go.

UTG Installation Method 2 – A UTG Installed on the Server

The second most common UTG installation method is to install a UTG on the POS/PMS server.



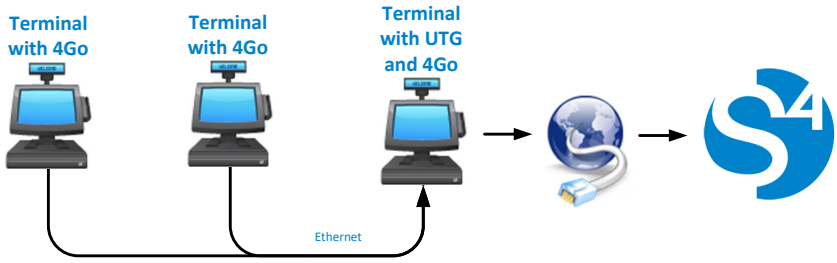
If this is how your UTG was installed, depending on your POS/PMS communication method with the UTG, you will be required to complete the following in the UTG.

POS/PMS Communicates with UTG via TCP/IP	POS/PMS Communicates with UTG via HTTP
1) Add one TCP/IP interface.	1) Add one HTTP interface.
2) Add or import all terminals as clients of the TCP/IP interface with an interface type of 4Go and Secure POS.	2) Add the POS/PMS server as a client of the HTTP interface with an interface type of Secure POS Only.
3) Enable 4Go.	3) Add one TCP/IP interface.
	4) Add or import all terminals as clients of the TCP/IP interface with an interface type of 4Go.
	5) Enable 4Go.

Important: The POS/PMS server sends the authorization requests to the UTG with this installation method.

UTG Installation Method 3 – A UTG Installed on a Terminal

The third most common UTG installation method is to install a UTG on one of the POS/PMS terminals.



If this is how your UTG was installed, depending on your POS/PMS communication method with the UTG, you will be required to complete the following in the UTG.

POS/PMS Communicates with UTG via TCP/IP	POS/PMS Communicates with UTG via HTTP
1) Add one TCP/IP interface.	1) Add one HTTP interface.
2) Add or import all terminals as clients of the TCP/IP interface with an interface type of 4Go and Secure POS.	2) Add or import all terminals as clients of the HTTP interface with an interface type of Secure POS Only.
3) Enable 4Go.	3) Add one TCP/IP interface.
	4) Add or import all terminals as clients of the TCP/IP interface with an interface type of 4Go.
	5) Enable 4Go.

Configuring the UTG to Communicate

Prior to installing and configuring 4Go, you must ensure the following:

- UTG is not running
- Add and configure the interface(s) in the UTG to communicate with the POS/PMS and 4Go
- Enable 4Go in the UTG
- Restart the UTG

If your POS/PMS communication method with the UTG is TCP/IP, follow the steps in the following two sections:

- *TCP/IP – Configuring the UTG to Communicate with the POS/PMS and 4Go*
- *Enabling 4Go in the UTG*

If your POS/PMS communication method with the UTG is HTTP, follow the steps in the following two sections:

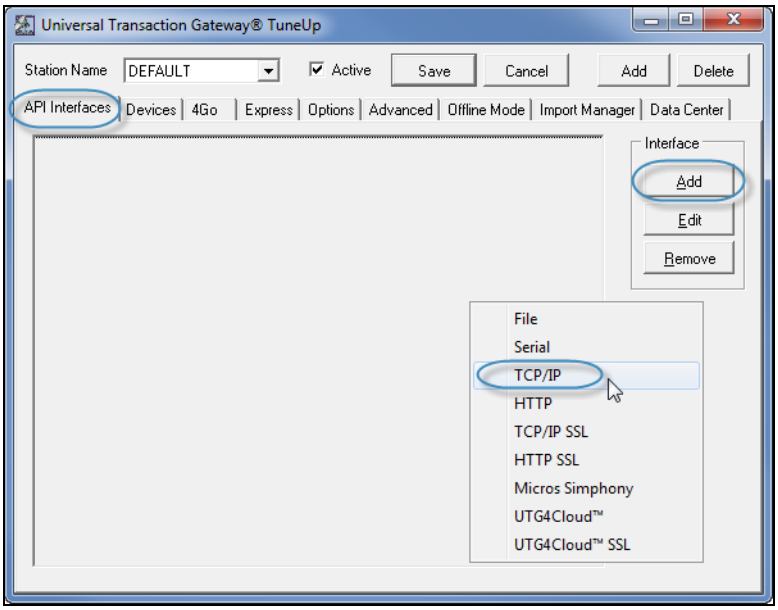
- *HTTP – Configuring the UTG to Communicate with the POS/PMS and 4Go*
- *Enabling 4Go in the UTG*

TCP/IP – Configuring the UTG to Communicate with the POS/PMS and 4Go

To configure the UTG to communicate with the POS/PMS and 4Go, complete the following steps:

1. *(If applicable)* If the UTG is running as a service, stop the service by completing the following steps:
   - From the Start menu, select **Programs > Administrative Tools > Services**.
   - Locate Shift4 UTG(v2), right-click, and select **Stop**.
2. *(If applicable)* If the UTG is running in Stand Alone, close it by completing the following steps:
   - In the UTG Task Explorer window, click  .
   - On the Shutdown Shift4's Universal Transaction Gateway screen, select **Yes**.
   - The UTG Task Explorer window will show a shutdown countdown and then close.
3. From the Start menu, select **Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp**.

4. In the UTG TuneUp window, verify the **API Interfaces** tab is selected. Under Interface, click **Add** and then select **TCP/IP**.



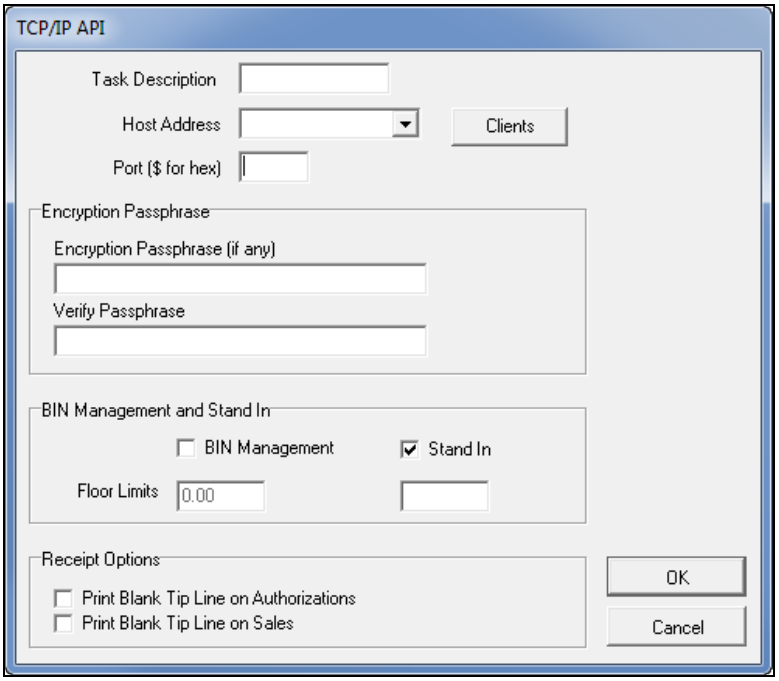
5. In the TCP/IP API window, complete the following steps:

- In the Task Description field, enter a name to identify the interface. For example, Pos4GoTCP.
- From the Host Address list, select the applicable option:
  - UTG Installation Method 1: Select the terminal's IP address currently being configured, or select 127.0.0.1.

Important: If 127.0.0.1 is selected, which is the loopback address and keeps all communication between the terminal and UTG on the terminal, the terminal's MAC address will need to be known to decipher which terminal processed a transaction in Lighthouse Transaction Manager.

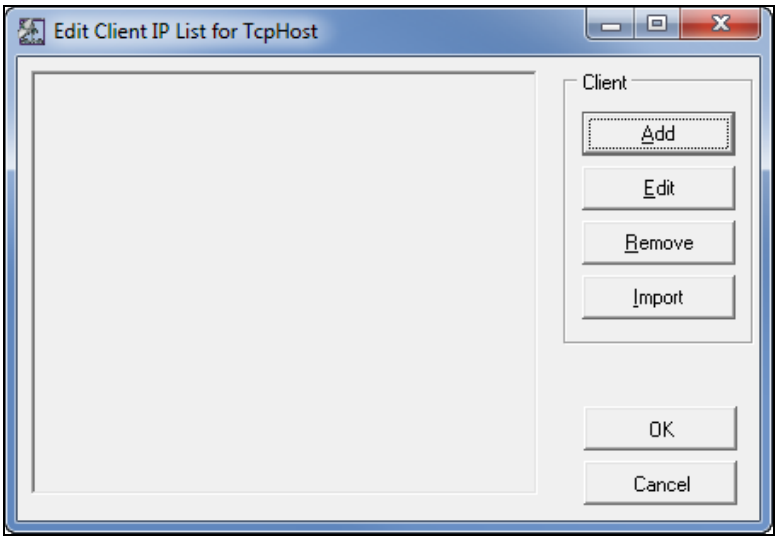
  - UTG Installation Method 2: Select the server's IP address.
  - UTG Installation Method 3: Select that terminal's IP address.
- Record the IP address selected for the interface; you will need it later.
- In the Port field, unless it is in use by another TCP/IP API, enter the default: 17476. If the default is in use, enter an open port number.
- Record the port number entered; you will need it later.
- Leave the Encryption Passphrase field blank.
- Leave the Verify Passphrase field blank.

- *(Optional)* Select **BIN Management** to enable. The default is to leave the option cleared – disabling the function.
    - If BIN Management is enabled, in the Floor Limits field, enter a limit. (The lowest amount for which the function is enabled.)
    - For additional information on BIN Management and Floor Limits, see the *UTG Quick Installation Guide*.
- *(Optional)* Select **Stand In** to enable. The default is to leave the option cleared – disabling the function.
    - If Stand In is enabled, in the Floor Limits field, enter a limit. (The highest amount for which an offline transaction will process without returning a referral.)
    - For additional information on Stand In, Enhanced Offline Mode, and Floor Limits, see the *UTG Quick Installation Guide*.

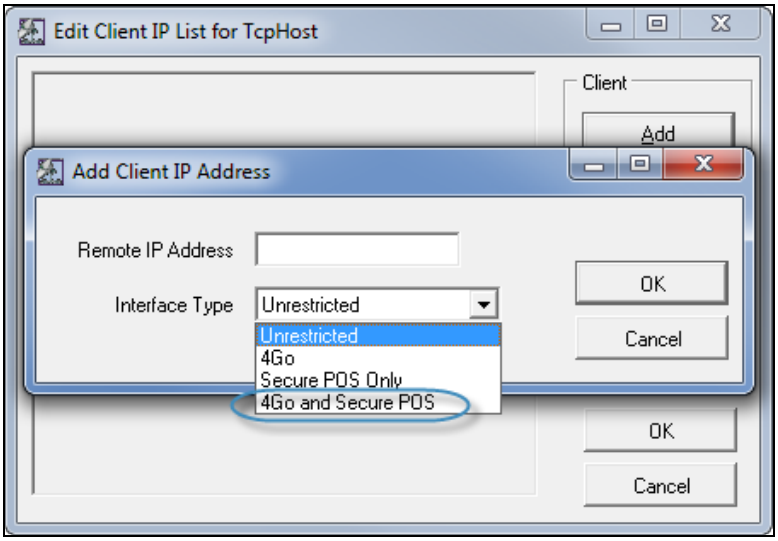


6. In the TCP/IP API window, click **Clients**.

7. In the Edit Client IP List for [Task Description] window, click **Add**.



8. In the Add Client IP Address window, complete the following steps:
   - In the Remote IP Address field, enter the applicable information:
     - UTG Installation Method 1: Based on your previous selection, enter the terminal's IP address that you are currently configuring, or enter 127.0.0.1.
     - UTG Installation Method 2: Enter the server's IP address.
     - UTG Installation Method 3: Enter that terminal's IP address.
   - In the Interface Type list, select **4Go and Secure POS**.
   - Click **OK**.

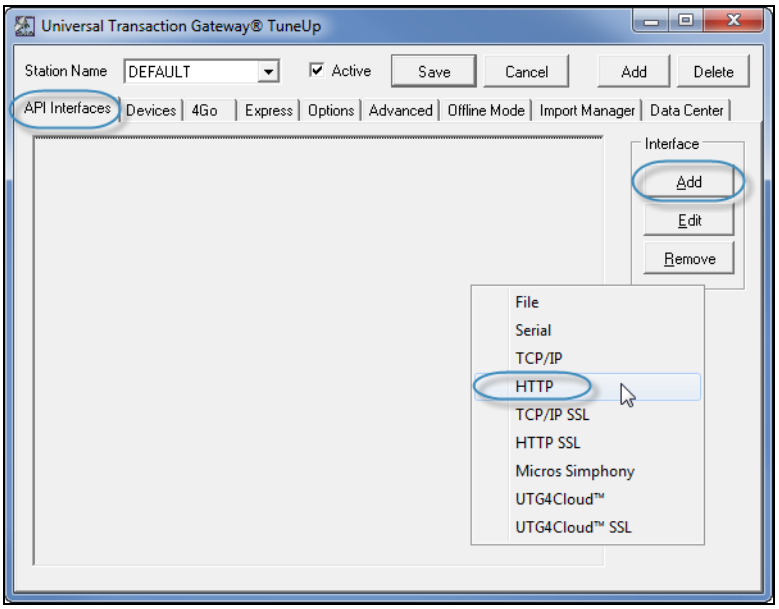


9. For UTG Installation Method 2 and 3, repeat step 7 and 8 until all terminals in the network are added as clients of the TCP/IP interface.
   - When repeating step 7 and 8, enter each terminal's specific IP address in the Remote IP Address field. This ensures the interface can communicate with all terminals in the network.
   - If a large number of terminals need to be added to the interface, they can be imported by completing the following steps:
     - In the Edit Client IP List for [Task Description] window, click **Import**.
     - In the Open window, browse to and select the .txt file that contains the POS/PMS terminal IP addresses (formatted one per line) and click **OK**.
     - In the Select Interface Type window, complete the following steps (which will apply to all imported terminals):
       - In the Interface Type list, select **4Go and Secure POS**.
       - Click **OK**.
10. In the Edit Client IP List for [Task Description] window, click **OK**.
11. In the TCP/IP API window, click **OK**.
12. Leave the UTG TuneUp window open and continue to the *Enabling 4Go in the UTG* section.

HTTP – Configuring the UTG to Communicate with the POS/PMS and 4Go

To configure the UTG to communicate with the POS/PMS and 4Go, complete the following steps:

1. *(If applicable)* If the UTG is running as a service, stop the service by completing the following steps:
   - From the Start menu, select **Programs > Administrative Tools > Services**.
   - Locate Shift4 UTG(v2), right-click, and select **Stop**.
2. *(If applicable)* If the UTG is running in Stand Alone, close it by completing the following steps:
   - In the UTG Task Explorer window, click  .
   - On the Shutdown Shift4's Universal Transaction Gateway screen, select **Yes**.
   - The UTG Task Explorer window will show a shutdown countdown and then close.
3. From the Start menu, select **Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp**.
4. In the UTG TuneUp window, verify the **API Interfaces** tab is selected. Under Interface, click **Add** and then select **HTTP**.

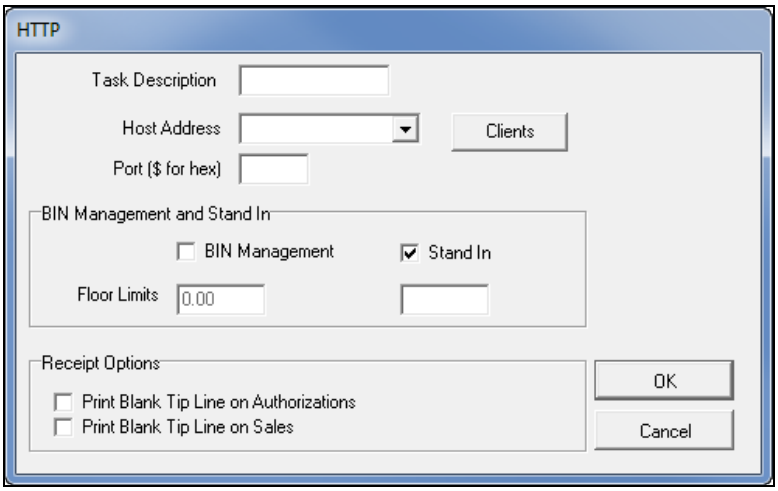


5. In the HTTP window, complete the following steps:

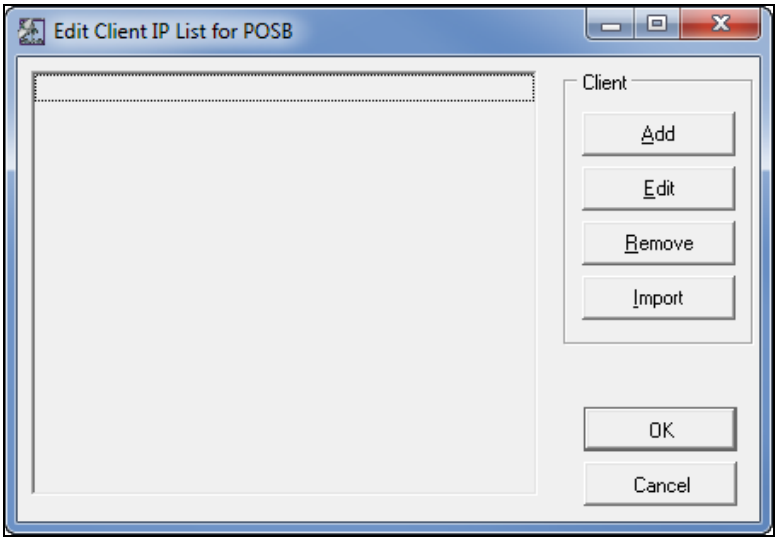
- In the Task Description field, enter a name to identify the interface. For example, PosHTTP.
- From the Host Address list, select the applicable option:
  - UTG Installation Method 1: Select the terminal's IP address currently being configured, or select 127.0.0.1.

> **Important:** If 127.0.0.1 is selected, which is the loopback address and keeps all communication between the terminal and UTG on the terminal, the terminal's MAC address will need to be known to decipher which terminal processed a transaction in Lighthouse Transaction Manager.

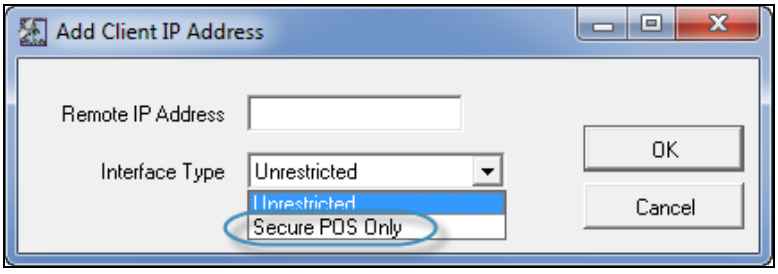
  - UTG Installation Method 2: Select the server's IP address.
  - UTG Installation Method 3: Select that terminal's IP address.
- In the Port field, unless it is in use by another HTTP API, enter the default: 16448. If the default is in use, enter an open port number.
- *(Optional)* Select **BIN Management** to enable. The default is to leave the option cleared – disabling the function.
  - If BIN Management is enabled, in the Floor Limits field, enter a limit. (The lowest amount for which the function is enabled.)
  - For additional information on BIN Management and Floor Limits, see the *UTG Quick Installation Guide*.
- *(Optional)* Select **Stand In** to enable. The default is to leave the option cleared – disabling the function.
  - If Stand In is enabled, in the Floor Limits field, enter a limit. (The highest amount for which an offline transaction will process without returning a referral.)
  - For additional information on Stand In, Enhanced Offline Mode, and Floor Limits, see the *UTG Quick Installation Guide*.



6. In the HTTP window, click **Clients**.
7. In the Edit Client IP List for [Task Description] window, click **Add**.



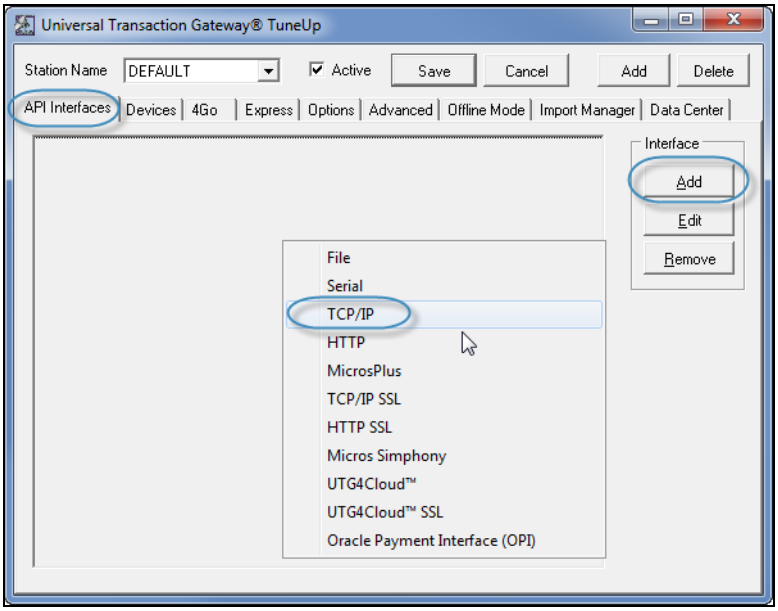
8. In the Add Client IP Address window, complete the following steps:
   - In the Remote IP Address field, enter the applicable information:
     - UTG Installation Method 1: Based on your previous selection, enter the terminal's IP address that you are currently configuring, or enter 127.0.0.1.
     - UTG Installation Method 2: Enter the server's IP address.
     - UTG Installation Method 3: Enter that terminal's IP address.
   - In the Interface Type list, select **Secure POS Only**.
   - Click **OK**.



9. For UTG Installation Method 3, repeat step 7 and 8 until all terminals in the network are added as clients of the HTTP interface.
   - When repeating step 7 and 8, enter each terminal's specific IP address in the Remote IP Address field. This ensures the interface can communicate with all terminals in the network.

- If a large number of terminals need to be added to the interface, they can be imported by completing the following steps:
    - In the Edit Client IP List for [Task Description] window, click **Import**.
    - In the Open window, browse to and select the .txt file that contains the POS/PMS terminal IP addresses (formatted one per line) and click **OK**.
    - In the Select Interface Type window, complete the following steps (which will apply to all imported terminals):
        - In the Interface Type list, select **Secure POS Only**.
        - Click **OK**.

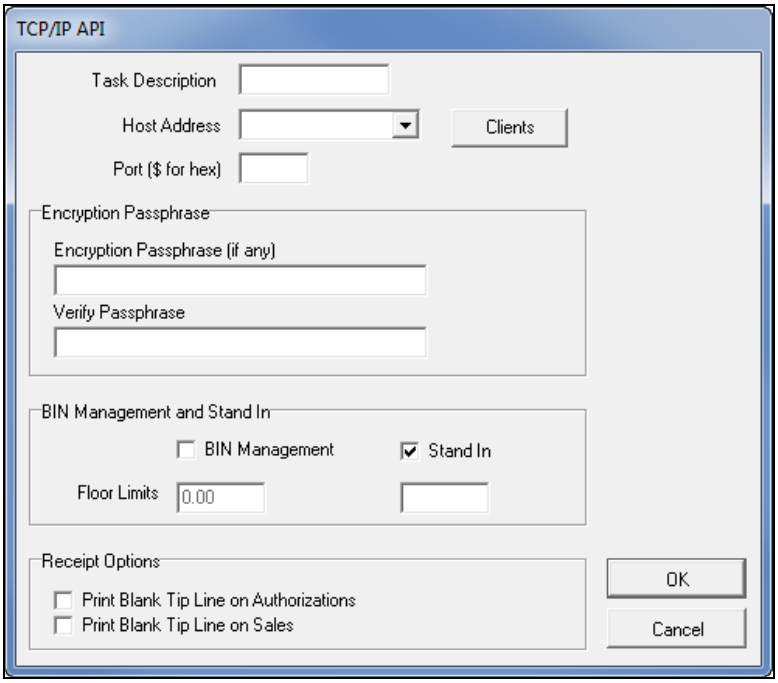
10. In the Edit Client IP List for [Task Description] window, click **OK**.
11. In the HTTP window, click **OK**.
12. In the UTG TuneUp window, verify the **API Interfaces** tab is selected. Under Interface, click **Add** and then select **TCP/IP**.



13. In the TCP/IP API window, complete the following steps:

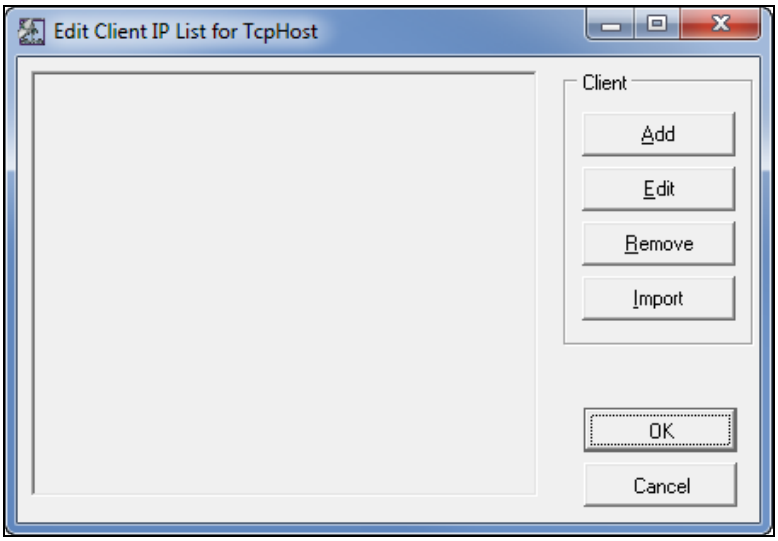
- In the Task Description field, enter a name to identify the interface. For example, 4GoTCP.
- From the Host Address list, select the applicable option:
    - UTG Installation Method 1: Based on your previous selection, select the terminal's IP address that you are currently configuring, or select 127.0.0.1.
    - UTG Installation Method 2: Select the server's IP address.
    - UTG Installation Method 3: Select that terminal's IP address.
- Record the IP address selected for the interface; you will need it later.
- In the Port field, unless it is in use by another TCP/IP API, enter the default: 17477. If the default is in use, enter an open port number.
- Record the port number entered; you will need it later.

- Leave the Encryption Passphrase field blank.
- Leave the Verify Passphrase field blank.
- *(Optional)* Select **BIN Management** to enable. The default is to leave the option cleared – disabling the function.
    - If BIN Management is enabled, in the Floor Limits field, enter a limit. (The lowest amount for which the function is enabled.)
    - For additional information on BIN Management and Floor Limits, see the *UTG Quick Installation Guide*.
- *(Optional)* Select **Stand In** to enable. The default is to leave the option cleared – disabling the function.
    - If Stand In is enabled, in the Floor Limits field, enter a limit. (The highest amount for which an offline transaction will process without returning a referral.)
    - For additional information on Stand In, Enhanced Offline Mode, and Floor Limits, see the *UTG Quick Installation Guide*.



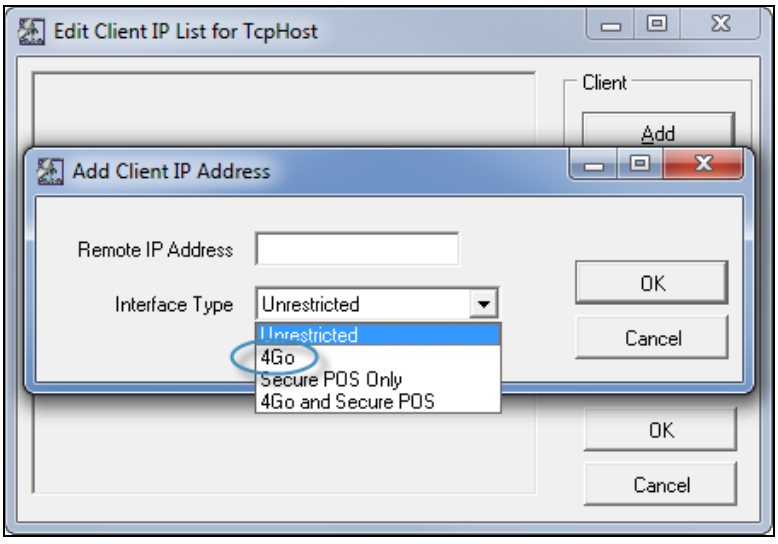
14. In the TCP/IP API window, click **Clients**.

15. In the Edit Client IP List for [Task Description] window, click **Add**.



16. In the Add Client IP Address window, complete the following steps:

- In the Remote IP Address field, enter the applicable information:
  - UTG Installation Method 1: Based on your previous selection, enter the terminal's IP address that you are currently configuring, or enter 127.0.0.1.
  - UTG Installation Method 2: Enter the server's IP address.
  - UTG Installation Method 3: Enter that terminal's IP address.
- In the Interface Type list, select **4Go**.
- Click **OK**.



17. For UTG Installation Method 2 and 3, repeat step 15 and 16 until all terminals in the network are added as clients of the TCP/IP interface.
    - When repeating step 15 and 16, enter each terminal's specific IP address in the Remote IP Address field. This ensures the interface can communicate with all terminals in the network.
    - If a large number of terminals need to be added to the interface, they can be imported by completing the following steps:
        - In the Edit Client IP List for [Task Description] window, click **Import**.
        - In the Open window, browse to and select the .txt file that contains the POS/PMS terminal IP addresses (formatted one per line) and click **OK**.
        - In the Select Interface Type window, complete the following steps (which will apply to all imported terminals):
            - In the Interface Type list, select **4Go**.
            - Click **OK**.
18. In the Edit Client IP List for [Task Description] window, click **OK**.
19. In the TCP/IP API window, click **OK**.
20. Leave the UTG TuneUp window open and continue to the *Enabling 4Go in the UTG* section.

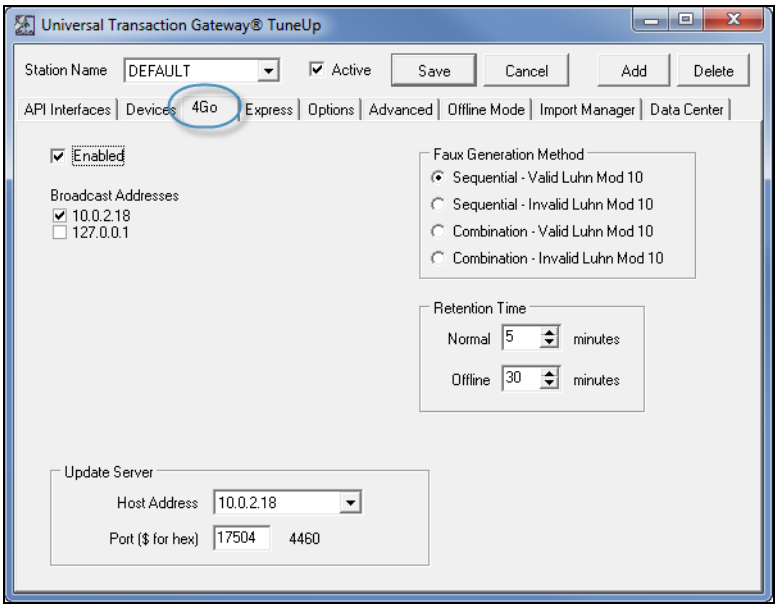
Enabling 4Go in the UTG

To enable and configure 4Go in the UTG, complete the following steps:

1. In the UTG TuneUp window, click the **4Go** tab and complete the following steps:

   - Select **Enabled**.
   - Under Broadcast Addresses, to enable 4Go to automatically broadcast for a UTG to communicate with, select the applicable option:
     - UTG Installation Method 1: Based on your previous selection, select the terminal's IP address that you are currently configuring, or select 127.0.0.1.
       - *(Recommended)* When multiple UTGs are in use, do not select the terminals IP address under the Broadcast Addresses area. Manually configure the communication between each terminal's UTG and 4Go – this will prevent 4Go from automatically connecting to a UTG that is not on its terminal. (This process is reviewed in the *Configuring 4Go to Communicate with the UTG* section.)
     - UTG Installation Method 2: Select the server's IP address.
     - UTG Installation Method 3: Select that terminal's IP address.
   - Under Faux Generation Method, select a method:
     - *(Preferred)* If the Luhn Mod 10 check can be disabled in the POS/PMS, select either **Sequential – Invalid Luhn Mod 10** or **Combination – Invalid Luhn Mod 10**.
     - If the Luhn Mod 10 check can not be disabled in the POS/PMS, select either **Sequential – Valid Luhn Mod 10** or **Combination – Valid Luhn Mod 10**.
     - For additional information on Faux Generation Method, see *Appendix C*.
   - Under Retention Time, select retention times for Normal (default is 5) and Offline (default is 30) modes. For additional information on Retention Time, see *Appendix C*.
   - Under Update Server, complete the following steps:
     - In the Host Address list, select the applicable option:
       - UTG Installation Method 1: Based on your previous selection, select the terminal's IP address that you are currently configuring, or select 127.0.0.1.
       - UTG Installation Method 2: Select the server's IP address.
       - UTG Installation Method 3: Select that terminal's IP address.

- In the Port field, unless it is in use by another interface, enter the default: 17504.



- Click **Save**.

2. To restart the UTG, complete the following steps:

- *(If applicable)* To restart the UTG as a service, from the Start menu, select **Programs > Administrative Tools > Services**. Locate Shift4 UTG(v2), right-click, and select **Start**.
- *(If applicable)* To restart the UTG in Stand Alone, from the Start menu, select **Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) Stand Alone**.

Requirement: Repeat the *Configuring the UTG to Communicate* section for each UTG.

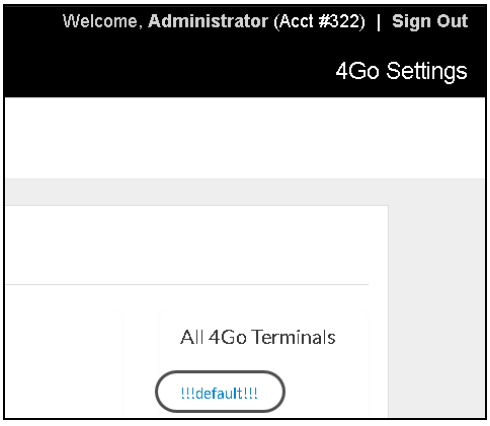
Configuring 4Go Settings in Lighthouse Transaction Manager

Prior to installing and configuring 4Go, Terminal Settings and Bin Ranges in Lighthouse Transaction Manager must be configured by the Account Administrator.

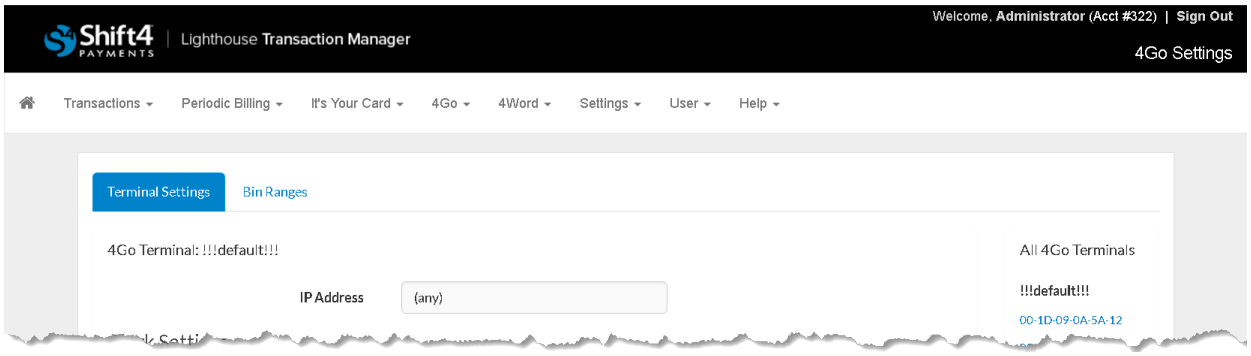
Configuring Terminal Settings

To configure Terminal Settings, complete the following steps:

1. Log in to Lighthouse Transaction Manager as the Account Administrator.
2. From the menu, select **4Go > Settings**.
3. To configure the default settings that will apply to each terminal added as a client of the TCP/IP interface in the UTG, on the 4Go Settings page, on the Terminal Settings tab, locate the All 4Go Terminals section and select **!!!default!!!**.



4. The IP Address field is a reference field. When "!!!default!!!" is selected, the field will display "(any)". If an individual terminal is selected for configuration under All 4Go Terminals, the IP address for that terminal will appear in the IP Address field. If the loopback address ("FF-FF-FF-FF-FF-FF") is selected, the loopback IP address will appear: 127.0.0.1.



5. *(If applicable)* 4Go requires the payment card number and expiration date. If additional payment card or customer identity information is needed, under Prompting, complete the following steps:

   - Next to Card Security Code (CVV2), select the applicable options:
     - **Manual** – 4Go will prompt for the Card Security Code (CVV2) when a payment card is manually entered. (The three- or four-digit code found on the front or back of the payment card.)
     - **Swipe** – 4Go will prompt for the Card Security Code (CVV2) when a payment card is swiped. (The three- or four- digit code found on the front or back of the payment card.)
   - Next to Street Number (AVS), select the applicable options:
     - **Manual** – 4Go will prompt for the Street Number (AVS) when a payment card is manually entered. (The numerical portion of the customer's street address that corresponds to the payment card.)
     - **Swipe** – 4Go will prompt for the Street Number (AVS) when a payment card is swiped. (The numerical portion of the customer's street address that corresponds to the payment card.)
   - Next to Postal Code (AVS), select the applicable options:
     - **Manual** – 4Go will prompt for the Postal Code (AVS) when a payment card is manually entered. (The postal/ZIP code from the customer's address that corresponds to the payment card.)
     - **Swipe** – 4Go will prompt for the Postal Code (AVS) when a payment card is swiped. (The postal/ZIP code from the customer's address that corresponds to the payment card.)

6. Under Interception Settings, complete the following steps:

   - In the Encrypted Device Type list, select an option:
     - **None** – Select if IDTECH devices will not be used.
     - **IDTECH** – Select if IDTECH devices will be used, enabling point-to-point encryption (P2PE). For additional information on P2PE, see the *Point-to-Point Encryption* document in Lighthouse Transaction Manager Help.

WARNING! By selecting **None** and thus disabling the requirement for a *True* P2PE® device, your payment application may potentially expose clear-text CHD to external threats, such as memory scraping malware. For legacy applications, the use of 4Go may be required for your PCI DSS compliance. If so, it is important to understand that 4Go is a foundation to security, but *True* P2PE is a necessary addition to provide security against today's threats. *True* P2PE can also reduce your PCI DSS footprint and potentially allow for a quicker path to compliance.

If *True* P2PE is disabled, your payment system will be fully in scope for PCI assessments according to the PCI DSS. Please review all applicable PA-DSS implementation guides (4Go, UTG, etc.) in order to assess your particular PCI DSS scope and decide your appropriate course of action in regards to PCI compliance. Those guides, along with other pertinent information, can be accessed using the links below.

- *True* P2PE
- 4Go PA-DSS Implementation Guide
- UTG PA-DSS Implementation Guide
- Payment Card Industry Security Standards Council (PCI SSC)
- PCI DSS
- PA-DSS

- In the Faux Method list, select an option:
  - **Standard** – The UTG will create a temporary, false card number that 4Go will return to the POS/PMS terminal. A temporary, false card number has a lifespan of minutes relative to the Normal or Offline Retention Time configured in the UTG.
  - **TrueToken** – The UTG will create a TrueToken that 4Go will return to the POS/PMS terminal. A TrueToken has a lifespan of up to two years.

Note: The format of the faux data returned by 4Go depends on how the CHD was entered. For additional information, see *Appendix D*.

- Next to Easy Pass Through, select an option:
  - **Enabled** – 4Go will detect when swiped card data is non-sensitive (for example, hotel room keys or membership cards) and let it pass through exactly as swiped; the non-sensitive card data will not be replaced by a temporary, false card number or a TrueToken. 4Go will only replace payment cards with a temporary, false card number or a TrueToken.

Important: If Easy Pass Through is Enabled, 4Go will not pass through cards with the POS/Pass-Through Bin Ranges configured in Lighthouse Transaction Manager.

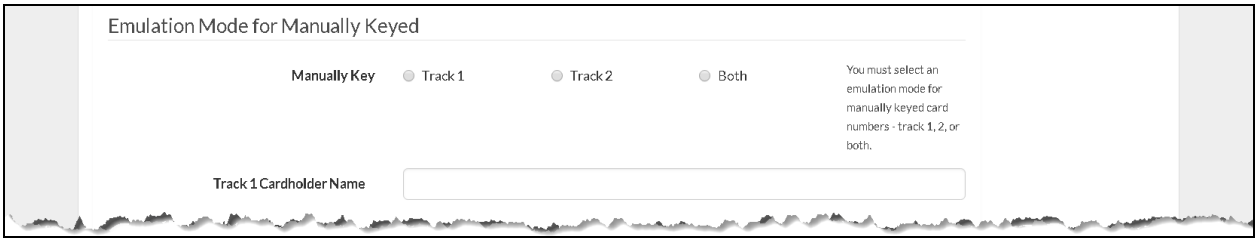
- **Disabled** – 4Go will replace all card data resembling payment cards with a temporary, false card number or a TrueToken.

Important: If Easy Pass Through is Disabled, 4Go will pass through cards with the POS/Pass-Through Bin Ranges configured in Lighthouse Transaction Manager.

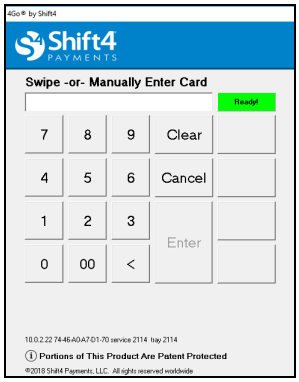
7. Under Emulation Mode for Manually Keyed, complete the following steps:
   - Next to Manually Key, select the applicable option(s):
     - **Track 1** – 4Go will mimic a Track 1 swipe data stream when a payment card is manually entered.
     - **Track 2** – 4Go will mimic a Track 2 swipe data stream when a payment card is manually entered.

Requirement: Track 1 or **Track 2** must be selected. In addition, **Both** may be selected.

   - In the Track 1 Cardholder Name field, leave Shift4 Payments' default "MANUAL ENTRY," or enter a generic name.



8. Under Screen Layout & Triggers, complete the following steps:
   - Next to Keypad Layout, select an option:
     - **Calculator** – 4Go screens will display the 10-key layout used on calculators and keyboards. For example, see the image below on the left.
     - **Phone** – 4Go screens will display the 10-key layout used on telephones. For example, see the image below on the right.



- Next to Mask Card Input, select an option:
  - **Enabled** – *(Recommended)* 4Go will mask the card payment number as it is swiped or manually entered on the 4Go screen.
  - **Disabled** – 4Go will not mask the card payment number as it is swiped or manually entered on the 4Go screen.
- In the Hot Key field, enter a key that will invoke 4Go when the clerk presses the key on the keyboard (also known as a keyboard shortcut). For example, F10.
- Next to Hot Key Modifier, select the applicable option(s):
  - **Ctrl** – The clerk will press Ctrl on the keyboard at the same time as the Hot Key to invoke 4Go.
  - **Alt** – The clerk will press Alt on the keyboard at the same time as the Hot Key to invoke 4Go.
  - **Shift** – The clerk will press Shift on the keyboard at the same time as the Hot Key to invoke 4Go.

Tip: Any of these options may be used. For example, Ctrl F10, Alt F10, Shift F10, or any combination, such as Ctrl Alt F10.

9. *(If applicable)* If serial-based magnetic swipe readers will be in use (the readers are plugged into a serial port, not a USB port), under Serial Swipe Readers, complete the following steps for up to three readers:

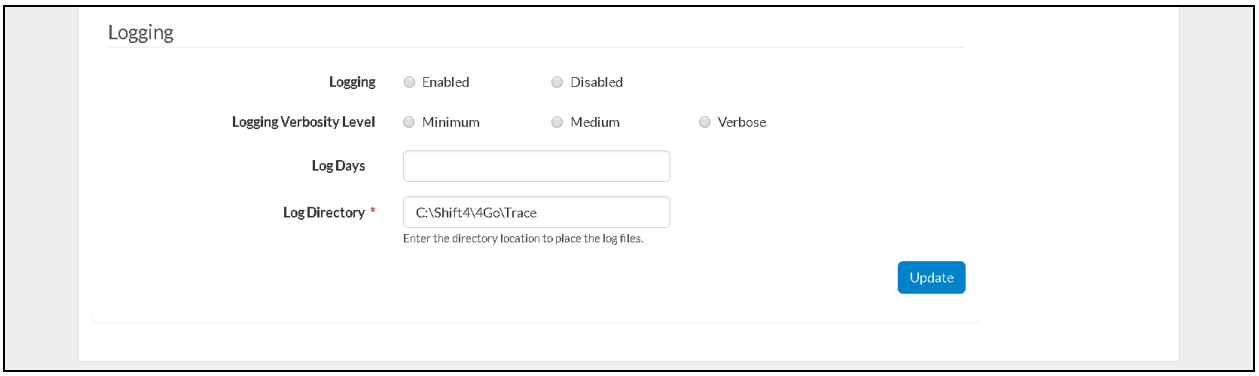
   - In the In Port list, select the COM port.
   - In the Baud list, use the manufacturer's settings.
   - In the Data Bits list, use the manufacturer's settings.
   - In the Parity list, use the manufacturer's settings.
   - In the Stop Bits list, use the manufacturer's settings.
   - In the Flow Control list, use the manufacturer's settings.
   - The Out Port list is inactive and reserved for future use.
   - The Virtual Out Port list is inactive and reserved for future use.
   - In the Device list, select the reader that will be in use.

10. Under Logging, complete the following steps:

    - Next to Logging, select an option:
      - **Enabled** – 4Go will collect and store log files with trace data on the terminal. Only use this setting if your terminal does not have storage limitations.
      - **Disabled** – 4Go will not collect and store log files with trace data on the terminal. Use this setting if your terminal does have storage limitations.
    - If Logging is Enabled, next to Logging Verbosity Level, select an option to configure how much terminal disk space is allocated to store log files with trace data and how much trace data is recorded in the log files:
      - **Minimum** – Records status messages, port information, verifications, and request and response headers.
      - **Medium** – Records all Minimum information listed above and additional status messages.
      - **Verbose** – Records all Minimum and Medium information listed above and faux payment card data, card ranges, and network adapter information.
      - **Diagnostic Mode (Not Shown)** - Enabled only on a case-by-case basis by Shift4 Payments; this level collects raw data and is **NOT** PCI compliant. After use, the merchant must disable it by selecting an option above. If used, the merchant must run the Shred and Delete utility after deactivating this

mode to remove the raw trace files. If a terminal is set to Diagnostic Mode, a reminder message will appear at the top of the 4Go screen: LOG LEVEL IS VERBOSE.

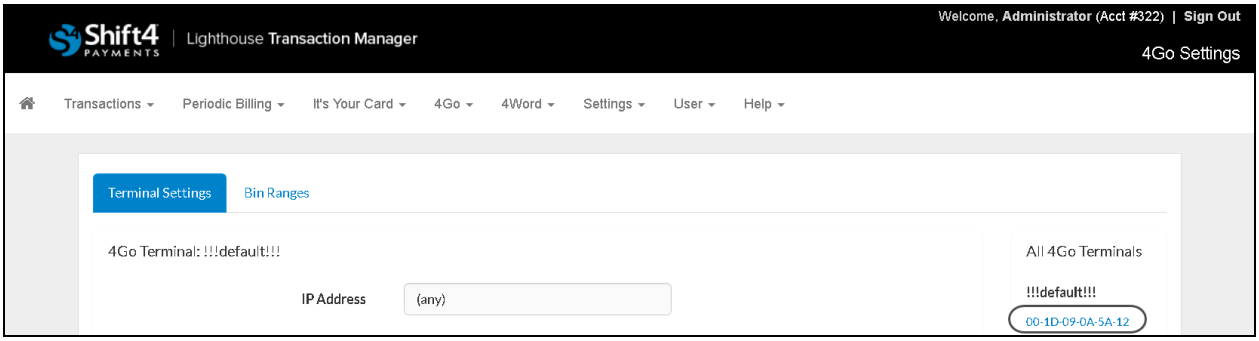
- If Logging is Enabled, in the Log Days field, enter a number of days to collect the log files with trace data.
- If Logging is Enabled, in the Log Directory field, enter the path to the folder where 4Go will save the log files. The default is …\Shift4\4Go\Trace.



11. Click **Update**. You must also update 4Go settings on each terminal by pressing the following three keys simultaneously on the keyboard.

WARNING! Failure to do step 11 will result in the UTG being out of sync with Terminal Settings in Lighthouse Transaction Manager. The UTG will update when restarted or when **Ctrl**, **Alt**, and **.** are pressed on the keyboard.

12. To configure a terminal individually, under the All 4Go Terminals section, select the terminal to be configured and repeat steps 4 through 11.



Understanding the All 4Go Terminals Section

After 4Go is installed and configured on each terminal, and successfully connects to the UTG, the terminal will receive the default (*!!!default!!!*) settings and be added to the All 4Go Terminals section.

The terminals are listed by their MAC address in the All 4Go Terminals section. Once the terminal appears in this section, it can be selected and individually configured if the default settings are not appropriate.

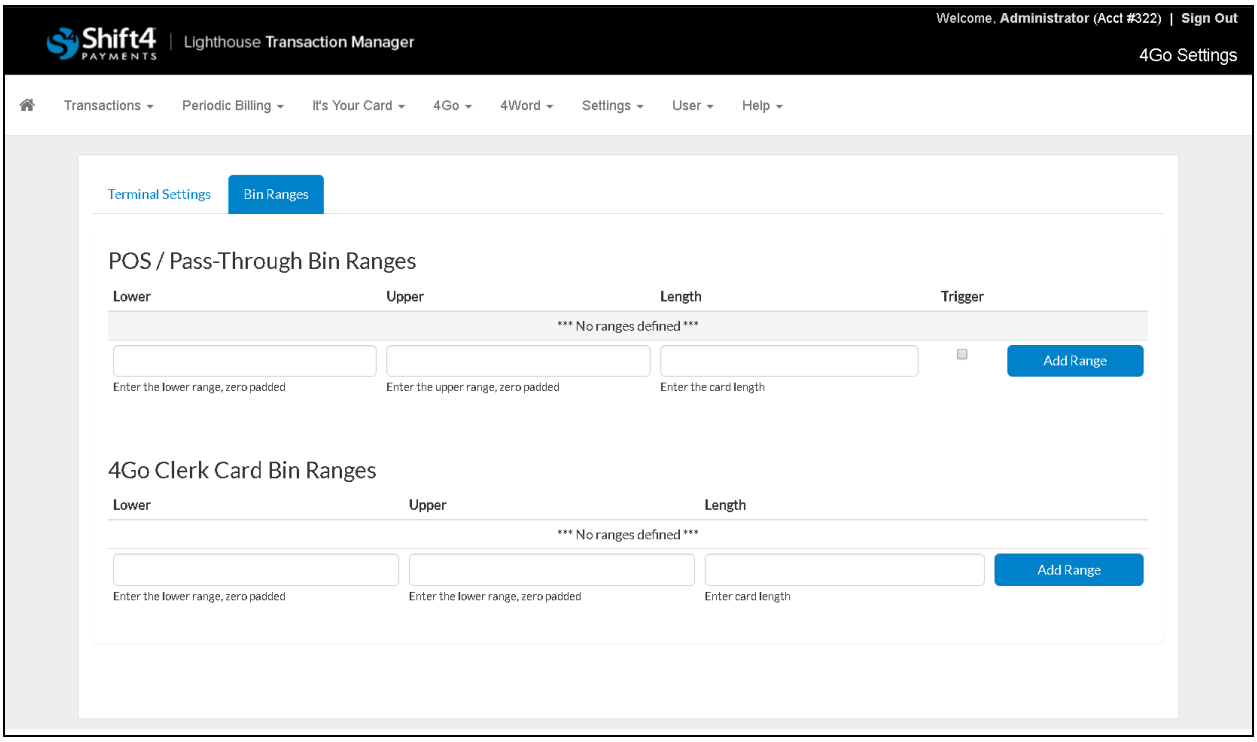
In regards to the loopback address, FF-FF-FF-FF-FF-FF, the settings configured will apply to all terminals configured with the loopback IP address: 127.0.0.1.

Lastly, if a terminal is configured individually but still retains some settings that match the default settings, if and when default settings are modified, the matching default settings under the individual terminal's settings will also be updated; however, the settings that differ from the default settings will not be modified.

Configuring Bin Ranges

To configure Bin Ranges that will allow cards with those Bin Ranges to pass through 4Go (instead of being replaced with a temporary, false card number or a TrueToken), complete the following steps:

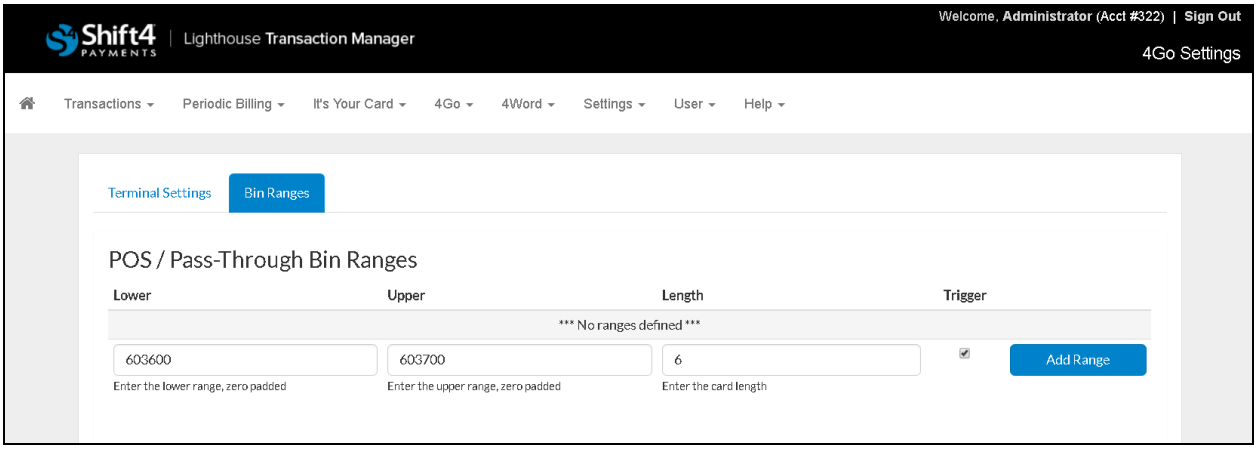
1. Log in to Lighthouse Transaction Manager as the Account Administrator.
2. From the menu, select **4Go > Settings**.
3. On the 4Go Settings page, click the **Bin Ranges** tab.



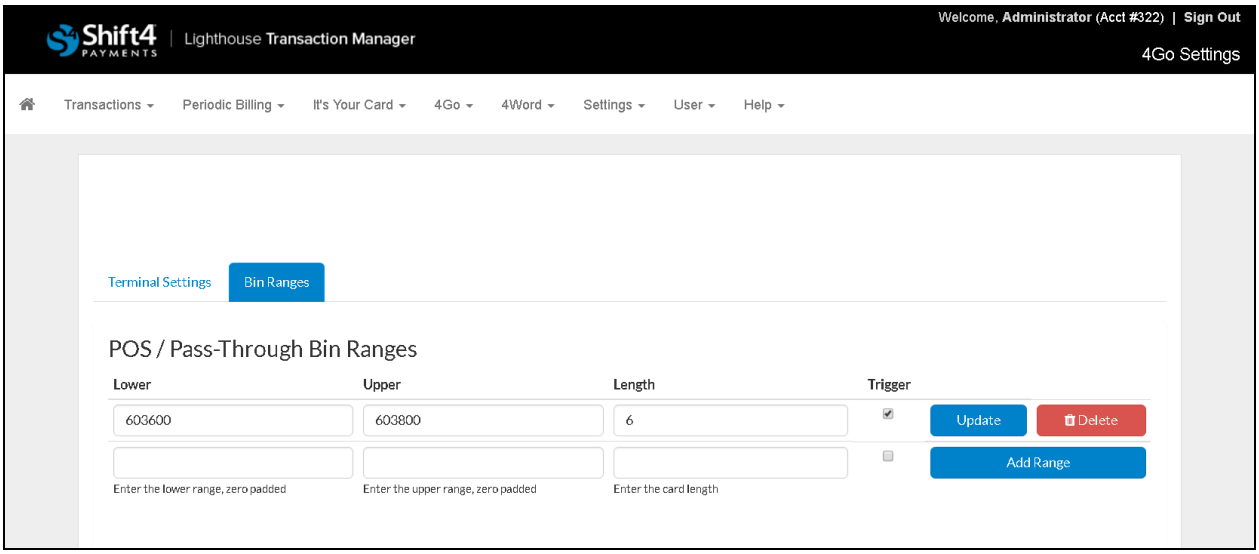
4. *(If applicable)* If POS/PMS Clerk Cards, hotel room keys, or membership cards will be in use, under POS/Pass-Through Bin Ranges, complete the following steps:

   - In the Lower field, enter the lower limit Bin Range for the card. For example, 603600.
   - In the Upper field, enter the upper limit Bin Range for the card. For example, 603700.
   - In the Length field, enter the length of the Bin Range for the POS/PMS Clerk Card. Continuing from the previous examples, 6.
   - If a magnetic swipe reader is available and a hot key/keyboard shortcut is not available to invoke 4Go, select **Trigger**. (When this option is selected and a card is swiped within range, the 4Go window will appear.)
   - Click **Add Range**.

Requirement: Easy Pass Through must be Disabled for POS/Pass-Through Bin Ranges to function.



5. *(If applicable)* To edit a Bin Range, enter the new information in the corresponding field and click **Update** next to the Bin Range.



6. *(If applicable)* To delete a Bin Range, click **Delete** next to the Bin Range.
7. You must update 4Go settings on each terminal by pressing the following three keys simultaneously on the keyboard.

WARNING! Failure to do step 7 will result in the UTG being out of sync with Bin Ranges in Lighthouse Transaction Manager. The UTG will update when restarted or when **Ctrl**, **Alt**, and **.** are pressed on the keyboard.

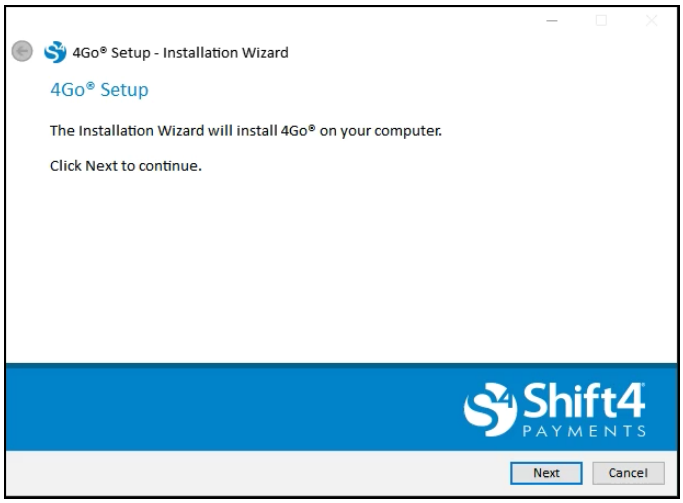
Installing and Configuring 4Go

After the UTG and Lighthouse Transaction Manager have been configured, 4Go must be installed and configured to communicate with the UTG on each terminal.

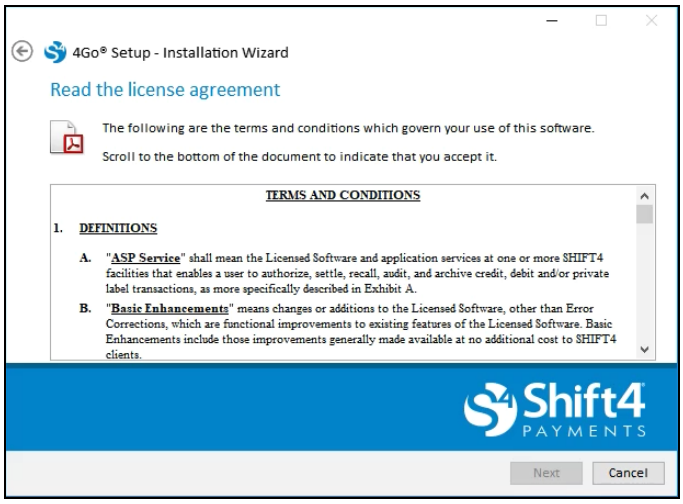
Installing 4Go

To install 4Go, complete the following steps:

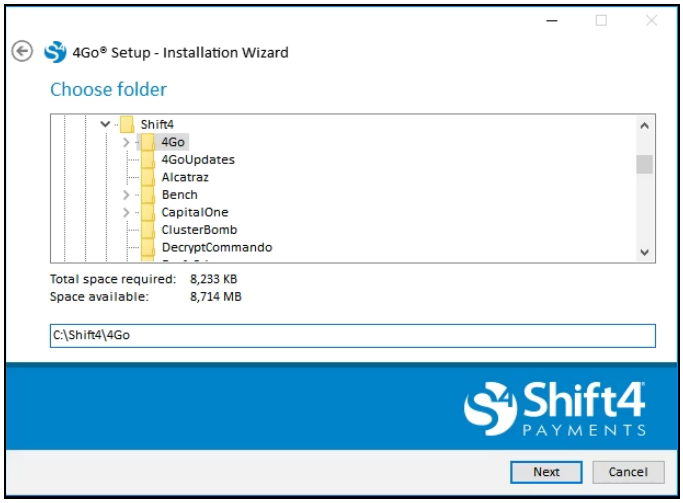
1. Download and save the 4Go Setup file located at www.shift4.com/downloads/4Gosetup.exe to the desktop.
2. Double-click the **4Gosetup.exe** file on the desktop to open Shift4 Payments' Installation Wizard and then click **Run**.
3. In the Installation Wizard window, click **Next** to continue the installation.



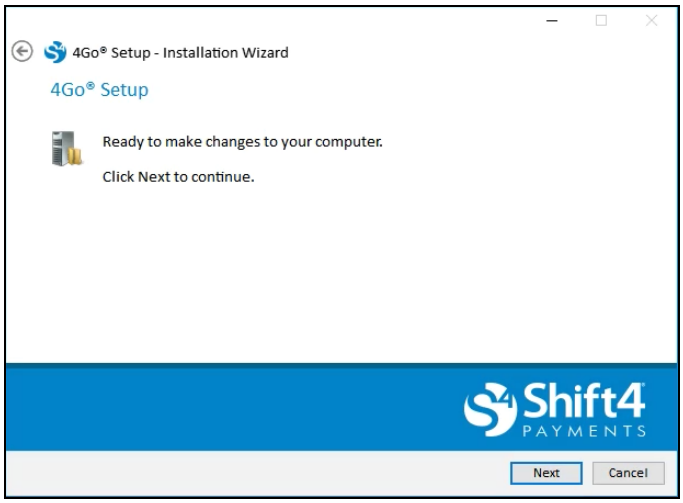
4. In the Installation Wizard window, read the license agreement, scroll to the bottom to indicate acceptance, and click **Next** to continue.



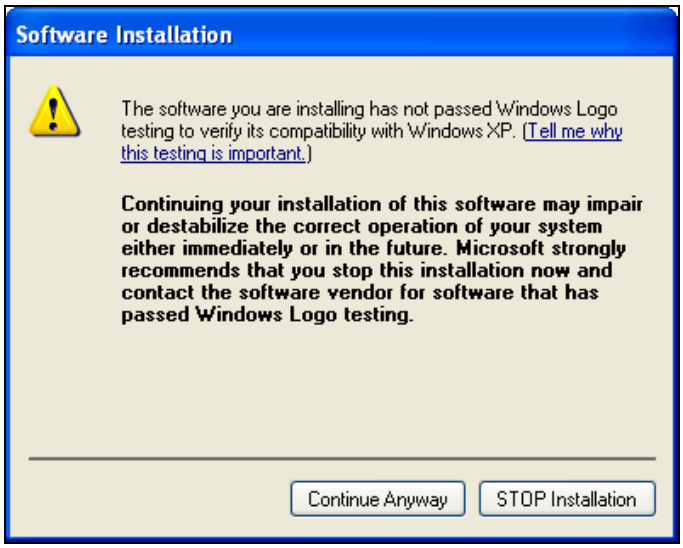
5. In the Installation Wizard window, choose the folder where 4Go's program files will be written to (the default is …\Shift4\4Go) and click **Next** to continue.



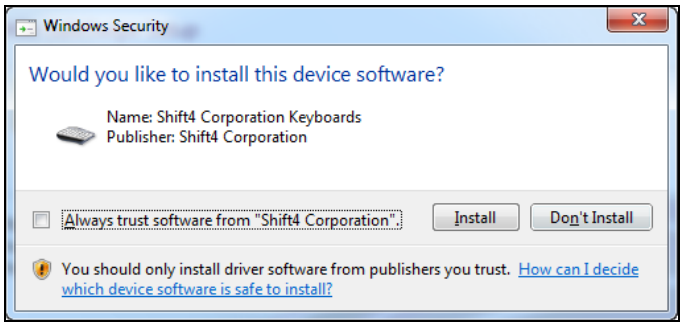
6. In the Installation Wizard window, click **Next** to begin to make changes to your computer.



7. If the following Software Installation window appears, click **Continue Anyway**.

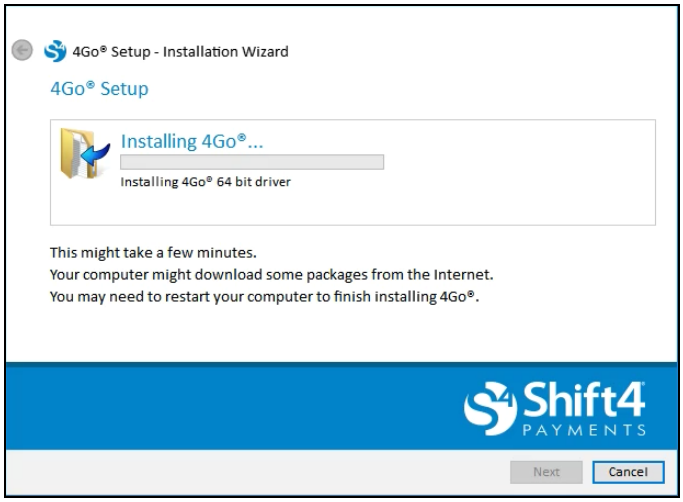


8. If the following Windows Security window appears, click **Install**.

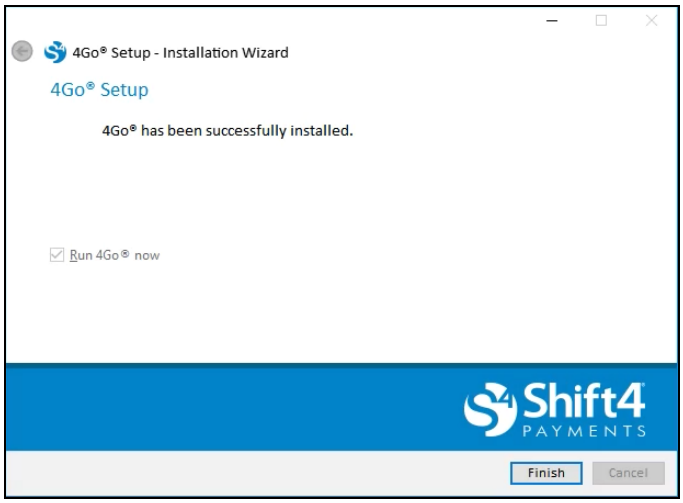


Tip: Refer to *Appendix B* for detailed instructions on *Configuring MSRs Connected After 4Go Has Been Installed and Configured on the Terminal*.

9. The Installation Wizard shows the progress of the installation.



10. When the installation is complete, click **Finish** to close the Installation Wizard window.



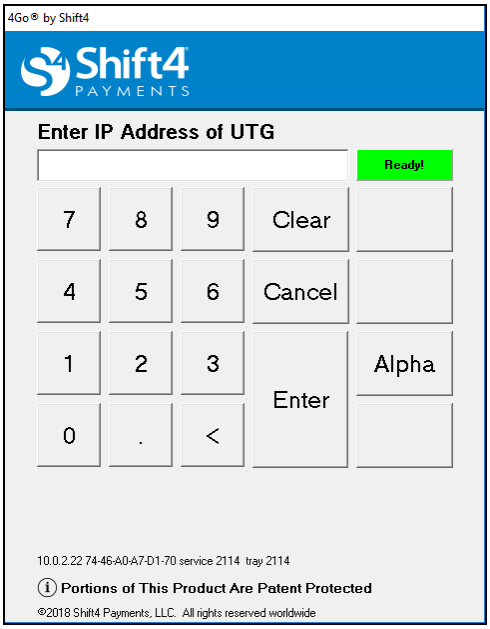
11. Repeat the *Installing 4Go* section on each terminal as required.

Configuring 4Go to Communicate with the UTG

After 4Go is installed it will send a broadcast message to locate the UTG. If the UTG is found, 4Go will automatically configure itself to communicate with the UTG.

If 4Go is unable to locate the UTG (ensure the UTG has been started), 4Go will prompt for the TCP/IP interface information configured in the UTG, which should have been recorded. If this occurs, to configure 4Go to communicate with the UTG, complete the following steps:

1. On the Enter IP Address of UTG screen, enter the TCP/IP interface IP address configured in the UTG and press **Enter**.



2. On the Enter Port of UTG screen, enter the TCP/IP interface port number configured in the UTG and press **Enter**.

3. 4Go should now be configured to communicate with the UTG.
4. Repeat the *Configuring 4Go to Communicate with the UTG* section on each terminal as required.

Post-Installation Process

After the UTG(s) and Lighthouse Transaction Manager are configured, and 4Go and the Shift4 Driver are installed and configured on each terminal, verify and test 4Go on each terminal using the processes outlined in this section.

Verifying File Placement

After installing and configuring 4Go, verify file placement by completing the following steps:

1. In the Windows Notification Area, verify 4Go is present. The 4Go logo cycles through three graphics in the notification area: Shift4's logo, 4, and Go.

2. Locate …Shift4\4Go and verify it is located in the destination folder specified during the installation of 4Go.
3. Verify the Shift4 Driver is present in the following folder:
    - Navigate to …Shift4\4Go\Driver and verify the "s4wf.sys" and "s4wf-usb.inf" files appear.
4. If Logging is Enabled in Lighthouse Transaction Manager, verify the Trace folder is in the destination that was specified in Lighthouse Transaction Manager. The default is …\Shift4\4Go\Trace.

Verifying the 4Go Invocation Methods

Verify the invocation methods configured are functioning by invoking 4Go. The three ways to invoke 4Go on the POS/PMS terminal are:

- Swiping a payment card
- Pressing the POS/PMS button or keyboard shortcut key
    - The default is Ctrl, Alt, and F10 pressed simultaneously
- Swiping a POS clerk card

Processing a Test Transaction

After 4Go has been invoked, test transactions can be processed. To process test transactions, complete the following steps:

1. Run a test credit transaction using 4Go and finalize it as you would normally finalize a real transaction.
2. In Lighthouse Transaction Manager, confirm that test transaction came through the right merchant.
3. Run a test gift card transaction using 4Go and finalize it as you would normally finalize a real transaction.
4. In Lighthouse Transaction Manager, confirm that test transaction came through the right merchant.
5. If your test transactions were successful, installation and configuration of 4Go is complete. Congratulations!

Appendix A – Additional Resources

Appendix A contains a list of additional resources that may be helpful and provide additional guidance when installing and configuring 4Go. Direct any specific questions about these documents to their respective publishers.

Product Support

For assistance with this and any other Shift4 Payments product, visit the website at www.shift4.com. It provides access to the Shift4 Payments FAQ page (under Client Center), where answers to general and technical questions regarding the entire Shift4 Payments product line are available.

Live Support

Information about troubleshooting techniques and handling special problems that may occur during installation, configuration, or use can be obtained by contacting the Shift4 Payments Customer Support team at 702.597.2480, option 2.

On the Web

The Shift4 Payments website at www.shift4.com offers technical notes, patches, and guides 24 hours a day, 7 days a week, 365 days a year. The Shift4 Payments website also contains troubleshooting and FAQ sections to provide additional guidance.

Feedback

Your feedback regarding Shift4 Payments products and documentation is welcome, encouraged, and we appreciate your comments. If you have any documentation comments or suggestions about this guide, please send them to us at techdocs@shift4.com.

Shift4 Payments Guides and Documentation

The following Shift4 Payments guides and documentation may provide additional helpful information:

- *4Go Reference Guide*
- *Point-to-Point Encryption*
- *UTG Quick Installation Guide*

Industry Websites

The following sites provide additional industry guidelines and standards:

- https://www.pcisecuritystandards.org/
- http://usa.visa.com/merchants/protect-your-business/index.jsp

Appendix B – Troubleshooting

Appendix B contains troubleshooting information for when 4Go is in use. It may be necessary to take a closer look at the system and the configuration to restore full functionality of the implementation.

Log Locations

Logs contain information about the system that is helpful for troubleshooting.

The Customer Support team may have you change logging settings to reveal more detailed information – refer to this section in the document, *Configuring Terminal Settings*, to complete their requests.

4Go Trace Logs

Logging must be enabled in Lighthouse Transaction Manager and the default location of the 4Go trace logs is …\Shift4\4Go\Trace.

UTG Trace Logs

The default location of the UTG trace logs is …\Shift4\UTG2\UTG Trace.

If the UTG trace logs are not in the default location, then the UTG has been configured to write them to a different directory and, possibly, a different file name.

To determine the directory and file name of the UTG trace logs, complete the following steps:

1. From the Start menu, select **Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) Tune Up**.
2. In the UTG TuneUp window, click the **Advanced** tab and then click the **Trace Configuration** button.
3. In the Trace Parameters window, the Directory field shows the path where the UTG trace files are located, and the Suffix field contains an optional suffix appended to the default file name.

Event Viewer Logs

The Event Viewer logs show 4Go activities. To view the Event Viewer logs, complete the following steps:

1. From the Start menu, select **Settings > Control Panel > Administrative Tools > Event Viewer > Application**.
2. Events using the following labels might be included:

    - Status – 4Go is ready.
    - Warning – If USB devices are added or removed, or if the logging level is changed, the Event Viewer records it as a warning.
    - Error – A "Manifest has failed validation" message appears after a partial update, the tray application has stopped, a timeout error occurs, a UTG error occurs, or if tampering is detected. The Event Viewer records it as an error.
    - Write Error – If a previous UTG version is running, or if clerks are not enabled for manual entry and manual entry is attempted, the Event Viewer records it as a write error.
    - Unexpected Response – If a conflict between the tray and services applications occurs, the Event Viewer records it as an unexpected response.

Resolving Issues and Errors

When errors and/or issues occur, document them accordingly.

Requirement: Have the clerk leave the screen up and call or contact the manager on duty.

In order to troubleshoot efficiently, it is important to gather the following data:

- What action the clerk was attempting when the error occurred.
- The date and time that the error occurred and the immediate action the clerk took prior to the error.
- Payment card information (type of card, last 4 numbers, and amount).
- The exact error description (if any).
- The exact terminal/server on which the error happened.
- Trends such as: issue occurs at a specific time, only on certain card types, when the internet is down, on all workstations, or on a certain workstation.

After documenting all of the above information, and prior to restarting any systems, make copies of the following files and email them to trace@shift4.com with all of the gathered information from above:

- The four most recent trace logs for 4Go and UTG.
- Any important Event Viewer logs.

Include your Shift4 Payments/DOTN serial/account number and the name of your establishment in your email message.

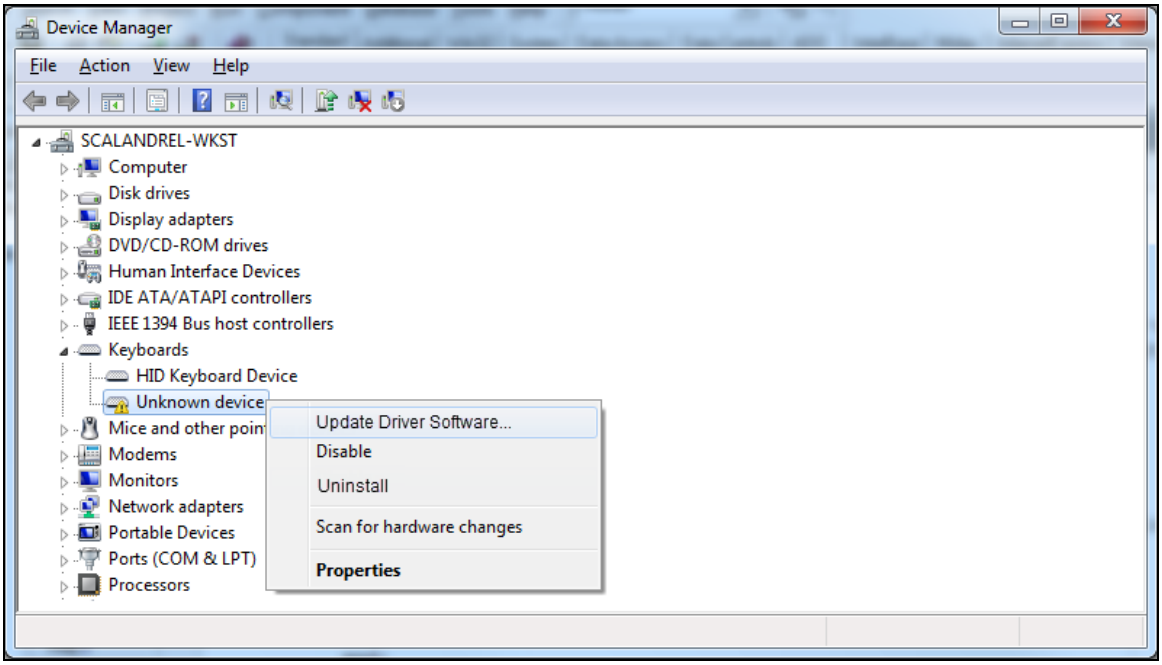
Calling for Technical Support

Immediately after completing the data gathering steps, call the Shift4 Payments Customer Support team to open a case at 702.597.2480, option 2. The Customer Support Representative will have the issue resolved as quickly as possible.

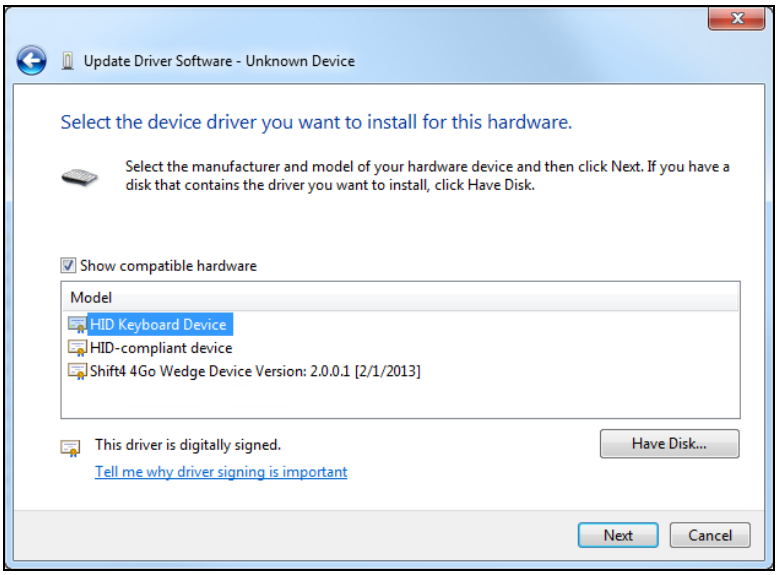
Configuring MSRs Connected After 4Go Has Been Installed and Configured on the Terminal

To configure an MSR that is connected after 4Go has been installed and configured on the terminal, complete the following steps:

1. When a new MSR is connected to a terminal with 4Go, the device will be displayed as an unknown device. In the Device Manager window, under Keyboards, select the **Unknown device**, right-click, and select **Update Driver Software**.



2. In the Update Driver Software - Unknown Device window, select **HID Keyboard Device** and then click **Next** to install.



WARNING! Do not attempt to install the Shift4 4Go Wedge Device (i.e., 4Go Driver) before installing the HID Keyboard Device.

If an attempt to install the 4Go Driver before the HID Keyboard Device is made, the following error message will appear: *Windows encountered a problem installing the driver software for your device.*

To recover from the error, complete the following steps:

1. Close the Update Driver Software - Unknown Device window.
2. In the Device Manager window, select the **Unknown device**, right-click, and select **Uninstall**.
3. Disconnect the MSR from the terminal, and then reconnect the MSR to the terminal.
4. Return to the *Configuring MSRs Connected After 4Go Has Been Installed and Configured on the Terminal* section, and start at step 1 again.

---

3. In the Device Manager window, under Keyboards, select the **Unknown device**, right-click, and select **Update Driver Software**.
4. In the Update Driver Software - Unknown Device window, select **Shift4 4Go Wedge Device** and click **Next** to install.
5. After installation is complete, close the Device Manager window.

Appendix C – Faux Generation Method and Retention Time

Faux Generation Method

When the Faux Method in Lighthouse Transaction Manager is set to Standard, the Faux Generation Method selected in UTG TuneUp (on the 4Go tab) is the process the UTG uses to create the temporary, false card number portion of the track swipe. (If the Faux Method in Lighthouse Transaction Manager is set to TrueToken, this method selection does not apply.)

There are four generation methods available. When selecting a method, consider the following:

- If the Luhn Mod 10 check can be disabled, select an invalid Luhn Mod 10 method (Sequential - Invalid Luhn Mod 10 or Combination - Invalid Luhn Mod 10).
- Combination methods offer greater security than sequential methods because when a sequential method is in use, there is a slight chance of guessing the next sequential card number.

Sequential - Valid Luhn Mod 10

This method creates the temporary, false card number portion of the track swipe sequentially; the resulting number will pass a Luhn Mod 10 check.

- In the example 4444xxxxxxxL7688: 4444 is the first four digits of the actual card number, xxxxxxxx starts at 1 and increments up through 99999, L is the valid Luhn digit, and 7688 is the last four digits of the actual card number.

Sequential - Invalid Luhn Mod 10

This method creates the temporary, false card number portion of the track swipe sequentially; the resulting number will NOT pass a Luhn Mod 10 check.

- In the example 4444xxxxxxxL7688: 4444 is the first four digits of the actual card number, xxxxxxxx starts at 1 and increments up through 99999, L is an invalid Luhn digit, and 7688 is the last four digits of the actual card number.

Combination - Valid Luhn Mod 10

This method creates the temporary, false card number portion of the track swipe by dividing it into three subsections, randomly selecting a subsection, and incrementing one of three counters; the resulting number will pass a Luhn Mod 10 check.

- In the example 444400xyyzzL7688: 4444 is the first four digits of the actual card number, x is a number 0 through 9, yy is a number 00 thru 99, zz is a number 00 thru 99, L is the valid Luhn digit, and 7688 is the last four digits of the actual card number.

Combination - Invalid Luhn Mod 10

This method creates the temporary, false card number portion of the track swipe by dividing it into three subsections, randomly selecting a subsection, and incrementing one of three counters; the resulting number will NOT pass a Luhn Mod 10 check.

- In the example 444400xyyzzL7688: 4444 is the first four digits of the actual card number, x is a number 0 through 9, yy is a number 00 thru 99, zz is a number 00 thru 99, L is an invalid Luhn digit, and 7688 is the last four digits of the actual card number.

Retention Time

Retention time settings in UTG TuneUp (on the 4Go tab) determine how long the UTG stores the actual card number locally before expiring.

- **Normal**: Specifies the amount of time the UTG retains the actual card number while in online mode. Select an interval between 5 and 10 minutes, in 1-minute increments. The default is 5 minutes.
- **Offline**: Specifies the amount of time the UTG retains the actual card number while in offline mode. Select an interval between 10 and 90 minutes, in 1-minute increments. The default is 30 minutes. (If an outage occurs, transactions will be sent to Shift4 Payments when service is restored. If a POS/PMS sends an authorization request after the Offline Retention Time expires, or the UTG is shut down, the UTG responds with an error. The clerk must swipe the card again.)

Appendix D – Returned Faux Data Format

The format of the faux data returned by 4Go depends on how the CHD was entered. The matrix below outlines the possibilities.

Return Format		
How was CHD entered?	**What will 4Go return?**	
	Standard Faux Method	**TrueToken Faux Method**
Manually	*Track 1 Format:* • %B • Faux card number • Generic name as specified in Lighthouse Transaction Manager ("MANUAL ENTRY") **-and/or*-** *Track 2 Format:* • ; • Faux card number	*Track 1 Format:* • %T • TrueToken† • Blank cardholder name
Track 1 Swipe	*Track 1 Format:* • %B • Faux card number • Cardholder name	*Track 1 Format:* • %T • TrueToken† • Cardholder name
Track 2 Swipe	*Track 2 Format:* • ; • Faux card number	*Track 1 Format:* • %T • TrueToken† • Blank cardholder name

Return Format		
How was CHD entered?	**What will 4Go return?**	
	Standard Faux Method	**TrueToken Faux Method**
Tracks 1 and 2 Swipe	*Track 1 Format:* • %B • Faux card number • Cardholder name **-and-** *Track 2 Format:* • ; • Faux card number	*Track 1 Format:* • %T • TrueToken† • Cardholder name

*If a card is manually entered and the Standard faux method is in use, 4Go can return Track 1, Track 2, or Tracks 1 and 2 data. What 4Go returns in this case depends on the Emulation Mode for Manual Entry settings in Lighthouse Transaction Manager.

†The TrueToken should be sent in the field UniqueID.

Requirement: MSR devices used with 4Go must not have a carriage return between the track data.