First Hawaiian Bank®

First Hawaiian Bank Commercial Online (FCO)

COMPANY SYSTEM ADMINISTRATOR USER GUIDE

First Hawaiian Bank
2339 Kamehameha Highway, Honolulu, Hi 96819

Table of Contents

1. Role and Responsibilities

Roles and Responsibilities of the Company System Administrator

As a Company System Administrator for commercial online banking, your primary responsibility is to manage user access and permissions, ensuring secure and efficient operations. This includes adding, updating, and removing users, assigning specific permissions, and managing account access and transaction limits.

Here's a more detailed breakdown of your roles and responsibilities:

User Management:

Adding and Deleting Users:

- You are responsible for adding new users to the online banking system and removing users who are no longer with the company or whose access is no longer needed.

Updating User Profiles:

- You'll need to update user information, such as contact details or roles, as needed.

Assigning Permissions:

- You will assign specific permissions to users, determining which accounts they can access and what actions they can perform (e.g., making transfers, viewing statements, etc.).

Managing User Access:

- You'll ensure that users have the correct level of access to the online banking system, based on their roles and responsibilities.

Managing Passwords:

- You will be responsible for resetting or unlocking passwords for users who have forgotten them.

Account and Transaction Management:

Assigning Transaction Limits:

- You can set transaction limits for specific users or accounts to control the amount of money that can be transferred or withdrawn.

Managing Account Access:

- You may be responsible for determining which accounts are accessible to specific users or roles.

Verifying External Accounts:

- You may be responsible for setting up and verifying external accounts that are linked to the online banking system.

Transferring Funds (if applicable):

- Depending on your permissions, you may be able to initiate and approve fund transfers.

Monitoring Transaction History

- You may be responsible for monitoring transactions histories and logs to In the online banking system to detect any suspicious activity.

Security and Compliance:

Ensuring Security:

- You are responsible for maintaining the security of the online banking system by following security protocols and procedures.

Monitoring User Activity:

- You may be responsible for monitoring user activity in the online banking system to detect any suspicious activity.

Responding to Security Incidents:

- You may be involved in responding to security incidents or breaches.

Ensuring Compliance:

- You need to ensure that all activities related to online banking comply with relevant regulations and policies.

Segregation of Duties:

- Ensure that account transaction reconciliation functions are performed utilizing segregation of duties processes and performed and reviewed timely.
- Dual control of outgoing payment transactions (ACH and/or Wires) ensure that two different people are drafting and approving payments.

Disclosure

The roles and responsibilities outlined in this guide are intended to provide general guidelines for Company System Administrator/System Manager using FCO. It is essential that Company System Administrator/System Manager stay informed about updates to the service, and modifications to security protocols. First Hawaiian Bank is not liable for any unauthorized access, misuse of the system, or failure to fulfill the responsibilities outlined. First Hawaiian Bank also does not assume responsibility for any consequences arising from the actions or inactions of the Company System Administrator/System Manager in managing user access, permissions, or other activities within the service. It is the responsibility of the Company System Administrator/System Manager to ensure proper system use and to report any issues or concerns promptly.

2. General

Protecting Your Information

At First Hawaiian Bank (FHB), protecting your information and provide you with a dependable online experience is essential. We also rely on you to take precautions to assure the safety of your accounts. By following our tips, FHB Commercial Online can be an even more secure and efficient method for your banking needs.

General Guidelines **KEY TIPS!**

1. Keep up to date with your operating system and antivirus software.
2. Always use secure wireless (Wi-Fi) networks that require a login ID and password.
3. Never leave your computer unattended while using FHB Commercial Online.
4. Regularly monitor your recent account history for unauthorized transactions.
5. Always log off FHB Commercial Online as soon as you're done and close the application and browser.

Login ID

As a valued Company System Administrator, safeguarding your company's data is a critical priority. One area that often goes overlooked is the selection of user naming conventions. Predictable or easily guessed usernames can increase the risk of unauthorized access by fraudsters. To help mitigate these risks, we've outlined best practices for creating secure user naming conventions.

1. **Avoid Using Full Names or Email Addresses:** Use a combination of initials, employee ID numbers, or other unique identifiers rather than full names or email addresses, which can be easily guessed.
2. **Incorporate Non-Sequential Patterns:** Introduce random or non-sequential patterns to usernames. For example, avoid using formats like "John.Smith" or "Employee1" that follow obvious patterns.
3. **Use Lengthy and Unique Identifiers:** Longer usernames with diverse combinations of letters and numbers are harder for attackers to guess.
4. **Avoid Repeating Legacy Formats:** If your organization has migrated from a legacy system, avoid repeating old naming conventions, as they may already be exposed.
5. **Regularly Review User Accounts:** Periodically review and update inactive accounts or any usernames that no longer comply with your updated naming convention standards.
6. **Provide Training to Employees:** Educate employees about the importance of strong usernames and reinforce your organization's security policies.

Passwords

1. Create strong passwords by using a mixture of upper and lowercase letters, numbers and special characters.
2. Do not create passwords containing your initials or birthday.
3. Change your passwords periodically.
4. Memorize your passwords instead of writing them down.
5. Only register personal devices and avoid using features that save your login IDs and passwords.

The FBI recommends no less than 12-14 characters and a mixture of upper- and lower-case letters, with numbers and special characters, and no common words. More importantly, you should have a unique password for every system or application log-in.

- A 12-digit password using these requirements would take 226 years to hack.
- A 15-digit password with these characteristics would take 77,000 years to figure out! That's why most federal agencies require a minimum 16-digit password.

Best Practices for Token Use

- Keep the Token Secure: Store the token in a safe place and do not share it with any unauthorized personnel. Treat it as you would any confidential information.
- Use Unique Credentials: Combine the token with a strong, unique password for your account. Avoid using passwords that are easily guessed or used for other applications or systems.
- Regular Monitoring: Regularly monitor your account for any unusual or unauthorized activity. If any suspicious activity is detected, contact us immediately.
- Replace if Lost or Compromised: In the event the token is lost, stolen, or compromised, notify us immediately to deactivate the token and issue a replacement.

First Hawaiian Bank will never ask you for your token ID number or any other sensitive information related to your token. If you receive any communication requesting your token ID, please consider it fraudulent and report it immediately.
Tokens are linked specifically to your account. For security reasons, do not share it with any third parties or unauthorized personnel. If you have any questions regarding the activation or use of this token, please contact Treasury Management Servicing.

Fraud Prevention **KEY TIPS!**

1. Do not open email attachments or click on links from unsolicited sources.
2. Avoid giving out personal information on the phone or through email.
3. Shred unwanted sensitive documents including receipts, checks, deposit slips, pre-approved credit card offers and expired cards.
4. Monitor your account activity daily.

5. Authenticate all requests to change payee information.
6. Educate all employees regarding current fraud trends.
7. Ensure all users contact information is up to date to receive security alerts.
8. Act quickly. If you suspect your financial information is compromised, call us immediately at 808-844-3303.

Take Precautions Against Computer Fraud

The integrity of the account information you have with First Hawaiian Bank (FHB) is very important. While we utilize various fraud monitoring technologies and strategies to protect your company's information, it is critical for you to review your company's internal procedures regularly. The sophistication and frequency of computer attacks is growing each year. Therefore, we urge you to review your security practices and take precautionary measures as you deem appropriate.

Please keep in mind that each business is responsible for taking adequate measures to ensure that its computer(s), network, and electronic communications systems are secure from unauthorized access and manipulation.

Education about new and changing fraud trends is also a key for long-term success in preventing cyber-attacks. Please share this information with your employees, customers, family and friends so they can remain vigilant against fraudsters.

According to law enforcement, one of the most common emerging threats in the financial industry is the Business Email Compromise (BEC) scam characterized as "a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds"[1].

BEC – A Common Fraud Scheme

In a typical BEC scheme, the victim receives an email they are led to believe comes from a company they normally conduct business with. However, this email requests funds be sent to a new account or otherwise alters the standard payment practices.

Recent examples of BEC attempts include:

- A financial institution received an email allegedly from the CEO of a company, who had previously scheduled a transfer of $1 million, requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." The email address used by the fraudsters was almost identical to the CEO's actual email

[1] Annual Reports - Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports.

address with only one letter changed.

- A bank customer was emailed by someone claiming to be one of the customer's Vendor in China. The Vendor requested that all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to "Corona Virus audits." The victim sent several wires to the new bank account for a significant loss before discovering the fraud.

To protect yourself from this fraud, the FBI advises you to be on the lookout for the following red flags:

- Unexplained urgency.
- Last minute changes in wire instructions or recipient account information.
- Last minute changes in established communication platforms or email account addresses.
- Communications only in email and refusal to communicate via telephone or online voice or video platforms.
- Requests for advanced payment of services when not previously required.
- Requests from employees to change direct deposit information.

KEY TIPS!

The FBI also recommends the following tips to help protect yourself and your assets:

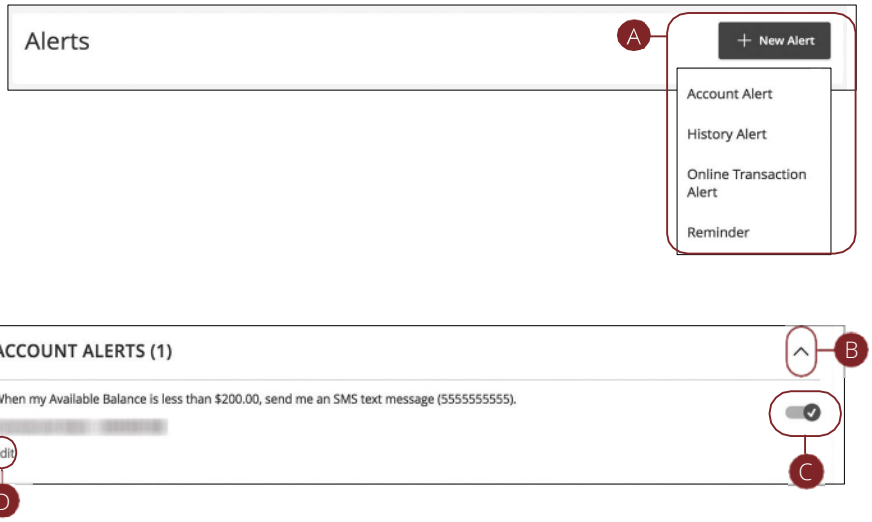
- Be skeptical of last-minute changes in wiring instructions or recipient account information.
- Verify any changes and Information via the contact on file—do not contact the vendor through the number provided in the email.
- Ensure the URL in emails is associated with the business it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.

If you discover you are the victim of unauthorized access to FCO or a fraudulent payment, immediately contact us for assistance.

3. Alerts

Alerts Overview

Having peace of mind is critical when it comes to your online banking experience. When you create an alert through FHB Commercial Online, you specify the conditions that trigger that alert, so you stay on top of what's important to you.

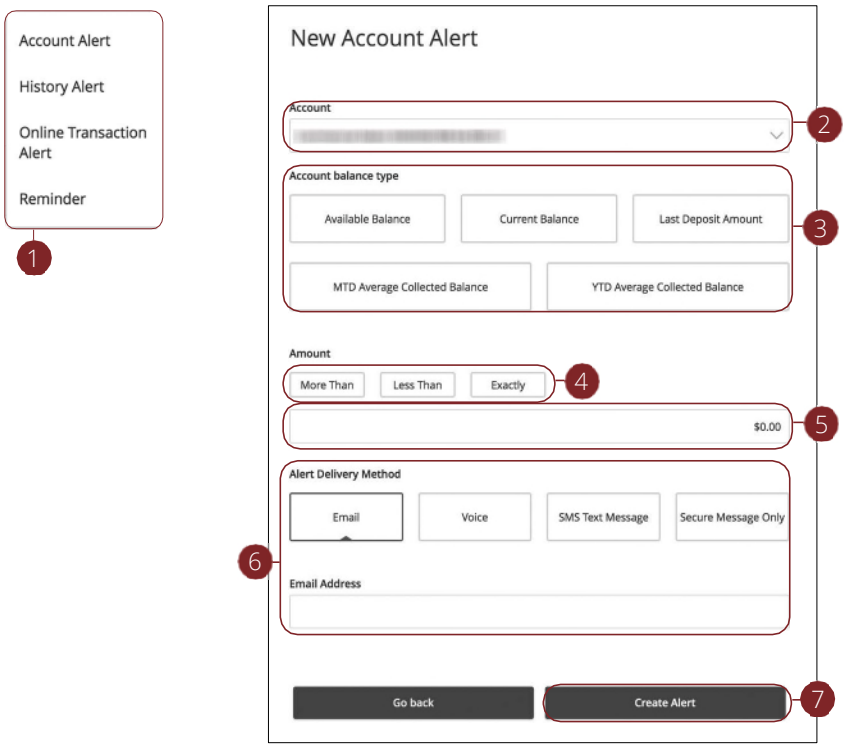


In the Settings tab, click Alerts.

9. The "New Alert" drop-down lets you create an account, history or transaction or reminder alert.
10. The ^ icon allows you to collapse or expand alert details for each category.
11. Toggling the switch turns an alert on or off without deleting it.
12. The "Edit" link lets you make changes to existing alerts.

Account Alerts

There should be no surprises when it comes to your finances. Account Alerts can notify you when the balances in your accounts go above or below a number you specify.

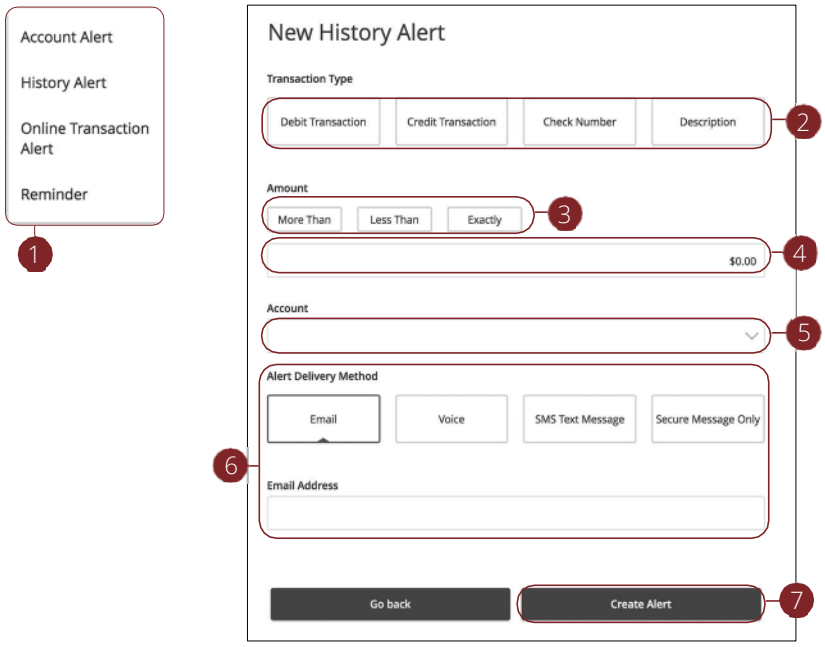


In the Settings tab, click Alerts.

1. Use the “New Alert” drop-down and select “Account Alert.”
2. Use the drop-down to select an account.
3. Choose an account balance type.
4. Select a comparison.
5. Enter an amount.
6. Select a delivery method and enter the corresponding information.
7. Click the Create Alert button when you are finished.

History Alerts

If you're ever concerned about amount limits or pending checks, you can create History Alerts to contact you when a check number posts or transactions meet an amount you choose.

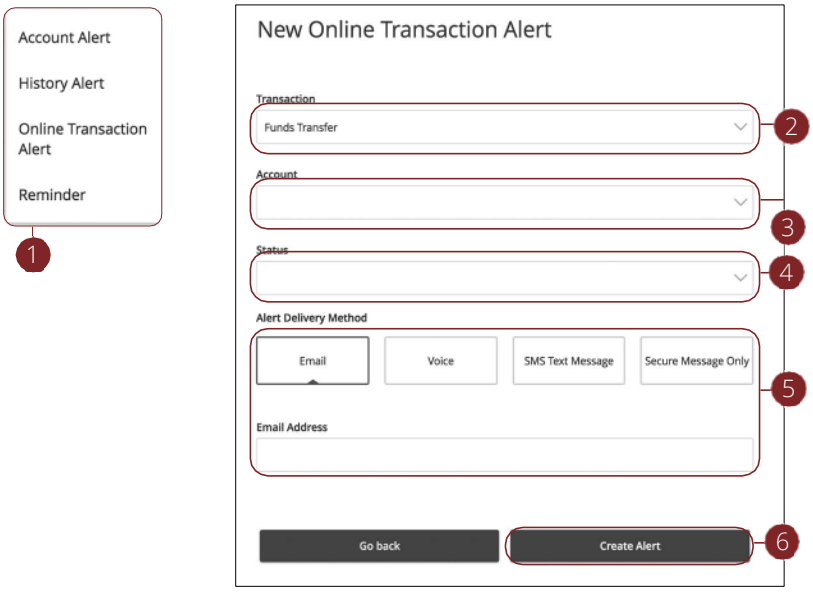


In the Settings tab, click Alerts.

1. Click the "New Alert" drop-down and select "History Alert."
2. Select a transaction type.
3. Select a comparison. These options vary depending on the chosen transaction type.
4. Enter an amount.
5. Use the drop-down to select an account.
6. Select a delivery method and enter the corresponding information.
7. Click the Create Alert button when you are finished.

Online Transaction Alerts

Different types of transactions can occur in your accounts. By creating Online Transaction Alerts, you can be notified when various transfers, payments or debits post to your account.

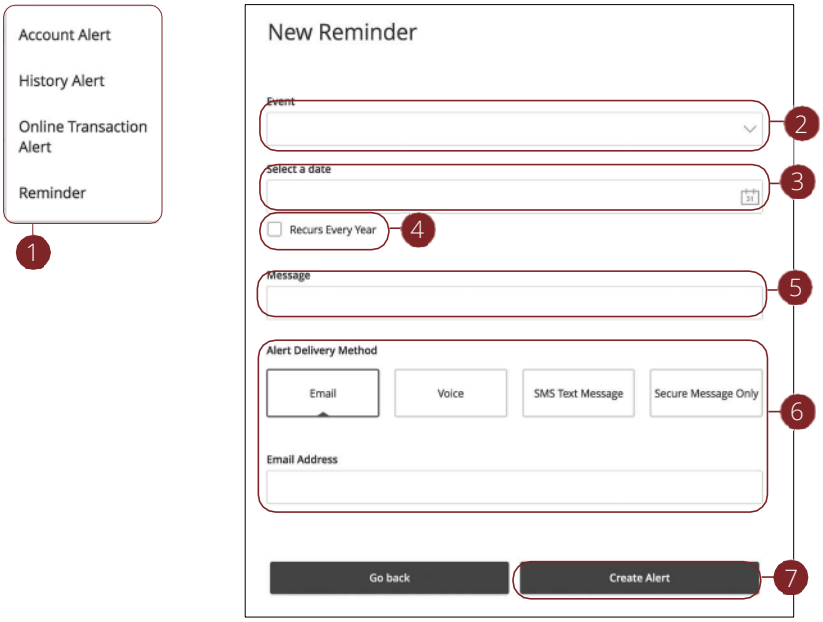


In the Settings tab, click Alerts.

1. Click the “New Alert” drop-down and select “Online Transaction Alert.”
2. Use the drop-down to select a transaction type.
3. Use the drop-down to select an account.
4. Use the drop-down to select a status.
5. Select a delivery method and enter the corresponding information.
6. Click the Create Alert button when you are finished.

Reminder

Just like marking a calendar, you can set up alerts to remind you of specific dates or events.



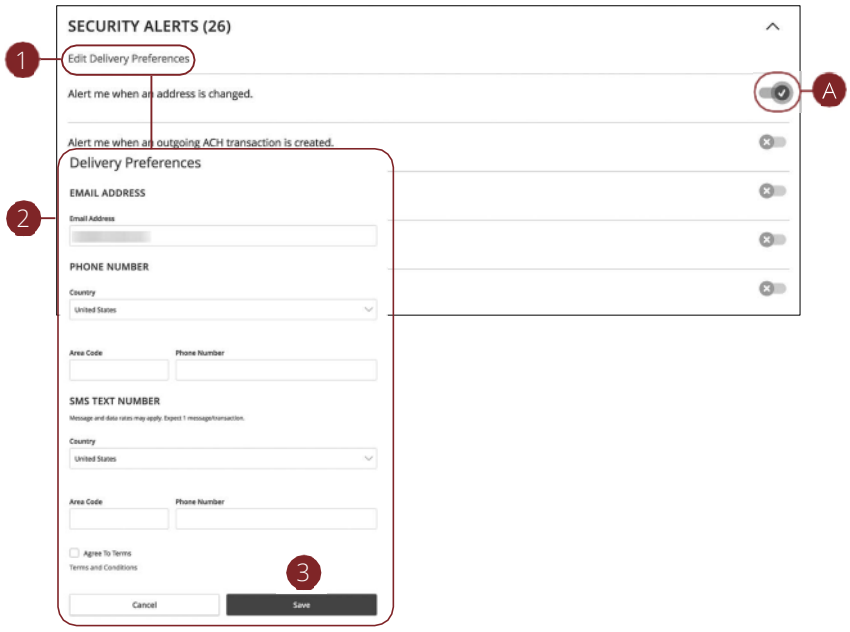
In the Settings tab, click Alerts.

1. Use the “New Alert” drop-down and select “Reminder.”
2. Use the drop-down to select an event.
3. Enter the date for the alert to occur.
4. Check the box next to “Recurs Every Year” to have your alert repeat annually.
   - (Optional) Enter a message.
5. Select a delivery method and enter the corresponding information.
6. Click the Create Alert button when you are finished.

4. Security

Security Alerts Overview

To help you feel safe and in control, Security Alerts are implemented on your accounts to notify you immediately when security scenarios occur.



In the Settings tab, click Alerts, then Security Alerts. Toggling the switch turns an alert on or off without deleting it.

Edit Delivery Preferences

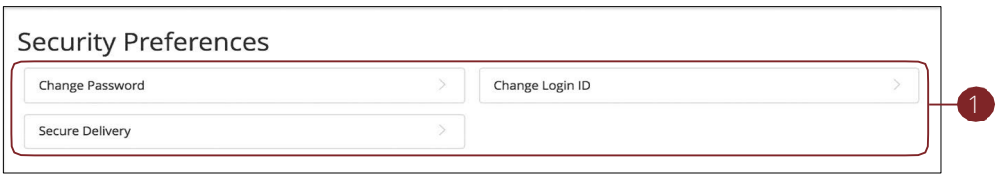
When a trigger occurs, Security Alerts are sent to you through secure messages. You can add additional delivery methods to notify you about your accounts wherever you are.

In the Settings tab, click Alerts, then Security Alerts.

1. Click the “Edit Delivery Preferences” link at the top. These changes will apply to all Security Alerts.
2. Enter the information for your preferred delivery method.
3. Click the Save button when you are finished making changes.

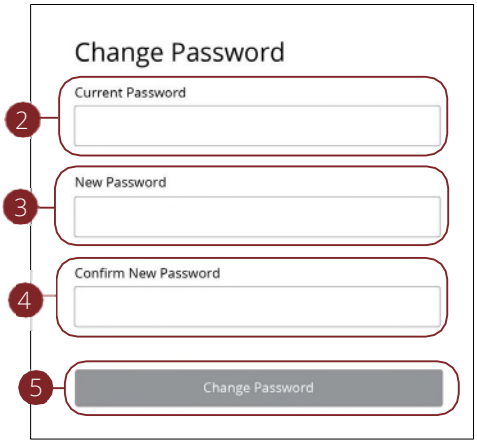
Security Preferences

We take security very seriously at FHB. Because of this, we've added various tools to help you better protect your account information. You can add and manage these features in Security Preferences to strengthen your FHB Commercial Online experience.



Change Password

When you need to, you can change your password within FHB Commercial Online Center. We recommend that you change your password regularly and follow our guidelines for creating a strong password.

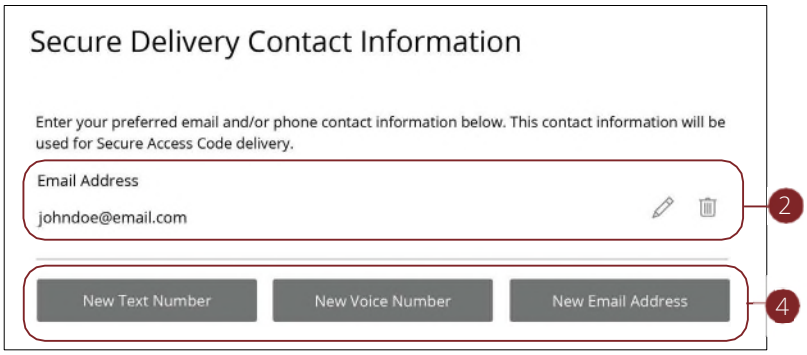


In the Settings tab, click Security Preferences.

6. Click the Change Password button.
7. Enter your old password.
8. Create a new password.
9. Reenter your new password.
10. Click the Change Password button when you are finished making changes.

Secure Delivery

FHB verifies your identity using Secure Access Codes (SACs), which are numbered codes that are sent to you by email, phone or text. Within Security Preferences, you can make changes to your delivery preferences or add new ways we can contact you.



In the Settings tab, click Security Preferences.

6. Click the Secure Delivery button.
7. Make changes to a secure delivery method by clicking the icon to make changes or the icon to delete a secure delivery method.
8. Enter your new contact information and click the icon when you are finished to save your changes.
9. Add a new delivery contact by clicking either the New Email Address, New Voice Number or New Text Number button at the bottom of the page.

Token User Quick Guide

Your new First Hawaiian Bank Commercial Online security token is a security device that adds another level of security authentication when initiating transactions (including ACH, Wires and/or Fund Transfers).

- First Hawaiian Bank's Treasury Management Servicing Department will issue a hardware token to each user approved to Authorize a transaction initiated through FCO.
- All tokens must be registered with FCO. The hardware token will be mailed to each user and ready to use upon arrival.

Using Tokens

After completing a transaction (ACH, Wire and/or Funds Transfer), the user with Approval rights will click on Approve button. Click OK when the window prompts you to confirm the transaction. Then the following window will appear:

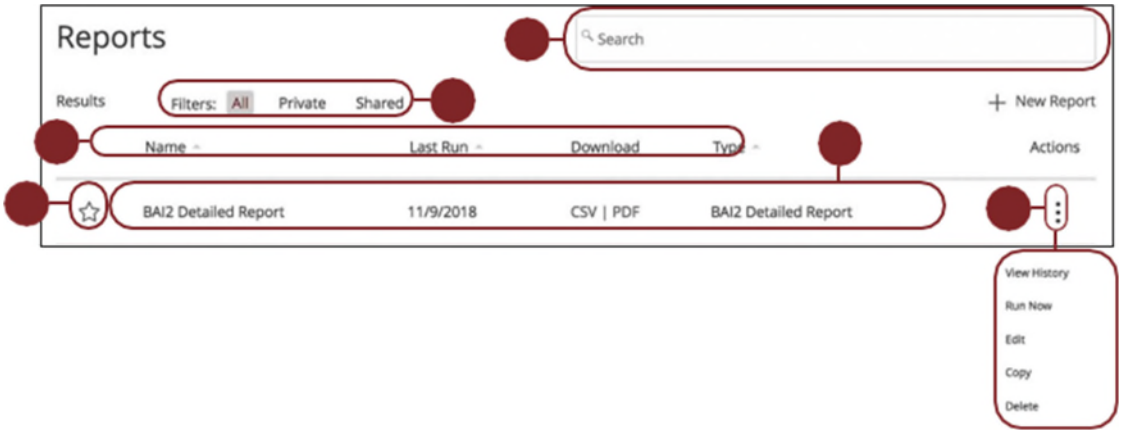
- The first time a token is used, the dialog box will require users to enter two consecutive security codes. Enter Security Code 1, wait until token shuts off then power back on to obtain the second token code. When the new number appears on the token, enter number in the Security Code 2 field.

- The Security Code keyed must match the numbers expected by our online banking system for the transaction to successfully transmit. The transaction will not transmit without a successful match.

5. Reports

Reports Overview

You can keep up with all the incoming and outgoing transactions within your accounts using the Reports feature. Viewing a report on certain transactions can prevent errors and make bookkeeping easy. Depending on which report you run, it can be saved to your computer or device as a PDF, XSL or a BAI.

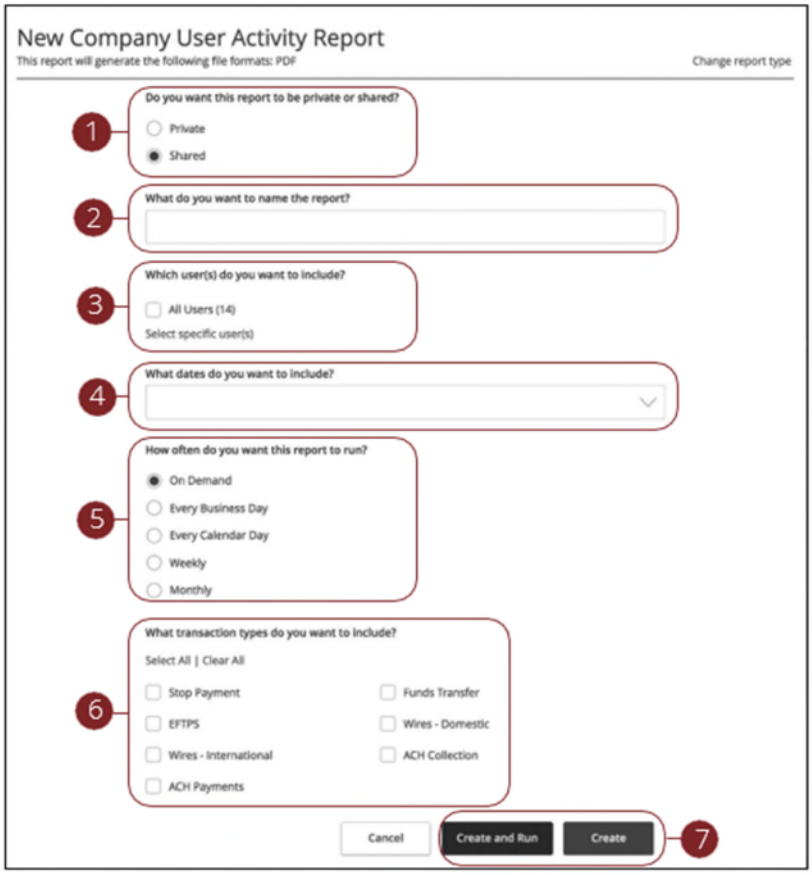


Click the Reports tab.

1. Use the search bar to locate existing reports.
2. All existing reports are available on this page. You will see the report name, date when it last run, whether it was download and the type of report.
3. The filters feature allows you sort your reports by all, private or shared.
4. Click the ▲ icon to search transactions by name, last run, download and type.
5. Click the ☆ icon to favorite a report.
6. Click the ⋮ icon to view history, run, edit, copy or delete a report.

Company User Activity Report

With the Company User Activity Report, you can create a report to view all transactions drafted and approved by a specified user. You can select the date range and how often to run the report.

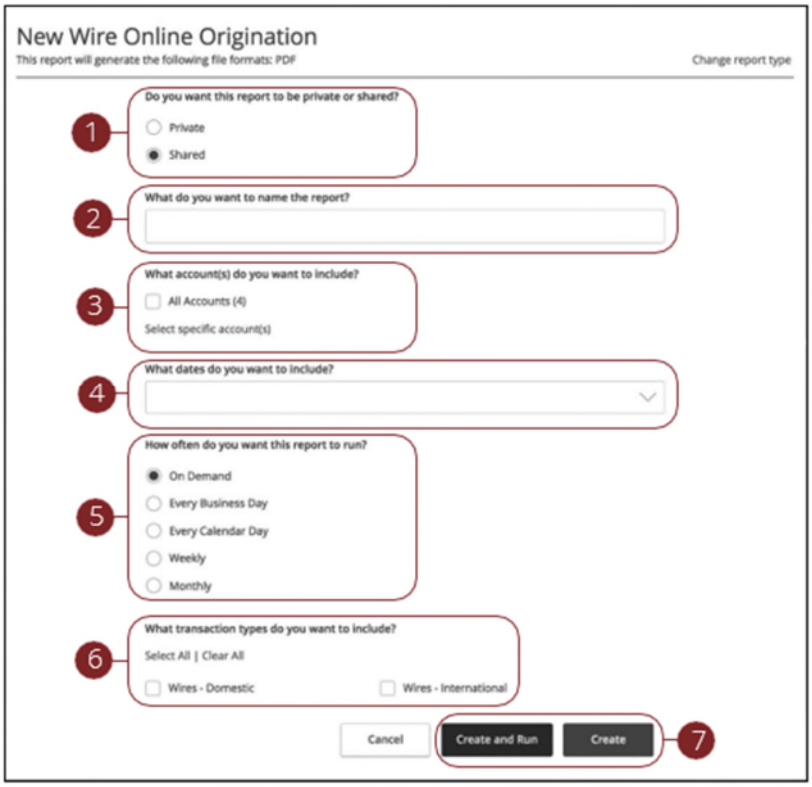


Click the Reports tab, then the "+New Report" link and select Company User Activity Report.

1. Decide whether the report should be private or shared.
2. Enter a report name.
3. Select a user.
4. Select a date range.
5. Schedule how often to run the report.
6. Select transaction types.
7. Click either the Create and Run or Create button when you are finished.

Wire Online Origination Report

No matter how many Wires your business sends, the Wire Online Origination Report can help you track your transactions. You can also choose the date range and how often to run the report.

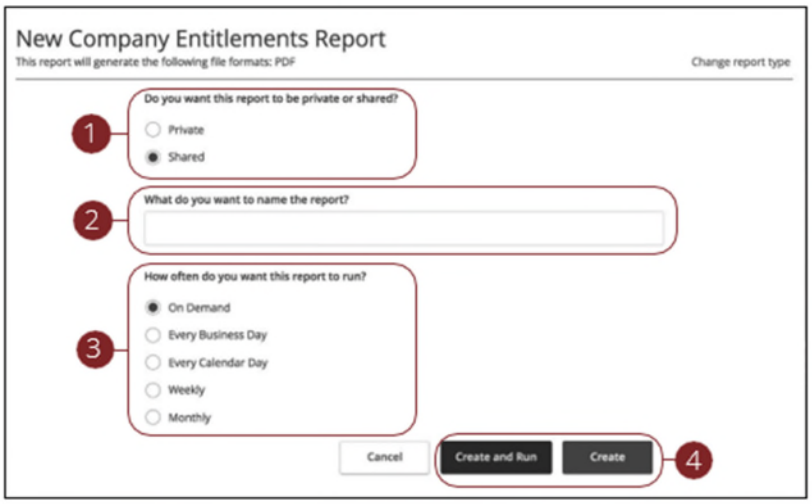


Click the Reports tab, then the "+New Report" link and select Wire Online Origination

1. Decide whether the report should be private or shared.
2. Enter a report name.
3. Select the accounts you want to include.
4. Select a date range.
5. Schedule how often to run the report.
6. Select transaction types.
7. Click either the Create and Run or Create button when you are finished.

Company Entitlements Report

The Company Entitlements Report is an easy way for you to monitor your entitlements over a certain time period. You can run this report on a daily, weekly or monthly schedule depending on your needs.

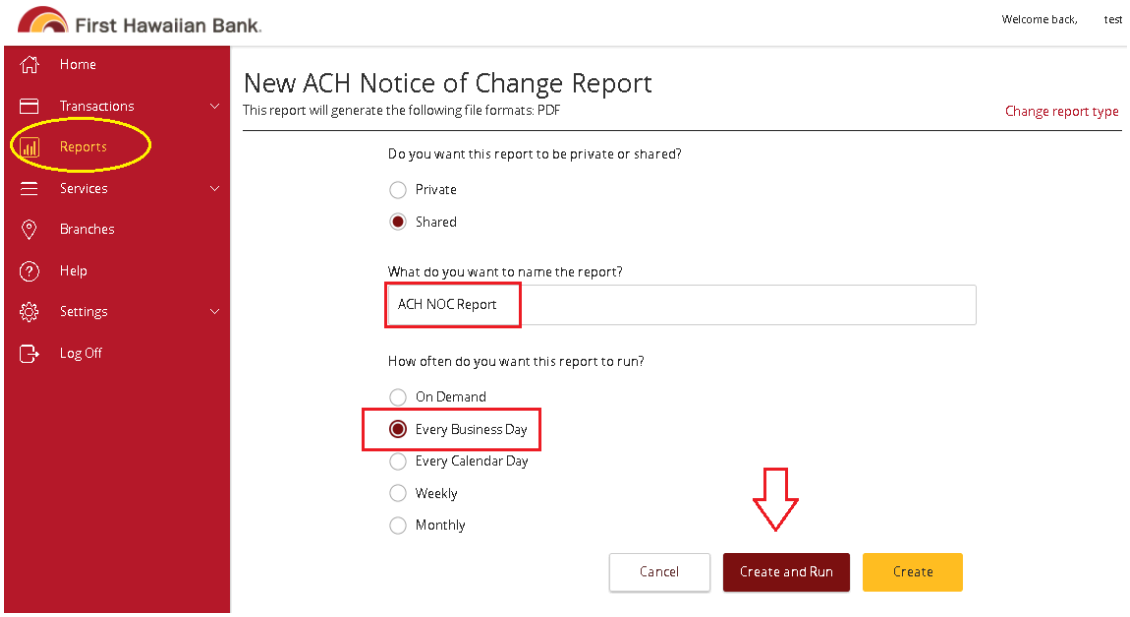


Click the Reports tab, then the "+New Report" link and select Company Entitlements Report.

1. Decide whether the report should be private or shared.
2. Enter a report name.
3. Click either the Create and Run or Create button when you are finished.

ACH Notice of Change Report

The ACH Notice of Change Report is an easy way for you to monitor any ACH returns or Notices of Changes. You can run this report on a Daily, weekly or monthly schedule depending on your needs.



1. From service menu, Click the Reports tab.
2. Click on New Report and select ACH Notice of Change Report.
3. Select Private or Shared and Naming convention of the report.
4. select Every Business Day then click on Create and Run:
    - If the report has no activity, report will state no data found.

6. User Access Management

Users Overview

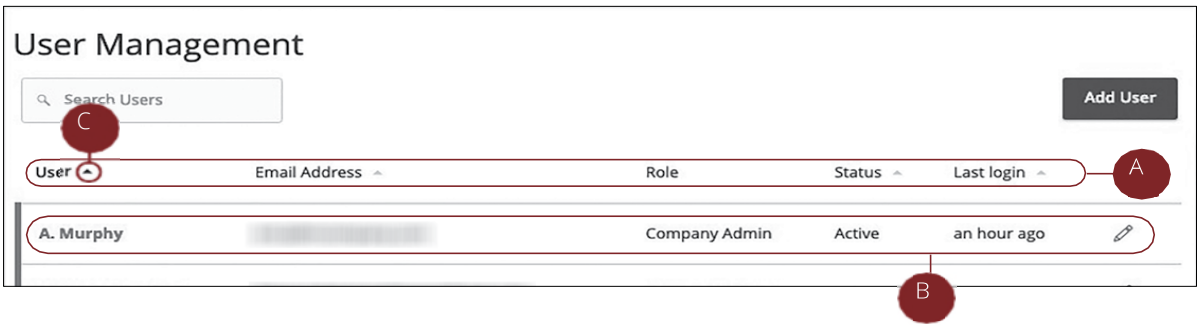
Depending on your number of employees, owners and company policies, FHB Commercial Online lets you set up multiple users with different responsibilities. After establishing a Company Policy with your accountant or financial advisor, new users can be created with their own unique login IDs and passwords. Each user is assigned a set of user rights that permits or prevents them from performing certain actions such as:

- Sending or drafting payments and creating templates for certain transaction types.
- The number of approvals that can be completed in a day or the dollar amount in a specific transaction.
- Accessing specific accounts.
- Managing recipients, users, subsidiaries and templates.

Authorized users can set up the features, accounts and rights each user needs to do their job. Establishing these rights gives users permission to perform specific tasks, helping you manage your business and making it run as smoothly as possible.

User Management Overview

The User Management page lets you view all your existing users and their contact information in one easy place. From here, you can create users, edit rights and oversee your employees on a day-to-day basis.

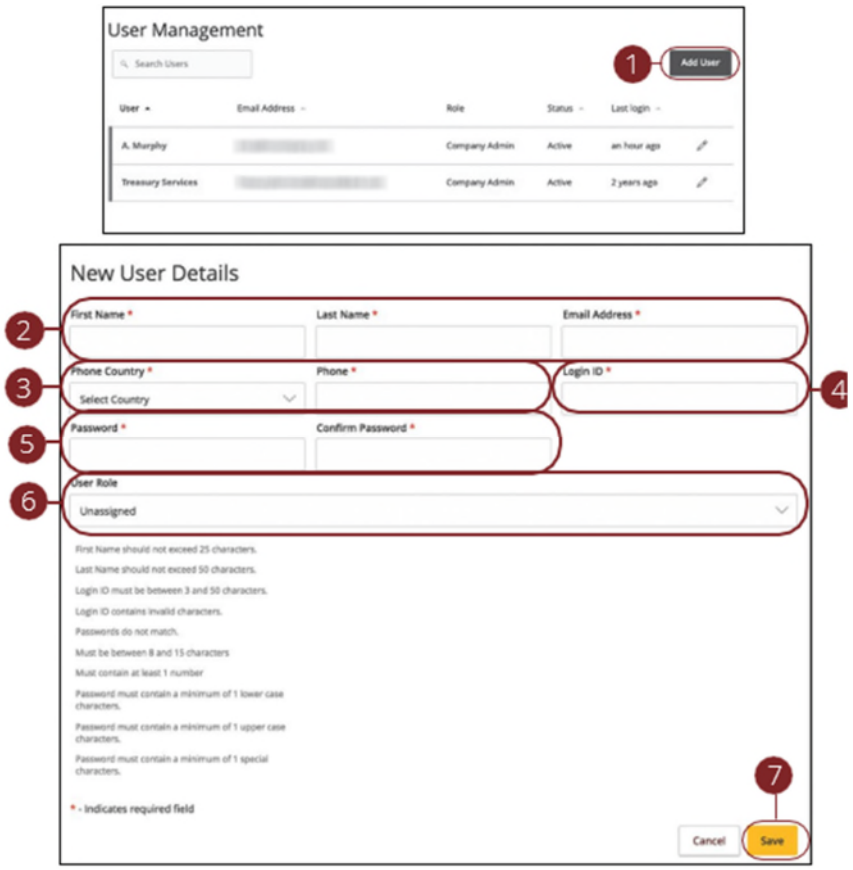


In the Administration tab, click Users.

A. The following information presents for each user:
   - Name
   - Email address
   - Applied user role
   - Status
   - Last login time
B. You can click on a user role to make edits.
C. You can sort users in alphabetical or reverse alphabetical order, by email address, role, status or last login order by clicking the ▲ icon next to the Users column.

Adding a New User

Each employee needs their own specific login ID and password to give them access to your business's online banking. This allows you to manage your business banking at multiple levels.

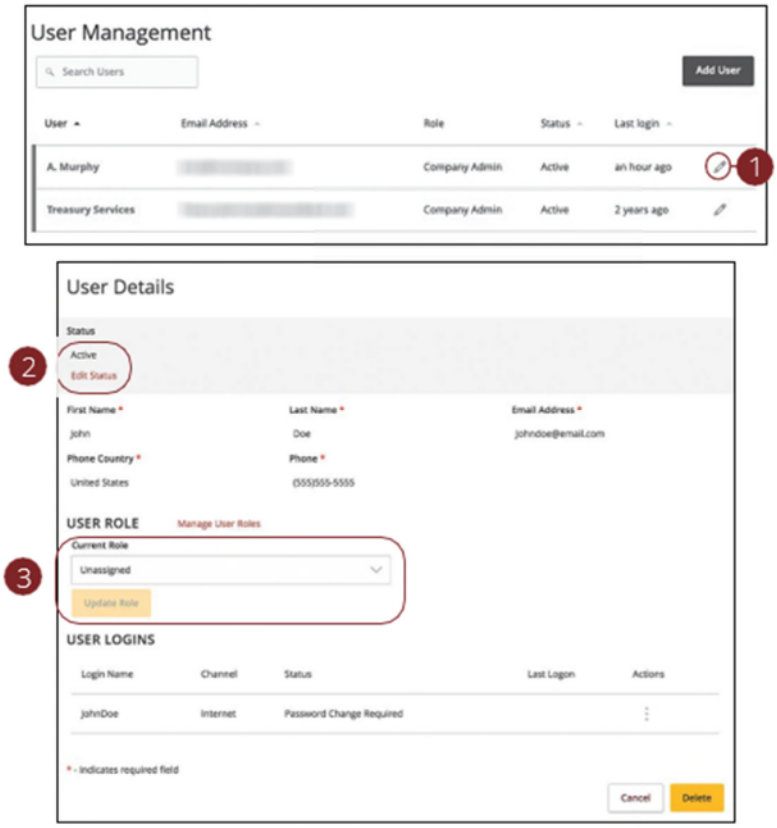


In the Administration tab, click Users.

1. Click the Add User button in the top right corner.
2. Enter the user's first name, last name and email address.
3. Select the user's country using the "Phone Country" drop-down and enter their phone number.
4. Create a unique login ID for the new user.
5. Enter a password following our guidelines and confirm it in the provided space.
6. Select the appropriate user role using the drop-down.
7. Click the Save button when you are finished.

Editing a User

Authorized users with the Manage Users right can make changes to existing users at any time. This is especially beneficial if someone's job title changes and their approval limits and responsibilities need to be adjusted.

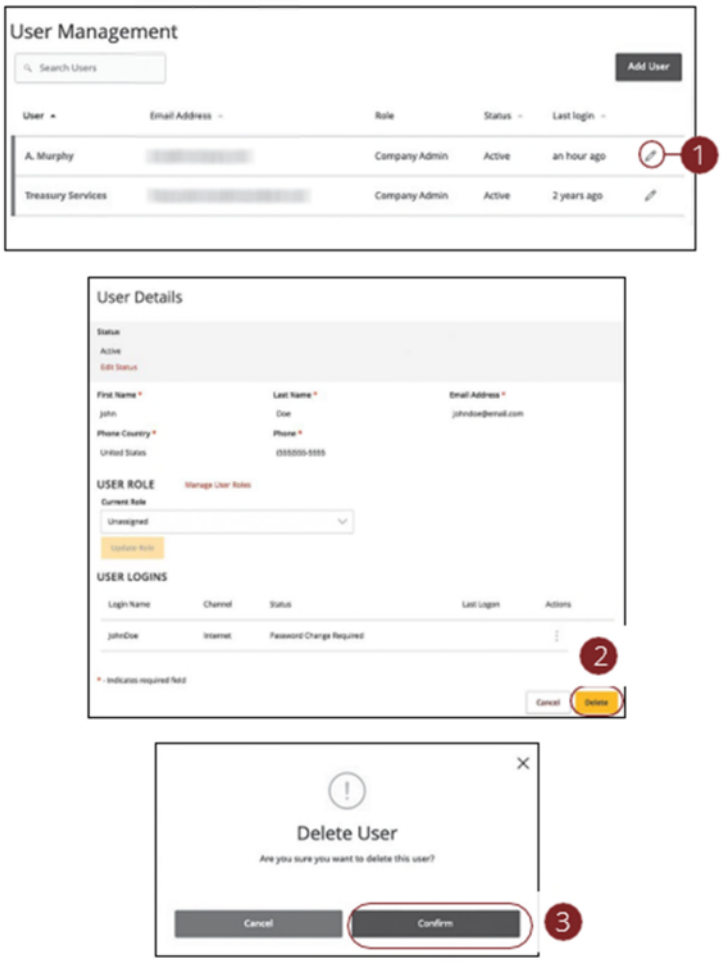


In the Administration tab, click Users.

1. Find the user you want to edit and click the icon.
2. Activate or deactivate a user by clicking the "Edit Status" link.
3. Select a different user role using the "User Role" drop-down. Click the Update Role button when you are finished making changes.

Deleting a User

If you are assigned the Manage Users right, you have the ability to permanently delete a user that is no longer needed. This deletes their contact information from the User Management page and deactivates their FHB Commercial Online login ID, but it does not erase the data from an existing payment using that person.



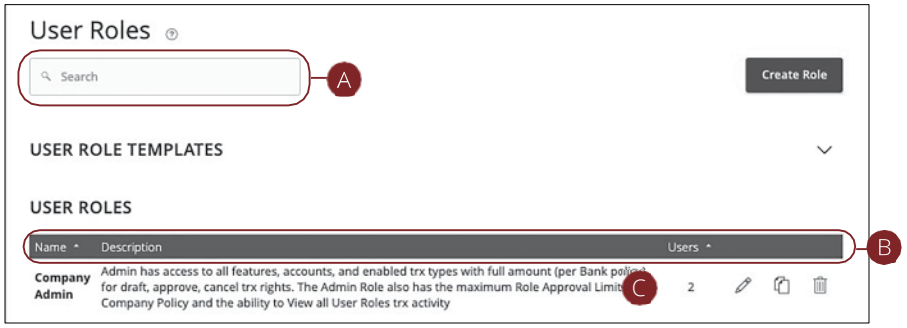
In the Administration tab, click Users.

1. Find the user you want to remove and click the icon.
2. Click the Delete button.
3. Click the Confirm button to permanently remove a user.

7. User Entitlement's Management

User Roles Overview

Once you establish your Company Policy, you can start creating user roles. User roles are the restrictions placed to shape a user's privileges, depending on the responsibilities a user has. Some users may have the ability to draft a transaction, while others can approve it. User roles must fit within the Company Policy and cannot exceed it.



In the Administration tab, click User Roles.

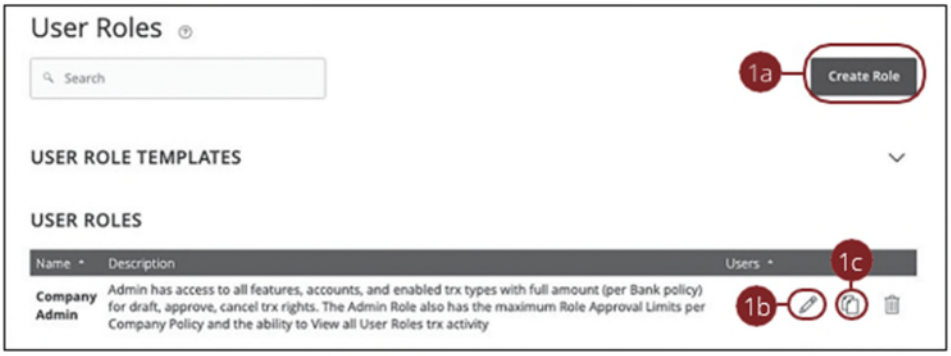
A. You can use the search bar to find specific user roles.

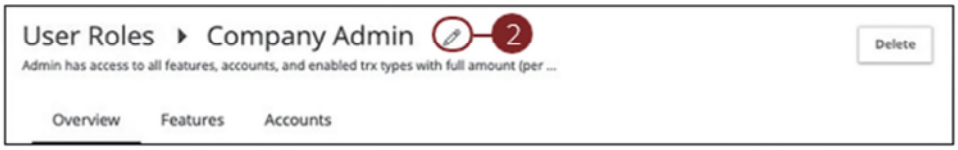
B. Clicking the ▲ icon next to a column title allows you to sort user roles by name, description or users.

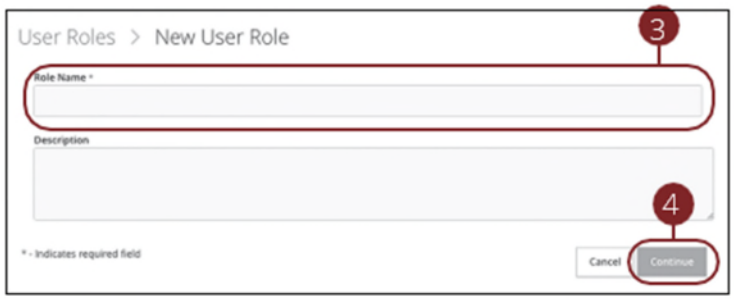
C. The number under the Users column indicates how many users are assigned to this role. Click the number to see who is assigned to a specific role.

Creating, Editing or Copying a User Role

To begin editing or creating a user role, you must decide what privileges and responsibilities a particular user has. You can then write a description of the role and give it a unique name.





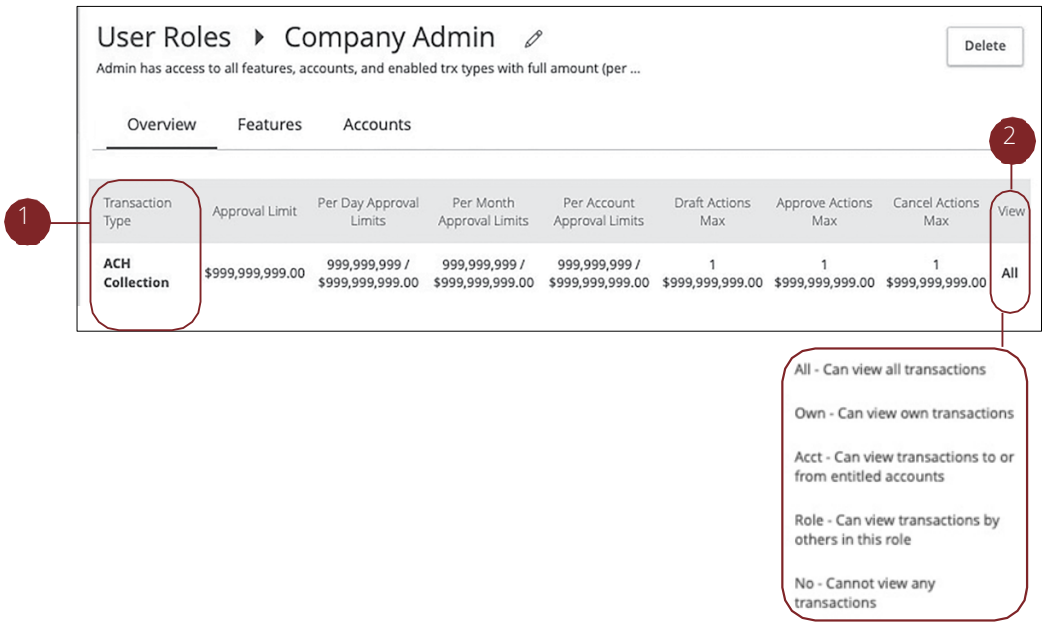


In the Administration tab, click User Roles.

1. Decide if you are making a new role, editing an existing role or copying a role.
    i. Click the Create Role button if you are making a new user role.
    ii. Click the ✎ icon to edit an existing role.
    iii. Click the ⧉ icon to copy and adjust an existing role.
2. Optional) If you are editing an existing user role, edit the role name by clicking the ✎ icon.
3. Enter a role name if you are making a new role or copying a role.
4. Click the Continue button.

Establishing Transaction Type Rights

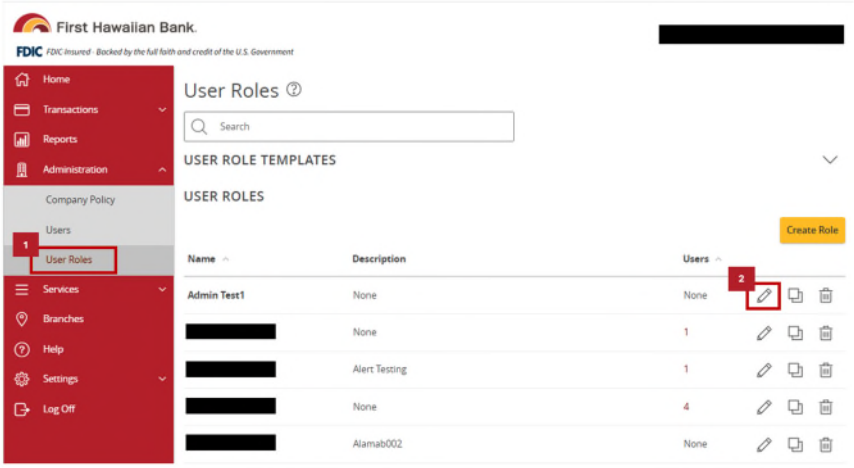
You can start assigning or editing a user's rights in the Overview tab, which helps you decide which responsibilities and limitations a user should have regarding certain transactions. Here, you can change a user's approval limits and decide which transaction types they can view, draft, approve or cancel.



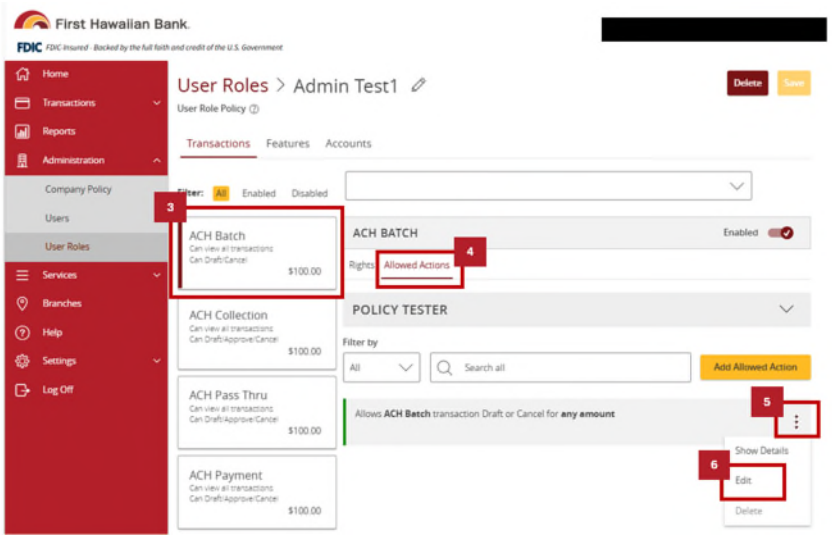
1. Choose a type of transaction to assign rights for under the Transaction Type column.
2. Click the "All" under the View column to change which transaction activity a user can view.
    - All- Can view all transactions.
    - Own- Can view own transactions.
    - Acct- Can view transactions to or from entitled accounts.
    - Role- Can view transaction by others in this role.
    - No- Cannot view any transactions.

Enabling Operation Rights

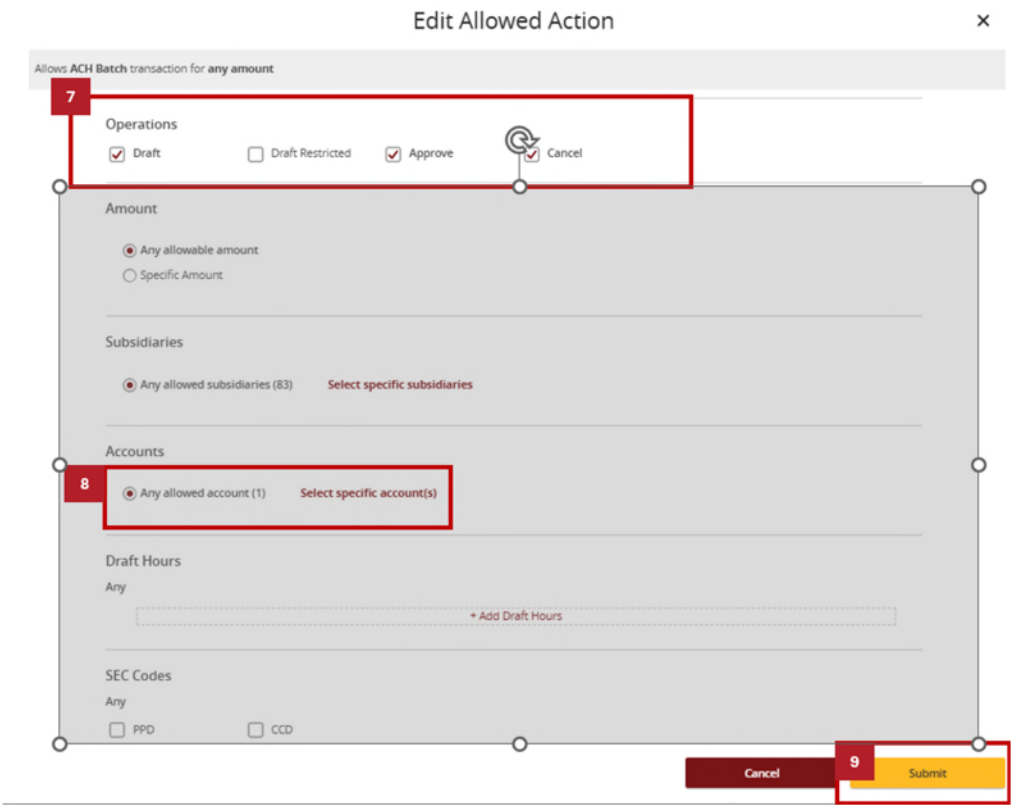
You can select the allowed operations a user can perform when handling a transaction, such as drafting, approving or cancelling rights.



1. Click the User Roles tab.
2. To edit a user profile, click the icon.



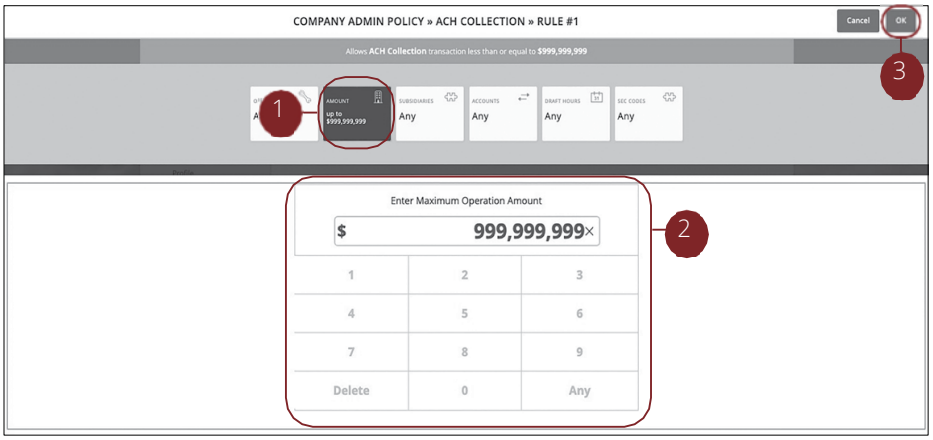
3. Select the transaction type.
4. Then toggle over to the Allowed Actions Tab.
5. Click the ⋮ Icon.
6. When the Drop-down menu appears select Edit.



7. Select Drafter And/or Approver permission.
8. Select the Allowed accounts the permission will be for.
9. Click the Submit button at the bottom of the form.
10. Click the  button at the top right of the screen.
11. Repeat Steps 3 through 10 for each transaction type for which you want to grant the user Drafter and/or Approver permissions.

Choosing the Maximum Draft Amount

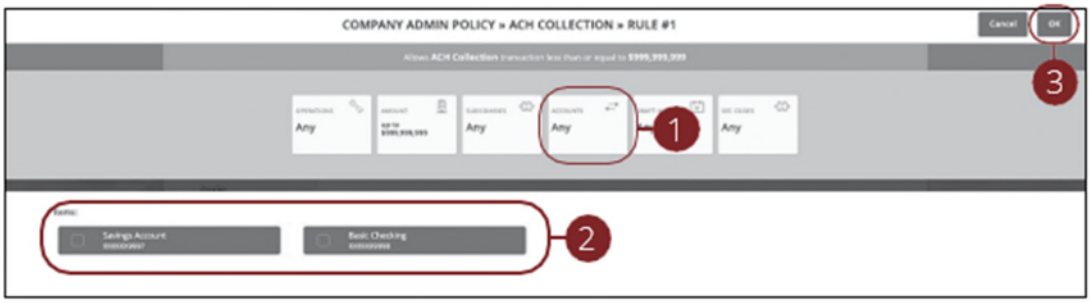
Using the Manage Company Policy rights, you can choose the maximum amount of funds that can be drafted per transaction. This cannot exceed the Company Policy.



1. Click the Amount action.
2. Enter the maximum draft amount using the number pad or click the Any button for an unlimited amount.
3. Click the OK button when you are finished making changes.

Enabling Allowed Accounts

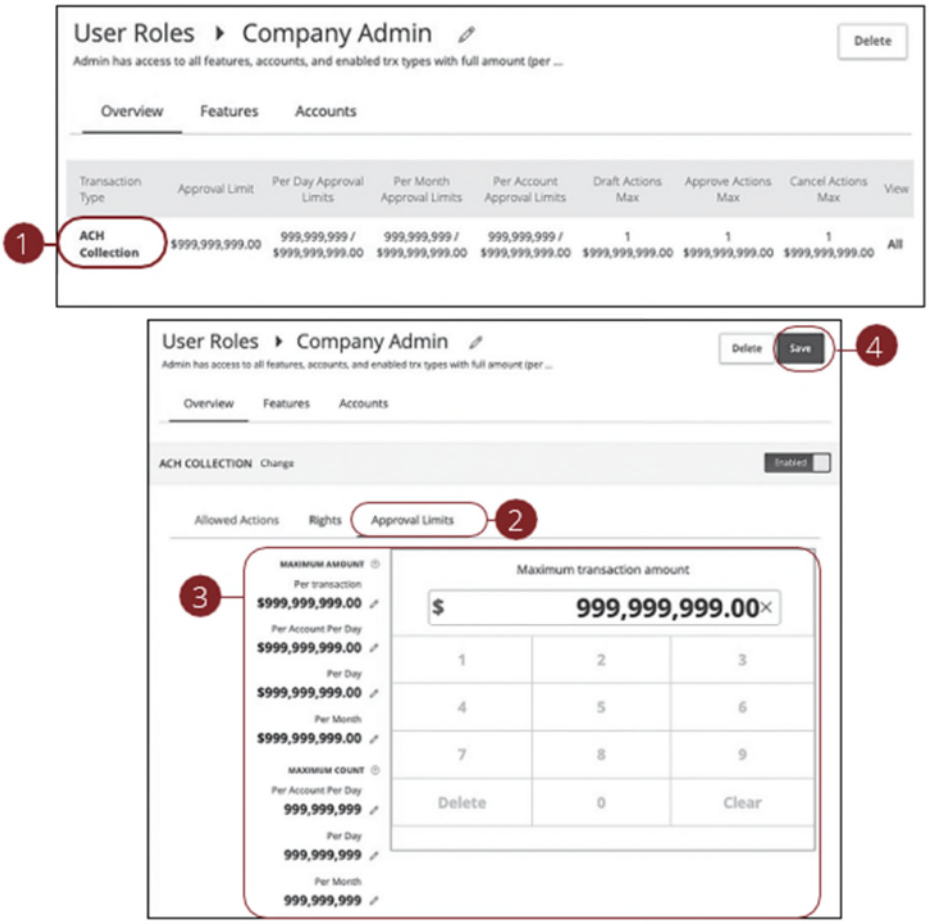
The Accounts tab lets you decide which users have access to perform specific tasks within an account, including viewing the account and transaction histories and making deposits or withdrawals.



1. Click the Accounts action.
2. Select the group or accounts the user has authorization to use.
3. Click the OK button when you are finished making changes.

Editing Approval Limits for a Transaction Type

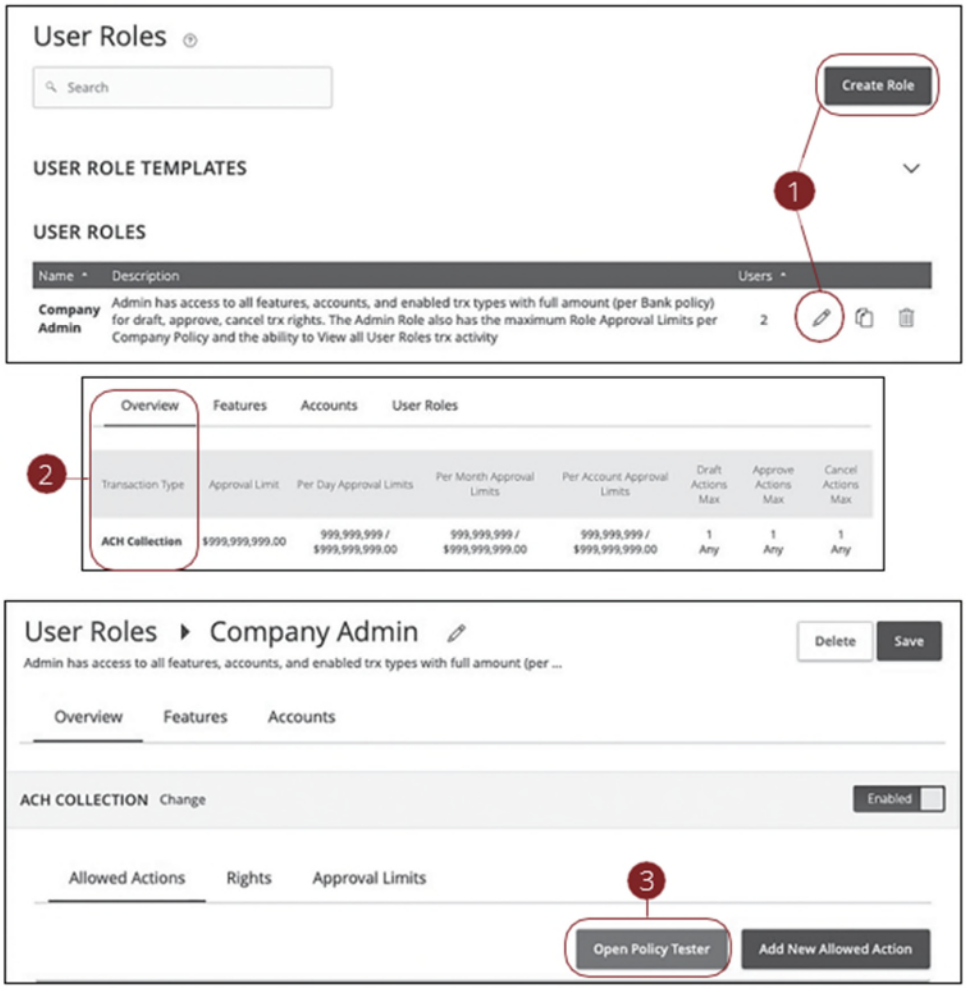
User's approval limits can be controlled and adjusted, to ensure they have the appropriate access and transactions limits so you can reduce the risk of errors or financial exposure. You can set these restrictions for a daily and monthly basis as well as per account.



1. Select a transaction type in the Overview tab to edit a user's approval limits.
2. Click the Approval Limits tab.
3. Click the ✎ icon to edit the maximum amounts a user can approve or draft and the maximum number of transactions a user can perform. Enter the amount or count using the keypad.
4. Click the Save button when you are finished making changes.

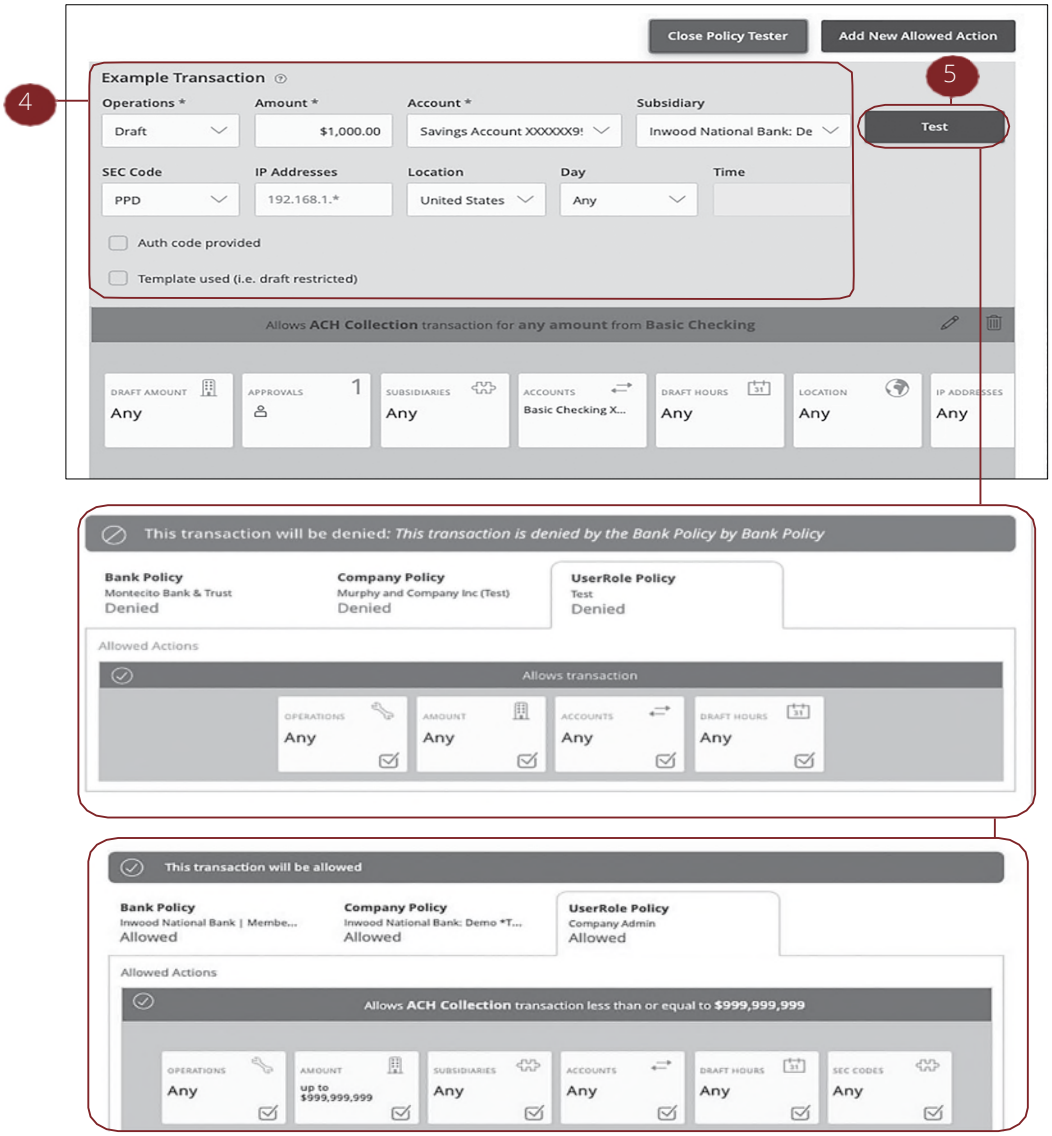
User Role Policy Tester

The Policy Tester gives you the ability to test possible actions before making the changes within the User Role. This allows you to see if the user can perform a certain transaction based on the Bank Policy, Company Policy and User Role Policy.



In the Administration tab, click User Roles.

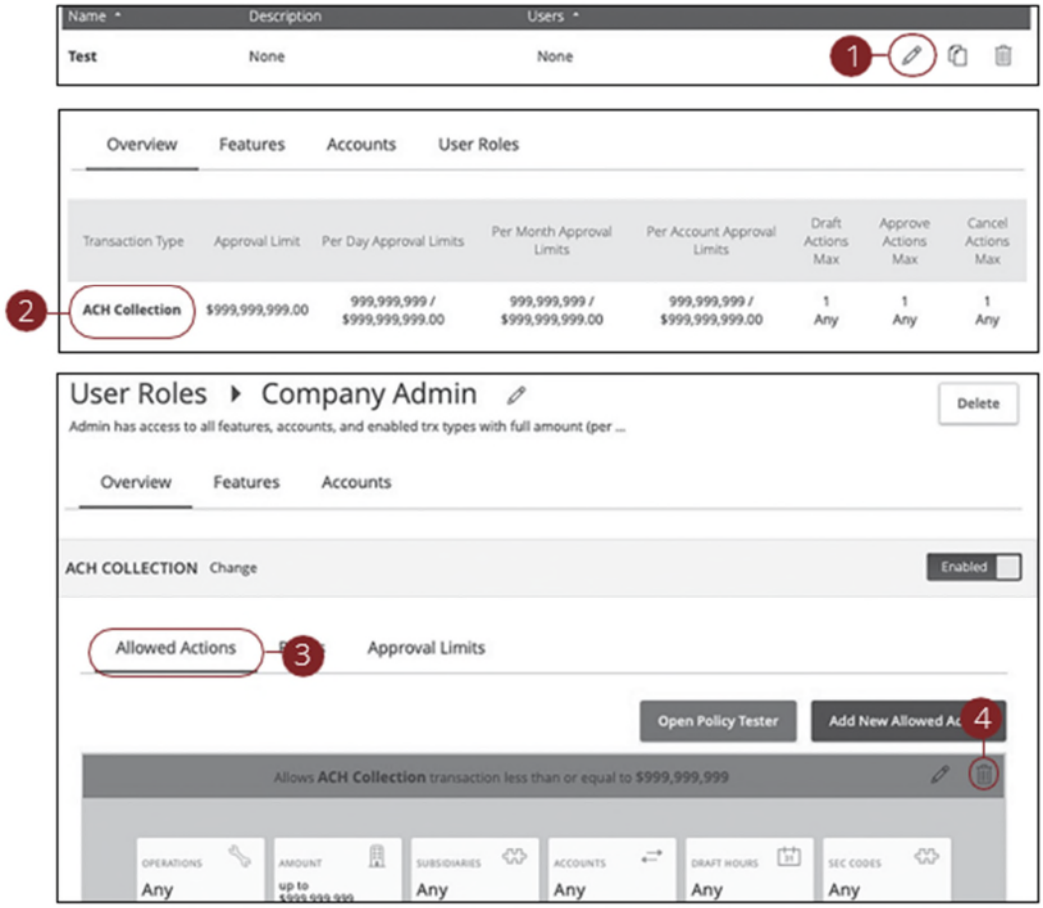
1. Click the icon next to an existing user role or click the Create Role button and follow the steps in section 6 to create a new user role.
2. Select the transaction type in the Overview tab that you would like to run a test on.
3. Click the Open Policy Tester button.



4. Create a sample transaction to test the user's policy.
5. Click the Test button. You can then see whether the user can perform the transaction.

Deleting Allowed Actions

You may need to delete a list of allowed actions within a specific transaction type.

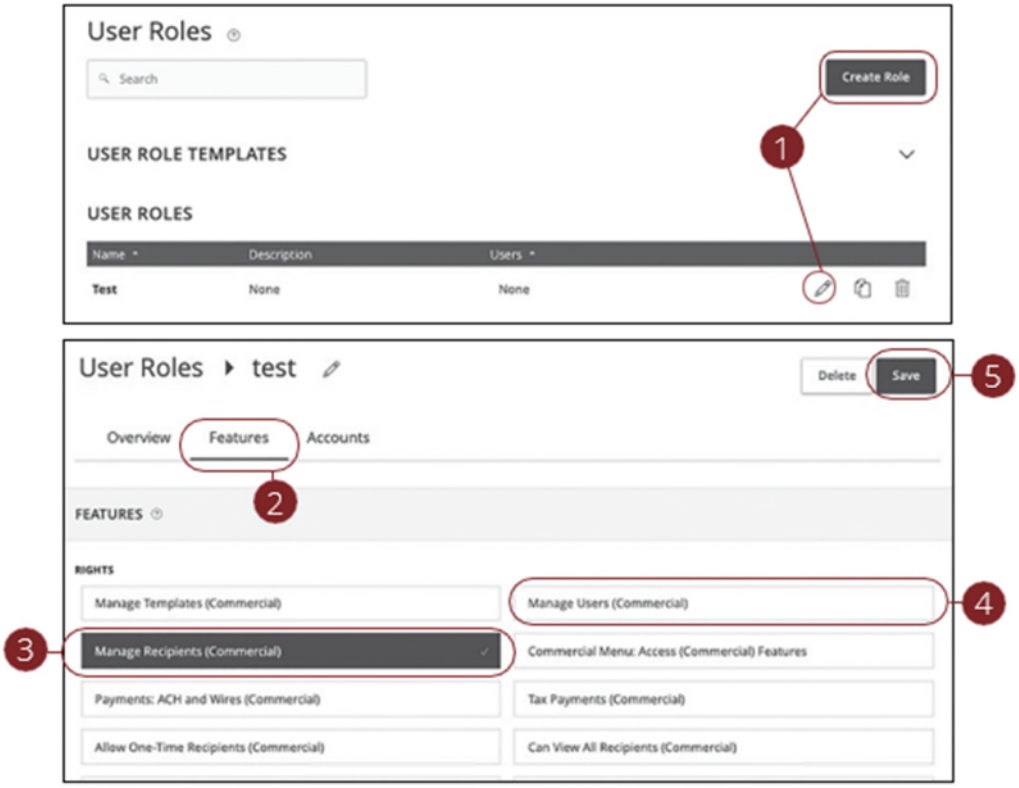


In the Administration tab, click User Roles.

1. Click the ✎ icon next to an existing user role.
2. Click on the appropriate transaction type.
3. Click the Allowed Actions tab.
4. Click the 🗑 icon to delete the transaction's specific allowed actions.

Establishing Rights to Access Features

When assigning user rights, the Features tab lets you control who can edit templates or manage users, subsidiaries or recipients. Depending on their User Policy or job duties, some users may have different responsibilities than others.



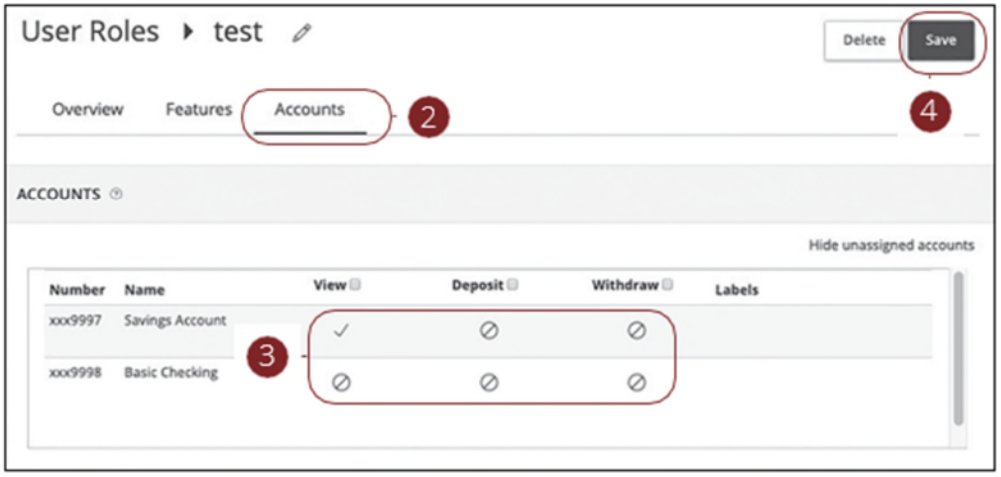
In the Administration tab, click User Roles.

1. Click the ✎ icon next to an existing user role or click the Create Role button and follow the steps on page 44 to create a new user role.
2. Click the Features tab.
3. Enable a feature by clicking on a specific right. Dark boxes with a check mark indicate that the feature is active.
4. Disable a feature by clicking on it to make the box white.
5. Click Save when you are finished making changes.

Note: If the Manage Users right is assigned to a user, they can change their own rights. Be sure to limit which users have this feature.

Establishing Rights to Access Accounts

The Accounts tab lets you decide which users have access to perform specific tasks within an account, including viewing the account and transaction histories and making deposits or withdrawals.



In the Administration tab, click User Roles.

1. Click the ✎ icon next to an existing user role or click the Create Role button and follow the steps on page 44 to create a new user role.
2. Click the Accounts tab.
3. Edit a user's ability to view, deposit to or withdraw from a specific account.
   - ✓ User right is active.
   - ⊘ User right is disabled.
4. Click the Save button when you are finished making changes.

Unlocking Users

As a Company System Administrator, you have ability to unlock users directly without requiring bank intervention. Users will lock themselves out of FCO after 3 consecutive failed password attempts. As the Company System Administrator you will see a notification in the right-hand panel notifying you that user is locked.

- To unlock the user, click the three-dot menu button, then click Unlock login.
- If more detail on the user is required before unlocking them, click View user detail.