Join us for treats
Thursday, Month Day,
at 3:00 p.m. in the kitchen.

Installation and Configuration Guide
Overview

The Universal Transaction Gateway® (UTG®) encrypts and securely transmits transaction data from interfaced merchant systems (POS, property management, e-commerce shopping cart, etc.) directly to Lighthouse Transaction Manager using Shift4’s proprietary Derived Unique Key Per Transaction with Moving Target Encryption (DUKPT w/MTE). The UTG is a small application that is installed on the merchant’s computer network that facilitates connectivity to Shift4’s data centers. It is proprietary Virtual Private Network (VPN) software that protects the transport of sensitive financial data from interfaced systems to the Lighthouse Transaction Manager system. It performs assured delivery, controls the most favorable route for transactions, and controls various smaller devices. You can also control various devices connected to the workstation (POS terminal) to offer online debit transactions, check verification, and electronic signature capture capabilities.

The UTG Installation and Configuration Guide

This version of the UTG Installation and Configuration Guide coincides with UTG release 2300 and provides the basic instructions for security, system preparation, installation and basic configuration of the UTG and Stub. For details on external devices, see the Using External Devices document.

Authorization Flow with the UTG

The following example shows the credit card authorization flow with the UTG in place:

1. The point-of-sale (POS) or property management system (PMS) initiates a non-debit transaction with the UTG.
2. The authorization transaction is encrypted by the UTG using DUKPT w/ MTE.
3. The authorization transaction is sent over the Internet or WAN to Shift4’s processing center running Lighthouse Transaction Manager.
4. The authorization request is stored in the Lighthouse Transaction Manager database.
5. The transaction is sent to the bank card processor for authorization.
6. The authorization response is sent from the processor to Lighthouse Transaction Manager.
7. The authorization response is saved in the Lighthouse Transaction Manager database.
8. The authorization response is encrypted by Lighthouse Transaction Manager using DUKPT w/ MTE.
9. The authorization response is sent to the UTG over the Internet.
10. The transaction response is sent back to the POS.
Product Support

Web: The website at www.shift4.com provides access to the Shift4 FAQ page, where answers to general and technical questions regarding the entire Shift4 product line are available. The Shift4 website at www.shift4.com offers technical notes 24 hours a day, 7 days a week, 365 days a year.

Live Support: Information about troubleshooting techniques and handling special problems that may occur during installation or configuration can be obtained by contacting the 24/7 Shift4 Support department at 702.597.2480, option 2.

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

Security and UTG

To ensure the UTG is installed, configured, and operating in a secure manner and environment that is compliant with PCI DSS standards, you must read the following documents:

- UTG PA-DSS Implementation Guide
- UTG Installation and Configuration Guide
- The latest version of the PCI DSS documentation at www.pcisecuritystandards.org

---

**Warning!** For security implementation and best practices, see the 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 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* (defined in this document). 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.
UTG Usage Configuration Examples

There are three common usage scenarios for UTG installations pictured below. The preferred method is to install the UTG on every POS/PMS terminal. There are several reasons why this is the best scenario. First, with a UTG on every terminal, the communication never has to leave the terminal before being encrypted. This is the ultimate way to protect cardholder data. Second, with a UTG on every terminal, if one of the terminals goes down, the rest of the system is not affected. Third, with a UTG on every terminal, the speed of the transaction may be enhanced since communication between the terminal and the UTG does not have to occur over the network.

There are two other common methods of UTG installation. One method is to install a UTG on one of the POS/PMS terminals and install a UTG Stub on the other terminals with PIN pads in the area. See the Stub section for more information.
The other common method of UTG installation is to install a UTG on the POS/PMS server or a dedicated PC behind the network firewall and install a UTG Stub on any of the POS/PMS terminals with a PIN pad device.

If you are using a Point-to-Point (P2PE) PIN pad, it can be connected directly to the server with the UTG, using an Ethernet connection.
High Availability Installation Considerations

Installing multiple UTG’s provides a number of benefits including the following:

- The ability to handle larger loads
- High-availability
- The ability to perform rolling maintenance

However, there are some factors to consider with multiple UTG installations:

If you are not using 4Go or UTG-controlled PINPads:

- You can deploy as many UTG instances as you want behind the load balancer. Any UTG can handle the requests as long as the correct data is being transferred, which would be a requirement for normal processing as well. The Load Balancer will be responsible for ensuring that the origins and destinations are kept in line with each other.
- You can distribute the load with various solutions such as physical load balancers, software load balancing, DNS, or whatever you are comfortable with. Shift4 does not advocate one method over the other, so long as the factors listed here are kept in mind.

If you are using 4Go:

- 4Go must hit the same instance of UTG that the POS/PMS hits.
- Your configuration must ensure that each instance of POS and 4Go is mapped to the same instance of UTG. If they do not match, the UTG will not have the initial authorization request.
- The recommended best practice is to install UTG on every terminal that uses 4Go. This is inherently a load balanced solution, as every end-point has a UTG assigned to it.

If you are using UTG-controlled PINPads:

- Each PINPad must be paired with a UTG. This is because the UTG broadcasts to the device and while one UTG can service multiple devices, each device cannot be serviced by multiple UTGs.
- The recommended best practice is to install UTG on every terminal that uses a device. Again, this is inherently a load balanced solution, as every end-point has a UTG assigned to it.

If you are using EMV:

- This will be under the same scope as using UTG-controlled PINPads.
Examples of High Availability Configurations

Below are two examples of configuring your UTG installation for high availability.

1. The first example uses 3rd party load balancing software as part of the POS/PMS system.
2. In the second example, 3rd party load balancing hardware devices are used.

Both application delivery systems can use methods such as “round robin,” “least connections,” and “fastest response” to maximize availability.

In this example a load balancer is used to distribute the load.
Installing UTG

Shift4 provides an installer file containing the Universal Transaction Gateway (UTG) files required for installation. Follow the steps in this chapter to install the UTG.

**WARNING!** Any prior versions of the UTG will be disabled once the current version of the UTG is installed on your machine. However, the previous settings of the UTG TuneUp will be retained.

Preparing for Installation

This section covers the infrastructure required to install and run the Shift4 UTG application and should be reviewed carefully. Contact the Shift4 Installations department to schedule the installation at 702.597.2480, option 4. The installation may be delayed if all items discussed in this section are not in place at the time of installation.

**Note:** Merchants, not Shift4, are responsible for magnetic card readers (MSRs or wedges), servers, terminals, external devices (PIN pads), network infrastructure, and the computer on which the UTG is installed.

System Specifications

To ensure a smooth installation process, the system should meet the following minimum requirements:

- Processor equal to Intel Pentium III, Intel Celeron, AMD Athlon, or newer
- Minimum 800 MHz processor speed
- Minimum 256 Megabytes RAM
- Minimum 40 Gigabytes Hard Drive
- Minimum 10/100 Megabit Network Interface Card
- Shift4-supported Windows operating system with appropriate service packs and security updates (See the bulleted list below for supported versions of Windows)
- Static internal IP address per UTG

Higher volume merchants may require a more powerful system.
Operating System Requirements

Verify that the PC chosen to run the UTG is using a supported Windows operating system with the appropriate service packs and security updates installed. The supported Windows operating systems are listed below.

---

**Important:** When installing a UTG, if US English is not selected as the language in Microsoft® Windows, the UTG may not function as designed.

---

Windows Requirements

The user account for the UTG must have full rights to the Shift4 UTG installation directory.

The UTG will be installed as a Service under the Local System account. If you are running UTG as a service, this should be changed in Windows services to an account that is securely locked down.

To change from the Local System account to a more secure account, complete the following steps:

1. From the Start menu, select **Control Panel > Administrative Tools > Services**.
2. Double-click the **Shift4 UTG2** service.
3. On the **Log On** tab, select **This account** and configure a different account with the full rights to the Shift4 UTG installation directory.
Windows Firewall

Shift4 conforms to the strictest security requirements. For security reasons, both the UTG and the UTG Stub must be installed on a machine behind a firewall. However, because a firewall restricts communication between your computer and the Internet, it is necessary to adjust the settings for the UTG or the UTG Stub so it can communicate through the Windows firewall. Listing the UTG or the UTG Stub as an exception will accomplish the task. If the UTG or the UTG Stub (if you are using UTG Stub) is not listed, you will need to add them to the exception list.

Supported Windows Operating Systems

**Note:** UTG will work in a 64-bit or 32-bit environment. UTG can also operate in a virtualized environment.

- Microsoft® Windows 10
- Microsoft® Windows 2016 Server
- Microsoft® Windows 2012 Server
- Microsoft® Windows 8
- Microsoft® Windows 2008 Server
- Microsoft® Windows 7
- Microsoft® Windows Vista

**WARNING!** Unless used with True P2PE™, installing the UTG on a non-supported operating system is a violation of PCI DSS Requirement 6.2 and may also render your systems more vulnerable to a security breach.

**Tip:** To stay fully compliant with security standards, as well as ensure machine stability while running the UTG, make sure you keep the machine up to date with the latest Windows updates.

Interface Requirements

The UTG communicates with external devices (such as PIN pads and signature capture devices) in conjunction with POS/PMS systems, or other systems through various API connectivity methods. Before installation, verify that all interfaces are listed as Shift4 certified on the Shift4 Partners web page [https://www.shift4.com/our-software-hardware-partners/](https://www.shift4.com/our-software-hardware-partners/). Not all interfaces are listed on the web page. If your interface is not listed, call Shift4. Verify that all interface drivers are completely loaded and current.
**Internet Connectivity Requirements**

For security reasons, an internal static IP address is required on every machine with the UTG installed. In addition, because of Card Association Security Requirements, the UTG must be installed on a machine that is protected behind a firewall. It is the merchant’s responsibility to configure static IP addresses or networks.

---

**Note:** If you are in a DHCP environment, you can reserve an IP address to make it appear static.

---

Connecting to Shift4’s data center requires outbound connections to TCP/IP ports 26880 and 26881. Configure the firewall for a pool of established, resultant, server, or ephemeral traffic across these ports to successfully connect. The exact name for the ephemeral type of resultant connection depends on the firewall’s naming conventions. Specifically defined inbound connectivity policies are not required.

---

**Warning!** If you have multiple Internet connections, you need to have a way to switch between connections. UTG does not automatically switch to an alternate Internet connection.

---

**Warning!** When the term SSL is used throughout this document, it should be interpreted as the newest version of TLS. In accordance with the PCI Data Security Standard, all versions of SSL and TLSv1.0 are no longer considered “strong encryption” and should never be used for non-console access to card data environments through public networks or to transport card data over public networks. Shift4 offers the option to use SSL and TLSv1.0 due to system incompatibility issues with legacy PMS/POS systems, but it should only be considered a temporary fix. If SSL or TLSv1.0 must be used, it should only be used inside protected, non-public networks. For more information see: https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf
CPU Utilization

If you experience high CPU utilization for a UTG, see the information below:

The UTG writes a large amount of log information for troubleshooting. It also securely wipes those files after encrypting and compressing them. Those operations can consume a significant amount of CPU time. Below are some ways to reduce the associated resource requirements:

1. Set the “Bytes Each” parameter to a larger size. UTG default size is 20 MB. This means that as soon as the trace file reaches that size, it will roll over and create a new file. When the number of trace files specified in the “Max Files” setting in the UTG is reached, it will add the oldest file to a queue that is then encrypted, compressed, and then securely wiped. The UTG then also starts a new file for the current trace. Increasing that size may reduce your CPU utilization because it is more efficient to do this roll over less frequently, even though the files are larger.

2. You may also want to consider excluding files with a .trc extension from your antivirus tool because antivirus tools also consume CPU time monitoring those files as they are written, compressed, encrypted, and securely wiped. Additionally, if the Antivirus has those files locked, the UTG may not be able to complete the process described above.

3. If you are using Trend Micro, there are publically known issues with resource utilization. Excluding .trc files, may mitigate some of those issues. Also, if you are running UTG on a VM and Trend Micro is monitoring the VHD files for the VM, that can cause high CPU usage independent of UTG. There are several sites describing related problems and solutions in more detail such as: https://success.trendmicro.com/solution/1059182.

**Warning!** Shift4 will not be responsible for any actions taken related to antivirus tools and settings. The merchant is responsible for understanding and applying any suggestions offered above.

Gathering Configuration Data

Refer to the Customer Configuration Report from Shift4 prior to proceeding with the installation. If you have not received the report or do not have all the needed information, contact the Shift4 Installations department. Record or have the following information available:

- Serial number
- Slot number

**Note:** If you are using an interface that is not using an Access Token(s), then you will also need apiSerialNumber and apiPassword.
Running the Probe Utility to Test Your Internet Connection

**Requirement:** Ports 26880 and 26881 must be configured for outbound traffic in your firewall before UTG installation. If the Shift4 Probe utility runs successfully, the ports are configured properly.

The Shift4 Probe utility tests the system’s connection to Shift4. You must run the Shift4 Probe utility prior to installing the UTG. To run the Shift4 Probe utility complete the following steps:


2. Click Open.

3. Double-click **s4Probe.exe** and click **Run**.

4. Click Next.

5. Verify that Connect to Lighthouse Transaction Manager via Internet using Normal Route is selected under Available Items. The Server, Port, and Route Code fields will fill in automatically.

6. If connecting to the test server, change the server name to ns.shift4test.com.

7. Click Next.

8. Click Test. The test result should read SUCCESS. A Score other than 0 indicates a communication problem between your system and Shift4. This may take some time.
9. Review the Results window.
The Results window will open and display the route scores. A max score is set up to determine the quickest and most reliable routes to the Shift4 data centers. The optimal score is 0; a score other than 0 indicates a communications problem on some level. The UTG will select routes with the best scores and use those routes at random.
If you think there might be a Shift4 communication issue, call the Shift4 Support department at 702.597.2480, option 2.

10. Click Close to exit.

**Downloading the UTG**
To download the UTG complete the following steps:

2. In the Downloads window, the name and location should read UTG2setup.exe and https://myportal.shift4.com/downloads/utg2setup.exe. Click UTG2setup.exe and then click Run to continue.

3. On the next window, the file name and publisher should read Universal Transaction Gateway (UTG) for DOLLARS ON... and Shift4 Corporation. Click Run.
Installing the UTG

If you have any questions during the installation, contact the Shift4 Support department at 702.597.2480, option 2.

To install the UTG, complete the following steps:

1. In the Universal Transaction Gateway Setup Installation Wizard window, click **Next**.

2. In the Read the license agreement section, review the terms and conditions and click **Next** to indicate you accept the license agreement.
3. Under Choose folder, choose the folder in which you would like UTG2 to be installed, or click **Next** to install the updated UTG files in the default Shift4 folder.

4. In the Universal Transaction Gateway Setup screen, click **Next**.
5. In the Universal Transaction Gateway Setup screen, you have the option to select Run Universal Transaction Gateway TuneUp now. If selected, UTG TuneUp will open when the installation is complete. Click Finish to complete the installation process.

6. In the Confirm screen, click Yes.

7. Configure the UTG. See Configuring UTG in this document.
Configuring UTG

The Universal Transaction Gateway TuneUp application is used to configure UTG settings, including interface and external devices settings, communicating with the Shift4 data centers, and selecting advanced parameters. This guide provides basic configuration for TCP/IP, HTTP, TCP/IP SSL, HTTP SSL, and UTG4Cloud interfaces. For other interface types or if you have any questions on the configuration process, contact the Shift4 Support department at 702.597.2480, option 2.

**Requirement:** If the UTG is running, you must shut it down before you can configure the UTG TuneUp settings.

**Configuring UTG TuneUp Settings Overview**

To configure the Universal Transaction Gateway TuneUp complete the following steps:

1. If the UTG is running, shut it down:
   - To shut down UTG Standalone, select **File > Exit** and click **Yes** when prompted to confirm shut down.
   - If UTG Standalone is in use, it may be necessary to select Override before clicking Yes.
   - To shut down the UTG service, stop the Shift4 UTG (v2) service from the Windows Services menu.

2. From the Start menu, select **Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp**.

3. In the UTG TuneUp window, configure the settings on each tab as required for your business processes.

4. To save your settings and changes in TuneUp, you must click **Save** on the Universal Transaction Gateway TuneUp screen. Since clicking Save closes TuneUp, you may want to wait until you have made all of your settings before you click **Save**. Click **Save** before closing the UTG TuneUp screen to save all your settings and changes.
Configuring Interfaces

The **API Interfaces** create connections from the UTG to the Interface Vendor system so that transactions can flow back and forth.

---

**Requirement:** You must have all the required information, such as interface connection, port address, device types and names, and other key configuration requirements on hand before you proceed. To configure Interfaces, the UTG Stand Alone must be shut down and the UTG TuneUp must be running.

---

**Requirement:** If you are using VT4 with UTG controlled devices, you must use the HTTP SSL interface for communication between VT4 and UTG.

---

**Note:** If an EMV device is selected, any Offline settings configured in the UTG will be ignored when processing an electronic chip transaction. This is because EMV has its own process for handling transactions in offline scenarios. The terminal and card both have settings to determine whether or not to approve a transaction in this scenario. UTG must honor the card’s decision to approve/decline rather than use the settings in the UTG.

---

Adding a TCP/IP Interface

The TCP/IP interface uses TCP socket communication to connect to the UTG. It optionally provides encryption through the use of a shared secret passphrase. To add a TCP/IP interface complete the following steps:

1. In the Universal Transaction Gateway TuneUp window, click the **API Interfaces** tab and complete the following tasks:
   - Under Interface, click **Add**.
   - From the Add menu, select **TCP/IP**.
2. To configure the new interface complete the following tasks:

- In the Task Description box, type a name that identifies this interface.
- From the Host Address list, select the IP address the interface will listen to for connections.
- In the Port box, type the port number defined by the Interface Vendor system. Default is 17476 (4444 for hex).
- *(Optional)* In the Encryption Passphrase box, type your passphrase. This encrypts traffic across the network if the Interface Vendor system included similar encryption methodology.
- *(Optional)* In the Verify Passphrase box, type your passphrase.
- *(Optional)* To enable Bank ID Number (BIN) management, select Bin Management. In general, merchants prefer to process transactions as debit when the transactions are above a certain amount and as credit when transactions are below that amount. When BIN Management is selected, the BIN Management tool will automatically determine the card type and process the transaction as debit if the amount is above the user defined Floor Limit, or the PIN pad will prompt the consumer to select credit or debit if the dollar amount is at or below that Floor Limit.

**Note:** When Swipe Ahead is used with BIN Management, the Floor Limit set in UTG TuneUp is ignored and BIN Management automatically selects debit if the card is debit capable. If the card is not debit capable, the UTG prompts the cardholder.

- The Bin Management Floor Limit specified is the lowest amount for which the Bin Management function is enabled.
- To enable Stand-in, select Stand-in. See the Configuring Offline Mode section for more information on Stand-in.
The Stand-in Floor Limit specified is the highest amount of an offline transaction without returning a referral. (The default setting is 0.00.)

- Above the Floor Limit, the UTG will return a referral and a Token.
- At or below the Floor Limit, the UTG will return an approval and a Token.

**Note:**
The authorization code received in offline mode is temporary and will be replaced with a permanent authorization code when the UTG is able to connect to the Shift4 data center if the transaction is approved by the processor.

3. *(Optional)* To print a tip line on the receipt when an authorization is performed, select **Print Blank Tip Line on Authorizations**.

4. *(Optional)* To print a tip line on the receipt when a sale is performed, select **Print Blank Tip Line on Sales**.

**Note:** If either **Print Blank Tip Line on Authorizations** or **Print Blank Tip Line on Sales** is selected, the following should be noted:

- If the POS sends the tip amount, the tip line will not print on the receipt.
- If the user enters a tip amount on the PIN pad, the tip line will not print on the receipt.

5. *(Optional)* The Clients option is only used with 4Go. If you are using 4Go, see the **4Go Technical Installation Guide** for more information.

6. Click **OK**.
Adding an HTTP Interface

The HTTP interface, encrypted by the UTG, allows web applications to send traffic to Shift4 with much greater security and reliability than using HTTPS posting directly over the Internet. To add an HTTP interface complete the following steps:

1. In the Universal Transaction Gateway TuneUp window, click the **API Interfaces** tab and complete the following tasks:
   - Under Interface, click **Add**.
   - From the Add menu, select **HTTP**.

2. To configure the new interface complete the following steps:
   - In the Task Description box, type a name that identifies this interface.
   - From the Host Address list, select the IP address the interface will listen to for connections.
   - In the Port box, type the port number defined by the Interface Vendor system. The default is the standard HTTP protocol port of 16448 ($4040 hex).
   - *(Optional)* To enable Bank ID Number (BIN) management, select **Bin Management**. In general, merchants prefer to process transactions as debit when the transactions are above a certain amount and as credit when transactions are below that amount. When BIN Management is selected, the BIN Management tool will automatically determine the card type and process the transaction as debit if the amount is above the user defined Floor Limit, or the PIN pad will prompt the consumer to select credit or debit if the dollar amount is at or below that Floor Limit.

---

**Note:** When Swipe Ahead is used with BIN Management, the Floor Limit set in UTG TuneUp is ignored and BIN Management automatically selects debit, if the card is debit capable. If the card is not debit capable, the UTG prompts the cardholder.
The BIN Management Floor Limit specified is the lowest amount for which the Bin Management function is enabled.

To enable Stand-in, select **Stand-in**. See *Configuring Offline Mode* for more information on Stand-in. The Stand-in Floor Limit specified is the highest amount of an offline transaction without returning a referral. (The default setting is 0.00.)

- Above the Floor Limit, the UTG will return a referral and a Token.
- At or below the Floor Limit, the UTG will return an approval and a Token.

**Note:** The authorization code received in offline mode is temporary and will be replaced with a permanent authorization code when the UTG is able to connect to the Shift4 data center if the transaction is approved by the processor.

---

3. *(Optional)* To print a tip line on the receipt when an authorization is performed, select **Print Blank Tip Line on Authorizations**.

4. *(Optional)* To print a tip line on the receipt when a sale is performed, select **Print Blank Tip Line on Sales**.

**Note:** If either Print Blank Tip Line on Authorizations or Print Blank Tip Line on Sales is selected, the following should be noted:

- If the POS sends the tip amount, the tip line will not print on the receipt.
- If the user enters a tip amount on the PIN pad, the tip line will not print on the receipt.

---

5. *(Optional)* The Clients option is only used with 4Go. If you are using 4Go, see the *4Go Technical Installation Guide* for more information.

6. Click **OK**.
Adding a TCP/IP SSL Interface

The TCP/IP SSL API interface uses TCP socket communication to connect to the UTG. It provides an added layer of security using SSL to secure the local network segment.

To add a TCP/IP SSL interface complete the following steps:

1. From the Start menu, select All Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp.

2. In the Universal Transaction Gateway TuneUp window, click the API Interfaces tab and complete the following tasks:
   - Under Interface, click Add.
   - From the Add menu, select TCP/IP SSL.

3. To configure the new interface complete the following steps:
   - In the Task Description box, type a name that identifies this interface.
   - From the Host Address list, select the IP address the interface will listen to for connections.
   - In the Port box, type the port number defined by the Interface Vendor system. Port 21845 ($5555 hex) is the default setting.
   - (Optional) The Clients option is only used with 4Go. If you are using 4Go, see the 4Go Technical Installation Guide for more information.
Warning! When the term SSL is used throughout this document, it should be interpreted as the newest version of TLS. In accordance with the PCI Data Security Standard, all versions of SSL and TLSv1.0 are no longer considered “strong encryption” and should never be used for non-console access to card data environments through public networks or to transport card data over public networks. Shift4 offers the option to use SSL and TLSv1.0 due to system incompatibility issues with legacy PMS/POS systems, but it should only be considered a temporary fix. If SSL or TLSv1.0 must be used, it should only be used inside protected, non-public networks. For more information see https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

- In the SSL/TLS Minimum Version section, leave the setting at the highest level (TLS 1.2). In accordance with the warning above, if you have temporary incompatibility issues with your POS/PMS, you may move the slider to another SSL/TLS minimum version. The level you choose and all levels listed above that setting will be supported.

- If you select a minimum version that is not secure, the following warning will appear:
4. Select a Certificate Information option. (See Appendix B – Security Certificates for details.)

5. *(Optional)* To enable Bank ID Number (BIN) management, select **Bin Management**.
   In general, merchants prefer to process transactions as debit when the transactions are above a certain amount and as credit when transactions are below that amount. When BIN Management is selected, the BIN Management tool will automatically determine the card type and process the transaction as debit if the amount is above the user defined Floor Limit, or the PIN pad will prompt the consumer to select credit or debit if the dollar amount is at or below that Floor Limit.
   - The Bin Management Floor Limit specified is the lowest amount for which the Bin Management function is enabled.
   - To enable Stand-in, select **Stand-in**. See the Configuring Offline Mode section for more information on Stand-in. The Stand-in Floor Limit specified is the highest amount of an offline transaction without returning a referral. (The default setting is 0.00.)
     - Above the Floor Limit, the UTG will return a referral and a Token.
     - At or below the Floor Limit, the UTG will return an approval and a Token.

   **Note:** The authorization code received in offline mode is temporary and will be replaced with a permanent authorization code when the UTG is able to connect to the Shift4 data center if the transaction is approved by the processor.

6. *(Optional)* To print a tip line on the receipt when an authorization is performed, select **Print Blank Tip Line on Authorizations**.

7. *(Optional)* To print a tip line on the receipt when a sale is performed, select **Print Blank Tip Line on Sales**.
Note: If either Print Blank Tip Line on Authorizations or Print Blank Tip Line on Sales is selected, the following should be noted:

- If the POS sends the tip amount, the tip line will not print on the receipt.
- If the user enters a tip amount on the PIN pad, the tip line will not print on the receipt.

8. Click **OK** on the TCP/IP SSL API window.

### Adding an HTTP SSL Interface

The HTTP SSL interface is a web-based interface. This allows web applications to send traffic to Shift4 with much greater security and reliability than using HTTPS posting directly over the Internet and provides an added layer of security using SSL to secure the local network segment.

To add an HTTP with SSL interface complete the following steps:

1. From the Start menu, select **All Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp.**
2. In the Universal Transaction Gateway TuneUp window, click the **API Interfaces** tab and complete the following steps:
   - Under Interface, click **Add**.
   - From the Add menu, select **HTTP SSL**.

3. To configure the new interface complete the following steps:
   - In the **Task Description** box, type a name that identifies this interface.
   - From the **Host Address** list, select the IP address the interface will listen to for connections.
   - In the Port ($ for hex) box, type the port number defined by the Interface Vendor system. Port 16448 ($4040 hex) is the default setting.
   - *(Optional)* The Clients option is only used with 4Go. If you are using 4Go, see the **4Go Technical Installation Guide** for more information.

---

**Warning!** When the term SSL is used throughout this document, it should be interpreted as the newest version of TLS. In accordance with the PCI Data Security Standard, all versions of SSL and TLSv1.0 are no longer considered “strong encryption” and should never be used for non-console access to card data environments through public networks or to transport card data over public networks. Shift4 offers the option to use SSL and TLSv1.0 due to system incompatibility issues with legacy PMS/POS systems, but it should only be considered a temporary fix. If SSL or TLSv1.0 must be used, it should only be used inside protected, non-public networks. For more information see [https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf](https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf)
- In the SSL/TLS Minimum Version section, leave the setting at the highest level (TLS 1.2). In accordance with the warning above, if you have temporary incompatibility issues, you may move the slider to another SSL/TLS minimum version. The level you choose and all levels listed above that setting will be supported.

![](image1.png)

- If you select a minimum version that is not secure, the following warning will appear:

![](image2.png)

4. Select a Certificate Information option. (See Appendix B – Security Certificates for details.)

5. *(Optional)* To enable Bank ID Number (BIN) management, select **Bin Management**.
   In general, merchants prefer to process transactions as debit when the transactions are above a certain amount and as credit when transactions are below that amount. When BIN Management is selected, the BIN Management tool will automatically determine the card type and process the transaction as debit if the amount is above the user defined Floor Limit, or the PIN pad will prompt the consumer to select credit or debit if the dollar amount is at or below that Floor Limit.

- The Bin Management Floor Limit specified is the lowest amount for which the Bin Management function is enabled.
• To enable Stand-in, select Stand-in. See the Configuring Offline Mode section for more information on Stand-in. The Stand-in Floor Limit specified is the highest amount of an offline transaction without returning a referral. (The default setting is 0.00.)
  o Above the Floor Limit, the UTG will return a referral and a Token.
  o At or below the Floor Limit, the UTG will return an approval and a Token.

Note: The authorization code received in offline mode is temporary and will be replaced with a permanent authorization code when the UTG is able to connect to the Shift4 data center if the transaction is approved by the processor.

6. (Optional) To print a tip line on the receipt when an authorization is performed, select Print Blank Tip Line on Authorizations.

7. (Optional) To print a tip line on the receipt when a sale is performed, select Print Blank Tip Line on Sales.

Note: If either Print Blank Tip Line on Authorizations or Print Blank Tip Line on Sales is selected, the following should be noted:
  • If the POS sends the tip amount, the tip line will not print on the receipt.
  • If the user enters a tip amount on the PIN pad, the tip line will not print on the receipt.
8. Click **OK** on the HTTP with SSL window.
Adding a REST Interface

The REST interface provides a simple integration using standard REST calls. The REST interface currently supports TLS 1.2 only. The REST API is only available for UTG version 3001 and above. See the requirement below.

To add a REST interface complete the following steps:

1. From the Start menu, select All Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp.

2. In the Universal Transaction Gateway TuneUp window, click the API Interfaces tab and complete the following tasks:
   - Under Interface, click Add.
   - From the Add menu, select REST.

3. To configure the new interface complete the following steps:
   - In the Task Description box, type a name that identifies this interface.
   - From the Host Address list, select the IP address the interface will listen to for connections.
   - In the Port box, type the port number defined by the Interface Vendor system. Port 277 ($0115 hex) is the default setting.
• *(Optional)* The Clients option is only used with 4Go. If you are using 4Go, see the 4Go Technical Installation Guide for more information.

![Certificate Generation](image)

• In the Certificate Information section you are provided with two certificate options. You can either use a valid, signed CA, or you can use the Shift4 Certificate Generator to build a certificate.
  
  o To Use the Shift4 Certificate Generator to build your own certificate, complete the following steps:
    
    ▪ In the Certificate Information section, click **Generate Certificate**.
    ▪ In the Shift4 Certificate Generator window, enter the information for all required fields and any desired optional fields. The required fields include the following:
      
      ▪ **Subject Common Name** – Enter a name for the certificate.
      ▪ **Organization**
      ▪ **Locality** – Location City.
      ▪ **State/Province** – Location State
      ▪ **Country** – Location country
      ▪ The IP address(es) the UTG will listen on for the REST Interface
      ▪ Select **SelfSigned** in the CA Self Signed/Intermediate section
      ▪ Select **Server Authentication**
      ▪ Select **Client Authentication**
      ▪ Select **CRT** – The CRT extension is used for certificates.
      ▪ Select **Embed Key**
      ▪ Enter a **Password** for the certificate. You will need this password during the installation.
      
      ▪ Set the valid cert dates in the Dates section. This is the amount of time the certificate can be used before having to be renewed.
        
        ▪ **From** – The date the certificate will go into effect.
        ▪ **To** – The date the certificate will no longer be accepted and must be renewed.
      
      ▪ **Select a Key Size:**
        
        ▪ **2048 bit**: In general, requests using this certificate will be faster.
- 4096 bit: In general, requests using this certificate will be more secure but slower.
  - Click **Generate**.

- Select a location to store the certificate and click **Save**.
- Close the Shift4 Certificate Generator
  - In the REST window, under Certificate File, select **Browse**.
  - Select **All Files** as the file type.
  - Locate the certificate you just generated.
  - Click **Open**.
- In the Certificate Password section, enter the certificate password you entered when creating the new certificate.
• **(Optional)** To enable Bank ID Number (BIN) management, select **Bin Management**.

In general, merchants prefer to process transactions as debit when the transactions are above a certain amount and as credit when transactions are below that amount. When BIN Management is selected, the BIN Management tool will automatically determine the card type and process the transaction as debit if the amount is above the user defined Floor Limit, or the PIN pad will prompt the consumer to select credit or debit if the dollar amount is at or below that Floor Limit.

  o The Bin Management Floor Limit specified is the lowest amount for which the Bin Management function is enabled.
  
  o To enable Stand-in, select **Stand-in**. See the *Configuring Offline Mode* section for more information on Stand-in. The Stand-in Floor Limit specified is the highest amount of an offline transaction without returning a referral. (The default setting is 0.00.)
    
    ▪ Above the Floor Limit, the UTG will return a referral and a Token.
    ▪ At or below the Floor Limit, the UTG will return an approval and a Token.

---

**Note:** The authorization code received in offline mode is temporary and will be replaced with a permanent authorization code when the UTG is able to connect to the Shift4 data center if the transaction is approved by the processor.

---

• Click **OK** on the REST with window.
Adding a UTG4Cloud Interface

Add a UTG4Cloud® interface to the locally installed UTG of any property that will be using a cloud-based POS/PMS. The cloud-based POS/PMS will use a standard HTTP or TCP interface based on their communication protocol. The UTG4Cloud API is added at the local property’s UTG. For more information, see Appendix A - Using a Cloud-Based POS/PMS With Shift4’s Universal Transaction Gateway (UTG).

To add a UTG4Cloud API complete the following steps:

1. From the Start menu, select All Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp.

2. In the Universal Transaction Gateway TuneUp window, click the API Interfaces tab and perform the following steps:
   - Under Interface, click Add.
   - From the Add menu, select UTG4Cloud.

3. To configure the new interface, complete the following steps:
   - In the Task Description field, enter a name that identifies this interface.
   - From the Host Address list, select the IP address the interface will listen to for connections.
   - In the Port field, enter the port number defined by the Interface Vendor system [The default is 13107 ($3333 hex)].
• From the Transport Format list, select **Http** (Tcp is for future use).

![UTG4Cloud API](image)

• *(Optional)* The Clients option is only used with 4Go. If you are using 4Go, see the *4Go Technical Installation Guide* for more information.

---

**Note:** If you are configuring a UTG4Cloud interface, it is not advisable to select the Convert Communication Errors to Referrals option when configuring the Advanced tab. See the *Configuring Advanced Parameters* for more information.

---

**Adding a UTG4Cloud SSL Interface**

Add a UTG4Cloud SSL API to the locally installed UTG of any property that will be using a cloud-based POS/PMS. The cloud-based POS/PMS will use a standard HTTP or TCP interface based on their communication protocol. The UTG4Cloud SSL API is added at the local property UTG. For more information, see *Appendix A - Using a Cloud-Based POS/PMS With Shift4’s Universal Transaction Gateway (UTG)*.

To add a UTG4Cloud SSL API Interface complete the following steps:

1. From the Start menu, select **All Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) TuneUp**.

2. In the Universal Transaction Gateway TuneUp window, click the **API Interfaces** tab and perform the following steps:
   
   • Under Interface, click **Add**.
• From the Add menu, select UTG4Cloud SSL.

![Universal Transaction Gateway Interface]

3. To configure the new interface, complete the following steps:
   • In the Task Description field, enter a name that identifies this interface.
   • From the Host Address list, select the IP address the interface will listen to for connections.
   • In the Port field, enter the port number defined by the Interface Vendor system [The default is 13107 ($3333 hex)].
   • From the Transport Format list, select Http (Tcp is for future use).

---

**Warning!** When the term SSL is used throughout this document, it should be interpreted as the newest version of TLS. In accordance with the PCI Data Security Standard, all versions of SSL and TLSv1.0 are no longer considered "strong encryption" and should never be used for non-console access to card data environments through public networks or to transport card data over public networks. Shift4 offers the option to use SSL and TLSv1.0 due to system incompatibility issues with legacy PMS/POS systems, but it should only be considered a temporary fix. If SSL or TLSv1.0 must be used, it should only be used inside protected, non-public networks. For more information see [https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf](https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf)
• In the SSL/TLS Minimum Version section, leave the setting at the highest level (TLS 1.2). In accordance with the warning above, if you have temporary incompatibility issues, you may move the slider to another SSL/TLS minimum version. The level you choose and all levels listed above that setting will be supported.

• If you select a minimum version that is not secure, the following warning will appear:

4. *(Optional)* The Clients option is only used with 4Go. If you are using 4Go, see the 4Go Technical Installation Guide for more information.

5. Select a Certificate Information option. (See Appendix B – Security Certificates for details.)
An example of the message generated by a user entering incorrect or invalid data is provided below.

![Message example](image)

6. When you have finished making all your selections, click **OK** on the UTG4Cloud SSL API window.
7. Click **Save** on the Universal Transaction Gateway TuneUp screen.

**Security Certificate Considerations for UTG4Cloud SSL Interfaces**

By default, the UTG generates a self-signed SSL certificate, which can cause an issue for vendors that are communicating with the UTG4Cloud SSL interface because the browser will be expecting a Certificate Authority (CA) signed certificate. There are several ways to resolve this issue:

1. You can act as your own CA by issuing your own root certificate and importing this certificate into the certificate stores of all of the browsers. This would then allow you to issue individual certificates for each UTG and sign them yourself, bypassing the cost of getting each one signed by a separate CA. You could also use this in conjunction with a wildcard certificate, if a subset of your systems is all on the same domain.

2. Obtain a CA signed wildcard certificate for a fixed domain for all of your locations. This will allow you to use a single certificate for all of your locations, but will require all of the UTG systems to be on the same domain.

3. Obtain a separate CA-signed certificate for each UTG instance. This could be a time-consuming and expensive process, especially if you are implementing a per-terminal UTG setup.

---

**Note:** If you are configuring a UTG4Cloud interface, it is not advisable to select the Convert Communication Errors to Referrals option when configuring the Advanced tab. See the *Configuring Advanced Parameters* for more information.
Adding an Oracle Payment Interface (OPI)

**Requirement:** The Oracle Payment Interface (OPI) version must be 6.1.1.14 or higher. If you are not certain what OPI version you are currently on, consult your OPI installer.

To add an Oracle API interface complete the following steps:

1. In the Universal Transaction Gateway TuneUp window, click the API Interfaces tab and complete the following tasks:
   - Under Interface, click **Add**.
   - From the Add menu, select **Oracle Payment Interface (OPI)**.

   ![Image of Universal Transaction Gateway TuneUp window](image)

   **Note:** Only one Oracle Payment Interface (OPI) can be configured per UTG. If an OPI has already been configured, the OPI option will be gray and unavailable.

2. To configure the new interface complete the following steps:
   - In the Task Description box, type a name that identifies this interface.
   - From the Host Address list, select the IP address the interface will listen to for connections.
   - In the Port box, type the port number defined by the Interface Vendor system. The default is 8084 (1F94 hex).
• (Optional) To enable Bank ID Number (BIN) management, select Bin Management. In general, merchants prefer to process transactions as debit when the transactions are above a certain amount and as credit when transactions are below that amount. When BIN Management is selected, the BIN Management tool will automatically determine the card type and process the transaction as debit if the amount is above the user defined Floor Limit, or the PIN pad will prompt the consumer to select credit or debit if the dollar amount is at or below that Floor Limit.

Note: When Swipe Ahead is used with BIN Management, the Floor Limit set in UTG TuneUp is ignored and BIN Management automatically selects debit, if the card is debit capable. If the card is not debit capable, the UTG prompts the cardholder.

- The BIN Management Floor Limit specified is the lowest amount for which the Bin Management function is enabled.
- To enable Stand-in, select Stand-in. See Configuring Offline Mode for more information on Stand-in. The Stand-in Floor Limit specified is the highest amount of an offline transaction without returning a referral. (The default setting is 0.00.)
  - Above the Floor Limit, the UTG will return a referral and a Token.
  - At or below the Floor Limit, the UTG will return an approval and a Token.

Note: The authorization code received in offline mode is temporary and will be replaced with a permanent authorization code when the UTG is able to connect to the Shift4 data center if the transaction is approved by the processor.

3. (Optional) To print a tip line on the receipt when an authorization is performed, select Print Blank Tip Line on Authorizations.

4. (Optional) To print a tip line on the receipt when a sale is performed, select Print Blank Tip Line on Sales.

Note: If either Print Blank Tip Line on Authorizations or Print Blank Tip Line on Sales is selected, the following should be noted:
- If the POS sends the tip amount, the tip line will not print on the receipt.
- If the user enters a tip amount on the PIN pad, the tip line will not print on the receipt.
5. *Optional* If you don’t want a receipt to be printed when performing a sales completion, select **Suppress Sales Completion Receipts**.

6. *Optional* The Clients option is only used with 4Go. If you are using 4Go, see the *4Go Technical Installation Guide* for more information.

7. Click **OK**.

---

**OPI Mapping in the UTG**

Once an Oracle interface has been configured and saved in TuneUp, you will need to Map the OPI Site ID to an Access Token in the UTG Stand Alone. To map the OPI, complete the following steps:

1. Start the UTG Stand Alone.
2. From the menu, click **OPI Mapping**
3. In the Oracle Payment Interface Site Id Mapping section, click **Add**.
4. In the Site Id field, enter the Site ID configured in OPI.

5. In the Description field, enter a description for the revenue center that will be easy to distinguish if multiple OPI maps are configured.

6. In the Auth Token field, enter the auth token generated in Lighthouse Transaction Manager.
   - Log in to Lighthouse Transaction Manager as the **Account Administrator** (only the Account Administrator can perform this function) and generate an auth token for the desired vendor and select **Oracle Payment Interface** from the Application list. For more information on generating an auth token, see the Appendix B – API Settings section of the Account Administrator Guide in Lighthouse Transaction Manager Help.

7. Click **OK**.

   It is also possible to map multiple site maps at one time by creating a simple text file containing a tab separated list of items where each item contains a Site ID, Description, and Auth Token. For example:

   ![Image of Notepad with site IDs and auth tokens]

   To import a file containing site maps, complete the following steps:
   1. Click **Import** in the Oracle Payment Interface Site Id Mapping section.
   2. Click **Load** and locate the text file containing the tab separated site mapping.
   3. Select the site mapping file and click **Open**.
   4. Click **Process** to import the site mapping data.

**Configuring Devices**

---

**Note:** If an EMV device is selected, any Offline settings configured in the UTG will be ignored when processing an electronic chip transaction. This is because EMV has its own process for handling transactions in offline scenarios. The terminal and card both have settings to determine whether or not to approve a transaction in this scenario. UTG must honor the card’s decision to approve/decline rather than use the settings in the UTG.
On the Devices tab, you will notice Limit Simultaneous Downloads. This setting is useful when you are using the auto form loading feature, as it limits the number of devices that will receive downloads at one time and prevents overloading. The default is 3. To enter a different number, complete the following steps:

1. Enter a number between 1 and 10.
2. Click Save.

It is necessary to configure devices when using a PIN pad. To configure devices complete the following steps:

1. In the Universal Transaction Gateway TuneUp window, click the Devices tab.
2. Under Device, click Add.

**Note:** If you have UTG installed on each terminal, you have to configure each UTG individually for each device.
RS-232 Connection Settings

An RS-232 connection is used if the device is directly connected to the UTG machine. To configure the device information for an RS-232 connection complete the following steps:

1. In the Device Name box, type a unique name that will identify this device. Do not enter a device name that has already been used. This will result in overwriting the previous device settings and only one device will be configured.

2. From the Device Type list, select the payment device. See Appendix C for a list of devices in UTG TuneUp.

3. In the API Terminal ID field, enter a terminal ID specific to the payment device. See the API Terminal ID note below for more information.
**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 POS/PMS provider. Shift4 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.

4. From the Connection box, select **RS-232**.

5. In the Timeout field, type or select a time in seconds. This is the amount of time in seconds (per screen) that the UTG will wait before returning a No input from customer error. The recommended time for most devices is 30 seconds. The set time is doubled for swipe/manual entry screens to allow time for manual data entry.

6. From the Port list, select the port to which the device is connected.

   - If you are only configuring one USB connected device for this UTG, you can select Auto from the Port list. If Auto is selected, the UTG will automatically search for the COM port assigned to the device. This makes finding and selecting the Windows assigned COM port unnecessary. The auto setting cannot be used for multiple devices on the same UTG or for serial connected devices. If you decide later to add more devices to the UTG, you will need to edit the original device configuration and select the actual COM port to which it is connected.

   **Important:** If you are using Ingenico devices with Windows 7, the Ingenico device driver must be version 3.14 or later in order to use the Auto setting.

   **Note:** If your device is shipped with a USB connection, you will need to virtualize the COM port using the driver supplied by the manufacturer.

7. From the Baud Rate list, select the connection speed as indicated by the device manufacturer. (See the Using External Devices guide for more information.)

8. If Manual Card Entry is enabled and available for the selected device, choose one of the following:

   - If Manual Card Entry is not desired, clear the Enable MCE option.
   - If Manual Card Entry is desired, to configure the selected device for Manual Card Entry, complete the following steps:
     - Select **Enable MCE**.
Select the desired setting for Card Security Code (CVV), Street Number, and Zip Code. Required is the default setting.

- **(If applicable)** To configure the Minimum Digits and Maximum Digits that can be entered on a payment device, complete the following steps:
  - In the Minimum Digits field, enter the minimum number of digits that can be entered on the payment device.
  - In the Maximum Digits field, enter the maximum number of digits that can be entered on the device.
  
  For example, if you want to restrict the number of digits entered to 20 digits, enter or select **20** in the Minimum Digits field and then enter or select **20** in the Maximum Digits field.

- **(If applicable)** To configure the BIN Range Overrides, complete the following steps:
  - Click **BIN Range Overrides**.
  - Enter the beginning six digit BIN in the Starting Range field.
  - Enter the ending six digit BIN in the Ending Range field.
  - Enter the Min PAN length.
  - Enter the Max PAN Length.

  **Note:** If your card ranges are always 16 digits, enter 16 for the Min PAN Length and 16 for the Max PAN Length.

Select all of the parameters that will be bypassed from the following list:
- Bypass CVV (Card security code)
- Bypass Exp Date (Card expiration date)
- Bypass Luhn (Luhn mod 10 check)
- Bypass Street
- Bypass Postal Code

**Important:** If your card range will not pass the Luhn mod 10 check, be sure to select **Bypass Luhn**.

- Click **Add**.
- **(If applicable)** Add additional ranges. (Up to nine ranges may be configured.)
9. If Additional Options are enabled for your selected device, complete the following steps:

- *(If applicable)* Enter a Line Length. This is the length of the text line on the device before wrapping the text.
- *(If applicable)* Enter a Beep Volume. This is the volume level the device will beep for actions, such as pressing a button, or EMV card removal prompt. Enter any number between 0 and 100 considering the following:
  - Entering 0 = volume off
  - Entering 100 = full volume
- *(If applicable)* Enter a Debit Key Index number. Ingenico Telium RBA devices have the ability to be injected with up to five keys. This allows the same device to be used for multiple processors. Debit Key Index 0, 1, 2, 3, and 5 are available. Debit Key Index 4 is reserved for P2PE keys. If you are using an Ingenico Telium RBA device and know the desired Debit Key Index, enter the number. The default is 0.
- *(If applicable)* Enter an Amex Key Index number to support using a different key slot for the Online PIN key when processing an Amex EMV card.
- *(If applicable)* Enter the Source Serial Number. This option is used if the device is going to be processing transactions under a different serial number than the one configured for the UTG on the Express tab.
  - For Example, if a merchant has a single UTG configured under SN 1, a device configured under SN 2 and another device configured under SN 3, the terminal download process would work for both of the devices even though they are under different serial numbers from the UTG.
- *(If applicable)* Select the default language to be displayed on the device. The current options include:
  - English
  - Spanish
  - French
- *(If applicable)* Select the Default Receipt language. Currently, this is only for configuring an Ingenico IPP320 CAN. The option sets the receipt language for the merchant copy when using enhanced receipts and both the merchant and customer copy when using non-enhanced receipts. It allows you to set the receipt language to either English or French.
- *(If applicable)* Enter the desired reboot time. The Reboot Time option is provided to satisfy a PCI requirement for devices that are PCI version 4 and above. To satisfy the PCI requirement, the devices must be rebooted every 24 hours. The Reboot Time option allows you to set a convenient time when the device will automatically be rebooted.
  - The Reboot Time setting will be read and set in the device and take effect ONLY after the device has rebooted once after it starts up. The device may or may not automatically reboot after it starts up.
For example, if the reboot time currently set in the device is different than the setting in UTG Tune-up and UTG restarts, the UTG will force the device to reboot once after it starts up. If the device does not reboot after it starts up, you can choose to manually reboot the device or it will reboot automatically based on the reboot time currently set in the device if the reboot flag is enabled in the device.

- The Reboot Time settings will be ignored for RBA PCI version 4 devices with application version below v21.5.6. The full model name for these devices cannot be read by the UTG. Without the full model name, the UTG cannot determine whether the device is PCI version 4 or above. Therefore, the device will automatically reboot every 24 hours based on the reboot time currently set in the device if the reboot flag is enabled in the device.

- **(If applicable)** Contactless Enabled is selected by default for all RBA devices. To disable Contactless, clear the option. Contactless payment systems use radio-frequency identification (RFID) or near field communication (NFC) for making secure payments.

- **(If applicable)** Select **EBT Cash Enabled** to enable the device to be prompted for EBT Cash in an EBT transaction.

- **(If applicable)** Select **EBT Food Enabled** to enable the device to be prompted for EBT Food in an EBT transaction.

- **(If applicable)** Select **Bypass Amount OK** to bypass the amount confirmation screen on the device.

10. **(If applicable)** Private Label cards is discussed in detail in the **Device Options for Private Label Cards** section.

11. **(If applicable)** Click **Cashback** to enable cashback to be prompted on the device.

---

**Requirement:** Cashback must be supported on your POS/PMS for the UTG TuneUp settings to work.

---

- **(Optional)** Edit the amounts and that will be displayed on the device as cashback options:
  - **(Optional)** Edit the First Amount. The default is 20.00.
  - **(Optional)** Edit the Second Amount. The default is 40.00.
  - **(Optional)** Edit the Third Amount. The default is 60.00.
  - **(Optional)** Edit the Fourth Amount. The default is 80.00.
  - **(Optional)** Edit the Maximum Amount. The default is 200.00.

---

**Note:** If Cashback is enabled, the five amounts configured above will be displayed. If you don’t want to display all of the buttons, refer to the Using External Device guide for help.

---

- Click **OK** on the Cashback Parameters window.
12. *(If applicable)* Click **Tip** to configure settings to enable tip to be prompted on the device and complete the following additional steps.

- *(Optional)* Select **Enable Tip** to enable the feature and choose one of the following:
  
  - *(Optional)* Select **No Presets** to disable the preset percentages or amounts and prompt the consumer to enter a tip amount.
  
  - *(Optional)* Select **Percent** and enter up to 4 tip percentages that will be displayed on the PIN pad when prompting for tip.
    
    - In the First Percent field, enter a percent tip option, such as 10.
    
    - In the Second Percent field, enter a percent tip option, such as 15.
    
    - In the Third Percent field, enter a percent tip option, such as 20.
    
    - In the Fourth Percent field, enter a percent tip option, such as 25.

---

**Note:** Percent fields are displayed on the device from left to right. Entering a zero in any of the fields will cause that field to not be displayed on the PIN pad. For example, if you only want to display 3 tip options (10%, 15%, and 20%), you could enter zero in the First Percent field, 10 in the Second Percent field, 15 in the Third Percent field, and 20 in the Fourth Percent field. Only the first three fields would be displayed on the PIN pad.

- *(Optional)* Select **Amount** to enter up to 4 set amounts that will be displayed when prompting for tip.
  
  - In the First Amount field, enter the desired set amount.
  
  - In the Second Amount field, enter the desired set amount.
  
  - In the Third Amount field, enter the desired set amount.
  
  - In the Fourth Amount field, enter the desired set amount.
Note: Amount fields are displayed on the device from left to right. Entering a zero in any of the fields will cause that field to not be displayed on the PIN pad. For example, if you only want to display 3 tip amount options (1, 5, and 10), you could enter zero in the First Amount field, 1 in the Second Amount field, 5 in the Third Amount field, and 10 in the Fourth Amount field. Only the last three fields would be displayed on the PIN pad.

- Click OK.

13. Click OK on the Add Device screen.
Once you have selected one of the listed device types, clicking Private Label brings up the Private Label Prompt window allowing you to customize what will be displayed on the PIN pad device when a customer applies for a private label card. The Private Label Prompt window provides options under the three headings listed below.

**Prescreen Application:**
The Prescreen Application uses the applicant’s postal code to determine the likelihood of the applicant being approved for a private label card based on the average credit rating in postal code entered.

**Prescreen Acceptance Application:**
The Prescreen Acceptance Application indicates a Prescreen Application approval and requests additional information from the applicant to complete a private label application approval.

**Quick Credit:**
The Quick Credit application is an abbreviated individual credit application requiring less applicant information than the full credit application. To be eligible to apply using the Quick Credit process, the applicant must have a major bank card (Visa, MasterCard, American Express or Discover).

**InstantCredit Application:**
The InstantCredit Application is a private label card application based solely on the supplied information, and forgoes any Prescreen Application.

**Pre-Approved:**
The Pre-Approved process starts with an applicant receiving a pre-approved offer in the mail. This offer contains a twelve digit certificate number which associates the applicant with a Pre-Approved offer of credit. The Pre-Approved application requires fewer input data items than the full application.

**Account lookup:**
Account Inquiries allow the merchant to obtain cardholder account information from the cardholder’s Social Security Number (SSN) or SSN and Zip code or SSN and Date of Birth. Inquiries are used when the cardholder does not have their card available at the time of purchase.

**Configuring Private Label Prompts**
To configure the options for Private Label Cards, complete the following steps:

1. From the Universal Transaction Gateway TuneUp window, click the **Devices** tab.

2. In the Add Devices window, from the Device Type list, select one of the devices listed at the beginning of this section. If you select a device type that is not listed, the Private Label option will not be available.
3. Click **Private Label**.
4. From the Private Label Prompt screen, select your desired options and click OK.

**Option Definition Table**

<table>
<thead>
<tr>
<th>Private Label Prompt Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN (Social Security Number)</td>
<td>If selected, the applicant will be prompted to enter their social security number.</td>
</tr>
<tr>
<td>SSN Last 4</td>
<td>If selected, the applicant will be prompted to enter the last four digits of their social security number.</td>
</tr>
<tr>
<td>Zip Code</td>
<td>If selected, the applicant will be prompted to enter their zip code.</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>If selected, the applicant will be prompted to enter their date of birth.</td>
</tr>
<tr>
<td>Income</td>
<td>If selected, the applicant will be prompted to enter their annual income.</td>
</tr>
<tr>
<td>Signature</td>
<td>If selected, the applicant will be prompted to sign the PIN pad.</td>
</tr>
</tbody>
</table>

**Note:** Contact your private label card processor to determine all required fields.
Private Label Prompt Options | Definition
--- | ---
 | device.

| Promo Text | If selected, the % of Amount entered for each Period selected will be displayed to the applicant on the device and printed on the receipt. Note: The % of Amount is used to calculate the required fixed monthly payment for the corresponding promotional time Period during a private label card promotion. |

**UTG Stub Connection Settings**

A UTG-Stub connection is used if the device is connected to a remote machine that is running the UTG Stub rather than directly connected to the machine running the UTG.

---

**Note:** All of the devices in the Device Type list support UTG stub.

---

To configure the device information for a UTG-Stub connection:

1. In the Device Name box, type a unique name that will identify this device. Do not type a name that has already been used.
2. From the Device Type list, select the payment device.
3. In the API Terminal ID field, enter a terminal ID specific to the payment device. See the note below for more information.

---

**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 POS/PMS provider. Shift4 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.

4. Under Connection, select UTG-Stub.
5. In the Timeout field, type or select a time in seconds. This is the amount of time in seconds (per screen) that the UTG will wait before returning a No input from customer error. The recommended time for most devices is 30 seconds. The set time is doubled for swipe/manual entry screens to allow time for manual data entry.

6. In the Address box, type the static IP address of the machine running the UTG Stub.

7. In the Port box, type the port to which the UTG Stub is listening. (the default port is 17478)

8. See steps 7 through 11 under the RS-232 Connection Settings section for help with Manual Card Entry, Additional Options, and Cashback settings.

9. Click OK.
TCP/IP Connection Settings

When a Point-to-Point Encryption (P2PE) PIN Pad device is selected, a third connection option is available.

A TCP/IP connection is used if the device is connected directly to the network via an Ethernet cable rather than directly connected to a PC. Only P2PE devices can use this connection.

To configure the device information for a TCP/IP connection, complete the following steps:

1. From the Device Type list, select the payment device. See Appendix C for a list of devices in UTG TuneUp.
2. In the API Terminal ID field, enter a terminal ID specific to the payment device. See the API Terminal ID note below for more information.

---

**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 POS/PMS provider. Shift4 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.

---

3. Under Connection, select **Direct TCP/IP**.
4. In the Timeout field, type or select a time in seconds. This is the amount of time in seconds (per screen) that the UTG will wait before returning a No input from customer error. The recommended time for most devices is 30 seconds. The set time is doubled for swipe/manual entry screens to allow time for manual data entry.
5. In the Address box, type the static IP address of the P2PE device.
6. In the Port box, type the port to which the P2PE device is listening. (The default port is 12000.)
7. See steps 7 through 11 under the RS-232 Connection Settings section for help with Manual Card Entry, Additional Options, and Cashback settings.
8. Click OK.

**Requirement:** For EMV devices, the UTG TuneUp API Terminal ID must match what is in the API Terminal field on the EMV Device Settings page in Lighthouse Transaction Manager.

---

**Configuring 4Go**

4Go® is a persistent application that intercepts cardholder data. It secures both swiped and manually entered cardholder data by replacing it with either a temporary false card number or a TrueToken®. The actual cardholder data is only stored by Shift4. No actual cardholder data ever exists in the POS/PMS application’s logs, database, or transport mechanisms.
While monitoring the swipe data, 4Go also helps prevent tampering of the keyboard or swipe device by ensuring that no other application is able to intercept the swipe device’s data stream. 4Go can be used with most standard swipe devices.

For complete instructions on installing and configuring 4Go, see the 4Go Technical Installation Guide.

**Configuring Express Parameters**

The Express parameters control and define the connections used to communicate with the Shift4 data centers. To configure UTG Express parameters, in the UTG TuneUp window, click the Express tab.

**Identity Parameters**

The Identity parameters must be set in order to identify the computer running the UTG and define the connection used to communicate with Shift4. To configure the Identity parameters complete the following steps:

1. To configure each option in the Identity section, complete the following steps:
   - In the Serial box, type the serial number provided by the Shift4 Installations department.
   - In the Slot box, type the slot number provided by the Shift4 Installations department.
     The unique slot number is used to verify the current connection to Shift4 as it applies to the UTG. Contact the Shift4 Installations department at 702.597.2480, option 4 for additional slots if multiple UTGs will be installed.
   - In the Host Address box, select the local IP address of the computer running the UTG. If the computer running the UTG has more than one IP address, use a static address (not DHCP) on the subnet that will route traffic to Shift4’s data centers using the Internet or a private TCP/IP connection.

   **WARNING!** Because of the extensive security requirements of Shift4, any change to the IP address will affect the UTG and prevent successful operation. Contact the Shift4 Support department to allow activation if the IP address needs to be changed after any transactions have been processed.

   - In the Location box, type the ZIP code (or postal code) where the UTG is installed.

   **Note:** If all of your interfaces are using Access Tokens, you can leave the API Serial Number, API Password, and Verify API Password boxes blank.
• In the Api Serial Number box, type the Shift4 API serial number. The API serial number, provided on the Customer Configuration Report, is used to route transactions to the appropriate merchant at Shift4’s data centers. The API serial number is used only if the data is not included in each API request of the interface vendor system.

• In the Api Password box, type the Shift4 API password. The API password, along with the API Serial Number, is used to authenticate transactions to ensure they are routed to the appropriate merchant at Shift4’s data centers. The password is case-sensitive and must always match the password given on the Customer Configuration Report.

• In the Verify Api Password box, retype the Shift4 API password.

2. The Gateway section contains necessary settings to connect to the Shift4 data center. In the Gateway section, review the Address, Port, Route Code, Max Score, and Environment.

• The Address will be automatically populated when you select Test or Production in the Environment section.
  o Production - Always use this option with actual card numbers. (Production is the default setting.)
  o Test - Use Test only during development and testing in a lab with test card numbers.

WARNING! Do not change the Gateway Address and Port Settings unless instructed to do so by your IT department or the Shift4 Support department.
**Configuring Options**

The UTG TuneUp Options tab provides options to configure the UTG’s internal web server, notifications, and the UTG FTP server.

- In the UTG TuneUp window, click the **Options** tab.

![UTG TuneUp Options Tab](image)

**Configuring Notifications**

The UTG will send alert and status e-mails to specified users through the Mail Notification window. If messages of either type are received, contact the Shift4 Support department at 702.597.2480, option 2.

**Alerts**

Alert emails notify users of abnormal conditions that require action. Conditions that generate alert emails include but are not limited to the following:

- Low disk space warnings, if configured
- Thread fails (Task fails to complete)
- Unmanaged restarts
- Failed connections
- Trace archive failed
- I/O errors
- PIN pad errors
Below are examples of Alerts:

![Unmanaged Restart Alerts](image1)

Fri 12/04 3:03:18pm
Unmanaged Restart Detected

![Inet Timeout Alerts](image2)

Fri 12/04 3:07:55pm
SN 9961 INTERNET FAILURE: Timeout waiting for response across the Internet DEFAULT

2 Routes
001 "WH01.10.0.2.114 26881 Score( 0)"
002 "WH02.10.0.2.115 26881 Score( 0)"

Reference = "W700000000001"
ApSignature = "5"
ApFormat = "0"
FunctionRequestCode = "1D"
ErrorIndicat = "A"
PrimaryErrorCode = "9961"
SecondaryErrorCode = "8"
MessageID = "128785"
**Status**

Status emails notify users of conditions that may require action.

Below is an example of a Status:

To add mail notifications complete the following steps:

1. In the Universal Transaction Gateway TuneUp window, click the **Options** tab.
2. In the Option box, click **Add**.
   - From the Add menu, select **Notification**.
   - In the Mail Server Name box, type the SMTP server name where the UTG will send e-mails.
   - In the Port box, type the port (usually 25) the UTG will use to send the notifications.
   - In the Source Domain box, type the message’s origination domain address.
   - *(Optional)* In the Alert Recipients box, type the e-mail addresses of alert message recipients. Use semicolons or commas to separate e-mail addresses.
   - *(Optional)* In the Status Recipients box, type the e-mail addresses of status message recipients. Use semicolons or commas to separate e-mail addresses.
   - Click **OK**.
Configuring Advanced Parameters

Advanced parameters contain a number of important settings, including Trace configuration. Many of the options are set by default and should not be changed unless instructed by Shift4.

To configure UTG Advanced parameters complete the following steps:

1. In the Universal Transaction Gateway TuneUp window, click the Advanced tab. Most of the visible options on the Advanced tab must be enabled or defined.

   **WARNING!** The options listed in this section can be configured as directed. Do not change default settings that are not listed in this document without contacting Shift4.

2. Do not change any of the default settings under System with the following exception:
   - Cloud Timeout Override – If you are using a UTG4Cloud or UTG4CloudSSL interface, Shift4 suggests that you set the Cloud Timeout Override at 120 seconds. Since the override setting is for the UTG in the cloud, this will allow time for the local UTG to complete transactions. If you experience data center timeouts happening before the local UTG can finish processing transactions, increase the Cloud Timeout Override setting accordingly.

3. Under Signature Compression, the default is set to Enabled and Maximum Bytes is at 4096 (in KB).

4. Under Memory Monitor, complete the following steps:
   - To send an e-mail snapshot of memory usage, current status, and current configuration to the destination e-mail address listed, select Enabled.
   - From the Frequency list, select a predefined interval.
   - In the Destination box, type the recipient’s e-mail address. Separate multiple addresses with semicolons or commas.

5. Under Options complete the following steps:
   - Max Threads – To change the maximum number of allowed threads in the UTG, you must obtain a unique code from the Shift4 Payments Customer Support team. Click the Max Threads button for further instructions.
   - The API Overrides option is customer specific; do not select this option unless instructed to do so by a Shift4 Support Representative. See the UTG Reference Guide for further instructions.
• Click **Trace Configuration** to configure the parameters for your trace files.

![Image of Trace Configuration](image)

- In the **Directory** box, the default path is `C:\Shift4UTG2UTG Trace`.
- In the **Max Files** box, type or select the maximum number of trace files. (This is the maximum number of files retained without enabling High Capacity.)
- In the **Blocks** box, type or select the number of lines of trace to be displayed in the Filter form. Above this number, the oldest blocks will be discarded from memory.
- In the **Bytes Each** box, type the amount of trace to save in each file.
- *(Optional)* In the **Suffix** box, type any two-digit character combination. Suffix characters are used to distinguish these trace files from other trace files. If unused, leave this box blank.
- *(Optional)* Select **High Capacity**. With High Capacity selected, the trace files will be zipped rather than overwritten when capacity is reached.
- *(Optional)* If High Capacity is selected, select the files per zip (between 8 and 64). This is the number of trace files generated before being zipped.
- *(Optional)* Select the **Days Cutoff** (between 5 and 120). This is the number of days zipped trace files will be kept before they begin to be overwritten. Example: If 5 is selected, zipped trace files will be stored for 5 days. On the 6th day, the first days trace files will be overwritten and the trace subsequently lost.
- Select **Verbose**. Selecting Verbose provides complete transaction data in the trace files and is necessary for any trouble shooting.
- Click **OK**.
• Click **Splunk Configuration** to configure the parameters for UTG to write out log files that are in a Splunk friendly format.

![Universal Transaction Gateway splash screen](image)

- **(Optional)** To enable Splunk logging, select **Enable**.

**Important:** Shift4 Payments highly recommends that you enable Splunk logging if you are using a REST interface.

- In the **Directory** box, enter the desired directory where the files will be stored.
- In the **Max Files** box, type or select the maximum number of Splunk files. (This is the maximum number of files retained without enabling High Capacity.)
- In the **Blocks** box, type or select the number of lines of Splunk files to be displayed in the Filter form. Above this number, the oldest blocks will be discarded from memory.
- In the **Bytes Each** box, type the amount of Splunk files to save in each file.
- **(Optional) Select High Capacity.** With High Capacity selected, the Splunk files will be zipped rather than overwritten when capacity is reached.
- **(Optional)** If High Capacity is selected, select the files per zip (between 8 and 64). This is the number of Splunk files generated before being zipped.
- **(Optional)** Select the Days Cutoff (between 5 and 120). This is the number of days zipped Splunk files will be kept before they begin to be overwritten.
- Click **OK**.
6. Under Preferences:

- Select **Convert Communication Errors to Referrals** if your Interface Vendor System allows handling communication error responses as referrals.

**Note:** If you are configuring a UTG4Cloud interface, it is not advisable to select the Convert Communication Errors to Referrals option.

- The Send Alert Messages to Shift4 option allows you to send alert messages to Shift4 in addition to recipients listed in the Mail Notification window. If this option is not selected, alert messages will only be sent to recipients listed in the Mail Notification window. Select **Send Alert Messages to Shift4** to send alert messages to Shift4, regardless of Mail Notification window settings.

- The Transaction Cache Enabled is selected by default. This enables the transaction cache to hold the last hours' worth of debit transactions and reply with the same response to a duplicate debit request received from an interface.
• In the Low Disk Space Warning Threshold box, type the minimum amount of disk space to use for trace before sending an alert e-mail to the addresses specified in the Mail Notification window.

• Do not modify UTG or in4m settings unless instructed to do so by Shift4’s Customer Support team.
Configuring Offline Mode

Offline mode provides additional functionality and security when the UTG cannot connect to the Shift4 data center and any of the following additional scenarios are true:

- A credit card is not EMV enabled
- The device being used to perform a transaction is not EMV enabled
- An EMV chip is not readable on an attended EMV enabled device and fallback mode is initiated

In Offline mode, the UTG closely mimics online mode by generating a Token on all authorization and sale requests. If you choose to take advantage of the Stand-in feature when you set up your API Interface, you can set a user-defined dollar amount, located beneath the checkbox, called the Floor Limit. With the Floor limit set, when the UTG is offline, it returns an approval on all authorization and sale requests that are below the Floor Limit and a referral on all authorization and sale requests that are above the Floor Limit.

The UTG will store the transaction requests below the Floor Limit in an encrypted file. Once back online, the UTG will attempt to authorize those transactions. Any transaction that is unable to be authorized will have to be resolved by the auditor. There is obviously a risk to the merchant when enabling this feature as not all of the transactions may be approved once the UTG comes back online. However, the benefits of being able to accept transactions while offline may be worth the risk.

Note: PIN Debit is not available in Offline Mode since it is not possible to validate the PIN number unless the system is online.

Several optional settings are found on the Offline Mode tab. To configure the optional settings complete the following steps:

1. The Offline Level has five settings: Low, Medium, High, Custom, or Never. After transactions collected in offline mode are sent to the Shift4 data center, the UTG automatically deletes them from the offline queue.
   - **Low**: Transactions will automatically be sent to the offline queue when the UTG detects 3 failed transactions in the past 2 minutes.
   - **Medium**: Transactions will automatically be sent to the offline queue when the UTG detects 5 failed transactions in the past 2 minutes.
   - **High**: Transactions will automatically be sent to the offline queue when the UTG detects 25 failed transactions in the past 5 minutes.
   - **Custom**: Transactions will be automatically sent to the offline queue when the UTG detects the number of failed transactions in the specified time span. When using Custom level, you must also set the Count and Time Span:
     - **Count**: This is the number of failed transactions required before the UTG automatically switches to Offline mode.
     - **Time Span**: This is the timeframe required for the count to be reached before the UTG to switch to Offline mode. If the count is not reached within the specified time span, the internal timer automatically resets.
   - **Never**: No number of failed transactions will cause UTG to switch to Offline mode. However, on startup, the UTG will operate in offline mode until it connects to the Shift4 data center.
**Note:** Offline Mode requires that the UTG have the capability to encrypt transactional data locally. This is predicated on the UTG being activated on Shift4’s servers and having obtained encryption keys. When it is first started, the UTG obtains sets of keys and activates on our servers. Once the UTG has activated, performed its first Key Page request successfully, and obtained an Offline Key, then on subsequent restarts, it will be able to start in Offline Mode while negotiating new keys.

2. **Under Offline Options:**
   - It is recommended that you select **Return Error on Void if Offline**. This option allows an error message (function not supported in offline mode) to be sent when the POS/PMS is attempting to send a void (08) and the UTG is unable to connect to the data center.
   - Selecting **Decline All Non-Bank Cards** returns a declined response for all non-bank cards if the UTG goes into Offline Mode.

**Note:** When in Offline Mode, if a gift card transaction is sent with a token rather than card information, the UTG cannot determine if the card is a gift card. The transaction will be treated as a credit card transaction, even if the Decline All Non-Bank Cards option is selected. The transaction will follow the other Offline Mode settings as a credit card.

---

**Data Center**

The Data Center tab is not currently used.
Finalizing your UTG Configuration

When you have finished configuring the UTG to your desired settings, click **Save** in the Universal Transaction Gateway TuneUp window to save all your settings.
Testing the UTG Configuration

To verify the UTG configuration, complete the following steps:

1. From the Start menu, select Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) Stand Alone. The default UTG functions start automatically and are marked by check boxes.

2. Verify the text NO ROUTES is not displayed in the Routes section of the screen. The text NO ROUTES in the Routes setting is significant; it indicates that there is either no connection to the Internet or the necessary ports are not open. If the words NO ROUTES appear, contact your IT department to correct the problem.

3. Verify that KeyPage SUCCESS is display next to TCPClient in the top section of the screen. If these words do not appear within 20 seconds and there is no problem with your Internet connection, contact the Shift4 Support team at 702.597.2480, option 2.
Running UTG as a Service

The UTG can also be configured to run as a service. The UTG service runs continuously in the background of its respective machines. By default it starts automatically when the machine boots up.

**Requirement:** If the UTG Stand Alone is running, you must stop it before running the UTG service. The UTG Stand Alone and the UTG service cannot run concurrently.

To start UTG as a service, start Shift4 UTG (v2) from the Windows Services menu.
UTG Stub

The UTG Stub is only necessary to communicate with a PIN Pad device connected to a machine that is not running the UTG. If the external device is connected directly to the UTG machine, you do not need to install the UTG Stub on the computer. All you have to do is configure the device for RS-232 communications. Refer to RS-232 Connection Settings for instructions.

What is the UTG Stub?

The UTG Stub application is an add-on companion to the UTG application. Use the UTG Stub whenever you have a PIN pad device connected to a remote POS/PMS terminal that does not have a UTG. The UTG Stub application links the remote POS/PMS terminal to the server running the UTG application so that the UTG can communicate with the external device. The UTG Stub accepts the TCP/IP traffic and then converts it back to USB/serial communication, such that the UTG Stub communicates directly to the device via the serial cable. To use UTG Stub, first you must configure the PIN pad device for UTG Stub communication on the Device tab in UTG TuneUp. Then you must install and configure the UTG Stub on the remote POS/PMS terminal connected to the PIN pad device. See the UTG usage configuration examples earlier in this document.

Follow the steps in this section to install, configure, and test the UTG Stub. If you have any questions during this process, call the Shift4 Customer Support team at 702.597.2480, option 2.

UTG Stub Encryption

The UTG supports an encrypted tunnel to the UTG Stub. The encryption is fully automated and does not require any changes to your existing UTG or PIN pad.

Downloading the UTG Stub

To download the UTG Stub files complete the following steps:

2. On the File Download window, the name and location should read UTGStubsetup.exe and https://myportal.shift4.com/downloads/utgstubsetup.exe. Click UTGStubsetup.exe to continue.

3. The file name and publisher should be as per example below.
4. Click Run.

**Installing the UTG Stub**

To install the UTG Stub, complete the following steps:

1. In the Shift4 UTG Stub Setup - Installation Wizard window for Shift4 UTG Stub Setup, click **Next**.
2. In the Read the license agreement window, review the terms and conditions, read the license agreement and click **Next** to indicate you accept the agreement.

3. The UTG Stub default installation folder is C:\Shift4. To change the destination folder, type or select the desired folder, or simply click **Next** to continue the installation in the default folder.
4. In the Ready to make changes to your computer window, click **Next**.

5. In the Shift4 UTG Stub has been successfully installed window, click **Finish**.
**Shift4 Modem Configuration Utility**

When using serial PIN pad devices, the UTG must be configured to recognize COM ports available for its use. The Shift4 Modem Configuration Utility automatically probes for COM ports. To open the Shift4 Modem Configuration Utility complete the following steps:

- From the *Start* menu, select *Programs > Shift4 Corporation > Universal Transaction Gateway > S4 Config.*

---

**Note:** If this is the first time running the utility, it may run and then close. It may also run and close if it runs a second time and no COM Port is found.
Configuring UTG Stub

This section describes how to configure the UTG Stub when using a PIN pad device on a remote machine.

**Requirement:** If the UTG Stub is running, you must shut it down before you can configure the UTG Stub TuneUp settings.

Configuring UTG Stub TuneUp Settings

To configure the UTG, follow the detailed instructions in these sections:

1. If the UTG Stub is running, shut it down by performing one of the following steps:
   - To shut down UTG Stub Standalone, select **File > Exit** and click **Yes** when prompted to confirm shut down. If Stub is in use, it may be necessary to select **Override** before clicking **Yes**.
   - To shut down the UTG Stub service, stop the Shift4 UTG Stub service from the Windows Services menu.

2. From the Start menu, select **Programs > Shift4 Corporation > UTG Stub > UTG Stub TuneUp**.

3. In the UTG Stub TuneUp window, configure the settings on each tab as required for the terminal.
**Configuring UTG Stub Devices**

To configure UTG Stub devices complete the following steps:

1. In the UTG Stub TuneUp window, click the **Device** tab.
2. Under Device, click **Add**.
3. In the Add Device window, apply the appropriate settings:
   - In the Description box, type a name that identifies this device.
   - From the Listen Address list, select the address the UTG Stub machine will use to listen for UTG connections. The Listen Address must be identical to the Address setting configured in the UTG.
   - In the Listen Port box, type the port number the UTG Stub will use to listen for UTG connections. The port entered must be identical to the port set when configuring the UTG. (The default port is 17478)
   - From the Com Port list, select the port to which the PIN pad device is connected. If the Com Port is not listed, run the Modem Configuration utility (S4 Config) and restart UTG Stub TuneUp.
   - From the Baud Rate list, select the baud rate for the PIN pad device.
   - From the Data Bits list, select the data bits for the PIN pad device.
   - From the Parity list, select the parity for the PIN pad device.
   - From the Stop Bits list, select the stop bits for the PIN pad device.
   - From the Flow Control list, select the flow control for the PIN pad device.
   - Click **OK**.

![Add Device window](image)

**Note:** See the *Using External Devices* guide for supported PIN pad settings.

---

**Configuring UTG Stub Options**

To configure the UTG Stub options, perform the following steps:

1. In the UTG Stub TuneUp window, select the **Options** tab.
2. In the Options box, click **Add**.

3. From the Add menu, select **Web Server** or **Notification**.

**Web Server for the UTG Stub**

The Web Server option is the internal web server for the UTG Stub. The Web Server option allows you to view the UTG Stub terminal configuration remotely, as well as perform tasks such as checking the UTG Stub system status and managing trace. To configure the web server, perform the following steps:

1. From the Host Address list, select the IP address of the machine.

2. Verify the Listen Port is 27033. Do not change the default setting unless instructed to do so by Shift4.

3. *(Optional)* In the Common Name box, type the server nickname, if used.

4. *(Optional)* In the Allowed IP Addresses list, type IP addresses of terminals that are allowed to access the UTG web server. If you do not enter allowed IP addresses, then any IP address is allowed to access the UTG web server.
5. Click **OK**.

**Notification for the UTG Stub**

The UTG Stub will send alert and status e-mails to specified users through the Mail Notification window. If messages of either type are received, contact the Shift4 Support department at (702) 597-2480, option 2.

**Alerts**

Alert e-mails notify customers of abnormal conditions that require action. Conditions that generate alert e-mails, include, but are not limited to:

- Low-disk space warnings, if configured
- Thread halts
- Unmanaged restarts
- Missing connections
- Failed actions
- I/O errors

**Status**

Status e-mails notify customers of logic faults that require action. Conditions that generate status e-mails occur in the offline, security, or import managers and may require software changes and testing for full resolution.

**Configuring Notifications**

To configure the **Mail Notification** window, perform the following steps:

1. In the UTG Stub TuneUp window, click the **Options** tab.
2. In the Options box, click **Add**.
3. From the Add menu, select **Notification**.
4. In the Mail Notification window, configure appropriate settings:
• In the Mail Server Name box, type the SMTP server name where the UTG Stub will send e-mails.
• In the Port box, type the port (usually 25) the UTG Stub will use to send the notifications.
• In the Source Domain box, type the message's origination domain address.
• *(Optional)* In the Alert Recipients box, type the e-mail addresses of alert message recipients. Use semicolons or commas to separate e-mail addresses.
• *(Optional)* In the Status Recipients box, type the e-mail addresses of status message recipients. Use semicolons or commas to separate e-mail addresses.

5. Click **OK**.

---

**Configuring Advanced UTG Stub Parameters**

The Advanced parameters allow configuration of low-level details of trace settings as shown in the example. To configure the Advanced parameters of the UTG Stub, perform the following steps:

1. In the UTG Stub TuneUp window, click the **Advanced** tab.

![UTG Stub TuneUp](image)

2. In the Low Disk Space Warning Threshold box, type the minimum amount of disk space to use for trace before sending an alert e-mail to the addresses specified in the Mail Notification window.

3. In the Environment box, select a setting *(Production is the default setting)*:
   - **Production**: Always use this option with actual card numbers.
   - **Test**: Use only during development and testing in a lab with test card numbers.

4. Click **Trace Configuration**.
5. In the Trace Parameters window, verify the following settings:

- In the Directory box, type the directory path where the transaction files will be placed. The directory path must be a local drive, not a UNC path.
- In the Max Files box, type or select the maximum number of trace files.
- In the Blocks box, type or select the amount of trace to save.
- In the Bytes Each box, type the amount of trace to save in each file.
- (Optional) In the Suffix box, type any two-digit character combination. Suffix characters used to distinguish these trace files from other trace files. If unused, leave this box blank.
- (Optional) To enable the Files per Zip and Days Cutoff options, select High Capacity.
- The Files per Zip and Days Cutoff features define how much trace to store. The maximum amount of stored trace is 120 days.
- (Optional) In the Files per Zip box, type or select the number of trace files to include in each zip file.
- (Optional) In the Days Cutoff box, type or select the number of days to include in each zip file.
- Click OK to return to the Advanced tab.

6. In the Universal Transaction Gateway TuneUp window, click Save.

---

**Requirement:** After installing the UTG Stub application on the required terminals, you must add the IP address of each terminal to the UTG.
Finalizing your UTG Stub Configuration

After configuring UTG Stub to your desired settings complete the following steps:

1. In the UTG Stub TuneUp window, click Save.
2. Start the UTG Stub and complete one of the following steps:
   - To start UTG Stub Standalone, from the Start menu, select Programs > Shift4 Corporation > UTG Stub > UTG Stub Standalone.
   - To start UTG Stub as a service, start Shift4 UTG Stub from the Windows® Services menu.

Testing the UTG Stub Configuration

Warning! Always connect your PIN pad device to the Stub machine before connecting the PIN pad to a power source.

To verify the UTG Stub configuration, connect the PIN pad device to the UTG Stub machine and to a power source, and then check the screen on the PIN pad device. If configured correctly, the PIN pad will display the Idle mode.
screens. The UTG Standalone will display an Idle mode message as well. Idle mode is a condition. The actual screen display on the PIN pad may vary.

If the screens are not in Idle, complete the following steps:

1. Check the connection between the PIN pad device and power cord.
2. Verify that the device is powered-on.
3. Verify that the device settings match the settings in the UTG Stub.
4. Verify the IP address and port settings in UTG match the Listen Address and port settings in UTG Stub.
5. Contact the Shift4 Support department for assistance if the screens still do not display Idle mode.
Appendix A – Using a Cloud-Based POS/PMS With Shift4’s Universal Transaction Gateway (UTG)

A UTG4Cloud interface option for Shift4’s Universal Transaction Gateway (UTG) provides security for local properties using cloud-based point of sale (POS) and property management systems (PMS). Using Shift4’s UTG4Cloud API with a cloud-based POS/PMS only requires a few additional device registration steps to process a request through a UTG-controlled PIN pad at the local property. The Processing an Authorization Request Using a Cloud-Based POS/PMS section describes the transaction flow and includes the use of a UTG-controlled device (for example, an EMV device).
Processing an Authorization Request Using a Cloud-Based POS/PMS

1. A transaction is initiated at a local property that is using an Internet browser to access a cloud-based POS/PMS.
2. The browser at the local property sends a request to connect their UTG to the Shift4 data center. Note: It is the local property’s UTG that uses the UTG4Cloud API Interface.
3. The local property’s UTG4Cloud establishes a connection to the Shift4 data center.
4. The Shift4 data center generates and returns DeviceService, DeviceGuid, and DeviceExtensions to the local property’s UTG4Cloud.
5. The local property’s UTG4Cloud sends the DeviceService, DeviceGuid, and DeviceExtensions to the local property’s browser.
6. The local property’s browser sends the DeviceService, DeviceGuid, DeviceExtensions, and TERMINALID to the cloud-based POS/PMS.
7. The cloud-based POS/PMS sends the authorization request, including the DeviceService, DeviceGuid, DeviceExtensions, and TERMINALID to the UTG in the cloud.
8. The UTG in the cloud sends the authorization request, including the DeviceService, DeviceGuid, DeviceExtensions and TERMINALID to the Shift4 data center.
9. The Shift4 data center sends the authorization request to the local property’s UTG4Cloud.
10. The local property’s UTG4Cloud processes the authorization request with a UTG-controlled device.
11. The local property’s UTG4Cloud returns the response to the Shift4 data center.
12. The Shift4 data center forwards the response to the UTG in the cloud.
13. The UTG in the cloud forwards the response to the cloud-based POS/PMS.
14. The cloud-based POS/PMS forwards the response to the local property’s browser.
Appendix B – Security Certificates

The UTG provides three options for Certificate generation when configuring a TCP/IP SSL, HTTP/SSL, or UTG4CloudSSL interface.

1. The UTG can generate a Certificate at each start up,
2. The UTG can generate a persistent certificate during configuration,
3. The user may provide a Certificate.

UTG Generated Certificate

If your POS/PMS application is not browser-based, this might be a good option. If you choose to generate a certificate using this feature, the default certificate duration is two years.

To allow the UTG to generate a certificate at each start up, complete the following steps:

1. Under Certificate Information, leave the default Use UTG Generated Certificate selected.
2. Click OK.
Generating a Persistent Certificate

If your POS/PMS needs a consistent certificate each time it connects to the UTG, even after a UTG reboot you can use this option to generate a persistent certificate. This might be a good option for browser-based POS/PMS systems.

When generating a persistent file the UTG will output two separate files:

- One file will contain both the public certificate and the private key.
- The other file will contain just the public certificate.

To generate a persistent Certificate during configuration, complete the following steps:

1. In the Certificate Information section, click **Generate Certificate**.
2. In the Certificate Format list, select the certificate type you want to generate.
   - Typically, PFX is used in Windows environments.
   - Typically, PEM is used in Linux environments.
3. In the Valid from and to section, select the date the certificate will begin being valid and the date it will end being valid.
4. In the Common Name field, enter the fully qualified domain name or IP address that clients will use to reach your server. This is typically the Host Address setting for the interface that you are generating the certificate for. (See the example below.)
5. In the Organization field, enter the exact legal name of your organization.
6. (Optional) In the Organizational Unit field, enter the department within your organization that you want to appear in the certificate.
7. (Optional) In the Email Address field, enter the email address that you want to appear in the certificate.
8. In the City field, enter the city where your organization is located.
9. In the State/Province field, enter the state or province where your organization is located.
10. In the Country field, enter the country where your organization is located. This is the 2 character ISO country code value. For example, the United States ISO code is US.
11. In the Key Size list, select the size of the RSA key to use for certificate generation. RSA 2048 is the standard key size. Selecting RSA 4096 will utilize a larger key for better security, but will require higher CPU utilization.
12. In the Private Key Password field, enter a password for your private key. This password will be used to encrypt the private key.

13. In the Verify Private Key Password field, reenter the password.

14. Click **Generate**.

**User Provided Certificate**

To provide a Certificate for use with the UTG, complete the following steps:

1. Clear Use UTG Generated Certificate if selected.
2. In the Certificate File box, enter the certificate path or click **Browse** and select the desired certificate file.
3. Enter the Certificate Password.
4. If a Private Key File is required, type the path in the Private Key File box or click **Browse** and select the Private Key File.
5. Enter the Private Key Password in the Private Key Password field.
6. Click **OK**.

If you select Use UTG Generated Certificate, you may also select the Use SHA1 Certificate option. However, the use of SHA1 SSL Certificates is being deprecated due to security issues and is not recommended. You should only utilize this option if your POS/PMS vendor has issues with the SHA2 certificate. If you choose this option, the following warning will be displayed.

The UTG will attempt to load and validate the certificate from the file. If there are any issues uploading or validating the provided file, the UTG will display a message describing the problem. The user will then be returned to the API screen with blank Certificate and Private Key boxes. Some examples would be:

- Choosing a certificate file that requires a separate private key file, but not providing the key file.
• Choosing a certificate file that already incorporates the private key, yet providing a private key file anyway.
• Providing no password, or the wrong password for a password protected certification/key file.

The UTG can NOT be used to specify the password. You must enter the password already associated with the file. An example of the message generated by a user entering incorrect or invalid data is provided below.

![Message Example]

Invalid private key or password chosen. Select a valid file, or check the "Use UTG Generated Certificate" box.

OK
## Appendix C – Table of Listed Devices in UTG TuneUp

<table>
<thead>
<tr>
<th>For this device...</th>
<th>Select this setting...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingenico iPP320 CAN</td>
<td>Ingenico iPP320 CAN</td>
</tr>
<tr>
<td>Ingenico iPP320</td>
<td>Ingenico iPP320</td>
</tr>
<tr>
<td>Ingenico iPP320 P2PE</td>
<td>Ingenico iPP320 RBA</td>
</tr>
<tr>
<td>Ingenico iPP350</td>
<td>Ingenico iPP350</td>
</tr>
<tr>
<td>Ingenico iPP350 P2PE</td>
<td>Ingenico iPP350 RBA</td>
</tr>
<tr>
<td>Ingenico iSC250</td>
<td>Ingenico iSC250</td>
</tr>
<tr>
<td>Ingenico iSC250 P2PE</td>
<td>Ingenico iSC250 RBA</td>
</tr>
<tr>
<td>Ingenico iSC350</td>
<td>Ingenico iSC350</td>
</tr>
<tr>
<td>Ingenico iSC350 P2PE</td>
<td>Ingenico iSC350 RBA</td>
</tr>
<tr>
<td>Ingenico iSC480</td>
<td>Ingenico iSC480</td>
</tr>
<tr>
<td>Ingenico iSC480 P2PE</td>
<td>Ingenico iSC480 RBA</td>
</tr>
<tr>
<td>Ingenico iUC285</td>
<td>Ingenico iUC285 RBA</td>
</tr>
<tr>
<td>Ingenico iUP 250</td>
<td>Ingenico iUP250 RBA</td>
</tr>
<tr>
<td>Ingenico iWL 252</td>
<td>Ingenico iWL252 RBA</td>
</tr>
<tr>
<td>Ingenico iWL 258</td>
<td>Ingenico iWL258 RBA</td>
</tr>
<tr>
<td>Ingenico iCMP</td>
<td>Ingenico iCM122 RBA</td>
</tr>
<tr>
<td>Ingenico iSMP Companion</td>
<td>Ingenico iMP352 RBA</td>
</tr>
<tr>
<td>Ingenico iMPv4</td>
<td>Ingenico iMP657 RBA</td>
</tr>
<tr>
<td>Verifone® SC 550</td>
<td>PinPad 550</td>
</tr>
<tr>
<td>Verifone® SC 5000 configured for Tip 1</td>
<td>PinPad 550 Tip 1</td>
</tr>
<tr>
<td>Verifone® SC 5000 configured for Tip 2</td>
<td>PinPad 550 Tip 2</td>
</tr>
<tr>
<td>Verifone® SC 5000 configured without Tips</td>
<td>PinPad 550</td>
</tr>
<tr>
<td>Verifone® MX915</td>
<td>Verifone MX915</td>
</tr>
<tr>
<td>Verifone® MX925</td>
<td>Verifone MX925</td>
</tr>
<tr>
<td>Verifone® MX915 P2PE</td>
<td>Verifone MX915 P2PE</td>
</tr>
<tr>
<td>Verifone® MX925 P2PE</td>
<td>Verifone MX925 P2PE</td>
</tr>
</tbody>
</table>
Note: The old Form Designer utility for the Ingenico 3070, 6550 and 6780 loads forms on those devices in upper and lower case, whereas the new Form Designer loads the forms in lower case only. Refer to your Ingenico documentation if you do not know which form designer is in use.