Account Administrator Guide

Introduction

The *Account Administrator Guide* reviews important details, like who should be the Account Administrator, why the account is so important, and how the account should be used.

In addition, the guide outlines required steps that must be done to successfully set up an account in Lighthouse Transaction Manager (LTM), as well as optional features that are available for use.

For additional information, use this link to access the Resource Library.

What Is So Important about This Account?

The Account Administrator is the master default user account. It is the only user account created by Shift4. All other user accounts, including other administrator-type accounts, are created by the Account Administrator. The settings in this account may have a financial impact on the company.

Note: Certain functions, such as resetting the password or removing an authenticator for the Account Administrator (if they have forgotten or lost both their password and recovery questions and/or reset code), can only be done by contacting the Shift4 Customer Support team at 888-276-2108, option 1.

How Should This Account Be Used?

The Account Administrator account should be used exclusively for account setup, maintenance, and for creating administrator-type user accounts.

Note: The Account Administrator account should not be used for daily auditing or settlement duties.

Only the Account Administrator has the right to access, configure, or change the settings that control the global LTM environment. No other user type has the ability to perform the following tasks:

- Configure Administrator-Type Users
- Configure General Settings
- Configure 4Go® Settings
- Configure Security Settings
- Configure IP Address Restrictions
- Configure API Settings
- Configure Auto-Settle Settings (if the option is enabled for the account)
- Configure IT'S YOUR CARD® (IYC) Settings (if the option is enabled for the account)
- Configure Debit Device Settings (if the option is enabled for the account)
- Configure EMV Devices (if the option is enabled for the account)

Note: EMV is a special chip embedded on a credit or debit card that helps to prevent card-present fraud. The EMV chip prevents counterfeiting, skimming, and the use of lost or stolen credit or debit cards. The specification for EMV chips was first created in 1994 by the credit card brands Europay, MasterCard, and Visa (EMV).

Menu Overview

The menu options displayed in LTM are based on what has been enabled for the account with Shift4.

The following is a quick overview of what the LTM menu could contain:

- Home: Clicking the house icon will return you to your chosen home page.
- Transactions: Under this menu option is where you will select merchants, view their current or archived transactions (and the transaction grid if enabled for your profile). It is also where you can enter transactions using the Online Entry or Offline Entry option.

Note: The Account Administrator account should not be used for daily auditing or settlement duties.

- Periodic Billing: Under this menu option is where you will access all the periodic billing settings and options.
- It's Your Card: Under this menu option is where you will access IYC gift cards sales, order fulfillment, issuance, reports, and SiteBuilder (where you can create your own gift card site).
- Shift4 Cares: This is only displayed if the "Shift4 Cares access" permission is enabled on the user's account, and is where gift card orders are managed when participating in the Shift4 Cares gift card program.
- 4Go: Under this menu option is where you can set your 4Go settings for LTM and manage 4Go clerk cards.
- 4Word: Under this menu option is where you can set up your 4Word® settings (including inviting users) and monitor 4Word usage.
- Billing Statements: This is only displayed if applicable to the account and the "Billing statements access" permission is enabled on the user's account. It is where billing statements can be viewed and downloaded.
- Settings: Under this menu option is where you will find all of your account setting options for LTM.
- User: Under this menu option is where you can create new users, edit current users, create user shifts, view user activity, change your profile, and change your password.
- Help: Help provides access to a number of task based guides and video tutorials that can assist you. The information is listed under various categories with a short description and list of covered topics.

Signing In to LTM

Accessing the User Sign In Page

Accessing the Lighthouse Transaction Manager User Sign In page through one of the entry points reviewed below ensures that even when routine maintenance has to be performed on one of the servers, you can still access your data.

Tip: Like most interactive websites, the LTM website does use cookies. You will need to ensure that these are allowed in your web browser, as well as website redirection.

To access the Lighthouse Transaction Manager User Sign In page, complete one of the following steps:

- Enter https://lh.shift4.com in the web browser's address bar, press **Enter**, and then click **Lighthouse Transaction Manager**. This will connect you to an active LTM server.
- Enter www.shift4.com in the web browser's address bar, press **Enter**, click **Log in**, and then click **Lighthouse Transaction Manager**. This will connect you to an active LTM server.

With either method, the Lighthouse Transaction Manager User Sign In page will be displayed.

Tip: Set a bookmark to https://lh.shift4.com to ensure that the fastest server available is accessed each time you sign in to LTM. Do not bookmark the actual server address because that would limit you to a single server, and you would not be able to take advantage of Shift4's load balancing.

Signing In for the First Time

After requesting a LTM account, the Account Administrator will receive an email from security@lh.shift4.com. This email will have the information the Account Administrator will need to sign in to their LTM account for the first time (account number, username, and temporary password).

If you have not received your login and account information, contact the Shift4 Customer Support team at 888-276-2108, option 1.

Note: The Shift4 Customer Support team does not have access to user accounts; therefore, they cannot supply password or other information associated with user accounts.

After signing in for the first time, you will be immediately prompted to change your temporary password to a personal password. This is a requirement before you can start using your account. Changing your temporary password to a personal password is also a requirement of the Payment Card Industry Data Security Standards (PCI DSS) because vendor supplied passwords should never be used.

Warning! You are about to configure settings that affect payment transaction security. For security implementation and best practices, see the PCI Security Standards Council website.

It is also required that each user (including the Account Administrator) select and answer five predefined password recovery questions as part of the signing-in-for-the-first-time process. You will not be able to proceed until this is completed.

In the event that a user (including the Account Administrator) forgets their password, the password recovery questions provide a means to reset their password. Password recovery questions are designed to be personal in nature so that the answers cannot be easily guessed.

In addition, you may be required to enable multifactor authentication on your account. If your account requires this security feature, you will be directed to the Change Profile page after successfully setting your personal password and recovery questions. You will not be able to use your account until this is completed.

Tip: After signing in for the first time, you can change your password or recovery questions at any time. For additional information, see the *Changing Your Password* document.

To sign in to your LTM account for the first time, complete the following steps:

1. Follow the directions in your welcome email.

Requirement: Regardless of the login method selected in the welcome email, you must change your password and select and answer your security questions. If your account requires multifactor authentication to be enabled, you must also enable it before your account can be used.

2. *(If applicable)* On the Lighthouse Transaction Manager User Sign In page, complete the following steps:
   - In the Account Number field, enter the account number provided in your welcome email.

Note: The account number is supplied by Shift4 and will be used by every user who signs in to this account. If an email address was provided when a user account was created in LTM, then the account number will be provided to the user in their welcome email.

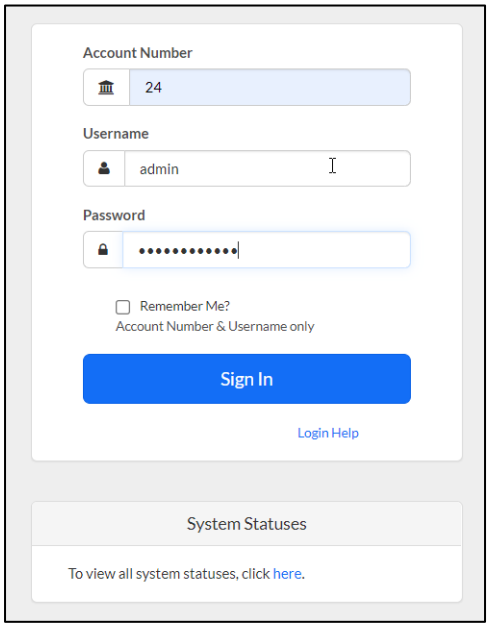
   - In the Username field, enter the username provided in your welcome email.

Note: When signing in as the Account Administrator, “Administrator” or “Admin” may be entered in the Username field. Usernames are not case sensitive. If an email address was provided when a user account was created in LTM, then the username will be provided to the user in their welcome email.

- In the Password field, enter the temporary password provided in your welcome email.

Note: If an email address was provided when a user account was created in LTM, then the temporary password will be provided to the user in their welcome email. The password is case sensitive.

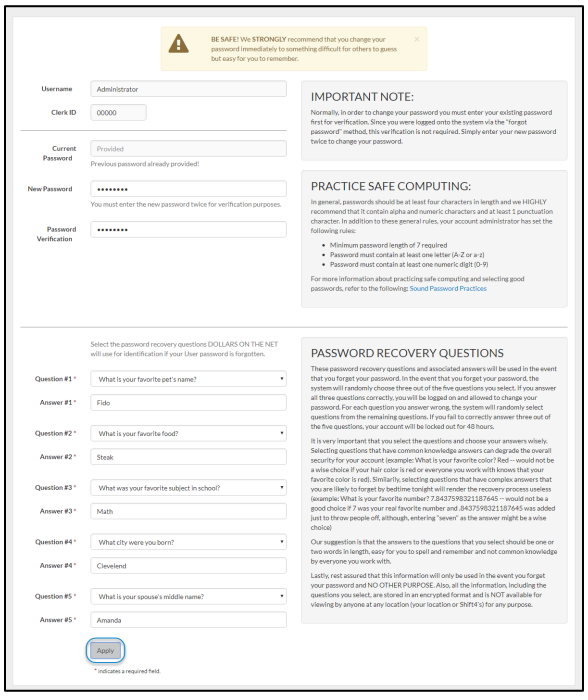
- Click **Sign In**.



3. On the Change Password page, complete the following steps:
   - *(If applicable)* In the Current Password field, enter your temporary password.
   - In the New Password field, enter a unique password.
   - In the Password Verification field, reenter your new password.
   - From the Question #1 list, select the desired question.
   - In the Answer #1 field, enter your personal answer to the question.
   - Repeat this process until all five questions have been selected and answered.

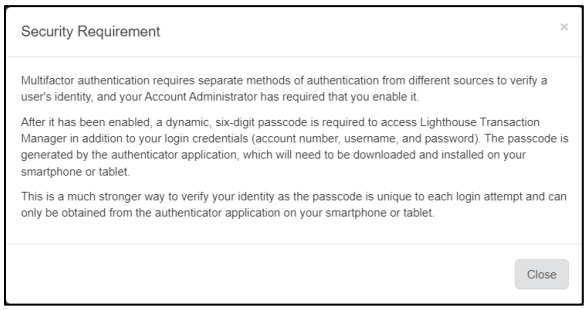
Note: You cannot select the same question more than once, and you cannot supply the same answer to more than one question. The security question answers are not case sensitive.

- Click **Apply**.



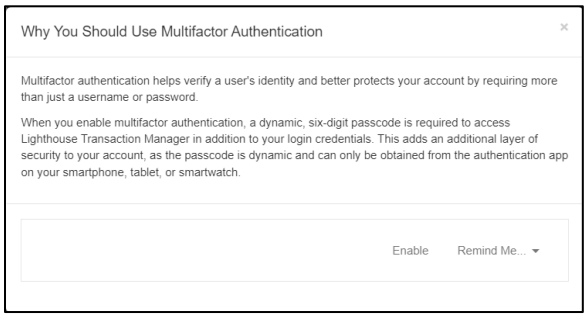
Note: Shift4 recommends storing the Account Administrator login and password in a physically safe location, such as a safe or vault. In the event you forget your password, see the *Appendix A – Password Recovery* section for instructions on resetting your password.

4. *(If applicable)* If your account requires multifactor authentication to be enabled, you will be directed to the Change Profile page to add it to your account. You will not be able to use your account until this is completed. Follow the directions displayed in LTM to complete this process.



5. *(If applicable)* Depending on settings configured, a notification about adding multifactor authentication may be displayed. For additional information on this feature and how to enable it, see the *Changing Your Profile* document. If you are not ready to enable it, select one of the following options from the Remind Me list:

   - **Tomorrow**
   - **Next Week**
   - **Next Month**



Tip: All LTM user accounts are encouraged to use multifactor authentication, especially administrator-type user accounts. For additional information, see the *Changing Your Profile* document.

Signing In a Subsequent Time

To sign in to LTM after you have changed your password and selected and answered your security questions, complete the following steps:

1. To access the Lighthouse Transaction Manager User Sign In page, complete one of the following steps:
    - Enter https://lh.shift4.com in the web browser's address bar, press **Enter**, and then click **Lighthouse Transaction Manager**. This will connect you to an active LTM server.
    - Enter www.shift4.com in the web browser's address bar, press **Enter**, click **Log in**, and then click **Lighthouse Transaction Manager**. This will connect you to an active LTM server.
2. *(If applicable)* On the Lighthouse Transaction Manager User Sign In page, complete the following steps:
    - In the Account Number field, enter the account number.
    - In the Username field, enter the username.

Note: When signing in as the Account Administrator, "Administrator" or "Admin" may be entered in the Username field. Usernames are not case sensitive.

    - In the Password field, enter your password.

Note: Passwords are case sensitive.

    - Click **Sign In**.

3. *(If applicable)* If you have enabled multifactor authentication, complete the following steps:
   - In the Passcode field, enter the dynamic, six-digit passcode generated by the authenticator app on your smart device.
   - Click **Sign In**.

Note: For more information on multifactor authentication, see the *Setting Up Your Security Standards Settings* section, or see the *Changing Your Profile* document.

Tip: If you forgot your password, see the *Appendix A – Password Recovery* section. If you lost access to the authenticator on your smart device, see the *Changing Your Profile* document.

Setting Your Account Settings

After you have signed in to LTM for the first time, changed your password, and set and answered your password recovery questions, the next step is to access and configure your account settings.

The following subsections detail how to set up your account settings:

- *Setting Up Your Security Standards Settings*
- *Setting Up Your User Shifts*
- *Setting Up Your IP Address Restrictions*
- *Setting Up Your General Settings*

Setting Up Your Security Standards Settings

Security settings define which security rules, standards, and policies are enforced by LTM. These settings affect overall user and site access regulations, such as password definitions, how many login attempts to allow, access rights, and suspension criteria.

The security settings help you remain compliant with several different industry-specific security programs. While these settings are not required by Shift4 or LTM, you are advised to consider using them to help protect your interests.

The Security Settings page has two sections:

- Security Program Compliance Overview: Allows you to select predefined security programs, which set multiple rules all at once.
- User Security: Allows you to select individual rules to create a custom security program.

To set up your security settings, complete the following steps:

1. From the menu, select **Settings > Security Settings**.
2. To set a predefined security program or programs, continue to the *Selecting Security Program Compliance Overview Settings* section. To select individual rules and create a custom security program, continue to the *Selecting User Security Settings* section.

Selecting Security Program Compliance Overview Settings

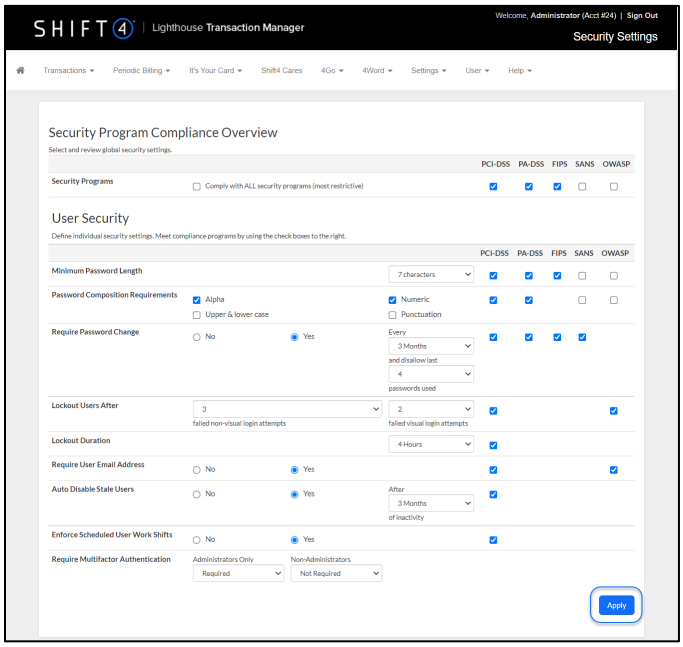
You can select a predefined security program that will set the necessary individual rules for that program.

For example, try selecting a program, such as PA-DSS. Notice the changes to the settings, including minimum password length and password composition requirements. Selecting an additional program will add the rules of that program to the one you already have selected. To undo your changes, from the menu, select **Settings > Security Settings** without clicking apply.

To set a predefined security program, complete the following steps:

1. On the Security Settings page, in the Security Program Compliance Overview section, select the desired programs:
    - **Comply with ALL security programs (most restrictive)**
    - **PCI-DSS**
    - **PA-DSS**
    - **FIPS**
    - **SANS**
    - **OWASP**

2. Click **Apply**.



Tip: After you click Apply, the rules are immediately enforced for all user types, including the Account Administrator. For example, on your next sign in as the Account Administrator, you may be required to change your password again if your current password does not meet the rules you have just applied to your account.

Selecting User Security Settings

You can create a custom security program by choosing individual rules in the User Security section.

When you make a change to an individual rule in the User Security section, if the change means all the necessary individual rules for a predefined security program have been enabled, then the program will be automatically selected. If the change means necessary rules for a predefined program are disabled, then the program will be automatically cleared.

If you select an option under one of the predefined security programs in the User Security section, you may notice numbers and/or times change for individual rules. For example, if you select PCI-DSS in the Minimum Password Length row, you will see the number of characters change to 7 in the Minimum Password Length list.

To set individual rules and create a custom security program, complete the following steps:

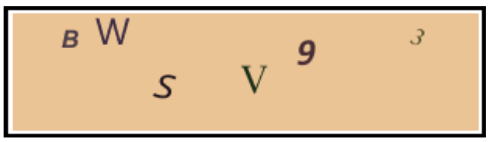
1. On the Security Settings page, in the User Security section, select the desired rules:

    - **Minimum Password Length:** Select the minimum number of characters that user passwords must contain from the list. Eight characters is the standard; however, you can choose to set this higher. Longer passwords can be harder to guess, but they are sometimes more difficult to remember. PCI DSS requirement is a minimum of seven characters.

    - **Password Composition Requirements:** Select all required elements that passwords must include from the **Alpha**, **Upper & lower case**, **Numeric**, and **Punctuation** options. Again, the more options selected, the more secure your password may be; however, you may also create a more difficult password for your users to remember when trying to sign in. For instance, requiring punctuation will make the password not consist of what is referred to as “dictionary words.” Dictionary words are used when trying to guess passwords, so this option will force your users to choose a password that does not exist in the dictionary and therefore negates this possibility. PCI DSS requirement is a combination of alphabetic and numeric characters.

    - **Require Password Change:** Select **Yes** to require users to change their password, and then select how often they will need to do this and how often they can reuse a previous password. If you choose a lower value, your users will be required to change their password on a regular basis. This is a good thing, as the password then becomes a moving target. This option, when used in conjunction with other settings, can make password retention harder on your users. For example, requiring a password to be changed often and be long with all composition requirements will make for a very difficult password to memorize. This can be a good thing, but may require you or administrator-type users for the account to have to respond to a higher number of user account reactivations. PCI DSS requirement is every 90 days.

- **Lockout Users After:** Select the maximum number of failed non-visual login attempts a user may have before being locked out of LTM. Setting this higher allows for more tries for your users, but will also allow for more tries for those people that should not be signing in and are just trying to guess the password. You also need to select the maximum number of failed visual login attempts, which are intended to prevent automated attacks. Below is an example of a visual verification screen. PCI DSS requirement is lock out after six failed attempts.



- **Lockout Duration:** Select the duration of time a user will remain locked out of LTM after the predetermined number of invalid login attempts. Setting this value lower will make it easier on your users, but also on those trying to basically "hack" your account. Higher values require the users to wait longer, but make it less tempting to people who shouldn't be trying to get in to your LTM account. PCI DSS requirement is a 30-minute lockout duration.
- **Require User Email Address:** Select **Yes** to require you or administrator-type users for the account to enter an email address when configuring users in LTM. (You can also use the entered email address to send a welcome email or a temporary password to the corresponding user.)

Requirement: Shift4 requires corporate email addresses. Personal email addresses (such as Gmail, AOL, Yahoo, etc.) are not acceptable.

- **Auto Disable Stale Users:** Select **Yes** and the time of inactivity that must pass before user accounts will be automatically suspended.
- **Enforce Scheduled User Work Shifts:** Select **Yes** to restrict access to LTM based on the user's assigned shifts. User shifts help you manage access and prevent users from signing in when not at work. User shifts do not apply to the Account Administrator, but they must be created by you or administrator-type users for the account and then appropriately assigned to each user.

- **Require Multifactor Authentication:** Multifactor authentication requires separate methods of authentication from different sources to verify a user's identity. All LTM user accounts are encouraged to use multifactor authentication, especially administrator-type user accounts. You can encourage or require the use of multifactor authentication by completing the following steps:
  - To require all administrator-type users to set up multifactor authentication, select **Required** from the Administrators Only list.
  - To encourage all administrator-type users to set up multifactor authentication, select **Remind Users Only** from the Administrators Only list.
  - To require all non-administrator users to set up multifactor authentication, select **Required** from the Non-Administrators list.
  - To encourage all non-administrator users to set up multifactor authentication, select **Remind Users Only** from the Non-Administrators list.
  - If you do not want to require multifactor authentication for non-administrators, select **Not Required** from the Non-Administrators list.

Note: If multifactor authentication is required when signing in to LTM, the user (including the Account Administrator) will be redirected to the Change Profile page where multifactor authentication is configured. You will not be able to proceed or use your account until you have configured multifactor authentication. Follow the directions displayed in LTM to complete this process.

2. Click **Apply**.

Tip: After you click Apply, the rules are immediately enforced for all user types, including the Account Administrator. For example, on your next sign in as the Account Administrator, you may be required to change your password again if your current password does not meet the rules you have just applied to your account.

Setting Up Your User Shifts

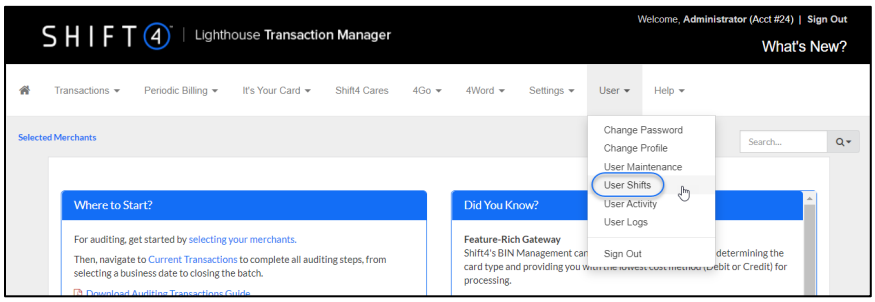
User shifts restrict access to LTM based on the user's assigned shifts. User shifts help you manage access and prevent users from signing in when not at work.

The Account Administrator and administrator-type users for the account can configure shifts on the User Shifts page.

Note: User shifts do not apply to the Account Administrator.

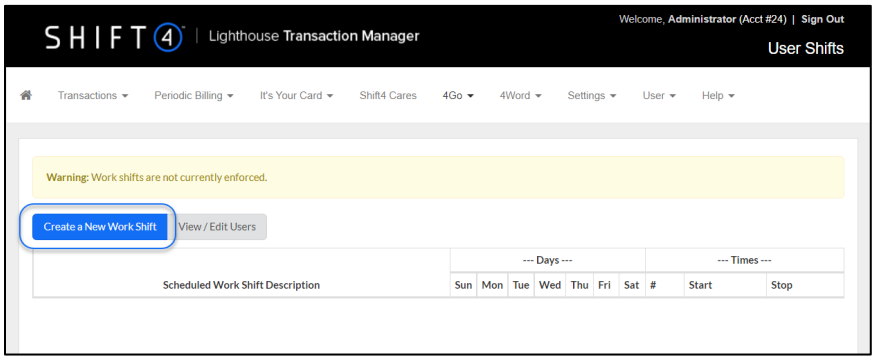
To create user shifts, complete the following steps:

1. From the menu, select **User > User Shifts**.



Tip: The User Shifts page can also be accessed by clicking the User Shifts link on the Administration Quick Links page and by clicking the View/Edit Shifts link on the User Maintenance page.

2. On the User Shifts page, click the **Create a New Work Shift** link.



3. In the Scheduled Work Shift Description field, enter a name, such as “Day Shift” or “Auditor.”
4. In the Start of Shift Days section, select the days on which the shift starts:
   - **Sun**
   - **Mon**
   - **Tue**
   - **Wed**
   - **Thu**
   - **Fri**
   - **Sat**

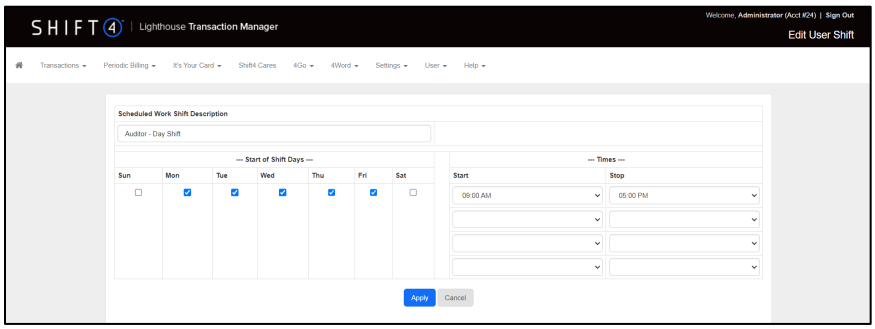
5. In the Times section, select the start and stop times from the appropriate list (from 12:00 AM to 11:30 PM or 24 hours).

Note: To create a shift that provides access to LTM 24 hours a day, select **24 Hours** in the Start list. Thus, when this shift is assigned to a user, the user will be able to access LTM at any time in relation to the selections made in the Start of Shift Days section. This type of shift should only be given to a completely trusted employee.

If an assigned shift crosses midnight (12 a.m.), you will need to create one shift for the time leading up to midnight and one shift for the time after midnight, ensuring the next day is selected in the Start of Shift Days section.

---

6. Click **Apply**.



Editing an Existing User Shift

To edit an existing user shift, complete the following steps:

1. On the User Shifts page, click an existing user shift name under Scheduled Work Shift Description.
2. On the Edit User Shift page, make any desired changes.

Tip: For additional information, see the *Setting Up Your User Shifts* section.

3. Click **Apply**.

Setting Up Your IP Address Restrictions

Only the Account Administrator can access and configure the IP Address Restrictions page.

WARNING! Lockout Hazard! Use extreme caution when adding IP addresses to the restriction list to avoid locking yourself out of your account. This feature is designed for those organizations that have redundant IP addresses or who perform auditing steps in a location external to clerks and managers. For assistance, contact the Shift4 Customer Support team at 888-276-2108, option 1.

An IP address is a number assigned to your computer to use the Internet. The servers for the LTM website identify your computer by its IP address.

There are two basic ways you can set up your IP address restrictions.

- Automatically populating IP addresses
- Manually entering IP addresses

Automatically Populating IP Addresses

To configure your IP addresses to populate automatically as users connect, complete the following steps:

- On the IP Address Restrictions page, in the IP Address Restriction Slots field, enter the maximum number of slots you want to allow for IP Address. Slots are the number of available spaces that you allow for IP addresses to be automatically inserted.
- As users sign in to LTM, their IP addresses are added to the IP Address Restriction List. When there are as many IP addresses as the number of slots specified, no other address will be able to connect to your LTM account unless the Account Administrator increases the number of slots.

For example, if you allow 6 slots, but you have 7 locations where users might sign in to LTM, one of the locations will be locked out and cannot connect to LTM.

Note: The IP address configuration method above does not restrict the Account Administrator from manually adding additional IP addresses. However, once the number of IP addresses reaches the number of slots entered in the IP Address Restriction Slots field, no further IP addresses can be automatically populated.

Manually Entering IP Addresses

Warning! Caution! Lockout Hazard! Use only with static IP addresses. If you use dynamic addresses, each web session will generate a new address. Eventually, you will reach the maximum number of slots selected, locking out any additional dynamic address connections. If you lock out the Account Administrator IP address, to start a formal request for help, contact the Shift4 Customer Support team at 888-276-2108, option 1.

To manually add explicit IP address to be allowed, complete one of the following options:

To create a selected list of permitted IP addresses, complete the following steps:

1. From the menu, select **Settings > IP Address Restrictions**.
2. In the IP Address Restrictions Slots field, enter the number of IP addresses you want to allow.

3. In the IP Address Restriction List field, enter the IP addresses that you want to allow separated by a comma (For example, 1.2.3.4,1.2.4.6) or leave the list blank and the system will dynamically populate the list as users sign in.

To create a range of permitted IP addresses, complete the following steps:

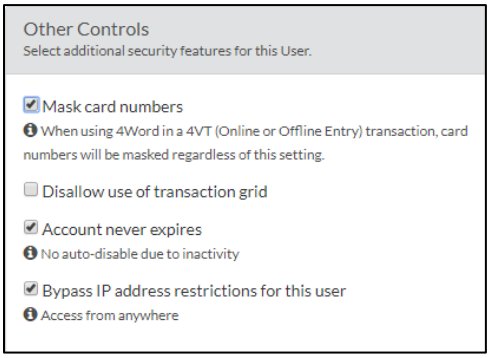
1. From the menu, select **Settings > IP Address Restrictions**.
2. In the IP Address Restrictions Slots field, enter a value of 1.
3. In the IP Address Restriction List field, enter the IP address range using the following format examples:
   - 1.2.3.* – This would provide 256 IP addresses with a range of 1.2.3.0 to 1.2.3.255
   - 1.2.* – This would provide 65536 IP addresses with a range of 1.2.0.0 to 1.2.255.255

Important: Only the first asterisk is honored. No embedded asterisks are permitted. For example, 1.*.3.4 would be invalid.

Tip: Use the Wide Area Network (WAN) address, not the Local Area Network (LAN) address. You can search the Internet for a website that will display your WAN IP address.

IP Address Override Assignment Rights

When adding or editing a user in LTM, it is possible to allow a user account to bypass IP address restrictions. This basically enables this user account to sign in from anywhere.

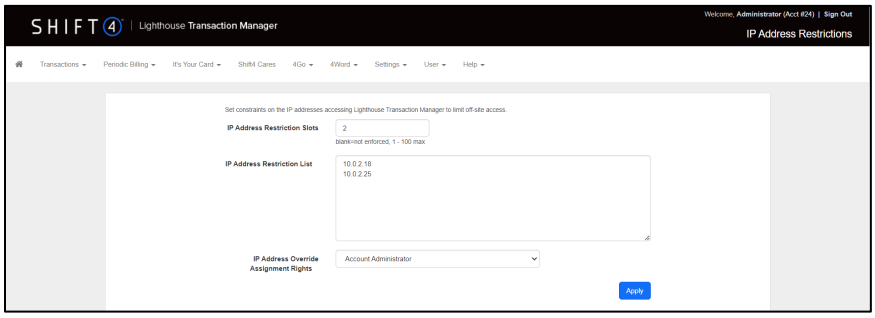


When setting the IP Address Restrictions, the Account Administrator can grant permission for any administrator-type user to bypass IP address restrictions for a user they create or edit, or the Account Administrator can retain that functionality alone.

To configure IP Address Override Assignment Rights, complete the following steps:

1. To only allow the Account Administrator to override the IP address restrictions when configuring users, select **Account Administrator** in the IP Address Override Assignment Rights list. To allow all administrator-type users to override the IP address restrictions when configuring users, select **Administrators**.

2. Click **Apply**.



Note: If LTM detects that changes being made to the IP Address Restrictions page will block access to the person making the change, a confirmation will be displayed prior to applying the new changes. This feature is to help prevent the Account Administrator from locking their IP address out of LTM.

Setting Up Your General Settings

To set up your general settings, complete the following steps:

1. From the menu, select **Settings > General Settings**.
2. Continue to one of the following sections to configure the appropriate settings:
    - *Configuring User Account Suspension Notifications*
    - *Configuring Fraud Sentry Notifications*
    - *Configuring Fraud Sentry Events*
    - *Configuring an Aging Warning*
    - *Configuring Card Grouping for Batches*
    - *Configuring Token Store Settings*
    - *Configuring Miscellaneous Account Settings*
    - *Configuring Encrypted Swipes*

Note: If this is your first time configuring these settings, Shift4 recommends each section be reviewed in the order listed above. After reviewing each section, you may determine the settings do not apply to your account, in which case you do not need to configure them.

Configuring User Account Suspension Notifications

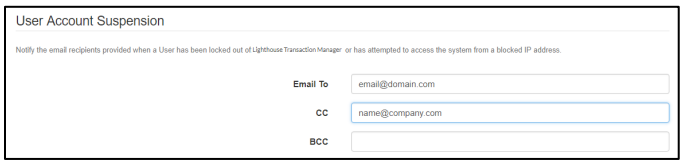
The User Account Suspension section allows the Account Administrator to configure who should receive an email notification when a user has been locked out of LTM or when a user has attempted to access LTM from a blocked IP address.

This allows the Account Administrator and administrator-type users for the account to quickly reset passwords, reactivate accounts (after verifying that the user did in fact lock out their account and that the lockout was not due to a hack attempt), or to address why a user is trying to access their account from an unauthorized location.

Tip: If you receive an email notification due to a blocked IP address, check the IP address to see if it is a known and trusted IP address. If it is, you might consider revising your IP address restrictions. For additional information, see the *Setting Up Your IP Address Restrictions* section.

To configure user account suspension notifications, complete the following steps:

1. In the User Account Suspension section, complete the following step:
    - In the Email To, CC, or BCC field, enter an email address. Multiple email addresses should be separated by a comma with no spaces.



2. On the General Settings page, click **Save Changes**.

Note: The Account Administrator and administrator-type users for the account can reactivate locked out user accounts. For additional information, see the *Reactivating a Suspended User Account* section.

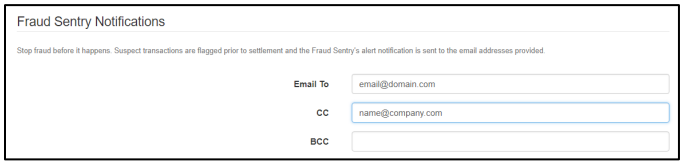
Configuring Fraud Sentry Notifications

Fraud Sentry® helps merchants identify, manage, and prevent suspicious and costly fraudulent transactions.

The Fraud Sentry Notifications section allows the Account Administrator to configure who should receive an email notification when a batch is closed containing a suspicious transaction (as defined by the configured settings in the Possible Duplicates, Unverified Refunds, or Suspicious Card Usage section).

To configure Fraud Sentry notifications, complete the following steps:

1. In the Fraud Sentry Notifications section, complete the following step:
    - In the Email To, CC, or BCC field, enter an email address. Multiple email addresses should be separated by a comma with no spaces.



2. On the General Settings page, click **Save Changes**.

Note: If a default email address was stored at the time the account was set up with Shift4 and you would like to change it, but the address does not appear in the Fraud Sentry Notifications section, contact the Shift4 Customer Support team at 888-276-2108, option 1.

Configuring Fraud Sentry Events

When the settlement process is initiated, Fraud Sentry will scan through all transactions in the batch and flag any suspicious transactions. Suspicious transactions are defined by configuring the Possible Duplicates, Unverified Refunds, or Suspicious Card Usage section.

Every card in the batch is checked against the configurations in these sections, so you should not add more than two or three checks to help ensure swift batch processing. Too many checks can slow down the batch processing.

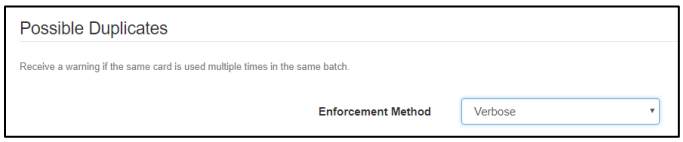
The options are discussed in detail in their respective sections to help you decide which are best suited for your business model.

Possible Duplicates

Fraud Sentry scans all transactions in the batch to check if a card is charged or refunded more than once in the same batch. If possible duplicates are present, Fraud Sentry takes action based on the option selected in the Enforcement Method list.

To configure possible duplicates, complete the following steps:

1. In the Possible Duplicates section, in the Enforcement Method list, select the desired option:
    - **Disabled:** Fraud Sentry will not scan for possible duplicates, and an email notification is not sent.
    - **Silent**: Fraud Sentry will scan for possible duplicates, settlement is allowed, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.
    - **Verbose:** Fraud Sentry will scan for possible duplicates, the user processing the batch is notified and required to reenter their login and password to complete settlement, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.
    - **Disallow:** Fraud Sentry will scan for possible duplicates, the user processing the batch is notified and required to correct the transactions before settlement can be completed, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.



2. On the General Settings page, click **Save Changes**.

Unverified Refunds

The most common internal credit card fraud involves corrupt employees issuing false or overstated refunds to their own cards or to those of their cohorts.

Fraud Sentry scans batches prior to settlement for unverified refunds. If unverified refunds are present, Fraud Sentry takes action based on the options selected in the Detection Method, Maximum Duration, and Enforcement Method lists.

Note: If your account is new, it may not have the data history required to check for unverified refunds.

To configure unverified refunds, complete the following steps:

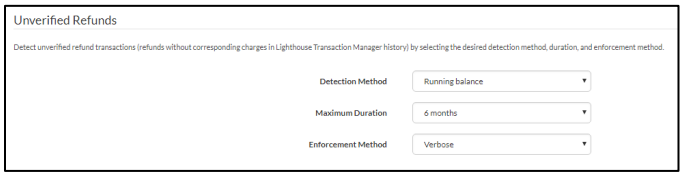
1. In the Unverified Refunds section, in the Detection Method list, select the desired option:
    - **Disabled:** Fraud Sentry will not scan for unverified refunds.
    - **Running Balance:** Fraud Sentry will scan for unverified refunds and compare the refunds to the running balance totals of the cards being refunded. If the refunds are more than the running balance totals, they will be flagged as unverified. This is the option Shift4 recommends.
    - **Exact Amount:** Fraud Sentry will scan for unverified refunds and flag refunds as unverified if they do not have corresponding charges in the exact amount.

2. In the Unverified Refunds section, in the Maximum Duration list, select how far back Fraud Sentry should go to calculate a card's running balance and to search for corresponding charges:
   - **3 months**
   - **6 months**
   - **9 months**
   - **1 year**
   - **2 years**
   - **3 years**

Note: While you can select up to three years, it is important to note that PCI DSS recommends not storing credit card data for this length of time; therefore, credit card transaction data can only be reviewed for two years. If three years is selected, it will only apply to IYC gift cards' history. Shift4 recommends selecting 6 months.

---

3. In the Unverified Refunds section, in the Enforcement Method list, select the desired option:
   - **Silent:** Fraud Sentry scans for unverified refunds, settlement is allowed, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.
   - **Verbose:** Fraud Sentry scans for unverified refunds, the user processing the batch is notified and required to reenter their login and password to complete settlement, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.
   - **Disallow:** Fraud Sentry will scan for unverified refunds, the user processing the batch is notified and required to correct the transactions before settlement can be completed, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.



4. On the General Settings page, click **Save Changes**.

Suspicious Card Usage

The Suspicious Card Usage section allows you to configure constraints for events regarding same-card usage, refunds, and voids that you know to be suspicious for your specific business. The following are possible constraints:

- Same card used by a clerk Within a Period: Fraud Sentry scans for cards that are used repeatedly by the same clerk within a specified period of time.
- Same card used at a merchant Within a Period: Fraud Sentry scans for cards that are used repeatedly at a single merchant location within a specified period of time.
- Same card used across all merchants Within a Period: Fraud Sentry scans for cards that are used at multiple locations within the merchant's network within a specified period of time.
- Credits entered by a clerk Within a Period: Fraud Sentry scans for refunds that are issued by each clerk within a specified period of time.
- Credits entered for a merchant Within a Period: Fraud Sentry scans for refunds that are issued at a single merchant location within a specified period of time.
- Credits entered across all merchants Within a Period: Fraud Sentry scans for refunds that are issued at multiple locations within the merchant's network within a specified period of time.
- Voids by a clerk Within a Period: Fraud Sentry scans for voids that are issued by each clerk within a specified period of time.
- Voids for a merchant Within a Period: Fraud Sentry scans for voids that are issued at a single merchant location within a specified period of time.
- Voids across all merchants Within a Period: Fraud Sentry scans for voids that are issued at multiple locations within the merchant's network within a specified period of time.

Note: If you do not use clerk IDs, the constraints that include "clerk" will not apply to you. Likewise, if you do not have multiple merchants, the constraints that include "across all merchants" will not apply to you.

After a constraint has been chosen, three items will need to be considered:

- Which timeframe threshold to configure?
- What number of transactions is suspicious?
- What amount processed is suspicious?

For example, if you chose to configure a 1-day threshold, entered 4 as the number of transactions that is suspicious, and entered $15 as the amount that is suspicious, the following would be true:

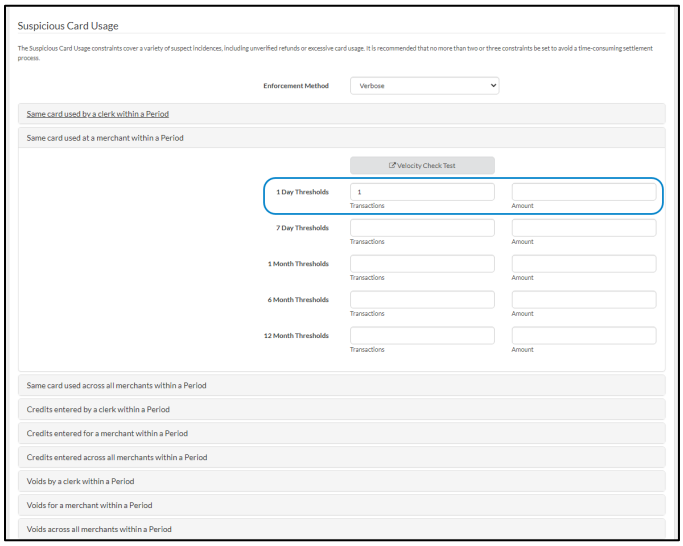
- It would not be suspicious to have a customer use their card three times, but on the fourth time it would be suspicious.
- It would not be suspicious for a customer to have a transaction of less than $15, but at or more than $15 would be suspicious.
- It would not be suspicious to have a customer use their card more than once but less than four times, if the total of their transactions is less than $15, but a total at or more than $15 would be suspicious.

To avoid a lengthy settlement process, it is recommended that no more than three constraints be configured. Fraud Sentry will scan the batch prior to settlement and take action on the constraints according to the option selected in the Enforcement Method list.

To configure suspicious card usage, complete the following steps:

1. In the Suspicious Card Usage section, in the Enforcement Method list, select the desired option:
   - **Silent:** Fraud Sentry scans for suspicious card usage, settlement is allowed, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.
   - **Verbose:** Fraud Sentry scans for suspicious card usage, the user processing the batch is notified and required to reenter their login and password to complete settlement, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.
   - **Disallow:** Fraud Sentry will scan for suspicious card usage, the user processing the batch is notified and required to correct the transactions before settlement can be completed, and an email notification is sent to the recipients specified in the Fraud Sentry Notifications section.

2. In the Suspicious Card Usage section, in the desired constraint section, enter the number of transactions that is suspicious and/or the amount that is suspicious in one or more of the threshold fields.
    - 1 Day Thresholds: When configured, transactions in the batch for the selected business date will be scanned during the settlement process.
    - 7 Day Thresholds: When configured, transactions in the batch for the selected business date and previous six days will be scanned during the settlement process.
    - 1 Month Thresholds: When configured, transactions in the batch for the selected business date's month will be scanned during the settlement process.
    - 6 Month Thresholds: When configured, transactions in the batch for the selected business date's month and previous five months will be scanned during the settlement process.
    - 12 Month Thresholds: When configured, transactions in the batch for the selected business date's month and previous 11 months will be scanned during the settlement process.



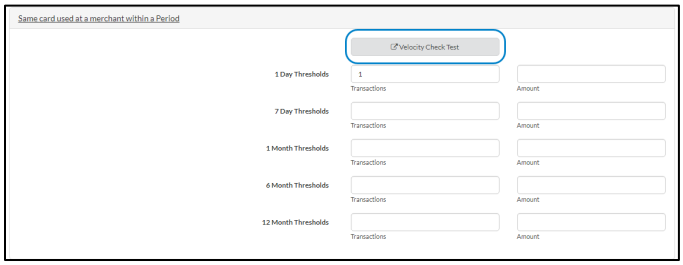
3. On the General Settings page, scroll down and click **Save Changes**.

Performing a Velocity Check Test

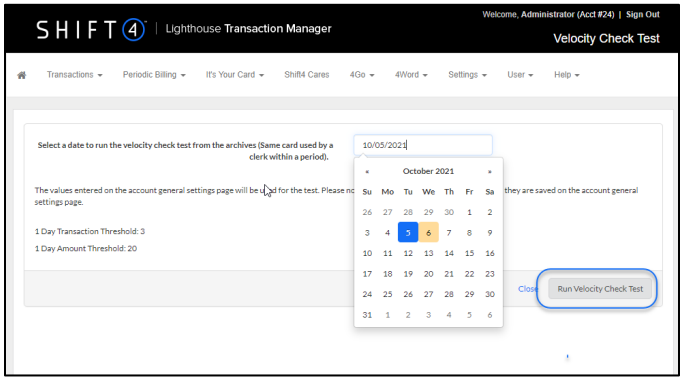
The Velocity Check Test allows you to test and adjust your constraint configurations based on real data, without waiting for a batch settlement to be processed. The test allows you to see the amount of alerts that would be received, as well as the time Fraud Sentry spends scanning the transactions. This information could be used to adjust your configurations to avoid a long settlement time each day.

To run a velocity check test, complete the following steps:

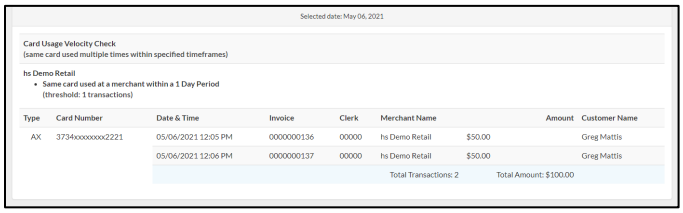
1. From the menu, select **Transactions > Select Merchant**.
2. Select the merchant(s) you want to run the velocity check for.
3. From the menu, select **Settings > General Settings**.
4. In the Suspicious Card Usage section, in the desired constraint section, click **Velocity Check Test**.



5. On the Velocity Check Test page, select a date on the calendar, and then click **Run Velocity Check Test**.



6. Fraud Sentry will scan your archived transactions, and then display results.

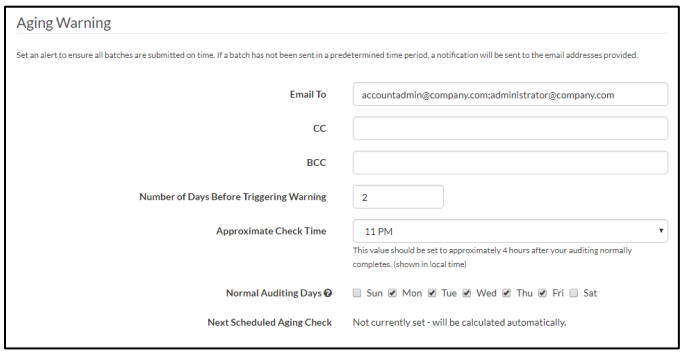


Configuring an Aging Warning

The Aging Warning section allows the Account Administrator to configure who should receive an email notification when a batch is not submitted in a timely manner.

To configure an aging warning, complete the following steps:

1. In the Aging Warning section, complete the following steps:
    - In the Email To, CC, or BCC field, enter an email address. Multiple email addresses should be separated by a comma with no spaces.
    - In the Number of Days Before Triggering Warning field, enter the number of auditing days to allow sale transactions to sit before an aging warning email notification is sent.
    - In the Approximate Check Time list, select the time when LTM should verify that the batches are settled (from 12 Midnight to 11 PM and shown in the browser's local time).
    - In the Normal Auditing Days area, select the days on which LTM should verify that batches were settled.



Requirement: Unlike Fraud Sentry email notifications, the default email address stored when this account was created (if any) does not receive aging warning email notifications. Therefore, all recipients who need to receive aging warning email notifications must have their email address entered into one of the fields.

2. On the General Settings page, click **Save Changes**.

Note: The Next Scheduled Aging Check area displays the date and time of the next scheduled aging verification.

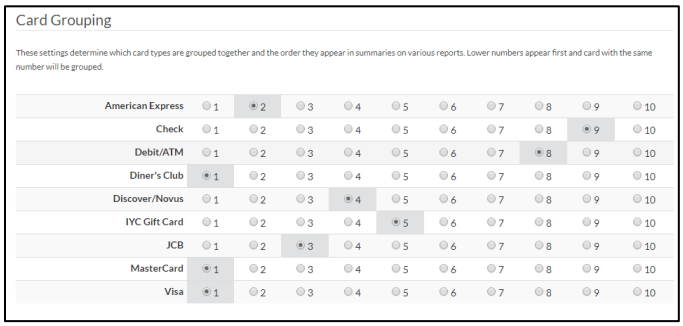
Configuring Card Grouping for Batches

The Card Grouping section allows the Account Administrator to group card types so that they display together and in a particular order when viewing batch summaries on various reports.

Cards that have the same number will be grouped together. Cards with the lowest group number will display before cards with higher group numbers. For example, if you select 1 as the group number for MasterCard and Visa, they will be displayed together and first in batch summaries.

To configure card groupings, complete the following steps:

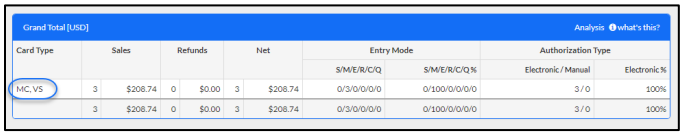
1. In the Card Grouping section, click the group number to which each card type belongs.



2. On the General Settings page, click **Save Changes**.

Example of Card Grouping

The result of the settings in the Card Grouping section can be seen in the summary areas of batch reports.



Configuring Token Store Settings

LTM uses TrueTokenization® to secure and protect card data. TrueTokenization replaces the card number with a token (a unique 16-character alphanumeric code). Tokens are stored in two repositories: the local TOKENSTORE and the global TOKENSTORE.

Local TOKENSTORE (Single Use)

Access to the local TOKENSTORE data is restricted to the single account number which initially stored the card information. The Access Token that the vendor uses to access the local TOKENSTORE is the same value established for the vendor account at Shift4.

Global TOKENSTORE (Multi-Use)

The global TOKENSTORE is designed for medium to large merchants who need a single repository of tokens that can be utilized by multiple locations.

For example, a hotel chain with a mini reservation website that allows their customer to book a reservation at any hotel under their brand would use the global TOKENSTORE rather than the local TOKENSTORE. The global TOKENSTORE removes the storage burden for merchants who are maintaining a large group of customer profiles containing card information that can be utilized across all properties. It also enables merchants to secure card data obtained from third-party central reservations vendors.

For the global TOKENSTORE, a separate account is set up with a separate Access Token that is in addition to the vendor accounts established at Shift4. Multiple vendor locations that have different Access Tokens can all access the same global TOKENSTORE using the global TOKENSTORE Access Token.

TOKENSTORE Security Settings

This section addresses security for cardholder data (CHD) stored in the TOKENSTORE as it applies to the PCI Data Security Standard (DSS). The provided information is applicable to both the local TOKENSTORE and the global TOKENSTORE.

Each time a credit card is registered with TOKENSTORE, a token is generated and issued to the registering entity. Full track data, if received, is retained during a card present registration process. The primary account number (PAN), expiration date, and card security code, if received, are retained during a card not present registration process. All CHD and sensitive authentication data (SAD) and track data that is received is stored on disk in a pre-authorization state and is encrypted to cryptography standards that exceed the requirements detailed in the DSS, Requirement 3.

Token Store Options

Sensitive Authentication Data Storage (Pre-authorization PCI-DSS compliant)

DSS-defined SAD and track data will automatically be securely deleted from disk after 96 hours or after the initial authorization request, whichever comes first. However, the registering entity may configure the deletion process to occur on a shorter interval. When a credit card is registered, it is assumed that it will be authorized immediately. In all cases, the retention time of pre-authorization SAD and full track data will never exceed 96 hours. If an authorization request occurs within 96 hours of registration or the interval set by the registering entity, the transaction will process with the PAN, expiration date, and associated token with either the card security code or full track data. If an authorization request occurs after the 96-hour retention period or interval set by the registering entity, the transaction will process with only the PAN, expiration date, and associated token. Upon registration, registering entities should opt to immediately authorize a transaction on a credit card to minimize the amount of time full track data and/or SAD is stored in the pre-authorization state.

Token Storage Duration

In all instances, the only data that is retained in the TOKENSTORE post-authorization is the PAN, expiration date, and associated token. The merchant can choose to set a **Token Storage Duration** time between 3 days and 24 months, or the merchant can choose **Card Expiration**, in which case the card data will be retained until the expiration date of the card. All post-authorization CHD is encrypted to cryptography standards that exceed the requirements detailed in the DSS, Requirement 3. It is not possible to view or extract CHD stored in a TOKENSTORE through any type of user interface.

Token Sharing Account Numbers

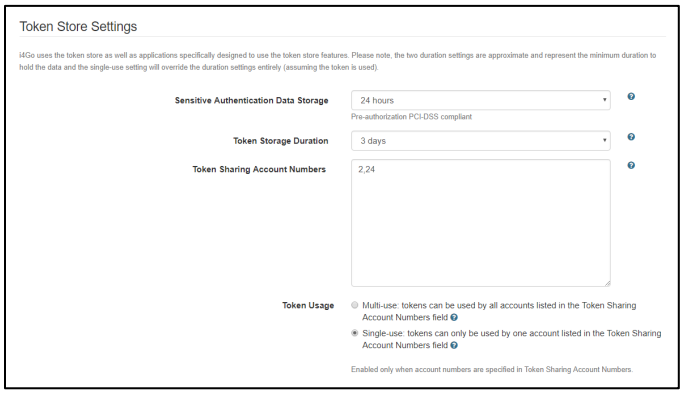
Enter the serial number(s) that you received from Shift4. If you are using local TOKENSTORE only, you will have one number. If you are using the global TOKENSTORE, too, then you will have two or more numbers.

Token Usage

If Token Sharing Account Numbers are specified, you have the choice of allowing all specified Token Sharing Accounts to use a Token in the token store or only allowing the first specified Token Sharing account to use the Token. Allowing all specified Token Sharing Account to use a Token might be selected if a merchant with multiple account numbers and multiple merchant locations wants customers using credit cards to be able to return merchandise at any of its merchant locations.

To configure your Token Store Settings, complete the following steps:

1. In the Token Store Settings section, from the Sensitive Authentication Data Storage list, select the appropriate time.
2. From the Token Storage Duration list, select the desired storage duration.
3. *(If applicable)* In the Token Sharing Account Numbers field, enter the account numbers that will be permitted to access tokens from this account.
4. *(If applicable)* In the Token Usage section, select one of the available options.
5. On the General Settings page, click **Save Changes**.

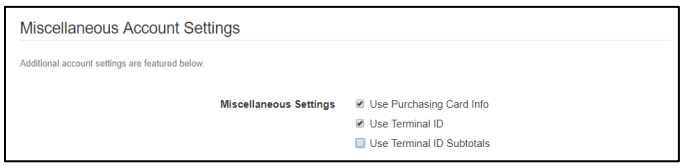


Configuring Miscellaneous Account Settings

Certain information is collected when transactions are entered using the Online Entry and Offline Entry options in LTM. This information is hardcoded and cannot be changed. However, the Account Administrator can choose to collect additional information by enabling options in the Miscellaneous Account Settings section.

To enable additional options, complete the following steps:

1. In the Miscellaneous Account Settings section, in the Miscellaneous Settings area, complete the following steps:
    - *(Optional)* If your company processes transactions with purchasing cards, such as in Business to Business transactions, select **Use Purchasing Card Info**. This selection will allow users to enter additional information related to the purchase when the transaction is being entered using the Online Entry or Offline Entry option in LTM.
    - *(Optional)* If your company's point-of-sale (POS) or property management system (PMS) uses terminal IDs, select **Use Terminal ID**. This selection will allow users to enter a terminal ID when the transaction is being entered using the Online Entry or Offline Entry option in LTM.
    - *(Optional)* If your company's POS/PMS uses terminal IDs, select **Use Terminal ID Subtotals**. This selection displays subtotals by terminal ID on the Current Transactions and Archived Transactions pages when viewing options are set to sort by terminal ID. This can be useful if your interface reports are based on this number.



2. On the General Settings page, click **Save Changes**.

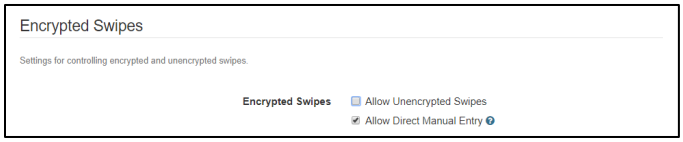
Configuring Encrypted Swipes

LTM supports encrypted and unencrypted Magnetic Swipe Readers (MSRs), and payment cards may be swiped directly into LTM during online entry, offline entry, and IYC transactions.

When encrypted swipe devices have been deployed to all users, LTM can be configured to only accept encrypted swipes.

To set LTM to only accept encrypted swipes, complete the following steps:

1. In the Encrypted Swipes section, complete the following steps:
    - Clear the **Allow Unencrypted Swipes** field.
    - *(If applicable)* If you have installed encrypted swipe devices at each POS/PMS and want to prevent manual entry, clear the **Allow Direct Manual Entry** field.



Note: If the Allow Direct Manual Entry field is cleared, the fields where payment card numbers and expiration dates can be manually entered will not be displayed.

2. On the General Settings page, click **Save Changes**.

Important: After you click Save Changes, unencrypted swipes will not be accepted and an error message will be displayed when unencrypted MSRs are used.

Creating User Accounts

Once you have set your account settings, the next step is to create an administrator-type account to use for daily tasks because the Account Administrator account should not be used for daily tasks.

The newly-created administrator-type account should be used for all tasks, and the Account Administrator account should only be used to access, configure, or change the settings that control the global LTM environment. In addition, the Account Administrator is the only account that can set up an administrator-type user or an IYC site administrator-type user. Other user types can be set up by administrator-type users for the account.

A variety of user types are available in LTM with configurable permissions that allow the Account Administrator and administrator-type users for the account to customize the abilities and permissions of each user created.

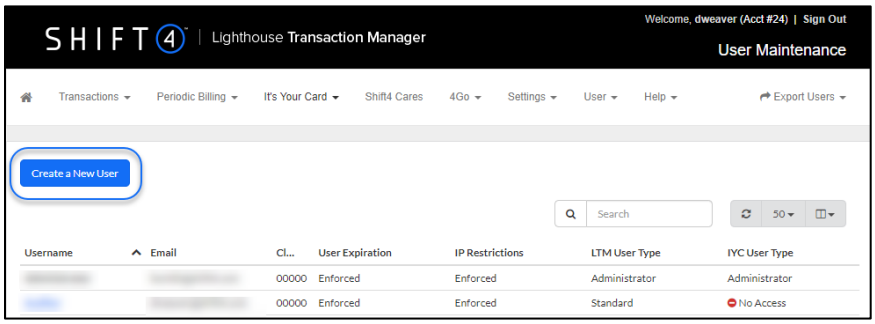
LTM currently has the following types of users available:

- No Access: This user type keeps the user's account active, while not allowing them to sign in to LTM. This user type is designed for employees taking extended periods away from the business, such as leaves of absence.
- Standard: This user type is the most common. It can be configured to access all features in LTM with the exception of the administrative menus. This user type is designed for auditors, clerks, or other non-management users.
- Administrator: This is a management user type and can be configured to access all features in LTM, except for the Account Administrator functions. In addition, this user type can create other users but cannot create administrator-type users. Only the Account Administrator can create administrator-type users.
- Site Admin: This user type is for creating a gift card site while the Account Administrator controls the global settings. For additional information, see the *IYC for Administrators* document.
- Online/Offline Entry: This user type allows access to the Online Entry and Offline Entry menu options and pages. It is designed for clerks who work at a business that use online entry and offline entry in LTM to process transactions instead of a traditional POS or PMS. The Online Entry and Offline Entry pages handle track swipes and printing to a receipt printer so all operations of an existing credit card terminal can be performed using a PC with a web browser and the appropriate add-on peripherals.
- API: This user type is specifically for third-party systems using direct server-to-server web service calls to communicate with LTM and cannot access menu options or sign in through normal means. It is designed for POS or PMS interface vendors. (This user type is not necessary for merchants using an Access Token to authenticate communication with LTM via direct server-to-server web service calls because the Access Token provides the authentication.).

Note: When setting up a new LTM user or editing an existing user, remember that the User Type and Permissions you select under Lighthouse Transaction Manager and It's Your Card will affect what the user will be able to view and what they will be able access. In some cases, they will not be able to see certain menu items, like It's Your Card. In other cases, they will see an option, such as Online Entry, but will not be able to access the functionality.

To create a user, complete the following steps:

1. From the menu, select **User > User Maintenance**.
2. On the User Maintenance page, click **Create a New User**.



3. In the Create User window, complete the following steps:

Requirement: If your web browser is configured to populate saved login information, ensure the fields in the Create User window are cleared before beginning.

- Enter a name in the Username field. Usernames are not case sensitive and the most common choice is some variation of first name, last name, and initials.

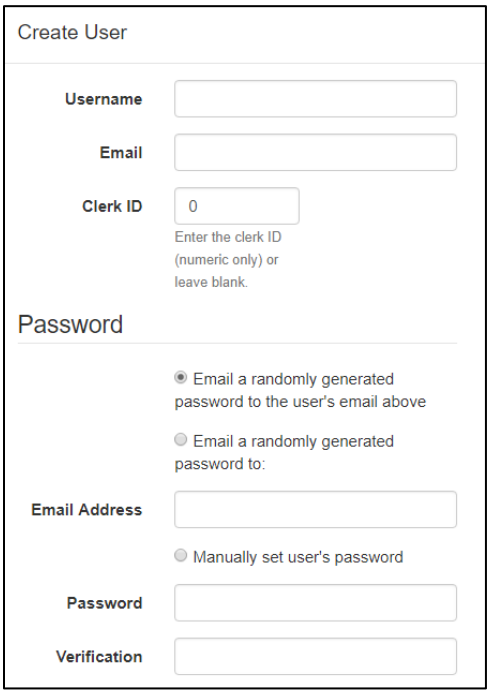
Note: You cannot use Admin or Administrator—this username is specifically for the Account Administrator account.

- *(If applicable)* Enter the user's email address in the Email field.

Requirement: An email address is required if the Account Administrator enabled Require User Email Address on the Security Settings page. Shift4 requires corporate email addresses. Personal email addresses (such as Gmail, AOL, Yahoo, etc.) are not acceptable.

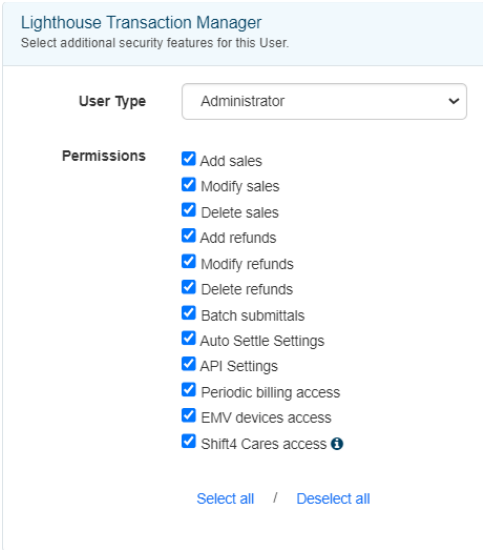
- *(Optional)* If clerk IDs are in use, enter the number that identifies the user in the Clerk ID field. Clerk IDs can contain up to five digits.
- In the Password area, select the desired option:
    - **Email a randomly generated password to the user's email above:** Select this option if you entered an email address in the Email field above. After this user account is created, a system generated email will be sent to the address in the Email field. It will contain the information (account number, username, and temporary password) the user will need to sign in to LTM for the first time. Immediately after signing in, the user will be prompted to change the temporary password to a unique, personal password and answer their five password recovery questions.
    - **Email a randomly generated password to: [Email Address]:** Select this option and then enter the user's email address in the Email Address field. LTM will not store the address entered into the Email Address field. After this user account is created, a system generated email will be sent to the address in the Email Address field. It will contain the information (account number, username, and temporary password) the user will need to sign in to LTM for the first time. Immediately after signing in, the user will be prompted to change the temporary password to a unique, personal password and answer their five password recovery questions.

- **Manually set user's password:** Select this option, enter a password in the Password field, and then reenter the password in the Verification field. Immediately after signing in, the user will be prompted to change the password to a unique, personal password and answer their five password recovery questions.



- In the Lighthouse Transaction Manager section, complete the following steps:
  - In the User Type list, select the desired option:
    - **No Access**
    - **Standard**
    - **Administrator**
    - **Online/Offline Entry**
    - **API**

- In the Permissions area, select the desired options:
  - **Add sales**
  - **Modify sales**
  - **Delete sales**
  - **Add refunds**
  - **Modify refunds**
  - **Delete refunds**
  - **Batch submittals**
  - **Auto Settle Settings**
  - **API Settings**
  - **Periodic billing access**
  - **EMV devices access**
  - **Shift4 Cares access**
  - **Billing statements access**



Note: If you are creating an administrator-type account, Shift4 recommends selecting Administrator and all permissions.

In addition, the *EMV devices access* permission will only be displayed and available if the account has EMV enabled.

The *Shift4 Cares access* permission will only be available if the account is participating in the Shift4 Cares gift card program:

When customers purchase one or more gift cards through the Shift4 Cares website, Shift4 will contribute an additional 5 percent to the merchant to increase the impact of every sale – up to $10 MILLION! This means their $100 purchase really gives the merchant $105 during this difficult time, and $210 MILLION goes back into the small business community!

When the permission is enabled, the user will have access to the Shift4 Cares page to manage orders (e.g., mark a gift card as being redeemed).

Lastly, the *Billing statements access* permission will only be displayed if applicable to your account. When enabled, the user can access the Billing Statements menu to view/download the PDFs.

- *(If applicable)* In the It's Your Card section, complete the following steps:
  - In the User Type list, select the desired option:
    - **No Access**
    - **Standard**
    - **Administrator**
    - **Site Admin**
    - **Online/Offline Entry**
    - **API**

- In the Permissions area, select the desired options:
  - **Issue cards**
  - **Activate cards**
  - **Deactivate cards**
  - **Sell cards**
  - **Fulfill orders**
  - **Delete authorizations**

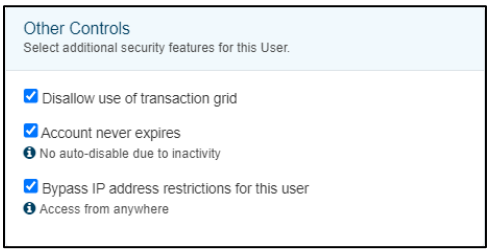
Tip: User types are defined in the *Creating User Accounts* section.

- In the Other Controls section, select the desired options:
  - **Disallow use of transaction grid:** If selected, the transaction grid is disabled. If cleared, the transaction grid, which is an advanced auditing tool and should only be used by those experienced in using this type of tool, is enabled. For additional information on the transaction grid, see the *Auditing Transactions* document.
  - **Account never expires:** If selected, this user account will never expire. If cleared, the account will expire in accordance with the configurations made by the Account Administrator.

Important: If the Account Administrator enabled Auto Disable Stale Users on the Security Settings page, selecting this option will override that setting and its configurations.

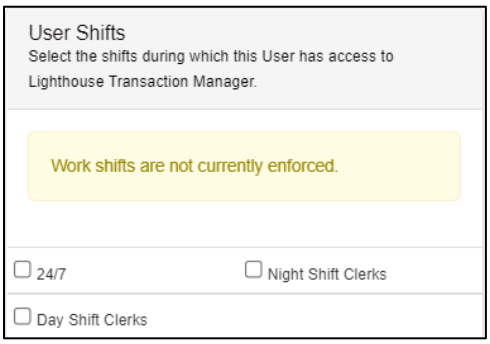
- **Bypass IP address restrictions:** If selected, this user account will be able to sign in to LTM from anywhere. If cleared, the account must sign in to LTM in accordance with the configurations made by the Account Administrator.

Important: If the Account Administrator enabled IP address restrictions, selecting this option will override those settings.



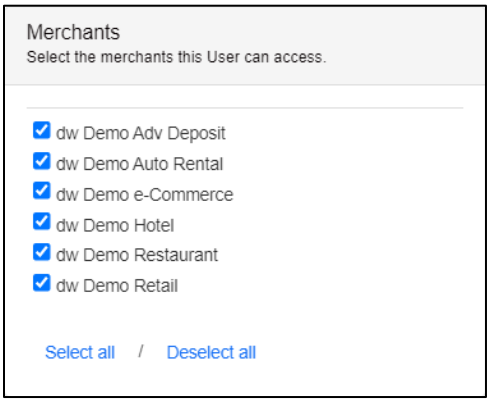
Note: If you are creating an administrator-type account, Shift4 recommends selecting all options.

- *(If applicable)* In the User Shifts section, select the shifts during which the user should be able to access LTM.



Requirement: User shifts must be selected if the Account Administrator enabled *Enforce Scheduled User Work Shifts* on the Security Settings page. If user shifts are not selected then the user will not be able to sign in to LTM.

- In the Merchants section, select the merchants that the user should be able to access in LTM.



Requirement: At least one merchant must be selected (even if it is the only option) in order to configure the account correctly.

Note: If you are creating an administrator-type account, Shift4 recommends selecting all merchants.

- Click **Create User**.

Note: If additional administrator-type accounts or IYC site administrator-type accounts are needed, repeat these steps. The Account Administrator is the only account that can create an administrator-type user or an IYC site administrator-type user. Other user types can be created by administrator-type users for the account.

Editing or Deleting a User Account

To edit or delete an existing user, complete the following steps:

1. From the menu, select **User > User Maintenance**.
2. On the User Maintenance page, click the Username you would like to edit or delete from LTM. This will open the Update User window.

Tip: To quickly locate a user, enter their username in the Search field.

3. *(If applicable)* To edit the user, complete the following steps:

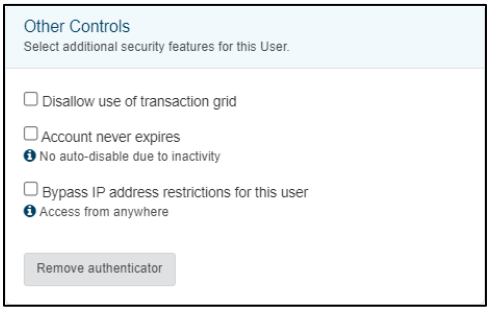
   - Edit any of the fields reviewed in the *Creating User Accounts* section. Note there is an additional option in the Password section:

     - **Keep user's current password:** This is selected by default when an existing user has been selected for editing. For example, when a suspended/locked user account needs to be reactivated by the Account Administrator or an administrator-type user, they can select **Reactivate** and then **Update User**. This will reactivate the user's account and they can attempt to sign in with their previously set password. If they don't remember their password, they can use Login Help on the User Sign In page to reset it.

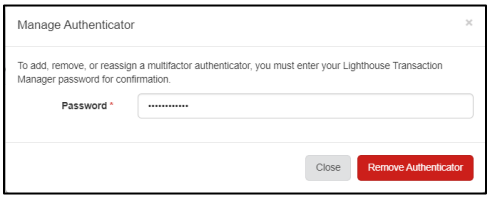
   - Click **Update User**.

4. *(If applicable)* To remove the authenticator from the user's account (because they lost their reset code), complete the following steps:

   - In the Other Controls section, click **Remove authenticator**.

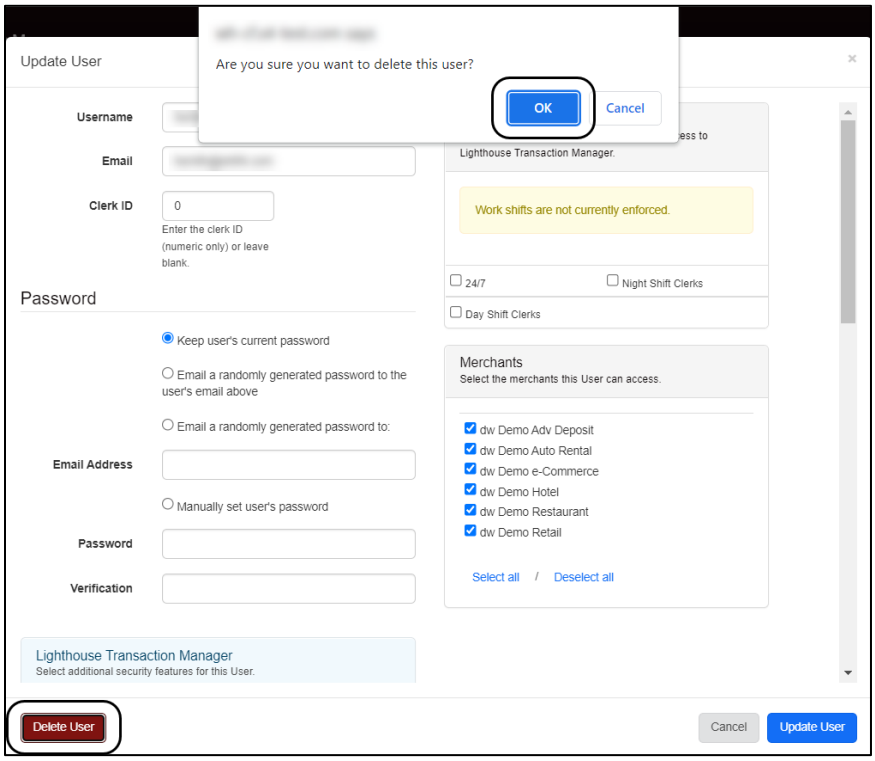


   - In the Manage Authenticator window, enter your LTM password, and then click **Remove Authenticator**.



5. *(If applicable)* To delete the user, click **Delete User** and then **OK**.

WARNING! Deleting a user account cannot be undone. Shift4 recommends editing user accounts to a No access user type in lieu of deleting user accounts.



Note: Deleting a user will not delete the information obtained by that user while they were active.

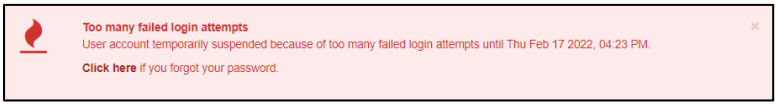
Reactivating a Suspended User Account

Accounts are automatically suspended if the number of login and visual verification attempts defined by the Account Administrator is exceeded.

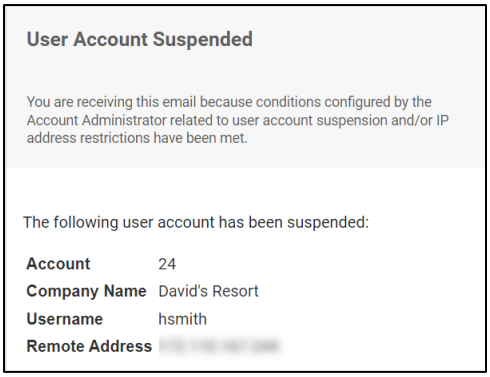
By default, the suspension lasts four hours. However, the time is configurable by the Account Administrator. Any additional invalid attempts suspend the account for 48 hours.

After the predetermined number of failures, three things happen:

1. The user account is locked out of LTM for the predetermined amount of time.



2. The user account suspension notifications are sent to the user(s) configured to receive them.

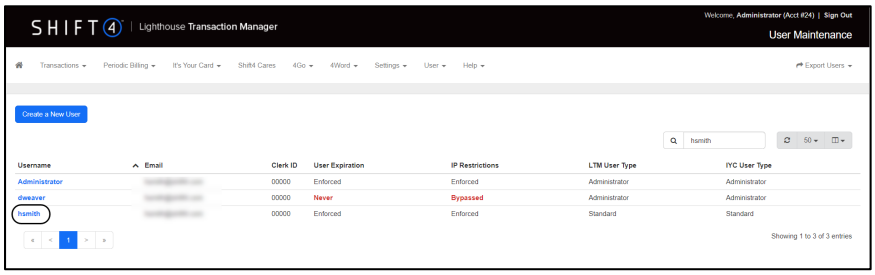


3. The user account is flagged as suspended in LTM.

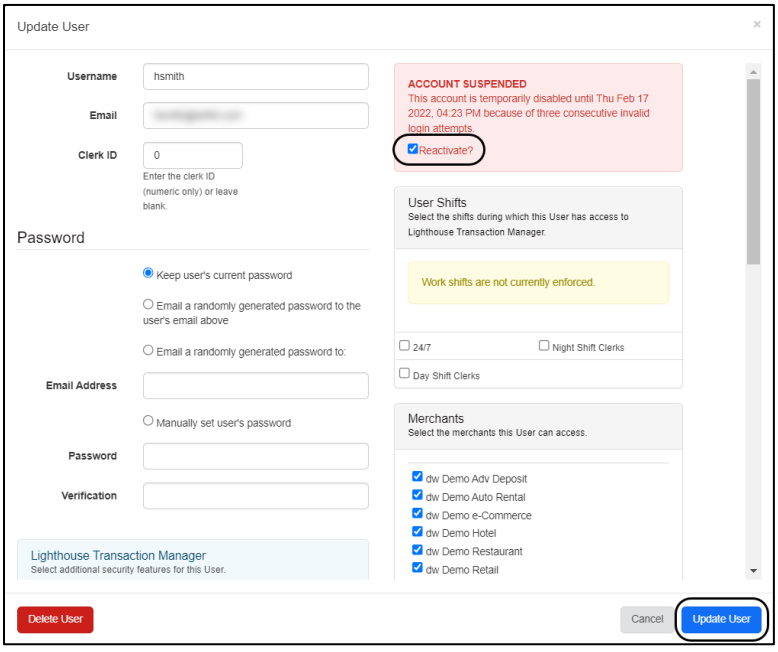
Note: If a non-administrative user is locked out, an administrator-type user can reactivate the account. If an administrator-type user is locked out, only the Account Administrator can reactivate the account. If the Account Administrator is locked out, contact the Shift4 Customer Support team at 888-276-2108, option 1.

To reactivate a suspended user account, complete the following steps:

1. On the User Maintenance page, click the Username that you would like to reactivate.



2. In the Update User window, locate the ACCOUNT SUSPENDED section.
3. Select **Reactivate** and then click **Update User**.



Using LTM Usage Monitoring

Any time a user signs in to LTM, their username, ID, session length, and other data is logged, and the information is available on the User Activity or User Logs page.

The pages are discussed in detail in their respective sections below.

Tip: The Account Administrator and administrator-type users for the account can use the information to ensure that all users are properly accessing and signing out of LTM.

Viewing User Activity

To view the User Activity page, complete the following steps:

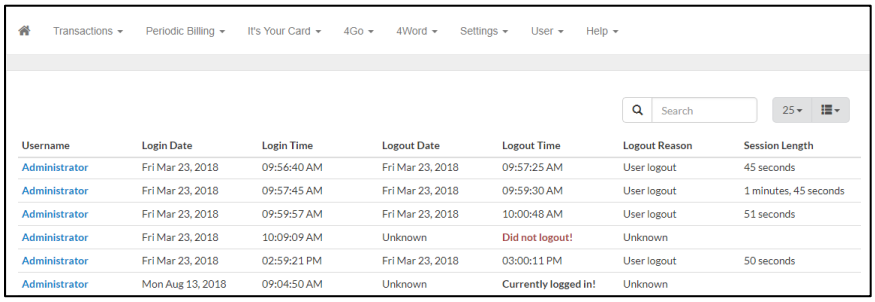
Tip: All columns on the User Activity page can be sorted by clicking on a column header.

1. From the menu, select **User > User Activity**.
2. The User Activity page displays the following information:
    - Username: Displays the user's LTM username, and the information on the page will be displayed alphabetically by them.
    - Last [10] Sessions: By default, the User Activity page displays the ten most recent LTM sessions for each user. However, additional session history can be displayed by clicking the **Last 25**, **Last 100**, or **All** link located at the bottom of the User Activity page.
    - Login Date: Displays the date that the user signed in to LTM.
    - Login Time: Displays the time that the user signed in to LTM.
    - Logout Date: Displays the date that the user signed out.
    - Logout Time: Displays the time that the user signed out.

- Logout Reason: Displays the reason for the user signing out is also displayed. The following are possible reasons:
  - Did Not Sign Out!: This signifies that the user closed the browser without signing out of LTM.
  - Inactivity Timeout: This signifies that the user was signed out by LTM due to inactivity.
  - User Sign-out: This signifies that the user signed out properly from their account.
  - Currently Signed In!: This signifies that the user is currently signed in to LTM.

Note: Not signing out of LTM creates potential security risks. Users whose accounts show Did Not Logout or Inactivity Timeout should be counseled on the importance of signing out properly.

- Session Length: Displays the amount of time the user spent in LTM.



Username	Login Date	Login Time	Logout Date	Logout Time	Logout Reason	Session Length
Administrator	Fri Mar 23, 2018	09:56:40 AM	Fri Mar 23, 2018	09:57:25 AM	User logout	45 seconds
Administrator	Fri Mar 23, 2018	09:57:45 AM	Fri Mar 23, 2018	09:59:30 AM	User logout	1 minutes, 45 seconds
Administrator	Fri Mar 23, 2018	09:59:57 AM	Fri Mar 23, 2018	10:00:48 AM	User logout	51 seconds
Administrator	Fri Mar 23, 2018	10:09:09 AM	Unknown	Did not logout!	Unknown	
Administrator	Fri Mar 23, 2018	02:59:21 PM	Fri Mar 23, 2018	03:00:11 PM	User logout	50 seconds
Administrator	Mon Aug 13, 2018	09:04:50 AM	Unknown	Currently logged in!	Unknown	

Note: If Unavailable is displayed across all fields, it means the user's session history is not available.

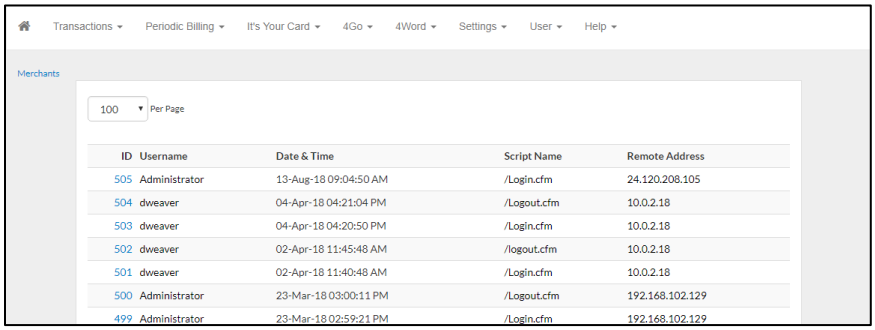
Viewing User Logs

The User Logs page displays a running total of users as they sign in to LTM, access pages, and sign out.

Tip: The Account Administrator and administrator-type users for the account can use the information to ensure that all users are properly accessing and signing out of LTM. In addition, the information can be used to confirm that users are only accessing the appropriate pages during their sessions.

To view the User Logs page, complete the following steps:

1. From the menu, select **User > User Logs**.
2. The User Logs page displays the following information:
    - ID: Displays the running total count, with the most recent action in LTM displayed first, by default.
    - Username: Displays who accessed LTM.
    - Date & Time: Displays when the user performed the action in LTM.
    - Script Name: Displays the page that the user accessed in LTM.
    - Remote Address: Displays the IP address from which the user accessed LTM.



3. *(Optional)* The information on the User Logs page can be sorted in the following ways:
    - Clicking the user's name (under User Name) will bring the user's history to the top of the page, with their most recent action displayed first.
    - Clicking the page's name (under Script Name) will bring the page's history to the top of the page, with the most recent action displayed first.
    - Clicking the IP address (under Remote Address) will bring the IP address' history to the top of the page, with the most recent action displayed first.

Tip: A sort can be cleared by clicking the web browser's back button.

4. *(Optional)* The user information log can be expanded to investigate suspicious activity. To expand the log, simply click the ID number of the user in question.

Note: A detailed information log will load under the corresponding ID number. Since this is a running total, the Page Index allows administrator-type users for the account to navigate through the information as far back as necessary. This information is typically only reviewed when investigating suspect user activity. For additional information and help interpreting this log, contact the Shift4 Customer Support team at 888-276-2108, option 1.

Tip: The detailed information log can be cleared by clicking the web browser's back button.

Conclusion

If this is your first time configuring your account, as the Account Administrator you should have completed the following:

- Signed in as the Account Administrator for the first time
- Changed your password
- Set and answered your password recovery questions
- Stored your login and password in a secure location, like a safe or vault
- Set your security settings
- Set your user shifts
- Set your IP address restrictions
- Set your general settings
- Created an administrator-type account for your daily use

Note: The Account Administrator account should not be used for daily auditing or settlement duties.

- Created other user accounts for your employees

Note: The Account Administrator is the only account that can create an administrator-type user or an IYC site administrator-type user. Other user types can be created by administrator-type users for the account.

- Reviewed how to edit and delete user accounts
- Reviewed how to monitor user activity

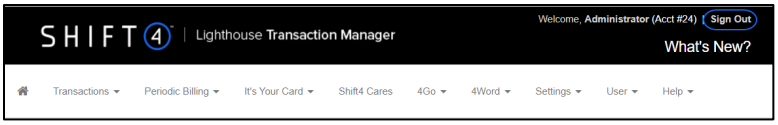
After these items have been completed and/or reviewed, the last step is signing out of LTM. For additional information on this important step, see the *Signing Out* section below.

Signing Out

Shift4 recommends that you manually sign out of your account. You should never close your browser prior to signing out properly.

To sign out, complete the following step:

1. Click **Sign Out** in the upper right corner of any LTM page.



Note: To minimize the risk of unauthorized access to account information, LTM will automatically sign users out after 20 minutes of inactivity. A warning message will appear five minutes before signing the user out; a final warning will appear one minute before.

Appendix A – Password Recovery

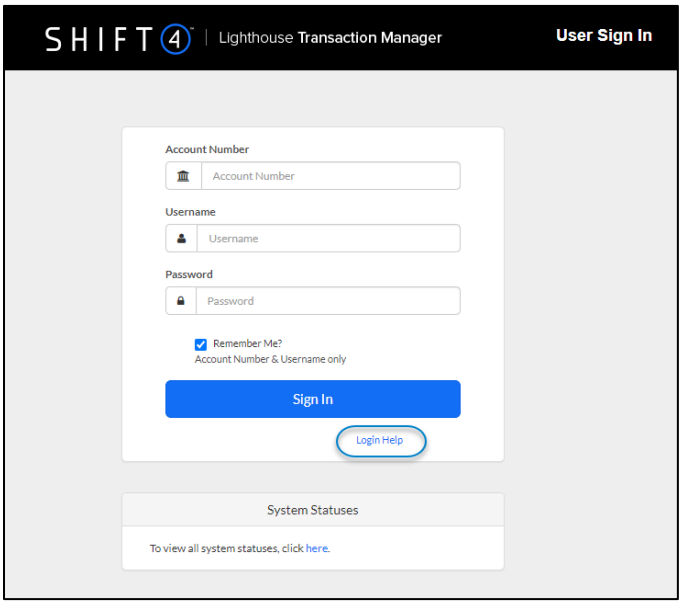
Using the Login Help

If you forget any of your login credentials, help is provided on the Lighthouse Transaction Manager User Sign In page.

The Login Help feature covers many scenarios, and we've highlighted the main ones in this document, including:

- *I Forgot My Account Number*
- *I Forgot My Username*
- *I Forgot My Password*
- *I Cannot Generate a Passcode*

If one of these situations applies to you, see the instructions below. If none of these sections applies to your situation, you can use the Login Help feature to get help signing in. If you are still unable to sign in, contact an administrator for your account.



I Forgot My Account Number

Unfortunately, Shift4 cannot provide this information to you. You will have to contact an administrator for your account.

I Forgot My Username

Depending on how your user account was configured, Shift4 may be able to help. To retrieve your username, complete the following steps:

1. On the Lighthouse Transaction Manager User Sign In page, click **Login Help**.
2. In the Account section, enter your account number and click **Next**.
3. In the Username section, click **Forgot Username**.
4. In the Forgot Username section, enter the email address associated with your LTM account and click **Next**.

Note: If you forgot your email address or don't have an email address associated with your LTM account, you will need to contact an administrator for your account.

5. You should receive an email from Shift4 that contains your username. After you receive the email, try and sign in using your valid credentials.

I Forgot My Password

Don't worry! Forgetting a password is one of the most common things that LTM users experience, and the Login Help feature can help you reset it. There are four options available to you. The option you choose is based on how your user account was configured.

- I Have Neither an Email Address nor a Passcode
- I Have an Email Address but Not a Passcode
- I Have a Passcode but Not an Email Address
- I Have a Passcode and an Email Address

I Have Neither an Email Address nor a Passcode

If you do not have an email address associated with your LTM account and did not set up multifactor authentication, complete the following steps to reset your password:

1. On the Lighthouse Transaction Manager User Sign In page, click **Login Help**.
2. In the Account section, enter your account number and click **Next**.
3. In the Username section, enter your username and click **Next**.
4. In the Password section, click **Forgot Password**.
5. In the Forgot Password section, click **No** when asked if you know the email address on your LTM account.
6. In the Forgot Password section, enter the answer to your secret question and click **Submit**. Repeat this process until the Change Your Password section is displayed.

Note: If you have not set answers to your security questions in LTM, you will need to contact your administrator for login credentials.

7. In the Change Your Password section, read the password composition requirements. Then, enter a unique password in the New Password field and reenter it in the Verify Password field. When you are done, click **Submit**.
8. You should now be able to sign in with your valid credentials.

I Have an Email Address but Not a Passcode

If you have an email address associated with your LTM account and did not set up multifactor authentication, complete the following steps to reset your password:

1. On the Lighthouse Transaction Manager User Sign In page, click **Login Help**.
2. In the Account section, enter your account number and click **Next**.
3. In the Username section, enter your username and click **Next**.
4. In the Password section, click **Forgot Password**.
5. In the Forgot Password section, click **Yes** when asked if you know the email address on your LTM account.
6. In the Forgot Password section, enter the email address associated with your LTM account. Then, click **Submit**.
7. In the Change Your Password section, read the password composition requirements while you are waiting for the email containing the verification code to be delivered.
8. After you receive the email with the verification code, enter it in the Verification Code field. Then, enter a unique password in the New Password field and reenter it in the Verify Password field. When you are done, click **Submit**.
9. You should now be able to sign in with your valid credentials.

I Have a Passcode but Not an Email Address

If you set up multifactor authentication on your LTM account but do not have an email address associated with it, complete the following steps to reset your password:

1. On the Lighthouse Transaction Manager User Sign In page, click **Login Help**.
2. In the Account section, enter your account number and click **Next**.
3. In the Username section, enter your username and click **Next**.
4. In the Password section, click **Forgot Password**.
5. In the Forgot Password section, enter the passcode generated by an authenticator app on your smart device. Then, click **Next**.
6. In the Forgot Password section, enter the answer to your secret question and click **Submit**. Repeat this process until the Change Your Password section is displayed.
7. In the Change Your Password section, read the password composition requirements. Then, enter a unique password in the New Password field and reenter it in the Verify Password field. When you are done, click **Submit**.
8. You should now be able to sign in with your valid credentials.

I Have a Passcode and an Email Address

If you set up multifactor authentication on your LTM account and have an email address associated with it, complete the following steps to reset your password:

1. On the Lighthouse Transaction Manager User Sign In page, click **Login Help**.
2. In the Account section, enter your account number and click **Next**.
3. In the Username section, enter your username and click **Next**.
4. In the Password section, click **Forgot Password**.
5. In the Forgot Password section, enter the passcode generated by the authenticator app on your smart device. Then, click **Next**.
6. In the Change Your Password section, read the password composition requirements while you are waiting for the email containing the verification code to be delivered.
7. After you receive the email with the verification code, enter it in the Verification Code field. Then, enter a unique password in the New Password field and reenter it in the Verify Password field. When you are done, click **Submit**.
8. You should now be able to sign in with your valid credentials.

I Cannot Generate a Passcode

If you set up multifactor authentication on your LTM account but can no longer generate a passcode with the authenticator app on your smart device, complete the following steps to remove the authenticator from your account:

1. On the Lighthouse Transaction Manager User Sign In page, click **Login Help**.
2. In the Account section, enter your account number and click **Next**.
3. In the Username section, enter your username and click **Next**.
4. In the Password section, enter your password and click **Next**.
5. In the Passcode section, click **No** when asked if you can generate a passcode.
6. In the Reset section, click **Yes** when asked if you have the reset code.

Note: If you do not have the reset code, you will require additional assistance. You will have to contact an administrator for your account.

7. In the Remove Authenticator section, enter the reset code and click **Remove**.
8. The authenticator will be removed from your account. You should now be able to sign in with your valid credentials.

Appendix B – API Settings

When a POS/PMS application will be communicating with LTM, Shift4 uses application programming interface (API) credentials to authenticate API requests, map the requests to the intended Merchant ID (MID), and enforce what is permitted by the application, such as sales or refunds.

The API Settings page in LTM is where an administrator-type user creates the API credentials.

Appendix B reviews how to use the API Settings page in LTM to generate, view, edit, or revoke API credentials.

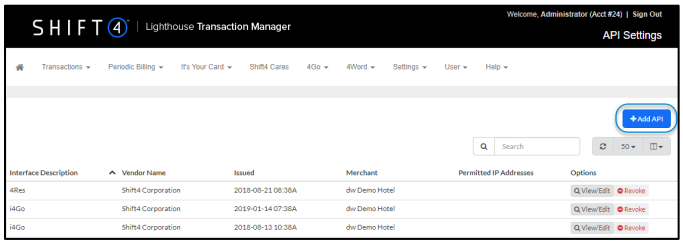
Note: Any administrator-type user can generate, view, edit, or revoke API credentials.

Generating API Credentials

To generate API credentials for production, complete the following steps:

Note: Depending on the vendor and application selected, an Auth Token, an Access Token, or an Account ID and Site ID may be generated.

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > API Settings**.
3. Click **Add API**.



4. In the Create API Credentials window, complete the following steps:
   - From the Vendor list, select the desired vendor.
   - From the Application list, select the desired application.

Tip: For detailed instructions on implementing Shift4 products like 4Res or i4Go, contact the Shift4 Customer Support team at 888-276-2108, option 1.

Note: All options are reviewed below; however, what is displayed to you depends on the application selected.

   - *(Optional)* In the Description field, enter a new description or leave the default.

Note: Shift4 recommends leaving the default description.

   - From the Merchant list, select the merchant for which you would like to generate API credentials.
   - *(If applicable)* In the API Type list, select the desired option:
     - **Standard (dual purpose, API & i4Go):** This is the most common selection.
     - **i4Go only, compatibility mode (1st generation):** This is deprecated and rarely used.
     - **i4Go Only (Access Token):** This is used when generating an Access Token for i4Go, which is not common practice.
     - **i4Go Only (Compatibility Mode):** This is deprecated and rarely used.
   - *(If applicable)* In the API Rules section, select the desired options:
     - **Allow sales**
     - **Allow refunds/returns**

Note: Depending on the vendor's application certification with Shift4, Allow sales and Allow refunds/returns may already be selected.

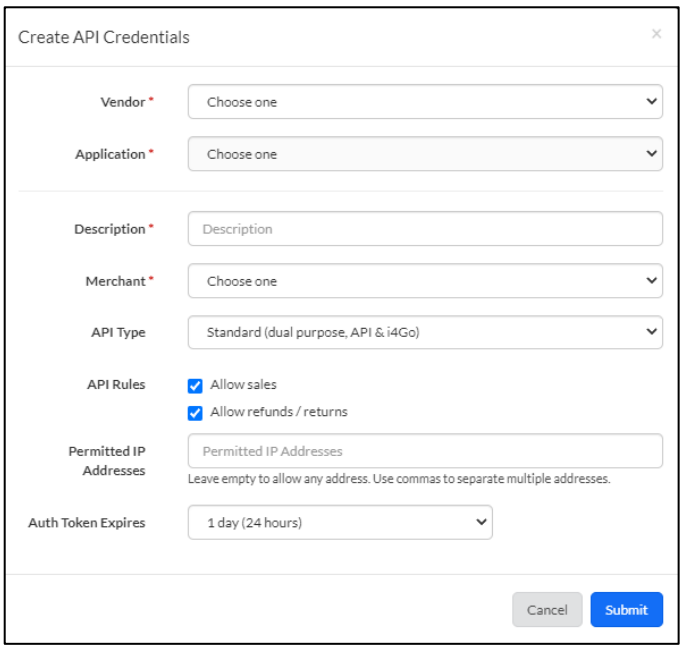
- *(If applicable)* In the Permitted IP Addresses field, add a comma-separated list of permitted addresses. This feature is only for server-to-server connections to LTM. If requests come from an IP address not listed, the following error will be displayed: "IP ADDRESS RESTRICTIONS IN EFFECT: Your account settings do not allow you access to this system from your present location. Please call your system administrator if you require expanded access."

Note: If you are using a server-to-server connection with LTM and you will be connecting from more than one IP address, you will need to enter a comma-separated list of the permitted IP addresses. If the Permitted IP Addresses field is left blank, the field will be automatically populated with the IP address currently in use. No other IP addresses will be able to connect.

- *(If applicable)* From the Auth Token Expires list, select the amount of time before the Auth Token will expire:
  - **1 day (24 hours)**
  - **3 days**
  - **7 days**
  - **30 days**
  - **60 days**
  - **90 days**

Note: The shortest time possible should be selected; however, the entire process will have to begin again at step 1 if the Auth Token expires before being exchanged for an Access Token.

- Click **Submit**.



5. In the View/Edit API Credentials window, verify the data is correct and complete one of the following steps:
   - If an Auth Token is displayed, record and provide the Auth Token to the person installing your interface, and then click **Submit.**
   - If an Access Token is displayed, record and provide the Access Token to the person installing your interface, and then click **Submit**
   - If an i4Go Access Token is displayed, record and provide the Access Token to the person installing your interface, and then click **Submit**.
   - If an i4Go Account ID and i4Go Site ID is displayed, record and provide them to the person installing your interface, and then click **Submit**.

Note: The information can be viewed or edited by clicking View/Edit in the credential's row. See the *Viewing or Editing API Credentials* section for more information.

Viewing or Editing API Credentials

To view or edit API credentials, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > API Settings**.
3. On the API Settings page, click **View/Edit** in the credential's row.

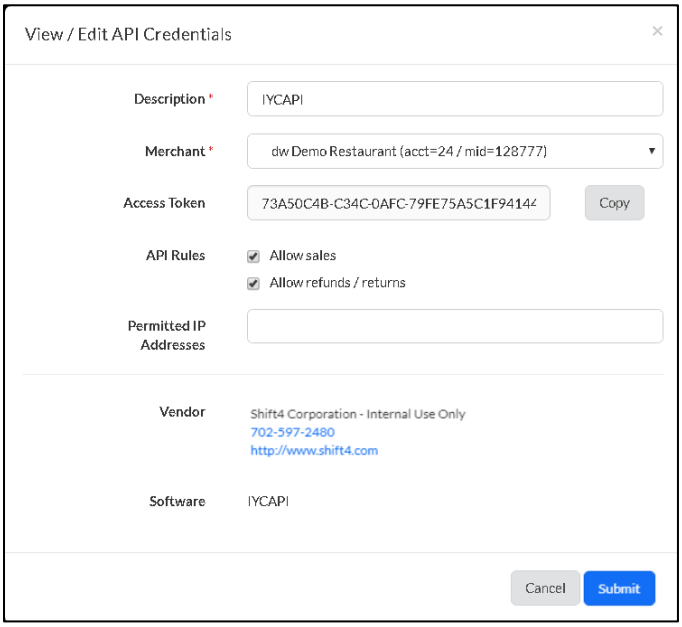
Note: All options are reviewed below; however, the information displayed in the View/Edit API Credentials window will vary according to the type of credentials generated and their current state.

4. In the View/Edit API Credentials window, complete the following steps:
   - *(Optional)* In the Description field, enter a new description.
   - *(Optional)* From the Merchant list, select a new merchant.

WARNING! Selecting a new merchant will cause all future transactions processed by the merchant using the API credentials to go to the newly selected merchant's LTM account. This means the merchant using the API credentials may not be able to view, edit, or batch out their transactions.

   - *(Optional)* Select or clear **Allow sales** or **Allow refunds/returns**.
   - *(Optional)* In the Permitted IP Addresses field, enter a comma-separated list of IP addresses from which the account can be accessed.
   - *(If applicable)* Click **Cancel** to close the View/Edit API Credentials window. Any changes made will not be saved.

- Click **Submit** to save your changes.

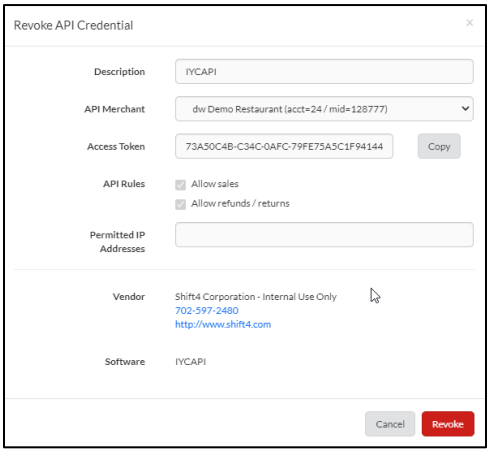


Revoking API Credentials

To revoke API credentials, complete the following steps:

WARNING! Revoking API credentials will stop the merchant using the revoked API credentials from being able to process transactions through LTM.

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > API Settings**.
3. On the API Settings page, click **Revoke** in the credential's row.
4. In the Revoke API Credential window, complete the following steps:
   - *(If applicable)* Click **Cancel** to close the Revoke API Credential window. The credentials will not be revoked.
   - Click **Revoke** to revoke the credentials.



Tip: You can generate new API credentials for a MID at any time by repeating the process described in the *Generating API Credentials* section.

Appendix C – Auto Settle

Appendix C reviews auto settle, which is a LTM feature that allows merchants to automatically transmit (and settle) batches to the processor on a predetermined schedule.

Auditing in LTM

Auditing in LTM provides merchants with the ability to:

- Compare LTM totals to their POS or PMS
- Review transactions and correct errors
- Add missing or inadvertently deleted transactions to a batch before submission to the processor
- Identify fraudulent chargeback activity

Requesting Auto Settle

Contact the Shift4 Installations team if you would like to request auto settle.

The process for requesting the feature is briefly outlined below.

1. Merchants submit auto settle activation requests to https://www.shift4.com/contact-support.
2. The Shift4 Installations team reviews, approves, and enables the auto settle feature in the merchant's LTM account.
3. After the feature has been enabled, the Shift4 Installations team will contact the merchant to explain how to configure the feature in LTM.

Auto Settle Options

Shift4 controls two options related to the auto settle feature: Auto Close Enabled and Auto Refunds. Both are options at the MID level. The terms of the merchant's signed Hold Harmless Agreement determine whether Auto Close Enabled or Auto Refunds is used.

- Auto Close Enabled**:** This option settles all sale transactions but will not settle any problem or refund transactions. Problem and refund transactions will be classified as ineligible transactions.
- Auto Refunds: This option settles all non-problem, fully authorized sale and refund transactions.

Configuring Auto Settle

The auto settle feature can only be configured by the Account Administrator, and it can be set up in many different ways at their discretion. For example, it can be activated at some locations and not at others, can work on some days of the week and not others, and can be set to work at different times for each location.

To configure the auto settle feature, complete the following steps:

1. Sign in to LTM as the Account Administrator.
2. From the menu, select **Settings > Auto Settle Settings**.
3. On the Auto Settle Settings page, for each merchant listed, complete the following steps:
   - From the Auto Close Time list, select the time at which the batch will close (from 12:00 AM to 11:00 PM).

> **Note**: The time displayed under Auto Close Time reflects the merchant time zone.

   - From the Second Close Time list, select the desired option:
     - **2 hours**
     - **4 hours**
     - **6 hours**

> **Note**: The second close time provides a second pass to pick up any additional transactions that may not have been included in the first submittal.

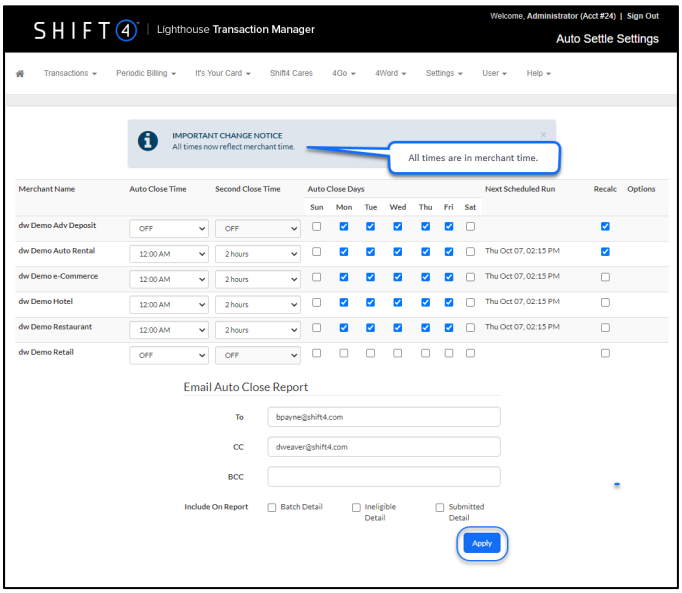
   - In the **Auto Close Days** section, select the days on which batches should automatically close.
   - Verify **Recalc** is selected. When selected, the next run day and time will be recalculated based on configurations made (after Apply is clicked in step 4).
   - *(If applicable)* If the merchant has been configured to include refunds in the process, Include refunds will be selected under Options. The following can also be selected:

- **Include unverified refunds (not recommended)**

Important: Shift4 does not recommend including unverified refunds in the batch because they could be fraudulent transactions. For additional information, see the *Unverified Refunds* section.

---

4. Click **Apply**.



5. Under Next Scheduled Run, for each merchant listed, verify the next run day and time are displayed.

Tip: If the next run day and time are not displayed, verify that **Recalc** is selected and then click **Apply**. The batch may be queued and will be submitted once the queue is cleared.

---

6. Continue to the *Configuring the Auto Close Report* section to configure the report and who should receive it.

Configuring the Auto Close Report

After each batch is closed using the auto settle feature, an Auto Close Report email notification can be sent. The Auto Close Report includes the batch totals for the day, the ineligible transaction totals, Auth totals, and the submitted transaction totals per batch. Additional information, such as transaction details, may also be included.

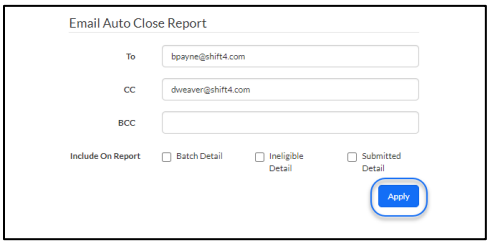
To configure the Auto Close Report, complete the following steps:

1. On the Auto Settle Settings page, in the Email Auto Close Report To, CC, or BCC field, enter an email address. Multiple email addresses should be separated by a comma with no spaces.

Note: After auto settle completes, a report containing a list of all unsettled Auth transactions (including totals, details, and summary) will automatically be sent to the email addresses listed in the Email Auto Close Report section. For merchants with a second auto settle time configured, the report will be emailed after the final auto settle has been completed.

2. In the Detail To Include On Report area, select the desired options:
    - **Batch Detail:** If selected, all transactions are included. For example, the transactions included in the Ineligible Detail and Submitted Detail options are included.
    - **Ineligible Detail:** If selected, all transactions that could not be submitted with the auto close feature are included. For example, problem or refund transactions (if refunds are not included in the auto close configurations for the merchant).
    - **Submitted Detail:** If selected, all transactions that were submitted to the processor are included.

3. Click **Apply**.



Note: Shift4 will not settle transactions that do not meet Fraud Sentry settings, unless you have selected **Include unverified refunds** in your Auto Settle Settings. For additional information, see the *Configuring Fraud Sentry Notifications* and *Configuring Fraud Sentry Events* sections.

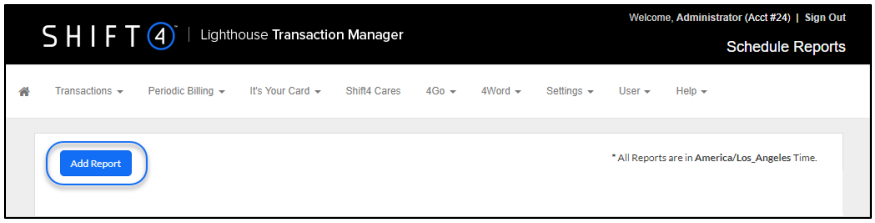
Appendix D – Schedule Reports

Appendix D reviews Schedule Reports which is a feature in LTM that provides a broad range of reporting options.

Adding a Report

To add a report, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > Schedule Reports**.
3. On the Schedule Reports page, click **Add Report**.



4. In the Name field, enter a name that will help identify the report when received.
5. *(If applicable)* In the Description field, enter a description that will be displayed in the email that will be received.
6. The Accounts field is view-only. Use the Accounts section to select the accounts that will be included in the report.
    - In the Accounts section, complete one of the following:
        - In the Search field, enter a name to search dynamically, and then select the account(s) for which you want a report generated.
        - Click **Expand All** to see a list of accounts which you have permission to view, and then select the account(s) for which you want a report generated.
        - Select the desired account(s) or click **Select All**.

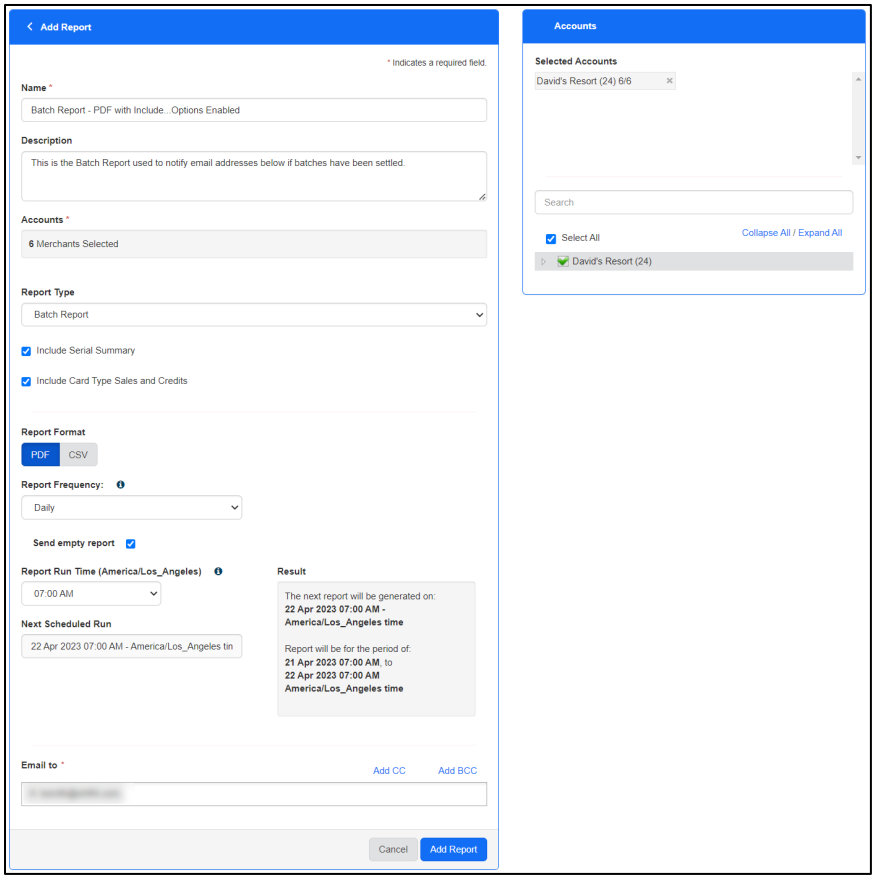
Note: Only the accounts you have permission to view will be displayed.

7. From the Report Type list, select the desired report type.
    - **Authorization Alert Report:** Schedule this report if you would like to be notified of any outstanding authorizations.
    - **Batch Report:** Schedule this report if you would like to be notified of batches that were settled.
    - **No Settlement Report:** Schedule this report if you would like to be notified when no batches were settled for that day.
        - Batches that are not submitted in a timely manner run the risk of being downgraded. Therefore, it is recommended that this report be set to the lowest report frequency, such as Daily.
    - **POS Entry Mode Report:** Schedule this report if you would like to be notified about the number and percent of transactions processed per entry mode.
    - **Unverified Refund Settlement Report:** Schedule this report if you would like to be notified about unverified refund transactions that were found during batching. (Unverified refunds are refund transactions without corresponding sale transactions. In addition, the report must be unzipped to view.)
8. Select the Report Format:
    - **PDF**
    - **CSV**
9. *(If applicable)* If you selected **Batch Report** and **PDF** in the previous steps, you have two additional options you can configure:
    - **Include Serial Summary:** Select this option if you would like the report to include an All Merchants section with a Card Type, Count, and Amount summary.
    - **Include Card Type Sales and Credits:** Select this option if you would like the report to include a Sale Count, Sale Amount, Credit Count, and Credit Amount summary.
10. From the Report Frequency list, select the report frequency. Choices include the following:
    - **Daily:** The report will be run on a daily basis at the configured run time.
    - **Weekly:** The report will be run on a weekly basis, on the configured day, and at the configured run time.
        - From the Generate Report On area, select the day of the week on which you want the report to be generated: **Mo**, **Tu**, **We**, **Th**, **Fr**, **Sa**, and/or **Su**.
    - **Monthly:** The report will be generated on the first day of the month for the previous month.
11. *(If applicable)* Select **Send empty report** to receive a report even when there is no data to include in it.

12. From the Report Run Time list, select the desired time at which the report will be generated.

> **Note:** The Next Scheduled Run field displays when the next report will be generated, and the Result field displays when the next report will be generated and what period the report will be for. (The Authorization Alert Report will always contain all unsettled authorizations rather than a specific period.)

13. In the Email to field, enter the email addresses of those whom you want to receive the report. (Ensure to click the email address after entering it so that it is added.)
14. When you have finished configuring the report, click **Add Report**.



Editing a Report

Once you have added a report, you can edit the report to make any needed changes. To edit a report, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > Schedule Reports**.
3. Click on the report name you want to edit.
4. Make any desired changes.
5. Click **Update Report**.
6. *(If applicable)* If you want to temporarily pause receiving the emails for any reason without deleting the report, completing the following steps:
    - Locate the report you want to turn off.
    - Under Status, click **Off** to change the status to Off.
    - When you want the report to run again, click **On** to turn the status to On.

Note: Columns displayed will depend on what is selected from the drop-down list.

Deleting a Report

If you are certain you will not need a report to run again you can delete it. To delete a report, complete the following steps:

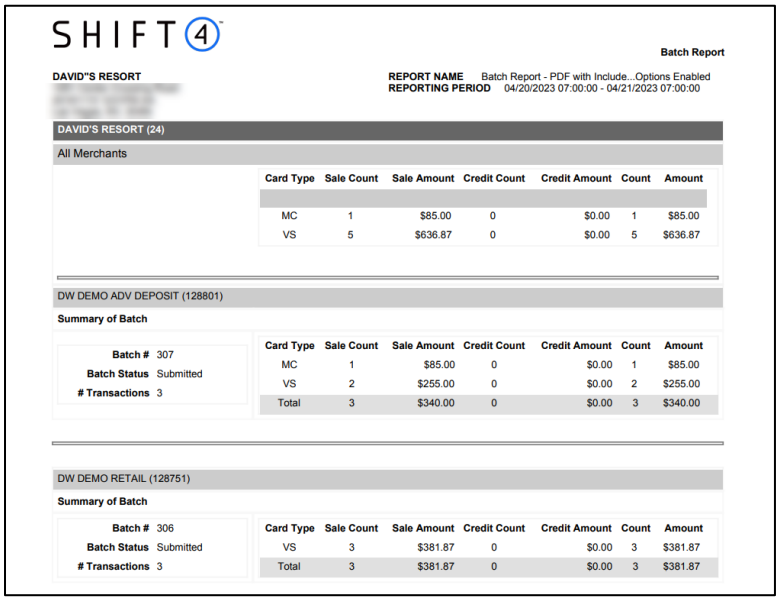
1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > Schedule Reports**.
3. Click  next to the report you want to delete.
4. When prompted, click **OK** to confirm the report's deletion.

Report Examples

There are many possibilities depending on the type of report and selected format. Below are two examples.

Batch Report

PDF format with options enabled.



SHIFT4

Batch Report

DAVID"S RESORT

REPORT NAME Batch Report - PDF with Include...Options Enabled
REPORTING PERIOD 04/20/2023 07:00:00 - 04/21/2023 07:00:00

DAVID'S RESORT (24)

All Merchants

Card Type	Sale Count	Sale Amount	Credit Count	Credit Amount	Count	Amount
MC	1	$85.00	0	$0.00	1	$85.00
VS	5	$636.87	0	$0.00	5	$636.87

DW DEMO ADV DEPOSIT (128801)

Summary of Batch

Batch # 307
Batch Status Submitted
Transactions 3

Card Type	Sale Count	Sale Amount	Credit Count	Credit Amount	Count	Amount
MC	1	$85.00	0	$0.00	1	$85.00
VS	2	$255.00	0	$0.00	2	$255.00
Total	3	$340.00	0	$0.00	3	$340.00

DW DEMO RETAIL (128751)

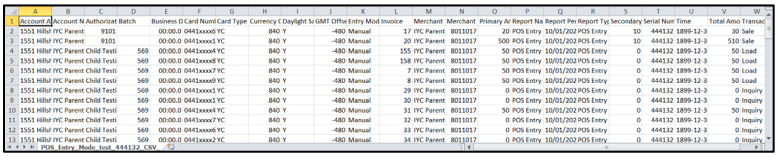
Summary of Batch

Batch # 306
Batch Status Submitted
Transactions 3

Card Type	Sale Count	Sale Amount	Credit Count	Credit Amount	Count	Amount
VS	3	$381.87	0	$0.00	3	$381.87
Total	3	$381.87	0	$0.00	3	$381.87

POS Entry Mode Report

CSV formatted using Excel®.



Account A	Account N	Authorizat	Batch	Business D	Card Numl	Card Type	Currency C	Daylight Sa	GMT Offse	Entry Mod	Invoice	Merchant	Merchant	Primary Ar	Report Na	Report Per	Report Typ	Secondary	Serial Num	Time	Total Amo	Transac
1551 Hills	IYC Parent	9101		00:00.0	0441xxxx6	YC	840	Y	-480	Manual	17	IYC Parent	8011017	20	POS Entry	10/01/202	POS Entry	10	444132	1899-12-3	30	Sale
1551 Hills	IYC Parent	9101		00:00.0	0441xxxx1	YC	840	Y	-480	Manual	20	IYC Parent	8011017	500	POS Entry	10/01/202	POS Entry	10	444132	1899-12-3	510	Sale
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx4	YC	840	Y	-480	Manual	155	IYC Parent	8011017	50	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	50	Load
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx8	YC	840	Y	-480	Manual	158	IYC Parent	8011017	50	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	50	Load
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx7	YC	840	Y	-480	Manual	7	IYC Parent	8011017	50	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	50	Load
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx9	YC	840	Y	-480	Manual	8	IYC Parent	8011017	50	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	50	Load
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx1	YC	840	Y	-480	Manual	29	IYC Parent	8011017	0	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	0	Inquiry
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx1	YC	840	Y	-480	Manual	30	IYC Parent	8011017	0	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	0	Inquiry
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx4	YC	840	Y	-480	Manual	31	IYC Parent	8011017	50	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	50	Inquiry
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx7	YC	840	Y	-480	Manual	32	IYC Parent	8011017	0	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	0	Inquiry
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx6	YC	840	Y	-480	Manual	33	IYC Parent	8011017	0	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	0	Inquiry
1551 Hills	IYC Parent Child Testi	569		00:00.0	0441xxxx2	YC	840	Y	-480	Manual	34	IYC Parent	8011017	0	POS Entry	10/01/202	POS Entry	0	444132	1899-12-3	0	Inquiry

Appendix E – Configuring Devices

Important: If the Universal Transaction Gateway® (UTG®) version in use is 3200 or greater, the steps outlined below are no longer applicable because the configurations are made in UTG TuneUp now. If a UTG version prior to 3200 is in use, then you may need to reference this information; however, please contact Shift4 Customer Support to update your UTG rather than using these directions.

Appendix E reviews configuring EMV or debit devices. If these types of devices will be in use, then either the Account Administrator or a user with the EMV devices access permission enabled must configure them in LTM.

Using EMV Devices

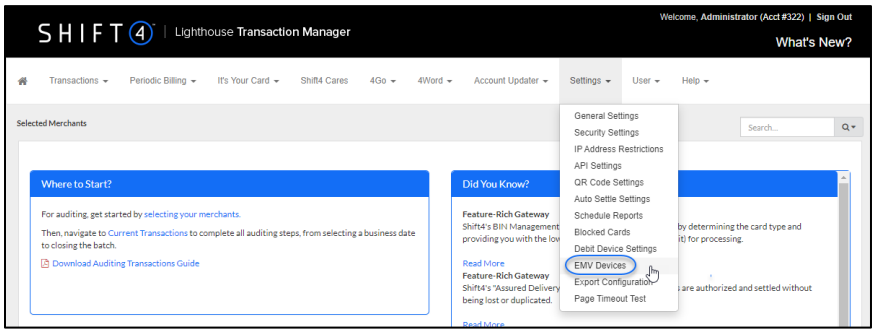
The Shift4 Customer Support team must enable EMV devices for the account.

After EMV is enabled, settings must be configured in LTM and UTG TuneUp to use EMV devices.

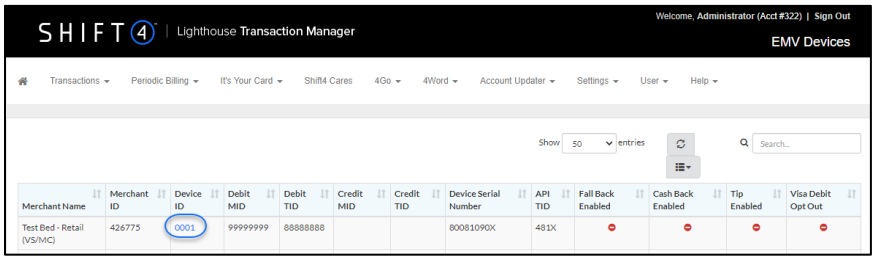
Configuring EMV Devices in LTM

To configure EMV devices in LTM, complete the following steps:

1. Sign in to LTM as the Account Administrator or a user with the EMV devices access permission enabled.
2. From the menu, select **Settings > EMV Devices**.



3. Under Device ID, click the device ID number that you would like to configure.



4. On the EMV Device Settings page, complete the following steps:
   - In the General Settings section, complete the following steps:
     - In the API Terminal field, enter the API Terminal ID (TID), which must match the PIN pad's configuration in the UTG and the POS/PMS. The field is not case sensitive.

API TID: The Application Programming Interface Terminal ID (API TID) 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 TID 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 TID must be set in the POS/PMS, UTG, and LTM. The value must match so that those systems can identify the PIN pad being used during the transaction.

     - If your API TIDs are not unique, then enter the device serial number in the Device Serial (Optional) field. See the *Using EMV Devices with Shift4* guide for information on locating the device serial number.

Important: Verify you have entered the device serial number correctly. If the wrong device serial number is entered, there will be no indication, but EMV will not be enabled on the device.

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

Tip: For additional information, click the Show/Hide Help link.

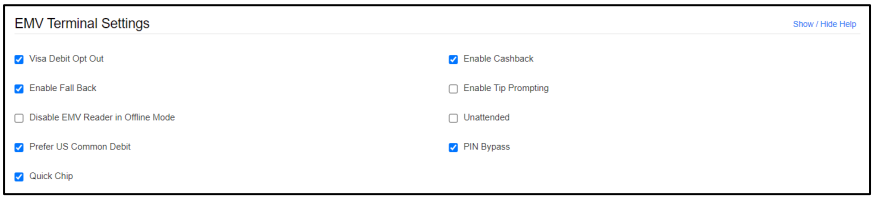
- In the EMV Terminal Settings section, select the desired options:
  - **Visa Debit Opt Out:** If selected, the use of Domestic Visa Debit cards is not allowed; however, Visa Credit cards will still be allowed. This only affects the VISA AID.

Warning! If you enable the Visa Debit Opt Out option, there may be some Visa debit cards that you will not be able to process because there isn't a common AID between the terminal and card.

  - **Enable Fall Back:** If selected, when the chip card fails, transactions can be processed by swiping the payment card.
  - **Disable EMV Reader in Offline Mode:** This field is deprecated. When in offline mode, transactions can be processed by dipping, swiping, tapping, and/or manually entering the number.
  - **Prefer US Common Debit:** Typically, Visa debit cards support two applications: Global Debit Application ID (labeled VISA DEBIT) and US Common Debit AID (labeled US DEBIT). If selected (and if the card supports the AID and the device is in the United States), the device will automatically process transactions through US DEBIT. If cleared, the cardholder will have to choose VISA DEBIT or US DEBIT on the device. The latter can be confusing to cardholders, so you may want to keep Prefer US Common Debit selected. (The option is only displayed if the merchant's currency code is set to 840/USD.)

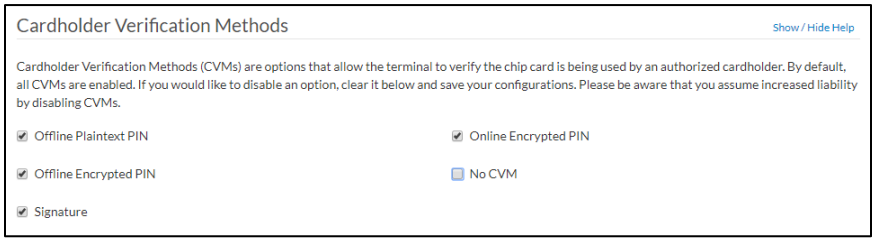
- **Quick Chip:** If selected, the cardholder can remove their card sooner (before the authorization response is received on the device). In addition, the cardholder can insert their card sooner (similar to swipe ahead on non-EMV transactions).
- **Enable Cashback:** If selected, the device is enabled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

Note: Visa Debit Opt Out is required due to VISA's particular implementation of EMV, and currently not required for other card types.



Important: LTM settings for Enable Cashback and Enable Tip Prompting should be the same as configured in UTG TuneUp. If they are not, UTG TuneUp settings will override the settings in LTM.

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

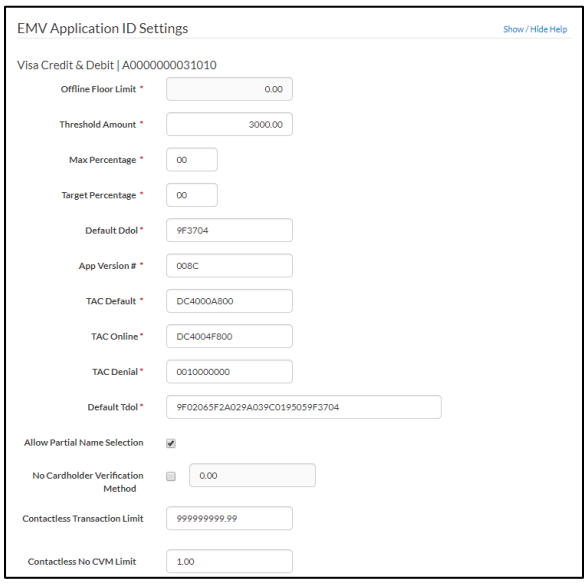


- When you have configured all your settings for the EMV device, complete one of the following steps:
  - Click **Save** to save your configuration settings for the current device.
  - Click **Save and Next** to save your configuration settings for the current device and load the next device under the current MID for configuration.

Tip: For additional information, click the Show/Hide Help link.

Important: Check with the processor before changing or updating configurations in the EMV Application ID Settings section. A description of each field is provided in the table in the *EMV Application ID Settings* section.

- *(If applicable)* In the EMV Application ID Settings section, configure the desired settings for the appropriate application.



Note: The Contactless Transaction Limit and Contactless No CVM Limit fields will only be displayed if contactless EMV is supported by your processor and your serial account has the correct schema.

Tip: For additional information, click the Show/Hide Help link. In addition, the *EMV Application ID Settings* section reviews the information.

- When you have configured your EMV Application ID Settings, complete one of the following steps:
  - Click **Save** to save your configuration settings for the current device.
  - Click **Save and Next** to save your configuration settings for the current device and load the next device under the current MID for configuration.

EMV Application ID Settings

The following table describes each setting in the EMV Application ID Settings section.

Note: With EMV, offline does not mean that the UTG is in offline mode. It means that the transaction is processed (approved or declined) without sending the request to the processor. The terminal uses the settings in this section to determine whether or not it will process the transaction offline. The card has a similar set of settings.

Field Name	Description
Offline Floor Limit	This is the maximum transaction amount that can be approved offline. Not all transactions under the floor limit are approved offline. This field will be set to 0.00 when Quick Chip is enabled.
Threshold Amount	This is the value (0 or a positive number less than the Offline Floor Limit) used in terminal risk management. Any transaction with a transaction amount less than the set Threshold Amount is subject to selection at random for online processing.
Max Percentage	This is the value (from 0 to 99) used in terminal risk management for random transaction selection; the desired percentage of transactions just below the floor limit that will be selected to process online.
Target Percentage	This is the value (from 0 to 99) used in terminal risk management for random transaction selection.
Default Ddol	While processing the transaction, the card sends a Dynamic Data Authentication Data Object List (DDOL) to the terminal containing a list of data items the card needs. If the card does not send that list, the Default Ddol list is used.
App Version #	The App Version # is the application version number for the application ID. It specifies which version of the card application was certified. The terminal compares its supported application version number with the one received from the card to determine their compatibility, and it sets a flag in the auth request if the app version the terminal supports doesn't match the one on the card.

Field Name	Description
TAC Default	TAC stands for Terminal Action Code. This is a set of flags that mirrors the Terminal Verification Results (TVR). If any of the bits set in this field are also set in the TVR during the transaction process, the transaction will be declined offline. This set of flags is used in the event that the terminal and card decided to process the transaction online but were unable to go online due to connectivity issues.
TAC Online	This is a set of flags that mirrors the TVR. If any of the bits set in this field are also set in the TVR during the transaction process, the request will be sent online for approval.
TAC Denial	This is a set of flags that mirrors the TVR. If any of the bits set in this field are also set in the TVR during the transaction process, the transaction will be declined offline.
Default Tdol	While processing the transaction, the card sends a Transaction Certificate Data Object List (TDOL) to the terminal containing a list of data items the card needs. If the card does not send that list, the Default Tdol list is used. Your processor may have a download process that overwrites these values, which could cause them to be blank. If this occurs, contact the Shift4 Customer Support team at 888-276-2108, option 1, for the appropriate value to place in this field.
Allow Partial Name Selection	Setting this flag allows the terminal to include application IDs that partially match rather than being a full match when building a list of mutually supported applications with the card.
No Cardholder Verification Method	To not perform a Cardholder Verification Method (CVM), select the option and enter an amount in the field. When the transaction is less than or equal to the amount, a CVM will not be performed (if the card supports not performing a CVM as well). When the field is cleared, a CVM will be performed no matter the amount.
Contactless Transaction Limit	Contactless Transaction Limit is the maximum dollar amount value that will allow a contactless transaction. Transactions above that amount must be done via inserting the card.
Contactless No CVM Limit	Contactless No CVM Limit is the maximum dollar amount value that will not require cardholder verification (PIN, Signature, etc.). Transactions above that amount will apply a CVM.

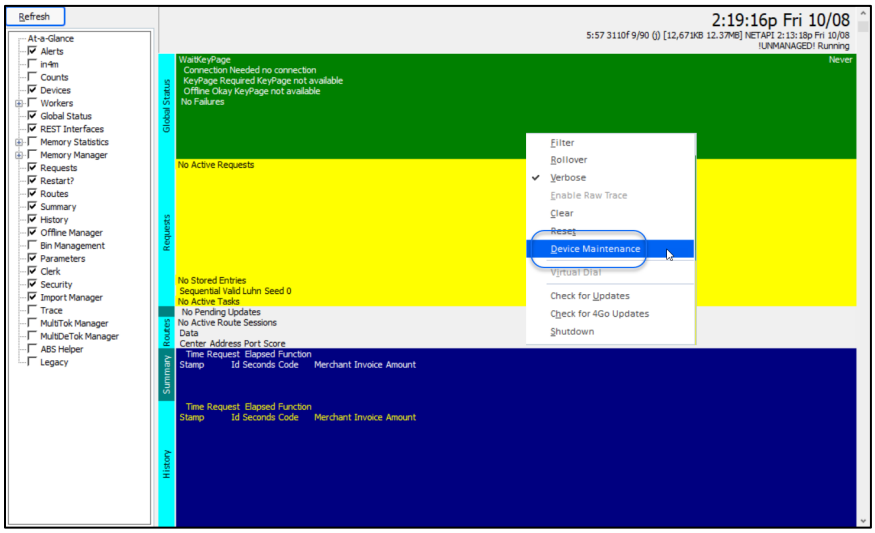
Configuring EMV Devices in UTG TuneUp

See *UTG Installation and Configuration Guide*, *Using EMV Devices with Shift4*, *Using Ingenico Tetra External Devices*, or *Using Ingenico Telium RBA External Devices*.

Updating EMV Device Configuration Settings

Device setting changes that have been configured successfully in both LTM and UTG TuneUp are automatically downloaded to the device every hour. To manually download the updated settings for an EMV device that has already been configured successfully in both LTM and UTG TuneUp, complete the following steps:

1. To open the UTG Stand Alone, from the start menu, select **All Programs > Shift4 Corporation > Universal Transaction Gateway > UTG (v2) Stand Alone**.
2. Right-click in the UTG Task Explorer window, and then click **Device Maintenance**.



3. In the Device Maintenance window, select the terminal(s) you want to download, and then click **Download Now**.

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

Note: The Personal Identification Number (PIN) pad will display a Please Wait message while downloading, and then it will go back to Idle when finished.

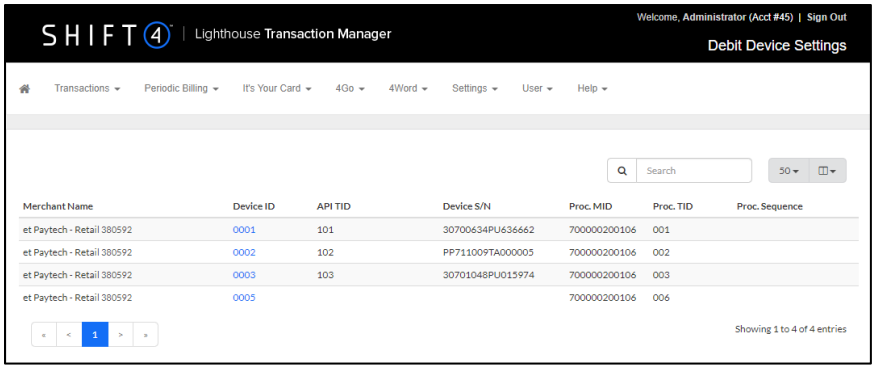
Configuring Debit Devices

The Debit Device Settings page in LTM is a mapping tool for properties using processors that require a certain mapping configuration. It provides the ability for the property to define the mapping between devices and the POS terminal.

This page is not used unless it is required by the merchant's processor for PIN pad/debit device handling. If it is required, the page must be configured by the Account Administrator.

The devices list is populated by settings in the internal Shift4 systems. To edit the details so that you can match the API Terminal ID (TID), which you will need to obtain from your POS provider, to the Processor TID, which will already be entered into the system, complete the following steps:

1. Sign in to LTM as the Account Administrator.
2. From the menu, select **Settings > Debit Device Settings**.
3. Under Device ID, click the device number that you would like to edit. (This is an arbitrary, sequential number based solely on its entry into the Shift4 internal database.)



4. In the Edit Device window, complete the following steps:
   - In the API Terminal ID field, enter the Terminal ID that you obtained from your POS vendor.

> **Warning!** Do not change any of the other values.

   - Click **OK**.

5. Process up to five debit transactions until the first transaction goes through without an error. This process is required to synch the numbers together. The processor will record this number and the Serial ID of the device; then, the device cannot be moved to a different terminal.

Appendix F – Export Configuration

The Export Configuration page in LTM allows administrator-type users to create custom reports by defining which transaction related fields should be included in the reports. (It is not necessary to use the Account Administrator account to take advantage of this feature.)

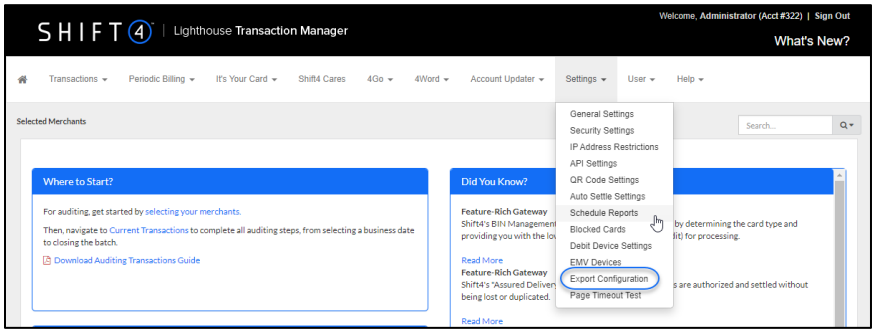
There are two types of reports, Account and System, and the type is displayed in the Scope column on the Export Configuration page. Account type reports are completely customizable, editable, and may be deleted. System type reports are designed as templates and can only be viewed or cloned.

Note: The reports are available for export on the Current Transactions and Archived Transactions page. For additional information, see the *Reporting* document.

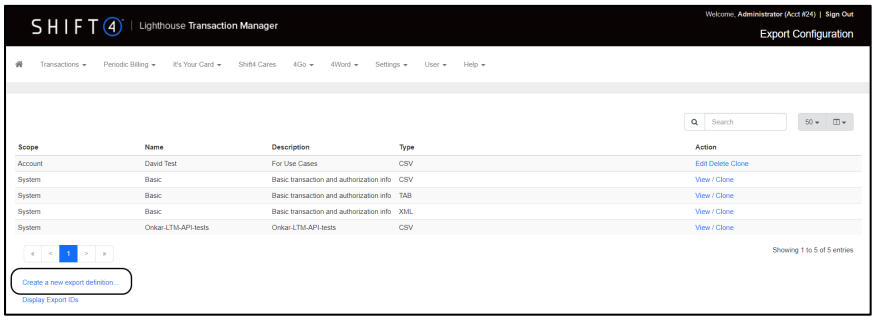
Creating a Report

To create a report, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > Export Configuration**.



3. On the Export Configuration page, click the **Create a new export definition** link.



4. On the Create Data Export Definition page, complete the following steps:
   - Enter a name for the report in the Export Name field. (A unique name will make it easier to find when you have a number of reports available for export.)
   - Enter a description for the report in the Description field.
   - Select an Export Type:
     - **CSV - Comma delimited**
     - **TAB delimited**
     - **XML**
   - In the Unused Fields area, click the field to be included in the report.

Tip: To add multiple fields that are listed next to each other, press **Shift** on the keyboard, click the first field, and then click the last field. To add multiple fields that are not listed next to each other, press **Control** on the keyboard and then click each field.

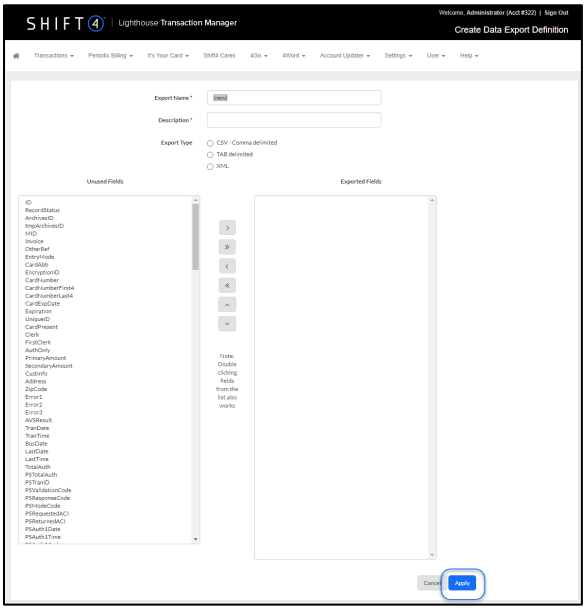
- When you have selected the field(s) to be included in the report, click  to move the selected field(s) from the Unused Fields area to the Exported Fields area.

Tip: Click  to move all fields listed in the Unused Fields area to the Exported Fields area.

- To set the order in which the selected fields will be displayed in the report, click on any field in the Exported Fields area, and then click  or  to move the field up or down in the list. (The top field displayed in the Exported Fields area will be the left column in the report.)

Tip: If a field was accidently added to the Exported Fields area, click the field and then click  to move the field back to the Unused Fields area. In addition, clicking  will move all fields back to the Unused Fields area.

- Click **Apply**.



Cloning a Report

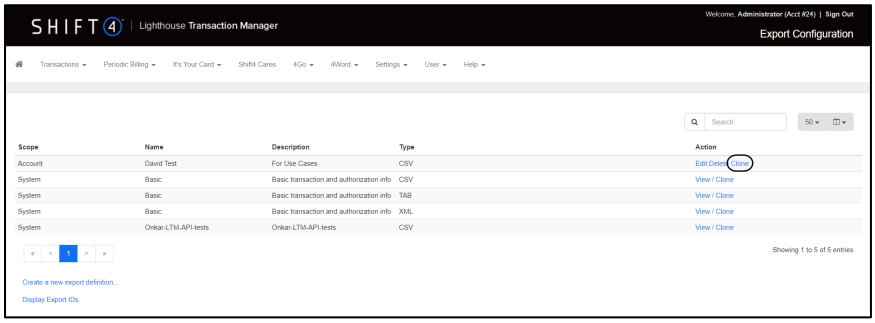
If your reports will contain a standard set of fields, you may want to use the clone feature because it will allow you to define the reports faster.

To use the clone feature, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > Export Configuration**.
3. Create a report that contains the fields to be included in multiple reports. Or, use a report that has System displayed in the Scope column on the Export Configuration page.

Note: If you create a new report, you may want to name it “Standard Configuration” for ease.

4. On the Export Configuration page, click **Clone** in the Action column of the desired report.



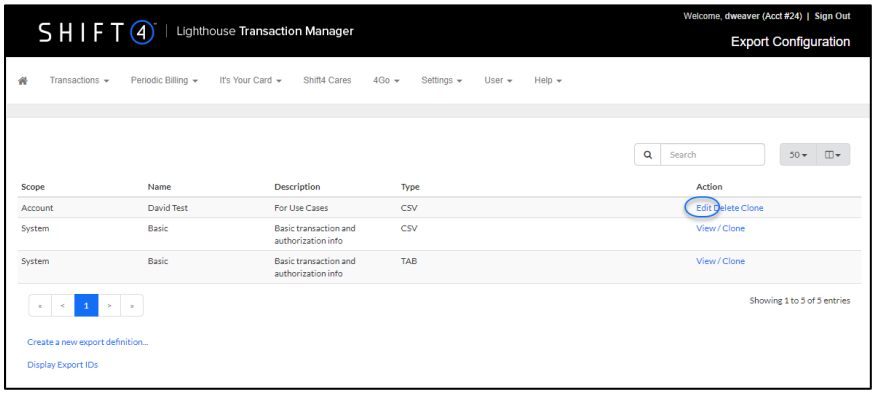
5. On the Clone Data Export Definition page, complete the following steps:
    - Enter a new name for the report in the Export Name field. (A unique name will make it easier to find when you have a number of reports available for export.)
    - Enter a new description for the report in the Description field.
    - *(Optional)* Select a new Export Type:
        - **CSV - Comma delimited**
        - **TAB delimited**
        - **XML**
    - Add fields to the Exported Fields area, or remove fields from the area. For additional information, see step 4 in the *Creating a Report* section.
    - Set the order in which the fields will be displayed in the report. For additional information, see step 4 in the *Creating a Report* section.
    - Click **Apply**.

Editing a Report

You can edit any report that has Account displayed in the Scope column on the Export Configuration page. Remember, if System is displayed in the Scope column, the report can only be viewed or cloned.

To edit a report, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > Export Configuration**.
3. On the Export Configuration page, click **Edit** in the Action column of the desired report.



4. On the Edit Data Export Definition page, complete the following steps:
   - Enter a new name for the report in the Export Name field. (A unique name will make it easier to find when you have a number of reports available for export.)
   - Enter a new description for the report in the Description field.
   - *(Optional)* Select a new Export Type:
     - **CSV - Comma delimited**
     - **TAB delimited**
     - **XML**
   - Add fields to the Exported Fields area, or remove fields from the area. For additional information, see step 4 in the *Creating a Report* section.
   - Set the order in which the fields will be displayed in the report. For additional information, see step 4 in the *Creating a Report* section.
   - Click **Apply**.

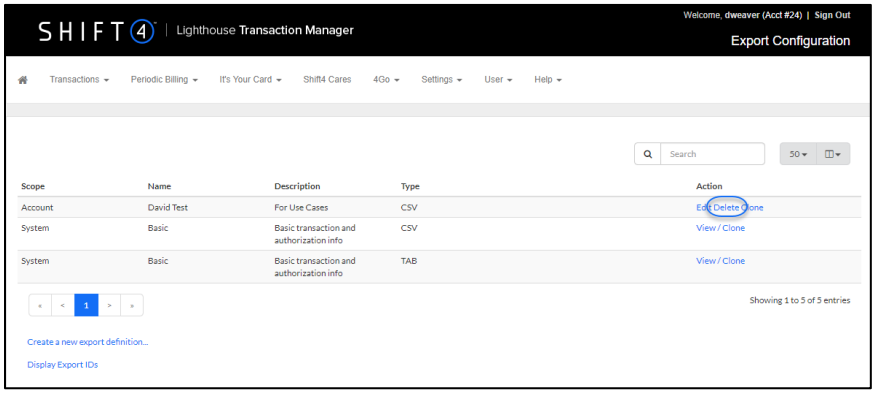
Deleting a Report

You can delete any report that has Account displayed in the Scope column on the Export Configuration page. Remember, if System is displayed in the Scope column, the report can only be viewed or cloned.

To delete a report, complete the following steps:

WARNING! Deleting a report cannot be undone.

1. From the menu, select **Settings > Export Configuration**.
2. On the Export Configuration page, click **Delete** in the Action column of the desired report.



Displaying the Export ID for Each Report

Shift4 allows merchants to automatically create and export reports instead of signing in to LTM on a daily basis to generate them. In addition to developing an API to download the exported reports via direct server-to-server communication with LTM, the export ID for each report is needed.

To display the export ID for each report, click the **Display Export IDs** link on the Export Configuration page. This allows the Export ID column to be displayed, which contains the export ID for each report.

Appendix G – 4Word Configuration

4Word is a secure, controlled method for sharing CHD with an authorized third-party while never exposing that data in your environment†.

4Word does this by enabling a business to process a charge using shared information without directly exchanging CHD via email, telephone, etc.

For example, there is a hotel that is a Shift4 customer. A guest at the hotel would like flowers delivered to their room, so the hotel concierge uses the PMS to request four words or a TrueToken® (which references the guest's real CHD) from LTM. The information will be displayed to the concierge on the PMS. Then, the concierge places an order with a florist and shares the four words or TrueToken as the form of payment. If the florist is a Shift4 customer too, they can charge the guest in LTM using the four words or TrueToken – there is no need for the real CHD. If the florist isn't a Shift4 customer, they can use the 4Word web app to exchange the four words or TrueToken for the real CHD. Once they have the real CHD, they can use it to process a charge according to their own business practices.

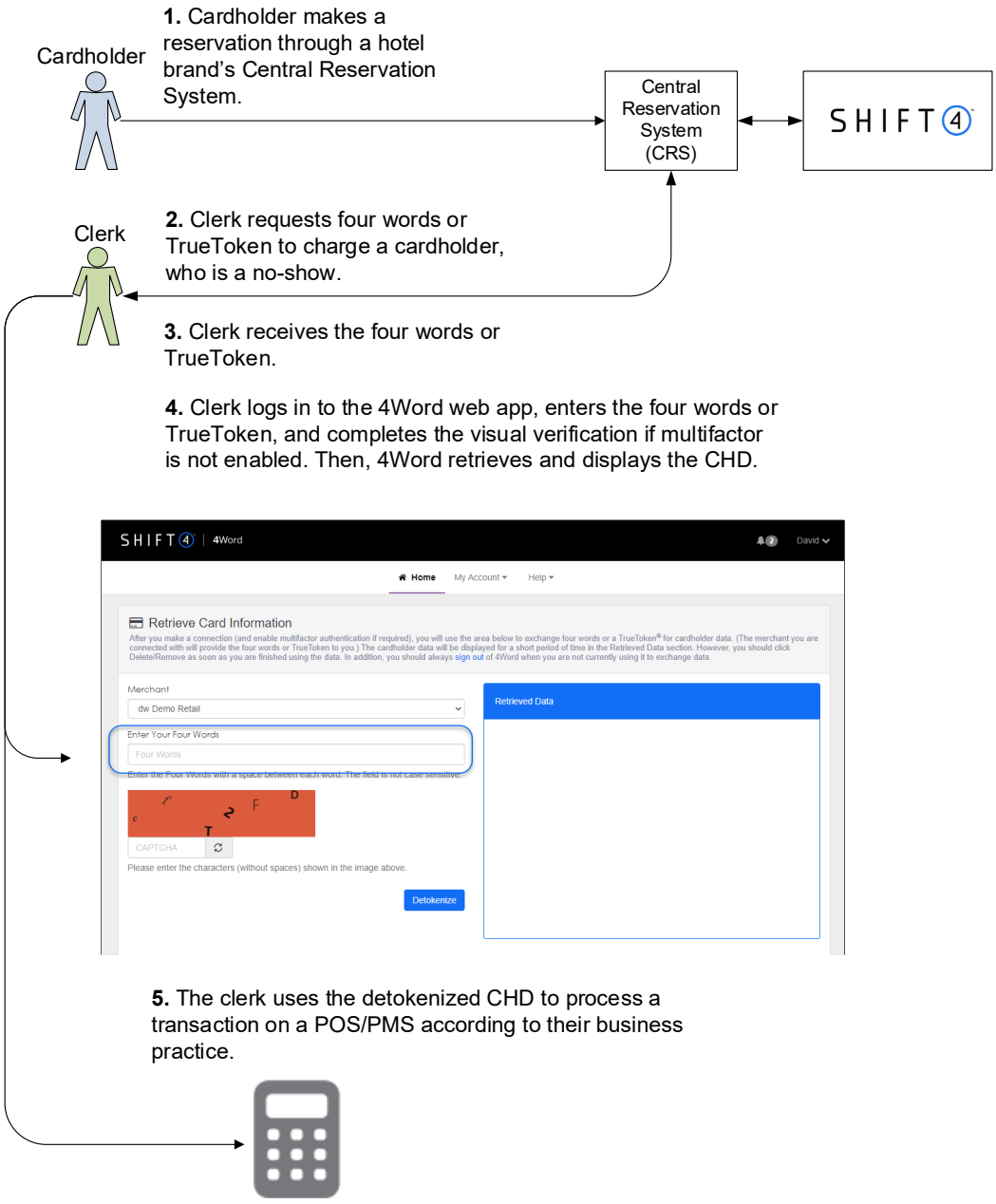
While this is just one example, 4Word meets many business needs and never exposes CHD in your environment†. The *Example of Using 4Word* section displays a diagram that outlines another popular use case.

†4Word supports two methods of data exchange. The first (and most secure) method allows two merchants who use LTM to securely exchange sensitive payment card information without ever exposing the actual CHD. The second method permits a merchant who does not have LTM (but has been granted access to 4Word by a merchant who does) to obtain access to the data for a single payment card.

Requirement: The Shift4 customer's POS/PMS must be configured to process 4Word API requests in order to get four words or a TrueToken from LTM.

Example of Using 4Word

An example of using 4Word might be a hotel brand with a Shift4 account. Let's say the hotel brand has a central reservation system for hotels that are located in multiple countries. If a full Shift4 account is not available in some of the locations, the hotel can still process transactions using the 4Word web app. The hotel brand with the Shift4 account can send 4Word invitations to locations where a Shift4 account is unavailable, allowing them to process charges.

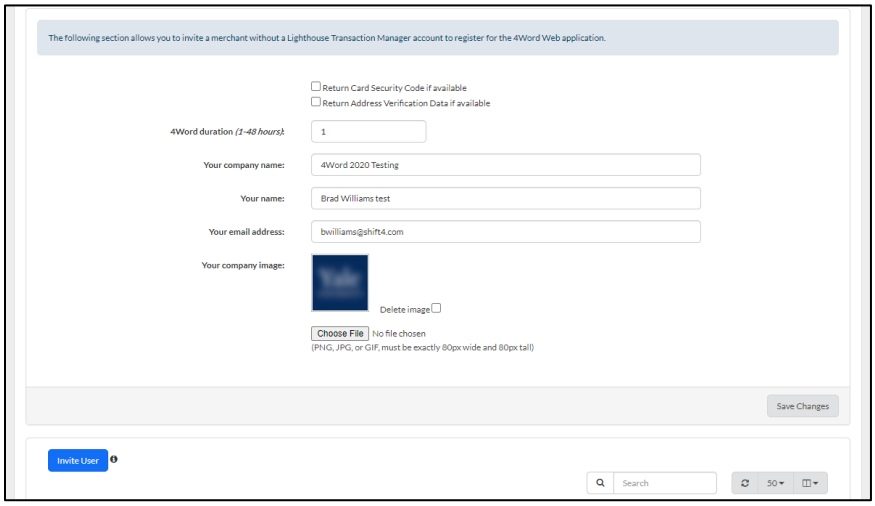


Sending a Merchant an Invitation to Use 4Word

In the example above, the Shift4 customer must invite the merchant to use the 4Word web app, allowing the merchant to exchange four words or a TrueToken for CHD.

If you are a Shift4 customer and do business with a merchant who is not, you can send a 4Word invitation to them by completing the following steps:

1. Sign in to LTM as the Account Administrator.
2. From the menu, select **4Word** > **Settings**.
3. Under *The following section allows you to invite a merchant without a Lighthouse Transaction Manager account to register for the 4Word Web application*, configure the following:
    - *(Optional)* Return Card Security Code if available: This option supplies the 4Word web application user with the Card Security Code if it is available.
    - *(Optional)* Return Address Verification Data if available: This option supplies the 4Word web application user with the Address Verification Data if it is available.
    - *(Required)* 4Word duration: Enter the time (1-48 hours) after which the four words or TrueToken expires.
    - *(Required)* Your company name: Enter your company name. It will be displayed in the invitation email.
    - *(Required)* Your name: Enter your name. It will be displayed in the invitation email.
    - *(Required)* Your email address: Enter your email address. The invitation email will show it was sent from this address.
    - *(Optional)* Your company image: Use the Choose File or Browse button (depending on the web browser you are using) to select your company's logo. The image must be exactly 80x80 pixels and a PNG, JPG, or GIF.



4. Click **Invite User**.

Note: Only one connection is made per serial account. The invited user will be able to use 4Word to exchange data for CHD for any of the MIDs in the serial account.

5. In the Invite User window, complete the following steps:
   - Enter the Email address for the user you would like to invite to use 4Word.
   - Enter the user's Name.
   - From the Merchant ID list, select the Merchant ID you wish the user to see in 4Word. (The user will be able to use 4Word with any of your Merchant IDs once set up.)
   - From the Type list, select the type of data that can be exchanged for CHD:

Requirement: Your POS/PMS must be configured to process 4Word API requests in order to get four words or a TrueToken from LTM.

     - **Four Words:** Select this option if the merchant you are inviting would like to exchange four words for CHD only.
     - **TrueToken:** Select this option if the merchant you are inviting would like to exchange a TrueToken for CHD only. (This may be the preferred option for countries where English is not the dominant language since the four words may not be easy to enter based on a country's keyboard layout.)
     - **Either:** Select this option if the merchant you are inviting would like to exchange four words or a TrueToken for CHD. (This is the more flexible option because the Shift4 customer can generate whichever is easiest for the user to enter into 4Word to get the CHD.)
   - From the Allow Delegation list, select one of the following options
     - **Yes:** Select this option to allow the user to create delegates. This will allow the user to create other 4Word users with the same privileges and restrictions as you are setting for the user you are currently inviting. For additional information on delegates, see the *4Word Reference Guide*.
     - **No:** Select this option if you do not want the user you are currently inviting to be able to create other 4Word users.

- From the Require Multifactor list, select one of the following options
  - **Yes:** Select this option to require the user you are currently inviting to use multifactor authentication. This is the recommended option.
  - **No:** Select this option if you do not want to require multifactor authentication.

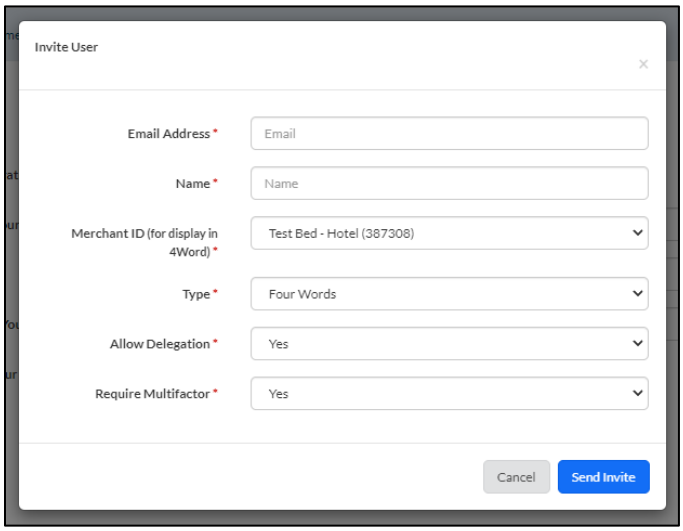
Tip: Multifactor authentication requires separate methods of authentication from different sources to verify a user's identity.

If required, a dynamic, six-digit passcode is required to access 4Word. (This is in addition to the user's login credentials.)

Consequently, this is a more secure way to verify a user's identity as the passcode is dynamic and can only be obtained from an authenticator app (like Google Authenticator) on the user's smart device.

It is highly recommended that multifactor authentication be required when accessing CHD.

- Click **Send Invite**.

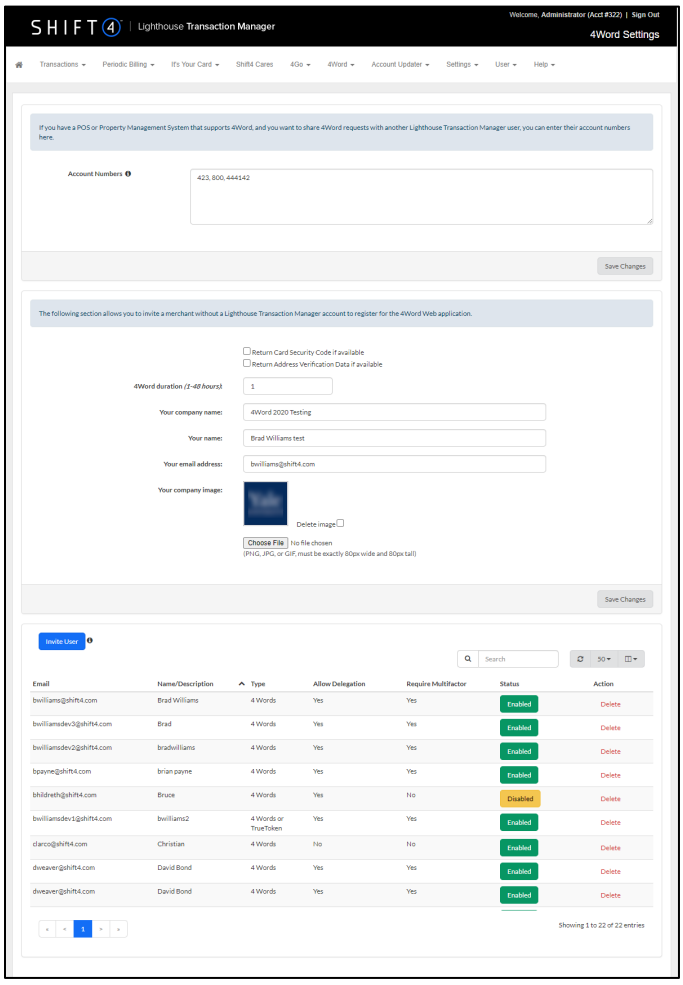


Viewing, Editing, or Deleting a 4Word User in LTM

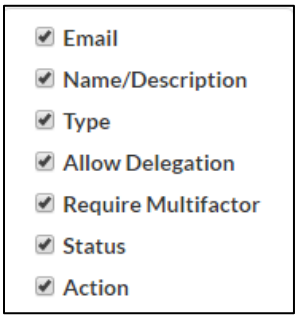
After you have invited a user to use 4Word in LTM, you can view the user's settings. If needed, the user can also be disabled or deleted.

To view or delete a 4Word user, complete the following steps:

1. Sign in to LTM as the Account Administrator.
2. From the menu, select **4Word** > **Settings**.
3. In the table at the bottom of the 4Word Settings page, locate the desired 4Word user. If the list is long, you can use one of the following options to view users:
    - In the Search field, enter the name of the user. The search is dynamic.
    - From the list at the top of the table, select how many users will be displayed.
    - Click the , , , or button to move through the pages of users.



4. The user's information is displayed in their row, and the information cannot be edited.
5. The user information displayed can be edited by clicking  and selecting the fields you would like to see displayed.

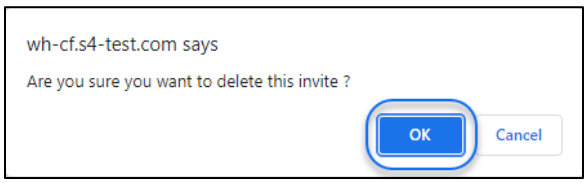


6. *(If applicable)* To disable or enable a user, click the desired option in the Status column:
    - To disable the user, click **Enabled**.
    - To enable the user, click **Disabled**.

Tip: When a new user is created their status is Enabled by default. If there is suspected fraud or other issues for the user account, the function allows you to disable an invited user, rather than deleting their account. If the issues get resolved, the user's account can be enabled without having to send a new invitation.

---

7. *(If applicable)* To delete a 4Word user, complete the following steps:
    - In the 4Word user's row, click **Delete**.
    - In the Delete User window, click **Delete**.

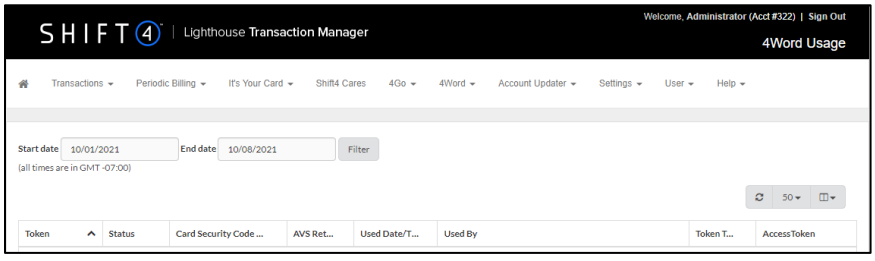


Checking 4Word Usage

It is possible to view the 4Word usage, including who used the four words or TrueToken and when they were used.

To see the 4Word usage, complete the following steps:

1. Sign in to LTM as the Account Administrator.
2. From the menu, select **4Word > Usage**.
3. *(If applicable)* Use the date filter to set a date range, or click a column header to sort by that column.
4. The following is the information displayed for each 4Word usage:
    - Token: This is the TrueToken that that was exchanged for CHD.
    - Status: This displays where the four words or TrueToken was exchanged for CHD.
    - Card Security Code Returned: This details if the information was returned and displayed in 4Word.
        - N: The information was not returned.
        - Y: The information was returned.
    - AVS Returned: This details if the information was returned and displayed in 4Word.
        - N: The information was not returned.
        - Y: The information was returned.
    - Used Date/Time: This is the date and time at which the four words or TrueToken was exchanged in 4Word for the CHD.
    - Used By: This is the account, Merchant ID, and merchant name in LTM where the TrueToken exists.
    - Token Type: This is the type of token exchanged in 4Word for the CHD.
        - Four Words: Four words (like cat, dog, house, and car) were exchanged in 4Word for the CHD.
        - TrueToken: A TrueToken was exchanged in 4Word for the CHD.
    - AccessToken - Displays the masked Access Token for accounts using multifactor authentication.

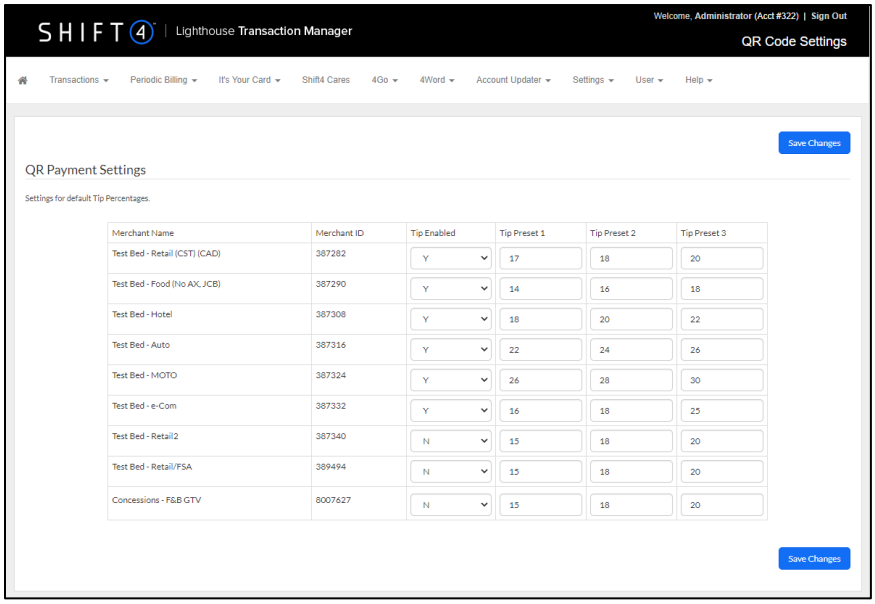


Appendix H – Configuring QR Code Settings

Appendix H reviews enabling tip and configuring default tip percentages for each merchant in the account that is processing payments using QR Pay. After the steps below are completed, the customer will be prompted to tip when completing the payment.

To enable and configure these settings, complete the following steps:

1. Sign in to LTM as an administrator-type user.
2. From the menu, select **Settings > QR Code Settings**.
3. The QR Payment Settings table will be displayed and contains the following information:
    - Merchant Name: The name of the merchant.
    - Merchant ID: The merchant's ID number.
    - Tip Enabled: Displays if tip is enabled for the merchant (Y) or not (N).
    - Tip Preset 1: Displays the first default tip percentage.
    - Tip Preset 2: Displays the second default tip percentage.
    - Tip Preset 3: Displays the third default tip percentage.



4. *(If applicable)* To enable/disable tip on a merchant, click in the corresponding Tip Enabled drop-down list and select **Y** to enable or **N** to disable.

5. *(If applicable)* To change a default tip preset, click in the corresponding Tip Preset field and enter a value between 0 and 30.
6. Click **Save Changes**.

Tip: If you change a tip preset, ensure Tip Enabled is set to Y in order for the tip preset change to be saved. When Tip Enabled is set to N, the tip presets will always be 15, 18, and 20 and cannot be changed.

Appendix I – Billing Statements

If applicable to your account, this is where billing statements can be viewed and downloaded. In addition, this is only displayed if the “Billing statements access” permission is enabled on the user’s account.